

Elements of Discrete Mathematics

Richard Hammack
Virginia Commonwealth University

Richard Hammack (publisher)
Department of Mathematics & Applied Mathematics
P.O. Box 842014
Virginia Commonwealth University
Richmond, Virginia, 23284

Elements of Discrete Mathematics

Edition 1.1

© 2017 by Richard Hammack

This work is licensed under the Creative Commons Attribution-No Derivative Works 3.0 License



Typeset in 11pt T_EX Gyre Schola using PDFL^AT_EX

For Adriana

Contents

I Symbols, Systems and Sets

| | |
|--------------------------------------|-----------|
| 1. Discrete Systems | 3 |
| 1.1. Analog versus Discrete Systems | 3 |
| 1.2. The Binary Number System | 7 |
| 1.3. The Hexadecimal Number System | 10 |
| 1.4. Solutions for Chapter 1 | 13 |
| 2. Sets | 14 |
| 2.1. Introduction to Sets | 14 |
| 2.2. The Cartesian Product | 20 |
| 2.3. Subsets | 24 |
| 2.4. Power Sets | 27 |
| 2.5. Union, Intersection, Difference | 30 |
| 2.6. Complement | 32 |
| 2.7. Venn Diagrams | 34 |
| 2.8. Indexed Sets | 37 |
| 2.9. Sets that Are Number Systems | 41 |
| 2.10. Case Study: Russell's Paradox | 42 |
| 2.11. Solutions for Chapter 2 | 44 |
| 3. Logic | 51 |
| 3.1. Statements | 52 |
| 3.2. And, Or, Not | 56 |
| 3.3. Conditional Statements | 59 |
| 3.4. Biconditional Statements | 63 |
| 3.5. Truth Tables for Statements | 65 |
| 3.6. Logical Equivalence | 68 |
| 3.7. Solutions for Chapter 3 | 71 |

II Counting, Probability and Algorithms

| | |
|---|-----------|
| 4. Counting | 79 |
| 4.1. Lists | 79 |
| 4.2. The Multiplication Principle | 81 |
| 4.3. The Addition and Subtraction Principles | 88 |
| 4.4. Factorials and Permutations | 92 |
| 4.5. Counting Subsets | 99 |
| 4.6. Pascal's Triangle and the Binomial Theorem | 104 |

| | |
|--|------------|
| 4.7. The Inclusion-Exclusion Principle | 107 |
| 4.8. Counting Multisets | 110 |
| 4.9. The Division and Pigeonhole Principles | 118 |
| 4.10. Combinatorial Proof | 122 |
| 4.11. Solutions for Chapter 4 | 125 |
| 5. Discrete Probability | 136 |
| 5.1. Sample Spaces, Events and Probability | 137 |
| 5.2. Combining Events | 141 |
| 5.3. Conditional Probability and Independent Events | 148 |
| 5.4. Probability Distributions and Probability Trees | 156 |
| 5.5. Bayes' Formula | 161 |
| 5.6. Solutions for Chapter 5 | 166 |
| 6. Algorithms | 173 |
| 6.1. Variables and the Assignment Command | 174 |
| 6.2. Loops and Algorithm Notation | 175 |
| 6.3. Logical Operators in Algorithms | 178 |
| 6.4. The Division Algorithm | 185 |
| 6.5. Procedures and Recursion | 186 |
| 6.6. Counting Steps in Algorithms | 191 |
| 6.7. Solutions for Chapter 6 | 198 |
| <i>III Conditional Proof</i> | |
| 7. Quantified Statements | 209 |
| 7.1. Quantifiers | 210 |
| 7.2. More on Conditional Statements | 212 |
| 7.3. Translating English to Symbolic Logic | 214 |
| 7.4. Negating Statements | 216 |
| 7.5. Logical Inference | 219 |
| 7.6. Solutions for Chapter 7 | 221 |
| 8. Direct Proof | 224 |
| 8.1. Theorems | 224 |
| 8.2. Definitions | 226 |
| 8.3. Direct Proof | 229 |
| 8.4. Using Cases | 235 |
| 8.5. Treating Similar Cases | 236 |
| 8.6. Solutions for Chapter 8 | 239 |
| 9. Contrapositive Proof | 242 |
| 9.1. Contrapositive Proof | 242 |
| 9.2. Congruence of Integers | 245 |
| 9.3. Mathematical Writing | 247 |
| 9.4. The Euclidean Algorithm | 250 |

| | |
|---|------------|
| 9.5. Solutions for Chapter 9 | 255 |
| 10. Proof by Contradiction | 259 |
| 10.1. Proving Statements with Contradiction | 260 |
| 10.2. Proving Conditional Statements by Contradiction | 263 |
| 10.3. Combining Techniques | 264 |
| 10.4. Case Study: The Halting Problem | 266 |
| 10.5. Solutions for Chapter 10 | 270 |
| 11. Proofs Involving Sets | 273 |
| 11.1. How to Prove $a \in A$ | 273 |
| 11.2. How to Prove $A \subseteq B$ | 275 |
| 11.3. How to Prove $A = B$ | 278 |
| 11.4. Case Study: Perfect Numbers | 281 |
| 11.5. Solutions for Chapter 11 | 288 |
| <i>IV Other Types of Proof</i> | |
| 12. Proving Non-Conditional Statements | 295 |
| 12.1. If-and-Only-If Proof | 295 |
| 12.2. Equivalent Statements | 297 |
| 12.3. Existence Proofs; Existence and Uniqueness Proofs | 298 |
| 12.4. Constructive Versus Non-Constructive Proofs | 302 |
| 12.5. Solutions for Chapter 12 | 305 |
| 13. Disproof | 310 |
| 13.1. Counterexamples | 312 |
| 13.2. Disproving Existence Statements | 314 |
| 13.3. Disproof by Contradiction | 316 |
| 13.4. Solutions for Chapter 13 | 318 |
| 14. Mathematical Induction | 321 |
| 14.1. Proof by Induction | 323 |
| 14.2. Proving Recursive Procedures Work | 328 |
| 14.3. Proof by Strong Induction | 329 |
| 14.4. Proof by Smallest Counterexample | 333 |
| 14.5. Fibonacci Numbers | 335 |
| 14.6. Solutions for Chapter 14 | 340 |
| 15. Introduction to Graph Theory | 350 |
| 15.1. Graphs and Subgraphs | 351 |
| 15.2. Vertex-degree and Trees | 356 |
| 15.3. Colorings and Chromatic Number | 358 |

| | |
|--|------------|
| 16. Relations | 364 |
| 16.1. Relations | 364 |
| 16.2. Properties of Relations | 368 |
| 16.3. Equivalence Relations | 373 |
| 16.4. Equivalence Classes and Partitions | 377 |
| 16.5. The Integers Modulo n | 380 |
| 16.6. Relations Between Sets | 383 |
| 16.7. Solutions for Chapter 16 | 385 |
| 17. Functions | 391 |
| 17.1. Functions | 391 |
| 17.2. Injective and Surjective Functions | 396 |
| 17.3. The Pigeonhole Principle Revisited | 400 |
| 17.4. Composition | 403 |
| 17.5. Inverse Functions | 406 |
| 17.6. Solutions for Chapter 17 | 410 |
| 18. Cardinality of Sets | 415 |
| 18.1. Sets with Equal Cardinalities | 415 |
| 18.2. Countable and Uncountable Sets | 421 |
| 18.3. Comparing Cardinalities | 426 |
| 18.4. Case Study: Computable Functions | 430 |
| 18.5. Solutions for Chapter 18 | 434 |
| 19. Review of Real-Valued Functions | 437 |
| 19.1. Exponent Review | 437 |
| 19.2. Linear Functions, Power Functions and Polynomials | 440 |
| 19.3. Exponential Functions | 441 |
| 19.4. Logarithmic Functions | 443 |
| 19.5. Solutions for Chapter 19 | 450 |
| 20. Complexity of Algorithms | 451 |
| 20.1. Big-O Notation | 453 |
| 20.2. Polynomial Algorithms | 460 |
| 20.3. Case Study: Sequential Search Versus Binary Search | 462 |
| 20.4. Case Study: Bubble Sort Versus Merge Sort | 463 |
| 20.5. Solutions for Chapter 20 | 471 |

Part I

Symbols, Systems and Sets

Discrete Systems

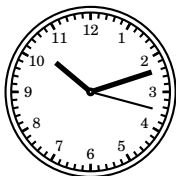
Discrete mathematics is the study of techniques, ideas and modes of reasoning that are indispensable in applied disciplines such as computer science or information technology. It is also a gateway into advanced theoretical mathematics.

To understand its focus, it is helpful to appreciate the meaning of—and differences between—*analog* and *discrete* systems. Discrete mathematics is the study of *discrete* (as opposed to *analog*) systems.

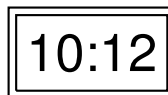
1.1 Analog versus Discrete Systems

The difference between analog and discrete systems is that analog systems involve smooth, continuous, unbroken movement or structures, whereas discrete systems involve individual parts or states that are clearly separate from one another.

This is illustrated by the difference between a traditional (analog) clock and a digital (discrete) clock. The hands of an analog clock move in a fluid, continuous motion. In the one minute between 10:12 and 10:13, the minute hand moves in a smooth, unbroken motion passing through all instants between these two times. In an hour it passes through infinitely many different instants of time. This is an analog system. By contrast, a digital clock jumps from 10:12 to 10:13 in an instant. In an hour it records a finite (in fact, 60) instants of time. This is a *discrete* system.



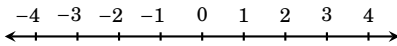
Analog clock



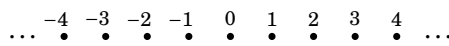
Discrete (digital) clock

Although calculus is not really essential to mastering most topics in discrete mathematics, it can help us gain a deeper understanding the difference between analog and discrete systems. Calculus is based on the

real number system, which is an analog system. We visualize the real numbers as a smooth, unbroken, infinitely long line. You can put your finger on 0 and move it continuously to the right in a fluid motion, stopping at (say) 3. As you do this, your finger moves through infinitely many numbers, one for each point on the line from 0 to 3. This is an analog system.



Real numbers (analog system)



Integers (discrete system)

Discrete mathematics is more concerned with number systems such as the integers (whole numbers) $\dots -3, -2, -1, 0, 1, 2, 3 \dots$ whose parts (numbers in this case) are discrete entities. Putting your finger at 0 and moving to the right, you jump from 0, to 1, to 2, to 3, and so on.

But discrete mathematics deals with much more than just integers. More broadly, it encompasses mathematical structures or processes that consists of individual parts. You can think of discrete mathematics as the discipline concerned with mathematical structures whose parts can be described by a finite sequence of characters from a computer keyboard.

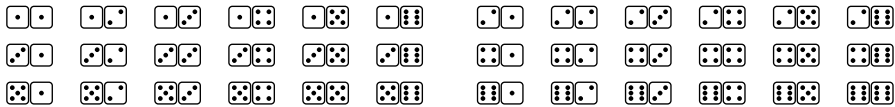
For example, the set of integers is a discrete mathematical system because even though there are infinitely many integers (and you'd never be finished typing all of them), any one integer can be expressed by typing a finite sequence of the digits 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, and possibly a minus sign “-” (for negative integers).

Similarly, the set of rational numbers (fractions of integers) is also a discrete system because any rational number, such as $-397/24$ is expressible as a finite sequence of the symbols 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, - and /.

By contrast, the system of real numbers is **not** a discrete system: it has irrational numbers like $\pi = 3.14159265359 \dots$ that cannot be typed because they involve infinitely many decimal places.

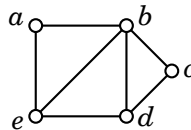
In this sense, the times represented by a digital clock are a discrete system because any time can be expressed with an integer from 1 to 12, followed by a colon, and then a number from 00 to 59. (As in 5:00, or 11:45.) An analog clock is inherently different. For an instant, an analog clock reads π o'clock, which occurs a small fraction of a second after 3:14. But a digital clock jumps from 3:14 to 3:15, blissfully ignoring the messiness of irrational numbers such as π . This is the spirit of discrete mathematics.

Even the process of rolling a dice two times in a row is a discrete system, as there are exactly 36 outcomes.



Any one of these outcomes could be encoded in symbols, as (x, y) , where x and y are integers between 1 and 6, representing the results of the first and second rolls. (For example, $\begin{smallmatrix} \square & \square \\ \cdot & \cdot \\ \square & \square \end{smallmatrix}$ is encoded as $(3, 5)$, etc.) The set of all such outcomes is called a *sample space*. Such sets can be useful. For example, if we wanted to know the probability of rolling a double, we can see that exactly 6 of these 36 equally likely outcomes is a double, so the probability of rolling a double is $\frac{6}{36} = \frac{1}{6}$. Chapters 2 and 4 introduce sets and counting, theories relevant to situations such as this, and we investigate the theory of probability in Chapter 5.

Another example of a discrete structure is a *graph*. In mathematics, the word “graph” is used in two different contexts. In algebra or calculus a *graph* is a visual description of a function, graphed on a coordinate axis. Although we do use such graphs in discrete mathematics, we more often use the word a *graph* to mean a network of nodes with connections between them. Here is a picture of a typical graph.



Its nodes are described by the discrete set $\{a, b, c, d, e\}$, and its connections (called *edges*) are $\{ab, bc, cc, de, ea, eb\}$. Therefore this particular graph is completely described by typing the information

$$\left(\{a, b, c, d, e\}, \{ab, bc, cc, de, ea, eb\} \right).$$

The theory of graphs is a major branch of discrete mathematics. Graphs have wide ranging applications. For example, the Internet is a huge graph whose nodes are web pages and whose edges are links between them. Google’s search algorithm involves the mathematics of this structure.

The fact that a graph can be described by sets of vertices and edges is another indication of the fundamental importance of sets, which we will study carefully in Chapter 2.

This book is organized as follows. Chapter 2 introduces the theory of sets, a language capable of describing any discrete (or analog) structure. This is followed by a short chapter on logic, a system that bridges the gap between natural language and mathematics, giving precision to the modes of speech we use in discussing mathematics.

Chapters 4 and 5 build on this, laying the foundation for enumerating or *counting* the parts of discrete structures. Chapter 6 introduces the study of *algorithms*, a fundamental idea that is at the heart of computer science. Chapter 7 covers some additional topics in logic.

As you delve deeper into mathematics and its applications, you will find yourself in situations where you need to *prove* that a certain result is correct (i.e., true), and you will need to read and understand proofs written by others. This is the topic of chapters 8 through 14. This is a major part of the text, and it will build on the previous chapters. This material is applied in Chapter 15, a brief introduction to graph theory. Chapters 16 and 17 deal with the important topics of relations and functions. All of this material is essential for real progress in mathematics and computer science.

Although calculus is not necessary to understand the ideas in this book, you have probably studied it, and that background will serve you well. For instance, calculus requires a certain fluency in algebra and arithmetic, and that fluency is equally essential in discrete mathematics. Calculus requires a working knowledge of functions, and that background will be useful. It has also given you a grounding in certain useful notations, such as the sigma notation for expressing sums. Given a list of numbers $a_1, a_2, a_3, \dots, a_n$, their sum is compactly expressed as

$$a_1 + a_2 + a_3 + \dots + a_n = \sum_{k=1}^n a_k.$$

All of these background topics will play a role for us.

Before beginning with the theory of sets, we pause to review the binary and hexadecimal number systems. Although not absolutely fundamental for most of this text, they are important because they are the number systems that form the basis for the internal workings of computer circuitry and computations. These systems will also show up in certain examples and exercises throughout the text.

Exponential notation makes an appearance here. Recall that for any number a and positive integer n , the power $a^n = a \cdot a \cdots a$ is the product of a with itself n times. Recall from algebra that if a is non-zero, then $a^0 = 1$. In the following pages you will encounter $10^0 = 1$, $2^0 = 1$ and $16^0 = 1$.

1.2 The Binary Number System

In daily life we use the familiar base-10 number system, also called the **Hindu-Arabic** number system, or the **decimal** number system. It uses ten symbols 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, representing the quantities zero through nine. There is no single symbol for the quantity ten – instead we express it as the combination “10,” signifying that ten equals 1 ten plus 0 ones. Any other positive integer is represented as a string of symbols 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, standing for the sum of the digits in the string times powers of ten, decreasing to the zeroth power $10^0 = 1$. For example,

$$\begin{aligned} 7406 &= 7 \cdot 10^3 + 4 \cdot 10^2 + 0 \cdot 10^1 + 6 \cdot 10^0 \\ &= 7 \cdot 1000 + 4 \cdot 100 + 0 \cdot 10 + 6 \cdot 1. \end{aligned}$$

Thus the number seven-thousand-four-hundred-six is represented as 7406, with a 7 in the *thousand's place*, a 4 in the *hundred's place*, a 0 in the *ten's place*, and a 6 in the *one's place*. There is little need to elaborate because you internalized this early in life.

There is nothing sacred about base of ten, other than the fact that it caters to humans (who have ten fingers). If we had eight fingers, our number system would surely be base-8. Actually, for any integer $n > 1$ there is a base- n number system using n symbols. Although base-10 is convenient for humans, base-2 is better suited for computer circuitry, because its two symbols can be represented by a zero or positive voltage.

The **base-2**, or **binary** number system uses only two digits, 0 and 1, representing the quantities zero and one. There is no single symbol for the number two – instead we express it as the combination “10,” signifying that two equals 1 two plus 0 ones. Any other quantity is represented as a string of the symbols 0, 1, standing for the sum of the digits in the string times powers of two, decreasing to $2^0 = 1$.

For example, the base-2 number **10011** equals the base-10 number

$$\begin{aligned} 1 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 &= \\ 1 \cdot 16 + 0 \cdot 8 + 0 \cdot 4 + 1 \cdot 2 + 1 \cdot 1 &= 19. \end{aligned}$$

The number nineteen is represented as “10011” in base-2 because it is the sum of **1** sixteen, **0** eights, **0** fours, **1** two and **1** one. It is represented as “19” in base-10 because it is the sum of **1** ten and **9** ones.

For clarity, we sometimes use a subscript to indicate what base is being used, so the above computation is summarized as $10011_2 = 19_{10}$.

Table 1.1 shows the first sixteen decimal numbers in the left column, with their corresponding binary representations on the right. Be sure you agree with this. For instance, $110_2 = 6_{10}$ because $1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 = 6$.

| binary number | powers of 2 | | | | | decimal number | |
|---------------|-------------|--|---|---|--|----------------|----|
| | 16 | 8 | 4 | 2 | 1 | | |
| 0 | = | | | | 0 ·1 | = | 0 |
| 1 | = | | | | 1 ·1 | = | 1 |
| 10 | = | | | | 1 ·2+ 0 ·1 | = | 2 |
| 11 | = | | | | 1 ·2+ 1 ·1 | = | 3 |
| 100 | = | | | | 1 ·4+ 0 ·2+ 0 ·1 | = | 4 |
| 101 | = | | | | 1 ·4+ 0 ·2+ 1 ·1 | = | 5 |
| 110 | = | | | | 1 ·4+ 1 ·2+ 0 ·1 | = | 6 |
| 111 | = | | | | 1 ·4+ 1 ·2+ 1 ·1 | = | 7 |
| 1000 | = | | | | 1 ·8+ 0 ·4+ 0 ·2+ 0 ·1 | = | 8 |
| 1001 | = | | | | 1 ·8+ 0 ·4+ 0 ·2+ 1 ·1 | = | 9 |
| 1010 | = | | | | 1 ·8+ 0 ·4+ 1 ·2+ 0 ·1 | = | 10 |
| 1011 | = | | | | 1 ·8+ 0 ·4+ 1 ·2+ 1 ·1 | = | 11 |
| 1100 | = | | | | 1 ·8+ 1 ·4+ 0 ·2+ 0 ·1 | = | 12 |
| 1101 | = | | | | 1 ·8+ 1 ·4+ 0 ·2+ 1 ·1 | = | 13 |
| 1110 | = | | | | 1 ·8+ 1 ·4+ 1 ·2+ 0 ·1 | = | 14 |
| 1111 | = | | | | 1 ·8+ 1 ·4+ 1 ·2+ 1 ·1 | = | 15 |
| 10000 | = | 1 ·16+ 0 ·8+ 0 ·4+ 0 ·2+ 0 ·1 | = | | | | 16 |

Table 1.1. Binary and decimal representations of numbers

In converting between binary and decimal representations of numbers, it's helpful to know the various powers of 2. They are listed in Table 1.2. For example, $2^5 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 32$, so 32 appears below 2^5 .

| | | | | | | | | | | | | | |
|-----|----------|----------|----------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|
| ... | 2^{12} | 2^{11} | 2^{10} | 2^9 | 2^8 | 2^7 | 2^6 | 2^5 | 2^4 | 2^3 | 2^2 | 2^1 | 2^0 |
| ... | 4096 | 2048 | 1024 | 512 | 256 | 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |

Table 1.2. Powers of 2


Table 1.1 suggests a method for converting binary numbers to decimal. To convert a given a binary number to decimal, multiply its digits by decreasing powers of two, down to $2^0 = 1$, and add them. For example,

$$\begin{aligned}
 1110 &= 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 \\
 &= 1 \cdot 8 + 1 \cdot 4 + 1 \cdot 2 + 0 \cdot 1 = 14.
 \end{aligned}$$

Example 1.1 Convert the binary number 110101 to decimal.

Solution: We simply write this number as a sum of powers of 2 in base-10.

$$\begin{aligned} 110101 &= 1 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 \\ &= 1 \cdot 32 + 1 \cdot 16 + 0 \cdot 8 + 1 \cdot 4 + 0 \cdot 2 + 1 \cdot 1 = 53 \end{aligned}$$

Thus $110101_2 = 53_{10}$, that is, 110101 (base 2) is 53 (base 10). 

Converting decimal to binary involves running this process in reverse, which can involve some reverse engineering.

Example 1.2 Convert the decimal number 347 to binary.

Solution: We need to find how 347 is a sum of powers of 2. Table 1.2 shows that the highest power of 2 less than 347 is $2^8 = 256$, and

$$\begin{aligned} 347 &= 256 + 91 \\ &= 2^8 + 91. \end{aligned}$$

Now look at the 91. Table 1.2 shows that the highest power of 2 less than 91 is $2^6 = 64$, and $91 = 64 + 27 = 2^6 + 27$, so the above becomes

$$347 = 2^8 + 2^6 + 27.$$

From here we can reason out $27 = 16 + 8 + 2 + 1 = 2^4 + 2^3 + 2^1 + 2^0$. Therefore

$$347 = 2^8 + 2^6 + 2^4 + 2^3 + 2^1 + 2^0.$$

Powers 2^7 , 2^5 and 2^2 do not appear, so we insert them, multiplied by 0:

$$347 = 1 \cdot 2^8 + 0 \cdot 2^7 + 1 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0.$$

Therefore 347 is the base-2 number 101011011. 

Various cultures throughout history have used base- n number systems. The ancient Babylonians used a base-60 system with 60 different cuneiform digits (including a blank, used for what we now call 0). The Aztecs used base-20. In the modern era, some early computers used the base-3 system, with three digits represented by a positive, zero or negative voltage.

Today the binary system is the foundation for computer circuitry, with 0 represented by a zero voltage, and 1 by a positive voltage. Though the binary system has just two digits, it is inefficient in the sense that many digits are needed to express even relatively small numbers. Base-16 remedies this. It is closely related to binary, but it is much more compact.

1.3 The Hexadecimal Number System

Base-16 is called the **hexadecimal** number system. It uses 16 symbols, including the familiar ten symbols 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 representing the numbers zero through nine, plus the six additional symbols A, B, C, D, E, and F, representing the numbers ten through fifteen.

Table 1.3 summarizes this. It shows the numbers zero through fifteen in decimal, binary and hexadecimal notation. For consistency we have represented all binary numbers as 4-digit strings of 0's and 1's by adding zeros to the left, where needed.

| decimal | binary | hexadecimal |
|---------|--------|-------------|
| 0 | 0000 | 0 |
| 1 | 0001 | 1 |
| 2 | 0010 | 2 |
| 3 | 0011 | 3 |
| 4 | 0100 | 4 |
| 5 | 0101 | 5 |
| 6 | 0110 | 6 |
| 7 | 0111 | 7 |
| 8 | 1000 | 8 |
| 9 | 1001 | 9 |
| 10 | 1010 | A |
| 11 | 1011 | B |
| 12 | 1100 | C |
| 13 | 1101 | D |
| 14 | 1110 | E |
| 15 | 1111 | F |

Table 1.3. The first sixteen integers in decimal, binary and hexadecimal

The number sixteen is represented as 10 in hexadecimal, because sixteen is **1** sixteen and **0** ones. Note $16_{10} = 10_{16} = 10000_2$.

Just as powers of two are fundamental to interpreting binary numbers, powers of sixteen are necessary for understanding hexadecimal. Here are the first few powers. (Memorizing these is *not* essential.)

| | | | | | | |
|-----|-----------|--------|--------|--------|--------|--------|
| ... | 16^5 | 16^4 | 16^3 | 16^2 | 16^1 | 16^0 |
| ... | 1,048,576 | 65,536 | 4096 | 256 | 16 | 1 |


Table 1.4. Powers of 16

We can convert between hexadecimal and decimal in the same way that we converted between binary and decimal.

Example 1.3 Convert the hexadecimal number 1A2C to decimal.

Solution: Simply write 1A2C as a sum of powers of sixteen in hexadecimal, then convert the sums to decimal. (In interpreting the first line, recall that 10 is the hexadecimal representation of sixteen, i.e., $10_{16} = 16_{10}$.)

$$\begin{aligned}
 1A2C &= 1 \cdot 10^3 + A \cdot 10^2 + 2 \cdot 10^1 + C \cdot 10^0 && \text{(hexadecimal)} \\
 &= 1 \cdot 16^3 + 10 \cdot 16^2 + 2 \cdot 16^1 + 12 \cdot 16^0 && \text{(decimal)} \\
 &= 1 \cdot 4096 + 10 \cdot 256 + 2 \cdot 16 + 12 \cdot 1 && \text{(decimal)} \\
 &= 6700 && \text{(decimal)}
 \end{aligned}$$

Thus $1A2C_{16} = 6700_{10}$, that is, 1A2C (base 16) is 6700 (base 10). 

Converting between hexadecimal and binary is extremely simple. We will illustrate the technique first, before explaining why it works. Suppose we wish to convert the binary number 111111001000001011 to hexadecimal. The first step is to divide the digits of this binary number into groups of four, beginning from the right.

11 1111 0010 0000 1011

If necessary, add extra zeros to left end of the left-most grouping, so that it too contains four digits.

0011 1111 0010 0000 1011

Now use Table 1.3 (or innate numerical reasoning) to convert each 4-digit binary grouping to the corresponding hexadecimal digit.

0011 1111 0010 0000 1011
3 F 2 0 B

We conclude that $111111001000001011_2 = 3F20B_{16}$.

The reverse process works for converting hexadecimal to binary. Suppose we wanted to convert 1A2C to binary. Taking the reverse of the above approach (and using Table 1.3 if necessary), we write

1 A 2 C
0001 1010 0010 1100.

Ignoring the three 0's on the far left, we see $1A2C_{16} = 1\ 1010\ 0010\ 1100_2$.

It is easy to see why this technique works. Just use the computation from Exercise 1.3 on page 11, but convert 1A2C to binary instead of decimal. (Here we use the fact that $10_{16} = 10000_2$.)

$$\begin{aligned} 1A2C &= 1 \cdot 10^3 + A \cdot 10^2 + 2 \cdot 10^1 + C \cdot 10^0 && \text{(base-16)} \\ &= 1 \cdot 10000^3 + 1010 \cdot 10000^2 + 10 \cdot 10000^1 + 1100 \cdot 10000^0 && \text{(binary)}. \end{aligned}$$

Doing the addition in columns, we get:

$$\begin{array}{r} 1\ 0000\ 0000\ 0000 \\ 1010\ 0000\ 0000 \\ 10\ 0000 \\ + \quad 1100 \\ \hline 1\ 1010\ 0010\ 1100 \end{array}$$

This is the same number we would get by replacing each digit in 1A2C with its binary equivalent.

Exercises for Chapter 1

A. Convert the decimal number to binary and hexadecimal.

- | | | | |
|--------|-----------|---------|--------|
| 1. 347 | 2. 10,000 | 3. 2039 | 4. 64 |
| 5. 256 | 6. 257 | 7. 258 | 8. 258 |

B. Convert the binary number to hexadecimal and decimal.

- | | | | |
|---------------|--------------|-------------|---------------|
| 9. 110110011 | 10. 10101010 | 11. 1111111 | 12. 111000111 |
| 13. 101101001 | 14. 10011010 | 15. 1000001 | 16. 100100101 |

C. Convert the hexadecimal number to decimal and binary

- | | | | |
|----------|------------|----------|----------|
| 17. 123 | 18. ABC | 19. 5A4D | 20. F12 |
| 21. B0CA | 22. COFFEE | 23. BEEF | 24. ABBA |

1.4 Solutions for Chapter 1

- 1.** $347 = 256 + 64 + 16 + 8 + 2 + 1 = 1 \cdot 2^8 + 0 \cdot 2^7 + 1 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$.
Thus $347_{10} = 101011011_2 = 0001\ 0101\ 1011_2 = 15B_{16}$.
- 3.** $2039 = 1024 + 512 + 256 + 128 + 64 + 32 + 16 + 4 + 2 + 1 = 1 \cdot 2^{10} + 1 \cdot 2^9 + 1 \cdot 2^8 + 1 \cdot 2^7 + 1 \cdot 2^6 + 1 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$.
Thus $2039_{10} = 1111110111_2 = 0111\ 1111\ 0111_2 = 7F7_{16}$.
- 5.** $256 = 2^8 = \cdot 2^8 + 0 \cdot 2^7 + 0 \cdot 2^6 + 0 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$.
Thus $256_{10} = 100000000_2 = 0001\ 0000\ 0000_2 = 100_{16}$.
- 7.** $258 = 256 + 2 = \cdot 2^8 + 0 \cdot 2^7 + 0 \cdot 2^6 + 0 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0$.
Thus $258_{10} = 100000010_2 = 0001\ 0000\ 0010_2 = 102_{16}$.
- 9.** $110110011_2 = 0001\ 1011\ 0011_2 = 1B3_{16} = 1 \cdot 16^2 + 11 \cdot 16^1 + 3 \cdot 16^0 = 435_{10}$
- 11.** $1111111_2 = 0111\ 1111_2 = 7F_{16} = 7 \cdot 16 + 15 = 127_{10}$.
- 13.** $101101001_2 = 0001\ 0110\ 1001_2 = 169_{16} = 1 \cdot 16^2 + 6 \cdot 16 + 9 = 361_{10}$.
- 15.** $1000001_2 = 0100\ 0001_2 = 41_{16} = 4 \cdot 16 + 1 = 65_{10}$.
- 17.** $123_{16} = 1 \cdot 16^2 + 2 \cdot 16^1 + 3 \cdot 16^0 = 256 + 32 + 3 = 291_{10}$.
 $123_{16} = 0001\ 0010\ 0011_2 = 100100011_2$.
- 19.** $5A4D_{16} = 5 \cdot 16^3 + 10 \cdot 16^2 + 4 \cdot 16^1 + 13 \cdot 16^0 = 5 \cdot 4096 + 10 \cdot 256 + 4 \cdot 16 + 13 = 23117_{10}$.
 $5A4D_{16} = 0101\ 1010\ 0100\ 1101_2 = 101101001001101_2$.
- 21.** $B0CA_{16} = 11 \cdot 16^3 + 0 \cdot 16^2 + 12 \cdot 16^1 + 10 \cdot 16^0 = 11 \cdot 4096 + 0 \cdot 256 + 12 \cdot 16 + 10 = 45258_{10}$.
 $B0CA_{16} = 1011\ 0000\ 1100\ 1010_2 = 101100001100_2$
- 23.** $BEEF_{16} = 11 \cdot 16^3 + 14 \cdot 16^2 + 14 \cdot 16^1 + 15 \cdot 16^0 = 11 \cdot 4096 + 14 \cdot 256 + 14 \cdot 16 + 15 = 48879_{10}$.
 $BEEF_{16} = 1011\ 1110\ 1110\ 1010_2 = 101111011101010_2$.

Sets

All of mathematics can be described with sets. This becomes more and more apparent the deeper into mathematics you go. It will be apparent in this course, and beyond it. The theory of sets is a language that is perfectly suited to describing and explaining all types of mathematical structures.

2.1 Introduction to Sets

A **set** is a collection of things. The things in the collection are called **elements** of the set. We are mainly concerned with sets whose elements are mathematical entities, such as numbers, points, functions, etc.

A set is often expressed by listing its elements between commas, enclosed by braces. For example, the collection $\{2, 4, 6, 8\}$ is a set which has four elements, the numbers 2, 4, 6 and 8. Some sets have infinitely many elements. For example, consider the collection of all integers,

$$\{\dots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \dots\}.$$

Here the dots indicate a pattern of numbers that continues forever in both the positive and negative directions. A set is called an **infinite** set if it has infinitely many elements; otherwise it is called a **finite** set.

Two sets are **equal** if they contain exactly the same elements. Thus $\{2, 4, 6, 8\} = \{4, 2, 8, 6\}$ because even though they are listed in a different order, the elements are identical; but $\{2, 4, 6, 8\} \neq \{2, 4, 6, 7\}$. Also

$$\{\dots -4, -3, -2, -1, 0, 1, 2, 3, 4, \dots\} = \{0, -1, 1, -2, 2, -3, 3, -4, 4, \dots\}.$$

We often use uppercase letters to stand for sets. In discussing the set $\{2, 4, 6, 8\}$ we might declare $A = \{2, 4, 6, 8\}$ and then use A to stand for $\{2, 4, 6, 8\}$. To express that 2 is an element of the set A , we write $2 \in A$, and read this as “2 is an element of A ,” or “2 is in A ,” or just “2 in A .” We also have $4 \in A$, $6 \in A$ and $8 \in A$, but $5 \notin A$. We read this last expression as “5 is not an element of A ,” or “5 not in A .” Expressions like $6, 2 \in A$ or $2, 4, 8 \in A$ are used to indicate that several things are in a set.

Some sets are so significant that special symbols are reserved for them. The set of **natural numbers** (the positive whole numbers) is denoted by \mathbb{N} :

$$\mathbb{N} = \{1, 2, 3, 4, 5, 6, 7, \dots\}.$$

The set of **integers**

$$\mathbb{Z} = \{\dots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \dots\}$$

is another fundamental set. The symbol \mathbb{R} stands for the set of all **real numbers**, a set that is undoubtedly familiar to you from calculus. Other special sets will be listed later in this section.

Context can play a role in our interpretation of sets. If we are using binary notation for integers, then $\mathbb{N} = \{1, 10, 11, 100, 101, 110, 111, \dots\}$. Thus

$$\{1, 2, 3, 4, 5, 6, 7, \dots\} = \{1, 10, 11, 100, 101, 110, 111, \dots\}$$

because both sets represent the same thing – the set of natural numbers. (The symbol for a particular number is not the same thing as the number itself, just as your name is not the same thing as you yourself. Here, for instance $5 = 101_2$, so 5 and 101 represent the same thing, namely the number five.) But if we are dealing strictly with decimal notation, then

$$\{1, 2, 3, 4, 5, 6, 7, \dots\} \neq \{1, 10, 11, 100, 101, 110, 111, \dots\}$$

because these sets contain different numbers. To keep things simple, we will almost use the binary number system when expressing sets of numbers.

Sets need not have just numbers as elements. The set $B = \{T, F\}$ consists of two letters, perhaps representing the values “true” and “false.” The set $C = \{a, e, i, o, u\}$ consists of the lowercase vowels in the English alphabet. The set $D = \{(0, 0), (1, 0), (0, 1), (1, 1)\}$ has as elements the four corner points of a square on the x - y coordinate plane. Thus $(0, 0) \in D$, $(1, 0) \in D$, etc., but $(1, 2) \notin D$ (for instance). It is even possible for a set to have other sets as elements. Consider $E = \{1, \{2, 3\}, \{2, 4\}\}$, which has three elements: the number 1, the set $\{2, 3\}$ and the set $\{2, 4\}$. Thus $1 \in E$ and $\{2, 3\} \in E$ and $\{2, 4\} \in E$. But note that $2 \notin E$, $3 \notin E$ and $4 \notin E$.

Consider the set $M = \left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \right\}$ of three two-by-two matrices. We have $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in M$, but $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \notin M$. Letters can serve as symbols denoting a set's elements: If $a = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, $b = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and $c = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$, then $M = \{a, b, c\}$.

If X is a finite set, its **cardinality** or **size** is the number of elements it has, and this number is denoted as $|X|$. Thus for the sets above, $|A| = 4$, $|B| = 2$, $|C| = 5$, $|D| = 4$, $|E| = 3$ and $|M| = 3$.

There is a special set that, although small, plays a big role. The **empty set** is the set $\{\}$ that has no elements. We denote it as \emptyset , so $\emptyset = \{\}$. Whenever you see the symbol \emptyset , it stands for $\{\}$. Observe that $|\emptyset| = 0$. The empty set is the only set whose cardinality is zero.

Be careful in writing the empty set. Don't write $\{\emptyset\}$ when you mean \emptyset . These sets can't be equal because \emptyset contains nothing while $\{\emptyset\}$ contains one thing, namely the empty set. If this is confusing, think of a set as a box with things in it, so, for example, $\{2, 4, 6, 8\}$ is a "box" containing four numbers. The empty set $\emptyset = \{\}$ is an empty box. By contrast, $\{\emptyset\}$ is a box with an empty box inside it. Obviously, there's a difference: An empty box is not the same as a box with an empty box inside it. Thus $\emptyset \neq \{\emptyset\}$. (You might also note $|\emptyset| = 0$ and $|\{\emptyset\}| = 1$ as additional evidence that $\emptyset \neq \{\emptyset\}$.)

This box analogy can clarify sets. The set $F = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}$ may look strange but it is quite simple. It is a box containing three things: an empty box, a box containing an empty box, and a box containing a box containing an empty box. Thus $|F| = 3$. The set $I = \{\mathbb{N}, \mathbb{Z}\}$ is a box containing two boxes, a box of natural numbers and a box of integers. Thus $|I| = 2$.

A special notation called **set-builder notation** is used to describe sets that are too big to list between braces. Consider the set of even integers $E = \{\dots, -6, -4, -2, 0, 2, 4, 6, \dots\}$. In set-builder notation this set is written as

$$E = \{2n : n \in \mathbb{Z}\}.$$

We read the first brace as "*the set of all things of form,*" and the colon as "*such that.*" So the expression $E = \{2n : n \in \mathbb{Z}\}$ is read as "*E equals the set of all things of form $2n$, such that n is an element of \mathbb{Z} .*" The idea is that E consists of all possible values of $2n$, where n takes on all values in \mathbb{Z} .

In general, a set X written with set-builder notation has the syntax

$$X = \{\text{expression} : \text{rule}\},$$


where X is understood to contain all values of "expression" that are specified by "rule." For example, the set E above is the set of all values of the expression $2n$ that satisfy the rule $n \in \mathbb{Z}$. The same set can be expressed many ways. For example, $E = \{2n : n \in \mathbb{Z}\} = \{n : n \text{ is an even integer}\} = \{n : n = 2k, k \in \mathbb{Z}\}$. Another common way of writing it is

$$E = \{n \in \mathbb{Z} : n \text{ is even}\},$$


read "*E is the set of all n in \mathbb{Z} such that n is even.*" Some writers use a bar instead of a colon; for example, $E = \{n \in \mathbb{Z} \mid n \text{ is even}\}$. We use the colon.

Example 2.1 Here are some further illustrations of set-builder notation.

1. $\{n : n \text{ is a prime number}\} = \{2, 3, 5, 7, 11, 13, 17, \dots\}$
2. $\{n \in \mathbb{N} : n \text{ is prime}\} = \{2, 3, 5, 7, 11, 13, 17, \dots\}$
3. $\{n^2 : n \in \mathbb{Z}\} = \{0, 1, 4, 9, 16, 25, \dots\}$
4. $\{x \in \mathbb{R} : x^2 - 2 = 0\} = \{\sqrt{2}, -\sqrt{2}\}$
5. $\{x \in \mathbb{Z} : x^2 - 2 = 0\} = \emptyset$
6. $\{x \in \mathbb{Z} : |x| < 4\} = \{-3, -2, -1, 0, 1, 2, 3\}$
7. $\{2x : x \in \mathbb{Z}, |x| < 4\} = \{-6, -4, -2, 0, 2, 4, 6\}$
8. $\{x \in \mathbb{Z} : |2x| < 4\} = \{-1, 0, 1\}$

Items 6–8 highlight a conflict of notation that we should be alert to. The expression $|X|$ means *absolute value* if X is a number and *cardinality* if X is a set. The distinction should always be clear from context. Consider $\{x \in \mathbb{Z} : |x| < 4\}$ in item 6 above. Here $x \in \mathbb{Z}$, so x is a number (not a set), and thus the bars in $|x|$ must mean absolute value, not cardinality. On the other hand, suppose $A = \{\{1, 2\}, \{3, 4, 5, 6\}, \{7\}\}$ and $B = \{X \in A : |X| < 3\}$. The elements of A are sets (not numbers), so the $|X|$ in the expression for B must mean cardinality. Therefore $B = \{\{1, 2\}, \{7\}\}$. 

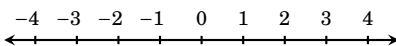
Example 2.2 Describe the set $A = \{7a + 3b : a, b \in \mathbb{Z}\}$.

Solution: This set contains all numbers of form $7a + 3b$, where a and b are integers. Each such number $7a + 3b$ is an integer, so A contains only integers. But *which* integers? If n is *any* integer, then $n = 7n + 3(-2n)$, so $n = 7a + 3b$ where $a = n$ and $b = -2n$. Thus $n \in A$, and so $A = \mathbb{Z}$. 

We close this section with a summary of special sets. These are sets that are so common that they are given special names and symbols.

- The empty set: $\emptyset = \{\}$
- The natural numbers: $\mathbb{N} = \{1, 2, 3, 4, 5, \dots\}$
- The integers: $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, 4, 5, \dots\}$
- The rational numbers: $\mathbb{Q} = \{x : x = \frac{m}{n}, \text{ where } m, n \in \mathbb{Z} \text{ and } n \neq 0\}$
- The real numbers: \mathbb{R}

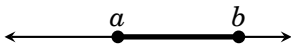
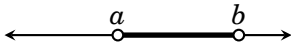
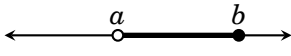
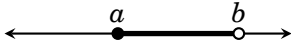
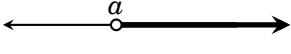
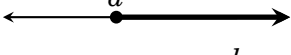
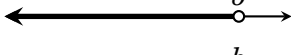

We visualize the set \mathbb{R} of real numbers as an infinitely long number line.



In the parlance of Chapter 1, \mathbb{R} is not a discrete system. But it is a fundamental set that is nonetheless important in discrete mathematics.

Notice that \mathbb{Q} is the set of all numbers in \mathbb{R} that can be expressed as a fraction of two integers. You may be aware that $\mathbb{Q} \neq \mathbb{R}$, as $\sqrt{2} \notin \mathbb{Q}$ but $\sqrt{2} \in \mathbb{R}$. (If not, this point will be addressed in Chapter 10.)

In calculus you encountered intervals on the number line. Like \mathbb{R} , these too are infinite sets of numbers. Any two numbers $a, b \in \mathbb{R}$ with $a < b$ give rise to various intervals. Graphically, they are represented by a darkened segment between a and b . A solid circle at an endpoint indicates that that number is included in the interval. A hollow circle indicates a point that is not included in the interval.

- | | |
|---|--|
| • Closed interval: $[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}$ |  |
| • Open interval: $(a, b) = \{x \in \mathbb{R} : a < x < b\}$ |  |
| • Half-open interval: $(a, b] = \{x \in \mathbb{R} : a < x \leq b\}$ |  |
| • Half-open interval: $[a, b) = \{x \in \mathbb{R} : a \leq x < b\}$ |  |
| • Infinite interval: $(a, \infty) = \{x \in \mathbb{R} : a < x\}$ |  |
| • Infinite interval: $[a, \infty) = \{x \in \mathbb{R} : a \leq x\}$ |  |
| • Infinite interval: $(-\infty, b) = \{x \in \mathbb{R} : x < b\}$ |  |
| • Infinite interval: $(-\infty, b] = \{x \in \mathbb{R} : x \leq b\}$ |  |

Each of these intervals is an infinite set containing infinitely many numbers as elements. For example, though its length is short, the interval $(0.1, 0.2)$ contains infinitely many numbers, that is, all numbers between 0.1 and 0.2. It is an unfortunate notational accident that (a, b) can denote both an open interval on the line and a point on the plane. The difference is usually clear from context. In the next section we will see yet another meaning of (a, b) .

Exercises for Section 2.1

A. Write each of the following sets by listing their elements between braces.

1. $\{5x - 1 : x \in \mathbb{Z}\}$

2. $\{3x + 2 : x \in \mathbb{Z}\}$

3. $\{x \in \mathbb{Z} : -2 \leq x < 7\}$

4. $\{x \in \mathbb{N} : -2 < x \leq 7\}$

5. $\{x \in \mathbb{R} : x^2 = 3\}$

6. $\{x \in \mathbb{R} : x^2 = 9\}$

7. $\{x \in \mathbb{R} : x^2 + 5x = -6\}$

8. $\{x \in \mathbb{R} : x^3 + 5x^2 = -6x\}$

- 9.** $\{x \in \mathbb{R} : \sin \pi x = 0\}$ **13.** $\{x \in \mathbb{Z} : |6x| < 5\}$
10. $\{x \in \mathbb{R} : \cos x = 1\}$ **14.** $\{5x : x \in \mathbb{Z}, |2x| \leq 8\}$
11. $\{x \in \mathbb{Z} : |x| < 5\}$ **15.** $\{5a + 2b : a, b \in \mathbb{Z}\}$
12. $\{x \in \mathbb{Z} : |2x| < 5\}$ **16.** $\{6a + 2b : a, b \in \mathbb{Z}\}$

B. Write each of the following sets in set-builder notation.

- 17.** $\{2, 4, 8, 16, 32, 64, \dots\}$ **23.** $\{3, 4, 5, 6, 7, 8\}$
18. $\{0, 4, 16, 36, 64, 100, \dots\}$ **24.** $\{-4, -3, -2, -1, 0, 1, 2\}$
19. $\{\dots, -6, -3, 0, 3, 6, 9, 12, 15, \dots\}$ **25.** $\{\dots, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, \dots\}$
20. $\{\dots, -8, -3, 2, 7, 12, 17, \dots\}$ **26.** $\{\dots, \frac{1}{27}, \frac{1}{9}, \frac{1}{3}, 1, 3, 9, 27, \dots\}$
21. $\{0, 1, 4, 9, 16, 25, 36, \dots\}$ **27.** $\{\dots, -\pi, -\frac{\pi}{2}, 0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}, 2\pi, \frac{5\pi}{2}, \dots\}$
22. $\{3, 6, 11, 18, 27, 38, \dots\}$ **28.** $\{\dots, -\frac{3}{2}, -\frac{3}{4}, 0, \frac{3}{4}, \frac{3}{2}, \frac{9}{4}, 3, \frac{15}{4}, \frac{9}{2}, \dots\}$

C. Find the following cardinalities of the following sets

- 29.** $\{\{1\}, \{2, \{3, 4\}\}, \emptyset\}$ **34.** $\{x \in \mathbb{N} : |x| < 10\}$
30. $\{\{1, 4\}, a, b, \{\{3, 4\}\}, \{\emptyset\}\}$ **35.** $\{x \in \mathbb{Z} : x^2 < 10\}$
31. $\{\{\{1\}\}, \{2, \{3, 4\}\}, \emptyset\}$ **36.** $\{x \in \mathbb{N} : x^2 < 10\}$
32. $\{\{\{1, 4\}, a, b, \{\{3, 4\}\}, \{\emptyset\}\}\}$ **37.** $\{x \in \mathbb{N} : x^2 < 0\}$
33. $\{x \in \mathbb{Z} : |x| < 10\}$ **38.** $\{x \in \mathbb{N} : 5x \leq 20\}$

D. Sketch the following sets of points in the x - y plane.

- 39.** $\{(x, y) : x \in [1, 2], y \in [1, 2]\}$ **46.** $\{(x, y) : x, y \in \mathbb{R}, x^2 + y^2 \leq 1\}$
40. $\{(x, y) : x \in [0, 1], y \in [1, 2]\}$ **47.** $\{(x, y) : x, y \in \mathbb{R}, y \geq x^2 - 1\}$
41. $\{(x, y) : x \in [-1, 1], y = 1\}$ **48.** $\{(x, y) : x, y \in \mathbb{R}, x > 1\}$
42. $\{(x, y) : x = 2, y \in [0, 1]\}$ **49.** $\{(x, x + y) : x \in \mathbb{R}, y \in \mathbb{Z}\}$
43. $\{(x, y) : |x| = 2, y \in [0, 1]\}$ **50.** $\{(x, \frac{x^2}{y}) : x \in \mathbb{R}, y \in \mathbb{N}\}$
44. $\{(x, x^2) : x \in \mathbb{R}\}$ **51.** $\{(x, y) \in \mathbb{R}^2 : (y - x)(y + x) = 0\}$
45. $\{(x, y) : x, y \in \mathbb{R}, x^2 + y^2 = 1\}$ **52.** $\{(x, y) \in \mathbb{R}^2 : (y - x^2)(y + x^2) = 0\}$

E. These problems concern sets of numbers in binary or hexadecimal notation.

- 53.** Consider the set $\{x \in \mathbb{N} : 100 \leq x \leq 1011\}$ whose elements are expressed in binary form. List the elements of this set.
54. Consider the set $\{x \in \mathbb{N} : 100 \leq x \leq 1011$ and x is even $\}$ whose elements are expressed in binary form. List the elements of this set.
55. Consider the set $\{x \in \mathbb{N} : A \leq x \leq 20\}$ whose elements are expressed in hexadecimal form. List the elements of this set.
56. Consider the set $\{x \in \mathbb{N} : EA4 \leq x \leq EB0\}$ whose elements are expressed in hexadecimal form. List the elements of this set.
-

2.2 The Cartesian Product

Given two sets A and B , it is possible to “multiply” them to produce a new set denoted as $A \times B$. This operation is called the *Cartesian product*. To understand it, we must first understand the idea of an ordered pair.

Definition 2.1 An **ordered pair** is a list (x, y) of two things x and y , enclosed in parentheses and separated by a comma.

For example, $(2, 4)$ is an ordered pair, as is $(4, 2)$. These ordered pairs are different because even though they have the same things in them, the order is different. We write $(2, 4) \neq (4, 2)$. Right away you can see that ordered pairs can be used to describe points on the plane, as was done in calculus, but they are not limited to just that. The things in an ordered pair don't have to be numbers. You can have ordered pairs of letters, such as (m, ℓ) , ordered pairs of sets such as $(\{2, 5\}, \{3, 2\})$, even ordered pairs of ordered pairs like $((2, 4), (4, 2))$. The following are also ordered pairs: $(2, \{1, 2, 3\})$ and $(\mathbb{R}, (0, 0))$. Any list of two things enclosed by parentheses is an ordered pair. Now we are ready to define the Cartesian product.

Definition 2.2 The **Cartesian product** of two sets A and B is another set, denoted as $A \times B$ and defined as $A \times B = \{(a, b) : a \in A, b \in B\}$.

Thus $A \times B$ is a set of ordered pairs of elements from A and B . For example, if $A = \{k, \ell, m\}$ and $B = \{q, r\}$, then

$$A \times B = \{(k, q), (k, r), (\ell, q), (\ell, r), (m, q), (m, r)\}.$$

Figure 2.1 shows how to make a schematic diagram of $A \times B$. Line up the elements of A horizontally and line up the elements of B vertically, as if A and B form an x - and y -axis. Then fill in the ordered pairs so that each element (x, y) is in the column headed by x and the row headed by y .

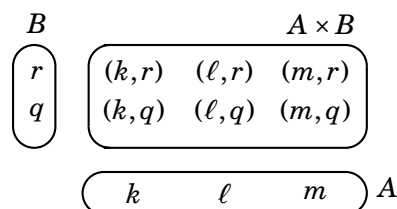
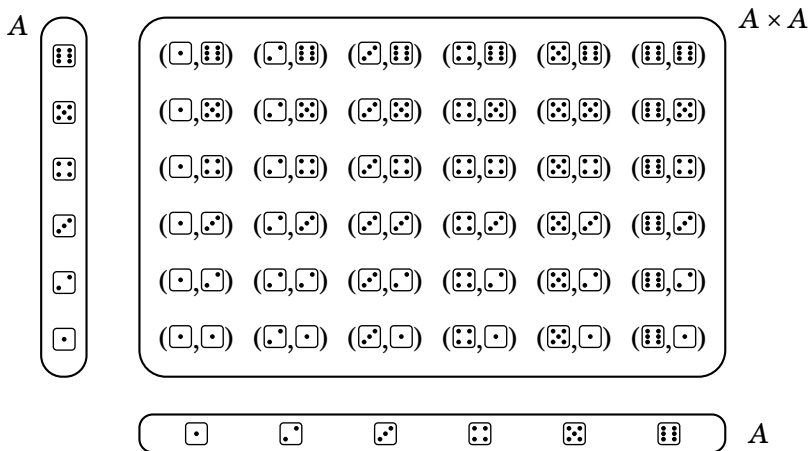


Figure 2.1. A diagram of a Cartesian product

For another example, $\{0, 1\} \times \{2, 1\} = \{(0, 2), (0, 1), (1, 2), (1, 1)\}$. If you are a visual thinker, you may wish to draw a diagram similar to Figure 2.1. The rectangular array of such diagrams give us the following general fact.

Fact 2.1 If A and B are finite sets, then $|A \times B| = |A| \cdot |B|$.

Example 2.3 Suppose $A = \{\square, \square, \square, \square, \square, \square\}$ is a set consisting of the six faces of a dice. The Cartesian product $A \times A$ is diagrammed below.



Note that $A \times A$ has $6 \cdot 6 = 36$ elements. We can think of it as the set of possible outcomes in rolling a dice two times in a row. Each element of the product is an ordered pair of form

$$(\text{result of 1st roll}, \text{result of 2nd roll}).$$

This models the sample space mentioned on page 5. Cartesian products are useful for describing and analyzing such situations.

The set $\mathbb{R} \times \mathbb{R} = \{(x, y) : x, y \in \mathbb{R}\}$ should be very familiar. It can be viewed as the set of points on the Cartesian plane, and is drawn in Figure 2.2(a). The set $\mathbb{R} \times \mathbb{N} = \{(x, y) : x \in \mathbb{R}, y \in \mathbb{N}\}$ can be regarded as all of the points on the Cartesian plane whose second coordinate is a natural number. This is illustrated in Figure 2.2(b), which shows that $\mathbb{R} \times \mathbb{N}$ looks like infinitely many horizontal lines at integer heights above the x axis. The set $\mathbb{N} \times \mathbb{N}$ can be visualized as the set of all points on the Cartesian plane whose coordinates are both natural numbers. It looks like a grid of dots in the first quadrant, as illustrated in Figure 2.2(c).

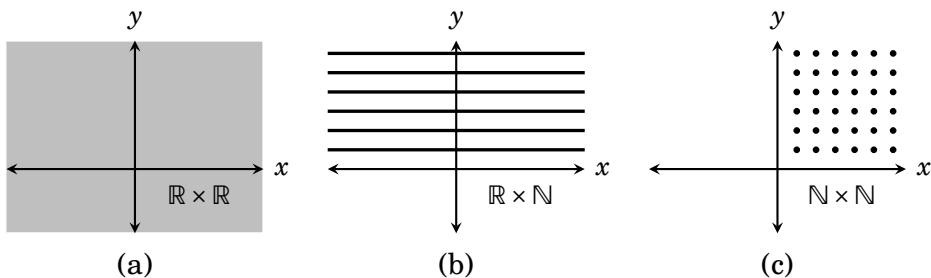


Figure 2.2. Drawings of some Cartesian products

It is even possible to form Cartesian products of Cartesian products, as in $\mathbb{R} \times (\mathbb{N} \times \mathbb{Z}) = \{(x, (y, z)) : x \in \mathbb{R}, (y, z) \in \mathbb{N} \times \mathbb{Z}\}$.

We can also define Cartesian products of three or more sets by moving beyond ordered pairs. An **ordered triple** is a list (x, y, z) . The Cartesian product of the three sets \mathbb{R} , \mathbb{N} and \mathbb{Z} is $\mathbb{R} \times \mathbb{N} \times \mathbb{Z} = \{(x, y, z) : x \in \mathbb{R}, y \in \mathbb{N}, z \in \mathbb{Z}\}$. Of course there is no reason to stop with ordered triples. In general,

$$A_1 \times A_2 \times \cdots \times A_n = \{(x_1, x_2, \dots, x_n) : x_i \in A_i \text{ for each } i = 1, 2, \dots, n\}.$$

Be mindful of parentheses. There is a slight difference between $\mathbb{R} \times (\mathbb{N} \times \mathbb{Z})$ and $\mathbb{R} \times \mathbb{N} \times \mathbb{Z}$. The first is a Cartesian product of two sets; its elements are ordered pairs $(x, (y, z))$. The second is a Cartesian product of three sets; its elements look like (x, y, z) . To be sure, in many situations there is no harm in blurring the distinction between expressions like $(x, (y, z))$ and (x, y, z) , but for now we regard them as different.

We can also take **Cartesian powers** of sets. For any set A and positive integer n , the power A^n is the Cartesian product of A with itself n times:

$$A^n = A \times A \times \cdots \times A = \{(x_1, x_2, \dots, x_n) : x_1, x_2, \dots, x_n \in A\}.$$

In this way, \mathbb{R}^2 is the familiar Cartesian plane and \mathbb{R}^3 is three-dimensional space. You can visualize how, if \mathbb{R}^2 is the plane, then $\mathbb{Z}^2 = \{(m, n) : m, n \in \mathbb{Z}\}$ is a grid of points on the plane. Likewise, as \mathbb{R}^3 is 3-dimensional space, $\mathbb{Z}^3 = \{(m, n, p) : m, n, p \in \mathbb{Z}\}$ is a grid of points in space.

In other courses you may encounter sets that are very similar to \mathbb{R}^n , but yet have slightly different shades of meaning. Consider, for example, the set of all two-by-three matrices with entries from \mathbb{R} :

$$M = \left\{ \begin{bmatrix} u & v & w \\ x & y & z \end{bmatrix} : u, v, w, x, y, z \in \mathbb{R} \right\}.$$

This is not really all that different from the set

$$\mathbb{R}^6 = \{(u, v, w, x, y, z) : u, v, w, x, y, z \in \mathbb{R}\}.$$


The elements of these sets are merely certain arrangements of six real numbers. Despite their similarity, we maintain that $M \neq \mathbb{R}^6$, for two-by-three matrices are not the same things as sequences of six numbers.

We close with one further example of a Cartesian power.

Example 2.4 We can describe the two sides of a coin by the set $S = \{H, T\}$. The possible outcomes of tossing the coin seven times in a row can be described with the Cartesian power S^7 . A typical element of S^7 looks like

$$(H, H, T, H, T, T, T),$$

meaning a head was tossed first, then another head, then a tail, then a head followed by three tails. We can thus regard the elements of S^7 as lists of length 7 made from the symbols H and T .

Note that $|S^7| = 2^7 = 128$. If this is not clear now, then it will be explained fully in Chapter 4, where we will undertake a careful study of lists. 

Exercises for Section 2.2

A. Write out the indicated sets by listing their elements between braces.

1. Suppose $A = \{1, 2, 3, 4\}$ and $B = \{a, c\}$.

- | | | | |
|------------------|------------------|-----------------------------|-----------------------------|
| (a) $A \times B$ | (c) $A \times A$ | (e) $\emptyset \times B$ | (g) $A \times (B \times B)$ |
| (b) $B \times A$ | (d) $B \times B$ | (f) $(A \times B) \times B$ | (h) B^3 |

2. Suppose $A = \{\pi, e, 0\}$ and $B = \{0, 1\}$.

- | | | | |
|------------------|------------------|-----------------------------|-----------------------------|
| (a) $A \times B$ | (c) $A \times A$ | (e) $A \times \emptyset$ | (g) $A \times (B \times B)$ |
| (b) $B \times A$ | (d) $B \times B$ | (f) $(A \times B) \times B$ | (h) $A \times B \times B$ |

3. $\{x \in \mathbb{R} : x^2 = 2\} \times \{a, c, e\}$

6. $\{x \in \mathbb{R} : x^2 = x\} \times \{x \in \mathbb{N} : x^2 = x\}$

4. $\{n \in \mathbb{Z} : 2 < n < 5\} \times \{n \in \mathbb{Z} : |n| = 5\}$

7. $\{\emptyset\} \times \{0, \emptyset\} \times \{0, 1\}$

5. $\{x \in \mathbb{R} : x^2 = 2\} \times \{x \in \mathbb{R} : |x| = 2\}$

8. $\{0, 1\}^4$

B. Sketch these Cartesian products on the x - y plane \mathbb{R}^2 (or \mathbb{R}^3 for the last two).

9. $\{1, 2, 3\} \times \{-1, 0, 1\}$

15. $\{1\} \times [0, 1]$

10. $\{-1, 0, 1\} \times \{1, 2, 3\}$

16. $[0, 1] \times \{1\}$

11. $[0, 1] \times [0, 1]$

17. $\mathbb{N} \times \mathbb{Z}$

12. $[-1, 1] \times [1, 2]$

18. $\mathbb{Z} \times \mathbb{Z}$

13. $\{1, 1.5, 2\} \times [1, 2]$

19. $[0, 1] \times [0, 1] \times [0, 1]$

14. $[1, 2] \times \{1, 1.5, 2\}$

20. $\{(x, y) \in \mathbb{R}^2 : x^2 + y^2 \leq 1\} \times [0, 1]$

2.3 Subsets

It can happen that every element of a set A is an element of another set B . For example, each element of $A = \{0, 2, 4\}$ is also an element of $B = \{0, 1, 2, 3, 4\}$. When A and B are related this way we say that A is a *subset* of B .

Definition 2.3 Suppose A and B are sets. If every element of A is also an element of B , then we say A is a **subset** of B , and we denote this as $A \subseteq B$. We write $A \not\subseteq B$ if A is *not* a subset of B , that is, if it is *not* true that every element of A is also an element of B . Thus $A \not\subseteq B$ means that there is at least one element of A that is *not* an element of B .

Example 2.5 Be sure you understand why each of the following is true.

1. $\{2, 3, 7\} \subseteq \{2, 3, 4, 5, 6, 7\}$
2. $\{2, 3, 7\} \not\subseteq \{2, 4, 5, 6, 7\}$
3. $\{2, 3, 7\} \subseteq \{2, 3, 7\}$
4. $\{2n : n \in \mathbb{Z}\} \subseteq \mathbb{Z}$
5. $\{(x, \sin(x)) : x \in \mathbb{R}\} \subseteq \mathbb{R}^2$
6. $\{2, 3, 5, 7, 11, 13, 17, \dots\} \subseteq \mathbb{N}$
7. $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$
8. $\mathbb{R} \times \mathbb{N} \subseteq \mathbb{R} \times \mathbb{R}$



This brings us to a significant fact: If B is any set whatsoever, then $\emptyset \subseteq B$. To see why this is true, look at the last sentence of Definition 2.3. It says that $\emptyset \not\subseteq B$ would mean that there is at least one element of \emptyset that is not an element of B . But this cannot be so because \emptyset contains no elements! Thus it is not the case that $\emptyset \not\subseteq B$, so it must be that $\emptyset \subseteq B$.

Fact 2.2 The empty set is a subset of every set, that is, $\emptyset \subseteq B$ for any set B .

Here is another way to look at it. Imagine a subset of B as a thing you make by starting with braces $\{\}$, then filling them with selections from B . For example, to make one particular subset of $B = \{a, b, c\}$, start with $\{\}$, select b and c from B and insert them into $\{\}$ to form the subset $\{b, c\}$. Alternatively, you could have chosen just a to make $\{a\}$, and so on. But one option is to simply select nothing from B . This leaves you with the subset $\{\}$. Thus $\{\} \subseteq B$. More often we write it as $\emptyset \subseteq B$.

This idea of “making” a subset can help us list out all the subsets of a given set B . As an example, let $B = \{a, b, c\}$. Let’s list all of its subsets. One way of approaching this is to make a tree-like structure. Begin with the subset $\{\}$, which is shown on the left of Figure 2.3. Considering the element a of B , we have a choice: insert it or not. The lines from $\{\}$ point to what we get depending whether or not we insert a , either $\{\}$ or $\{a\}$. Now move on to the element b of B . For each of the sets just formed we can either insert or not insert b , and the lines on the diagram point to the resulting sets $\{\}$, $\{b\}$, $\{a\}$, or $\{a, b\}$. Finally, to each of these sets, we can either insert c or not insert it, and this gives us, on the far right-hand column, the sets $\{\}$, $\{c\}$, $\{b\}$, $\{b, c\}$, $\{a\}$, $\{a, c\}$, $\{a, b\}$ and $\{a, b, c\}$. These are the eight subsets of $B = \{a, b, c\}$.

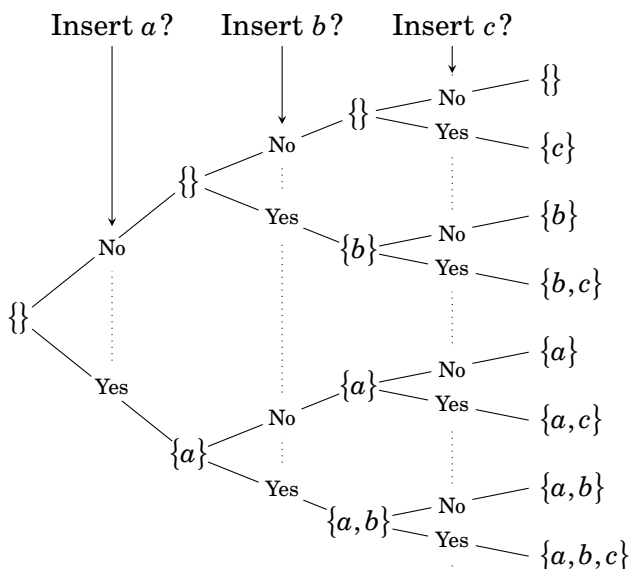


Figure 2.3. A “tree” for listing subsets

We can see from the way this tree branches out that if it happened that $B = \{a\}$, then B would have just two subsets, those in the second column of the diagram. If it happened that $B = \{a, b\}$, then B would have four subsets, those listed in the third column, and so on. At each branching of the tree, the number of subsets doubles. Thus in general, if $|B| = n$, then B must have 2^n subsets.

Fact 2.3 If a finite set has n elements, then it has 2^n subsets.

For a slightly more complex example, consider listing the subsets of $B = \{1, 2, \{1, 3\}\}$. This B has just three elements: 1, 2 and $\{1, 3\}$. At this point you probably don't even have to draw a tree to list out B 's subsets. You just make all the possible selections from B and put them between braces to get

$$\{\}, \{1\}, \{2\}, \{\{1, 3\}\}, \{1, 2\}, \{1, \{1, 3\}\}, \{2, \{1, 3\}\}, \{1, 2, \{1, 3\}\}.$$

These are the eight subsets of B . Exercises like this help you identify what is and isn't a subset. You know immediately that a set such as $\{1, 3\}$ is *not* a subset of B because it can't be made by selecting elements from B , as the 3 is not an element of B and thus is not a valid selection. Notice that although $\{1, 3\} \notin B$, it *is* true that $\{1, 3\} \in B$. Also, $\{\{1, 3\}\} \subseteq B$.

Example 2.6 Be sure you understand why the following statements are true. Each illustrates an aspect of set theory that you've learned so far.

1. $1 \in \{1, \{1\}\}$ 1 is the first element listed in $\{1, \{1\}\}$
2. $1 \notin \{1, \{1\}\}$ because 1 is not a set
3. $\{1\} \in \{1, \{1\}\}$ $\{1\}$ is the second element listed in $\{1, \{1\}\}$
4. $\{1\} \subseteq \{1, \{1\}\}$ make subset $\{1\}$ by selecting 1 from $\{1, \{1\}\}$
5. $\{\{1\}\} \notin \{1, \{1\}\}$ because $\{1, \{1\}\}$ contains only 1 and $\{1\}$, and not $\{\{1\}\}$
6. $\{\{1\}\} \subseteq \{1, \{1\}\}$ make subset $\{\{1\}\}$ by selecting $\{1\}$ from $\{1, \{1\}\}$
7. $\mathbb{N} \notin \mathbb{N}$ \mathbb{N} is a set (not a number) and \mathbb{N} contains only numbers
8. $\mathbb{N} \subseteq \mathbb{N}$ because $X \subseteq X$ for every set X
9. $\emptyset \notin \mathbb{N}$ because the set \mathbb{N} contains only numbers and no sets
10. $\emptyset \subseteq \mathbb{N}$ because \emptyset is a subset of every set
11. $\mathbb{N} \in \{\mathbb{N}\}$ because $\{\mathbb{N}\}$ has just one element, the set \mathbb{N}
12. $\mathbb{N} \notin \{\mathbb{N}\}$ because, for instance, $1 \in \mathbb{N}$ but $1 \notin \{\mathbb{N}\}$
13. $\emptyset \notin \{\mathbb{N}\}$ note that the only element of $\{\mathbb{N}\}$ is \mathbb{N} , and $\mathbb{N} \neq \emptyset$
14. $\emptyset \subseteq \{\mathbb{N}\}$ because \emptyset is a subset of every set
15. $\emptyset \in \{\emptyset, \mathbb{N}\}$ \emptyset is the first element listed in $\{\emptyset, \mathbb{N}\}$
16. $\emptyset \subseteq \{\emptyset, \mathbb{N}\}$ because \emptyset is a subset of every set
17. $\{\mathbb{N}\} \subseteq \{\emptyset, \mathbb{N}\}$ make subset $\{\mathbb{N}\}$ by selecting \mathbb{N} from $\{\emptyset, \mathbb{N}\}$
18. $\{\mathbb{N}\} \notin \{\emptyset, \{\mathbb{N}\}\}$ because $\mathbb{N} \notin \{\emptyset, \{\mathbb{N}\}\}$
19. $\{\mathbb{N}\} \in \{\emptyset, \{\mathbb{N}\}\}$ $\{\mathbb{N}\}$ is the second element listed in $\{\emptyset, \{\mathbb{N}\}\}$
20. $\{(1, 2), (2, 2), (7, 1)\} \subseteq \mathbb{N} \times \mathbb{N}$ 👉

Though they should help you understand the concept of subset, the above examples are somewhat artificial. But in general, subsets arise very naturally. For instance, consider the unit circle $C = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$.

This is a subset $C \subseteq \mathbb{R}^2$. Likewise the graph of a function $y = f(x)$ is a set of points $G = \{(x, f(x)) : x \in \mathbb{R}\}$, and $G \subseteq \mathbb{R}^2$. Surely sets such as C and G are more easily understood or visualized when regarded as subsets of \mathbb{R}^2 . Mathematics is filled with such instances where it is important to regard one set as a subset of another.

Exercises for Section 2.3

A. List all the subsets of the following sets.

- | | |
|--------------------------|---|
| 1. $\{1, 2, 3, 4\}$ | 5. $\{\emptyset\}$ |
| 2. $\{1, 2, \emptyset\}$ | 6. $\{\mathbb{R}, \mathbb{Q}, \mathbb{N}\}$ |
| 3. $\{\{\mathbb{R}\}\}$ | 7. $\{\mathbb{R}, \{\mathbb{Q}, \mathbb{N}\}\}$ |
| 4. \emptyset | 8. $\{\{0, 1\}, \{0, 1, \{2\}\}, \{0\}\}$ |

B. Write out the following sets by listing their elements between braces.

- | | |
|---|--|
| 9. $\{X : X \subseteq \{3, 2, a\} \text{ and } X = 2\}$ | 11. $\{X : X \subseteq \{3, 2, a\} \text{ and } X = 4\}$ |
| 10. $\{X \subseteq \mathbb{N} : X \leq 1\}$ | 12. $\{X : X \subseteq \{3, 2, a\} \text{ and } X = 1\}$ |

C. Decide if the following statements are true or false. Explain.

- | | |
|---|---|
| 13. $\mathbb{R}^3 \subseteq \mathbb{R}^3$ | 15. $\{(x, y) : x - 1 = 0\} \subseteq \{(x, y) : x^2 - x = 0\}$ |
| 14. $\mathbb{R}^2 \subseteq \mathbb{R}^3$ | 16. $\{(x, y) : x^2 - x = 0\} \subseteq \{(x, y) : x - 1 = 0\}$ |

2.4 Power Sets

Given a set, you can form a new set with the *power set* operation, defined as follows.

Definition 2.4 If A is a set, the **power set** of A is another set, denoted as $\mathcal{P}(A)$ and defined to be the set of all subsets of A . In symbols, $\mathcal{P}(A) = \{X : X \subseteq A\}$.

For example, suppose $A = \{1, 2, 3\}$. The power set of A is the set of all subsets of A . We learned how to find these subsets in the previous section, and they are $\{\}$, $\{1\}$, $\{2\}$, $\{3\}$, $\{1, 2\}$, $\{1, 3\}$, $\{2, 3\}$ and $\{1, 2, 3\}$. Therefore the power set of A is

$$\mathcal{P}(A) = \{ \emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\} \}.$$

As we saw in the previous section, if a finite set A has n elements, then it has 2^n subsets, and thus its power set has 2^n elements.

Fact 2.4 If A is a finite set, then $|\mathcal{P}(A)| = 2^{|A|}$.

Example 2.7 Be sure you understand the following statements.

1. $\mathcal{P}(\{0, 1, 3\}) = \{ \emptyset, \{0\}, \{1\}, \{3\}, \{0, 1\}, \{0, 3\}, \{1, 3\}, \{0, 1, 3\} \}$
2. $\mathcal{P}(\{1, 2\}) = \{ \emptyset, \{1\}, \{2\}, \{1, 2\} \}$
3. $\mathcal{P}(\{1\}) = \{ \emptyset, \{1\} \}$
4. $\mathcal{P}(\emptyset) = \{ \emptyset \}$
5. $\mathcal{P}(\{a\}) = \{ \emptyset, \{a\} \}$
6. $\mathcal{P}(\{\emptyset\}) = \{ \emptyset, \{\emptyset\} \}$
7. $\mathcal{P}(\{a\}) \times \mathcal{P}(\{\emptyset\}) = \{ (\emptyset, \emptyset), (\emptyset, \{\emptyset\}), (\{a\}, \emptyset), (\{a\}, \{\emptyset\}) \}$
8. $\mathcal{P}(\mathcal{P}(\{\emptyset\})) = \{ \emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\} \}$
9. $\mathcal{P}(\{1, \{1, 2\}\}) = \{ \emptyset, \{1\}, \{\{1, 2\}\}, \{1, \{1, 2\}\} \}$
10. $\mathcal{P}(\{\mathbb{Z}, \mathbb{N}\}) = \{ \emptyset, \{\mathbb{Z}\}, \{\mathbb{N}\}, \{\mathbb{Z}, \mathbb{N}\} \}$

Next are some that are **wrong**. See if you can determine why they are wrong and make sure you understand the explanation on the right.

11. $\mathcal{P}(1) = \{ \emptyset, \{1\} \}$ meaningless because 1 is not a set
12. $\mathcal{P}(\{1, \{1, 2\}\}) = \{ \emptyset, \{1\}, \{1, 2\}, \{1, \{1, 2\}\} \}$ wrong because $\{1, 2\} \notin \{1, \{1, 2\}\}$
13. $\mathcal{P}(\{1, \{1, 2\}\}) = \{ \emptyset, \{\{1\}\}, \{\{1, 2\}\}, \{\emptyset, \{1, 2\}\} \}$... wrong because $\{\{1\}\} \notin \{1, \{1, 2\}\}$

In 1–10, notice that $|\mathcal{P}(A)| = 2^{|A|}$, in accordance with Fact 2.4. ✍

If A is finite, it is possible (though maybe not practical) to list out $\mathcal{P}(A)$ between braces as was done in Example 2.7 above. That is not possible if A is infinite. For example, consider $\mathcal{P}(\mathbb{N})$. If you start listing its elements you quickly discover that \mathbb{N} has infinitely many subsets, and it's not clear how (or if) they could be arranged as a list with a definite pattern:

$$\mathcal{P}(\mathbb{N}) = \{ \emptyset, \{1\}, \{2\}, \dots, \{1, 2\}, \{1, 3\}, \dots, \{39, 47\}, \\ \dots, \{3, 87, 131\}, \dots, \{2, 4, 6, 8, \dots\}, \dots ? \dots \}.$$

The set $\mathcal{P}(\mathbb{R}^2)$ is mind boggling. Think of $\mathbb{R}^2 = \{(x, y) : x, y \in \mathbb{R}\}$ as the set of all points on the Cartesian plane. A subset of \mathbb{R}^2 (that is, an *element* of $\mathcal{P}(\mathbb{R}^2)$) is a set of points in the plane. Let's look at some of these sets. Since $\{(0, 0), (1, 1)\} \subseteq \mathbb{R}^2$, we know that $\{(0, 0), (1, 1)\} \in \mathcal{P}(\mathbb{R}^2)$. We can even draw a picture of this subset, as in Figure 2.4(a). For another example, the graph of $y = x^2$ is the set of points $G = \{(x, x^2) : x \in \mathbb{R}\}$ and this is a subset of \mathbb{R}^2 , so $G \in \mathcal{P}(\mathbb{R}^2)$. Figure 2.4(b) is a picture of G . This can be done for any function, so the graph of any imaginable function $f : \mathbb{R} \rightarrow \mathbb{R}$ is an element of $\mathcal{P}(\mathbb{R}^2)$.

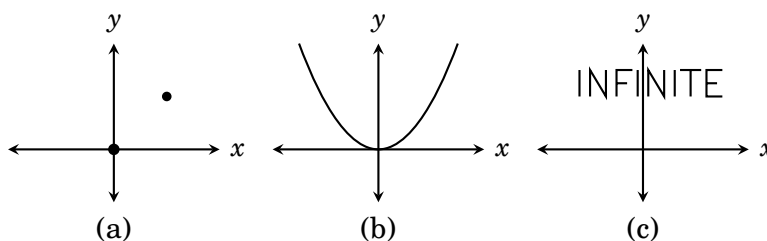


Figure 2.4. Three of the many, many sets in $\mathcal{P}(\mathbb{R}^2)$

In fact, any black-and-white image on the plane can be thought of as a subset of \mathbb{R}^2 , where the black points belong to the subset and the white points do not. So the text “INFINITE” in Figure 2.4(c) is a subset of \mathbb{R}^2 and therefore an element of $\mathcal{P}(\mathbb{R}^2)$. By that token, $\mathcal{P}(\mathbb{R}^2)$ contains a copy of the page you are reading now.

Thus in addition to containing every imaginable function and every imaginable black-and-white image, $\mathcal{P}(\mathbb{R}^2)$ also contains the full text of every book that was ever written, those that are yet to be written and those that will never be written. Inside of $\mathcal{P}(\mathbb{R}^2)$ is a detailed biography of your life, from beginning to end, as well as the biographies of all of your unborn descendants. It is startling that the five symbols used to write $\mathcal{P}(\mathbb{R}^2)$ can express such an incomprehensibly large set.

Homework: Think about $\mathcal{P}(\mathcal{P}(\mathbb{R}^2))$.

Exercises for Section 2.4

A. Find the indicated sets.

- | | |
|--|---|
| 1. $\mathcal{P}(\{\{a, b\}, \{c\}\})$ | 7. $\mathcal{P}(\{a, b\}) \times \mathcal{P}(\{0, 1\})$ |
| 2. $\mathcal{P}(\{1, 2, 3, 4\})$ | 8. $\mathcal{P}(\{1, 2\} \times \{3\})$ |
| 3. $\mathcal{P}(\{\{\emptyset\}, 5\})$ | 9. $\mathcal{P}(\{a, b\} \times \{0\})$ |
| 4. $\mathcal{P}(\{\mathbb{R}, \mathbb{Q}\})$ | 10. $\{X \in \mathcal{P}(\{1, 2, 3\}) : X \leq 1\}$ |
| 5. $\mathcal{P}(\mathcal{P}(\{2\}))$ | 11. $\{X \subseteq \mathcal{P}(\{1, 2, 3\}) : X \leq 1\}$ |
| 6. $\mathcal{P}(\{1, 2\}) \times \mathcal{P}(\{3\})$ | 12. $\{X \in \mathcal{P}(\{1, 2, 3\}) : 2 \in X\}$ |

B. Suppose that $|A| = m$ and $|B| = n$. Find the following cardinalities.

- | | |
|--|---|
| 13. $ \mathcal{P}(\mathcal{P}(\mathcal{P}(A))) $ | 17. $ \{X \in \mathcal{P}(A) : X \leq 1\} $ |
| 14. $ \mathcal{P}(\mathcal{P}(A)) $ | 18. $ \mathcal{P}(A \times \mathcal{P}(B)) $ |
| 15. $ \mathcal{P}(A \times B) $ | 19. $ \mathcal{P}(\mathcal{P}(\mathcal{P}(A \times \emptyset))) $ |
| 16. $ \mathcal{P}(A) \times \mathcal{P}(B) $ | 20. $ \{X \subseteq \mathcal{P}(A) : X \leq 1\} $ |

2.5 Union, Intersection, Difference

Just as numbers are combined with operations such as addition, subtraction and multiplication, there are various operations that can be applied to sets. The Cartesian product (defined in Section 2.2) is one such operation; given sets A and B , we can combine them with \times to get a new set $A \times B$. Here are three new operations called union, intersection and difference.

Definition 2.5 Suppose A and B are sets.

The **union** of A and B is the set $A \cup B = \{x : x \in A \text{ or } x \in B\}$.

The **intersection** of A and B is the set $A \cap B = \{x : x \in A \text{ and } x \in B\}$.

The **difference** of A and B is the set $A - B = \{x : x \in A \text{ and } x \notin B\}$.

In words, the union $A \cup B$ is the set of all things that are in A or in B (or in both). The intersection $A \cap B$ is the set of all things in both A and B . The difference $A - B$ is the set of all things that are in A but not in B .

Example 2.8 Suppose $A = \{a, b, c, d, e\}$, $B = \{d, e, f\}$ and $C = \{1, 2, 3\}$.

1. $A \cup B = \{a, b, c, d, e, f\}$
2. $A \cap B = \{d, e\}$
3. $A - B = \{a, b, c\}$
4. $B - A = \{f\}$
5. $(A - B) \cup (B - A) = \{a, b, c, f\}$
6. $A \cup C = \{a, b, c, d, e, 1, 2, 3\}$
7. $A \cap C = \emptyset$
8. $A - C = \{a, b, c, d, e\}$
9. $(A \cap C) \cup (A - C) = \{a, b, c, d, e\}$
10. $(A \cap B) \times B = \{(d, d), (d, e), (d, f), (e, d), (e, e), (e, f)\}$
11. $(A \times C) \cap (B \times C) = \{(d, 1), (d, 2), (d, 3), (e, 1), (e, 2), (e, 3)\}$

Observe that for any sets X and Y it is always true that $X \cup Y = Y \cup X$ and $X \cap Y = Y \cap X$, but in general $X - Y \neq Y - X$.

Continuing the example, parts 12–15 below use the interval notation discussed in Section 2.1, so $[2, 5] = \{x \in \mathbb{R} : 2 \leq x \leq 5\}$, etc. Sketching these examples on the number line may help you understand them.

12. $[2, 5] \cup [3, 6] = [2, 6]$
13. $[2, 5] \cap [3, 6] = [3, 5]$
14. $[2, 5] - [3, 6] = [2, 3]$
15. $[0, 3] - [1, 2] = [0, 1) \cup (2, 3]$



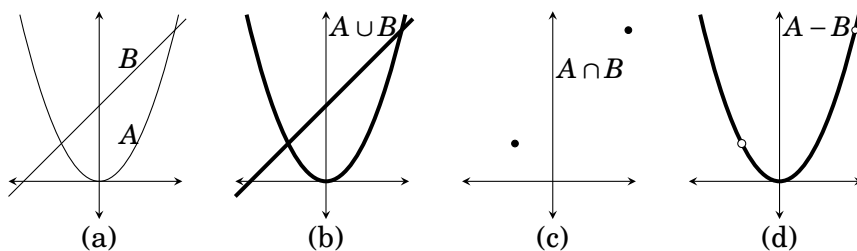


Figure 2.5. The union, intersection and difference of sets A and B

Example 2.9 Let $A = \{(x, x^2) : x \in \mathbb{R}\}$ be the graph of the equation $y = x^2$ and let $B = \{(x, x+2) : x \in \mathbb{R}\}$ be the graph of the equation $y = x+2$. These sets are subsets of \mathbb{R}^2 . They are sketched together in Figure 2.5(a). Figure 2.5(b) shows $A \cup B$, the set of all points (x, y) that are on one (or both) of the two graphs. Observe that $A \cap B = \{(-1, 1), (2, 4)\}$ consists of just two elements, the two points where the graphs intersect, as illustrated in Figure 2.5(c). Figure 2.5(d) shows $A - B$, which is the set A with “holes” where B crossed it. In set builder notation, we could write $A \cup B = \{(x, y) : x \in \mathbb{R}, y = x^2 \text{ or } y = x+2\}$ and $A - B = \{(x, x^2) : x \in \mathbb{R} - \{-1, 2\}\}$. \curvearrowright

Exercises for Section 2.5

- Suppose $A = \{4, 3, 6, 7, 1, 9\}$, $B = \{5, 6, 8, 4\}$ and $C = \{5, 8, 4\}$. Find:

| | | |
|----------------|----------------|----------------|
| (a) $A \cup B$ | (d) $A - C$ | (g) $B \cap C$ |
| (b) $A \cap B$ | (e) $B - A$ | (h) $B \cup C$ |
| (c) $A - B$ | (f) $A \cap C$ | (i) $C - B$ |
- Suppose $A = \{0, 2, 4, 6, 8\}$, $B = \{1, 3, 5, 7\}$ and $C = \{2, 8, 4\}$. Find:

| | | |
|----------------|----------------|----------------|
| (a) $A \cup B$ | (d) $A - C$ | (g) $B \cap C$ |
| (b) $A \cap B$ | (e) $B - A$ | (h) $C - A$ |
| (c) $A - B$ | (f) $A \cap C$ | (i) $C - B$ |
- Suppose $A = \{0, 1\}$ and $B = \{1, 2\}$. Find:

| | | |
|--------------------------------------|--|---------------------------------------|
| (a) $(A \times B) \cap (B \times B)$ | (d) $(A \cap B) \times A$ | (g) $\mathcal{P}(A) - \mathcal{P}(B)$ |
| (b) $(A \times B) \cup (B \times B)$ | (e) $(A \times B) \cap B$ | (h) $\mathcal{P}(A \cap B)$ |
| (c) $(A \times B) - (B \times B)$ | (f) $\mathcal{P}(A) \cap \mathcal{P}(B)$ | (i) $\mathcal{P}(A \times B)$ |
- Suppose $A = \{b, c, d\}$ and $B = \{a, b\}$. Find:

| | | |
|--------------------------------------|--|--|
| (a) $(A \times B) \cap (B \times B)$ | (d) $(A \cap B) \times A$ | (g) $\mathcal{P}(A) - \mathcal{P}(B)$ |
| (b) $(A \times B) \cup (B \times B)$ | (e) $(A \times B) \cap B$ | (h) $\mathcal{P}(A \cap B)$ |
| (c) $(A \times B) - (B \times B)$ | (f) $\mathcal{P}(A) \cap \mathcal{P}(B)$ | (i) $\mathcal{P}(A) \times \mathcal{P}(B)$ |

5. Sketch the sets $X = [1, 3] \times [1, 3]$ and $Y = [2, 4] \times [2, 4]$ on the plane \mathbb{R}^2 . On separate drawings, shade in the sets $X \cup Y$, $X \cap Y$, $X - Y$ and $Y - X$. (Hint: X and Y are Cartesian products of intervals. You may wish to review how you drew sets like $[1, 3] \times [1, 3]$ in the exercises for Section 2.2.)
6. Sketch the sets $X = [-1, 3] \times [0, 2]$ and $Y = [0, 3] \times [1, 4]$ on the plane \mathbb{R}^2 . On separate drawings, shade in the sets $X \cup Y$, $X \cap Y$, $X - Y$ and $Y - X$.
7. Sketch the sets $X = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 \leq 1\}$ and $Y = \{(x, y) \in \mathbb{R}^2 : x \geq 0\}$ on \mathbb{R}^2 . On separate drawings, shade in the sets $X \cup Y$, $X \cap Y$, $X - Y$ and $Y - X$.
8. Sketch the sets $X = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 \leq 1\}$ and $Y = \{(x, y) \in \mathbb{R}^2 : -1 \leq y \leq 0\}$ on \mathbb{R}^2 . On separate drawings, shade in the sets $X \cup Y$, $X \cap Y$, $X - Y$ and $Y - X$.
9. Is the statement $(\mathbb{R} \times \mathbb{Z}) \cap (\mathbb{Z} \times \mathbb{R}) = \mathbb{Z} \times \mathbb{Z}$ true or false? What about the statement $(\mathbb{R} \times \mathbb{Z}) \cup (\mathbb{Z} \times \mathbb{R}) = \mathbb{R} \times \mathbb{R}$?
10. Do you think the statement $(\mathbb{R} - \mathbb{Z}) \times \mathbb{N} = (\mathbb{R} \times \mathbb{N}) - (\mathbb{Z} \times \mathbb{N})$ is true, or false? Justify.

2.6 Complement

This section introduces yet another set operation, called the *set complement*. The definition requires the idea of a *universal set*, which we now discuss.

When dealing with a set, we almost always regard it as a subset of some larger set. For example, consider the set of prime numbers $P = \{2, 3, 5, 7, 11, 13, \dots\}$. If asked to name some things that are *not* in P , we might mention some composite numbers like 4 or 6 or 423. It probably would not occur to us to say that Vladimir Putin is not in P . True, Vladimir Putin is not in P , but he lies entirely outside of the discussion of what is a prime number and what is not. We have an unstated assumption that

$$P \subseteq \mathbb{N}$$

because \mathbb{N} is the most natural setting in which to discuss prime numbers. In this context, anything not in P should still be in \mathbb{N} . This larger set \mathbb{N} is called the **universal set** or **universe** for P .

Almost every useful set in mathematics can be regarded as having some natural universal set. For instance, the unit circle is the set $C = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$, and since all these points are in the plane \mathbb{R}^2 it is natural to regard \mathbb{R}^2 as the universal set for C . In the absence of specifics, if A is a set, then its universal set is often denoted as U . We are now ready to define the complement operation.

Definition 2.6 Let A be a set with a universal set U . The **complement** of A , denoted \bar{A} , is the set $\bar{A} = U - A$.

Example 2.10 If P is the set of prime numbers, then

$$\overline{P} = \mathbb{N} - P = \{1, 4, 6, 8, 9, 10, 12, \dots\}.$$

Thus \overline{P} is the set of composite numbers and 1. ✎

Example 2.11 Let $A = \{(x, x^2) : x \in \mathbb{R}\}$ be the graph of the equation $y = x^2$. Figure 2.6(a) shows A in its universal set \mathbb{R}^2 . The complement of A is $\overline{A} = \mathbb{R}^2 - A = \{(x, y) \in \mathbb{R}^2 : y \neq x^2\}$, illustrated by the shaded area in Figure 2.6(b).

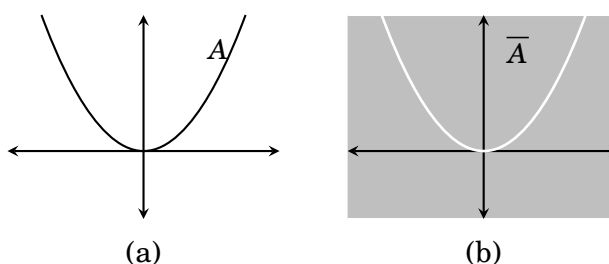


Figure 2.6. A set and its complement

Exercises for Section 2.6

- Let $A = \{4, 3, 6, 7, 1, 9\}$ and $B = \{5, 6, 8, 4\}$ have universal set $U = \{0, 1, 2, \dots, 10\}$. Find:

| | | |
|---------------------------|---------------------------|-----------------------------------|
| (a) \overline{A} | (d) $A \cup \overline{A}$ | (g) $\overline{A} - \overline{B}$ |
| (b) \overline{B} | (e) $A - \overline{A}$ | (h) $\overline{A} \cap B$ |
| (c) $A \cap \overline{A}$ | (f) $A - \overline{B}$ | (i) $\overline{A} \cap B$ |
 - Let $A = \{0, 2, 4, 6, 8\}$ and $B = \{1, 3, 5, 7\}$ have universal set $U = \{0, 1, 2, \dots, 8\}$. Find:

| | | |
|---------------------------|---------------------------|--------------------------------------|
| (a) \overline{A} | (d) $A \cup \overline{A}$ | (g) $\overline{A} \cap \overline{B}$ |
| (b) \overline{B} | (e) $A - \overline{A}$ | (h) $\overline{A} \cap \overline{B}$ |
| (c) $A \cap \overline{A}$ | (f) $\overline{A \cup B}$ | (i) $\overline{A} \times B$ |
 - Sketch the set $X = [1, 3] \times [1, 2]$ on the plane \mathbb{R}^2 . On separate drawings, shade in the sets \overline{X} and $\overline{X} \cap ([0, 2] \times [0, 3])$.
 - Sketch the set $X = [-1, 3] \times [0, 2]$ on the plane \mathbb{R}^2 . On separate drawings, shade in the sets \overline{X} and $\overline{X} \cap ([-2, 4] \times [-1, 3])$.
 - Sketch the set $X = \{(x, y) \in \mathbb{R}^2 : 1 \leq x^2 + y^2 \leq 4\}$ on the plane \mathbb{R}^2 . On a separate drawing, shade in the set \overline{X} .
 - Sketch the set $X = \{(x, y) \in \mathbb{R}^2 : y < x^2\}$ on \mathbb{R}^2 . Shade in the set \overline{X} .
-

2.7 Venn Diagrams

In thinking about sets, it is sometimes helpful to draw informal, schematic diagrams of them. In doing this we often represent a set with a circle (or oval), which we regard as enclosing all the elements of the set. Such diagrams can illustrate how sets combine using various operations. For example, Figures 2.7(a–c) show two sets A and B that overlap in a middle region. The sets $A \cup B$, $A \cap B$ and $A - B$ are shaded. Such graphical representations of sets are called **Venn diagrams**, after their inventor, British logician John Venn, 1834–1923.

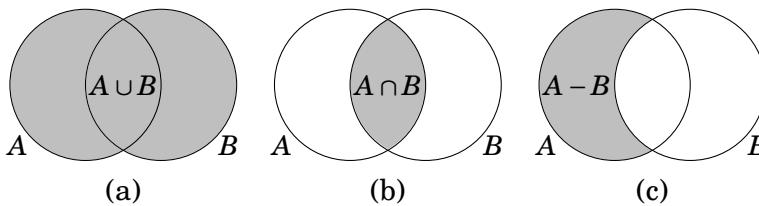


Figure 2.7. Venn diagrams for two sets

Though you may never draw a Venn diagram in writing up the solution of a problem, you will probably find them to be useful “scratch work” devices that help you to understand how sets combine, and to develop strategies for proving certain theorems or solving certain problems. The remainder of this section uses Venn diagrams to explore how three sets can be combined using \cup and \cap .

Let’s begin with the set $A \cup B \cup C$. Our definitions suggest this should consist of all elements which are in one or more of the sets A , B and C . Figure 2.8(a) shows a Venn diagram for this. Similarly, we think of $A \cap B \cap C$ as all elements common to each of A , B and C , so in Figure 2.8(b) the region belonging to all three sets is shaded.

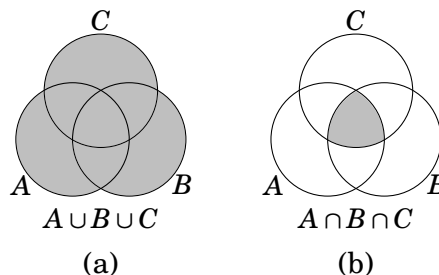


Figure 2.8. Venn diagrams for three sets

We can also think of $A \cap B \cap C$ as the two-step operation $(A \cap B) \cap C$. In this expression the set $A \cap B$ is represented by the region common to both A and B , and when we intersect *this* with C we get Figure 2.8(b). This is a visual representation of the fact that $A \cap B \cap C = (A \cap B) \cap C$. Similarly, we have $A \cap B \cap C = A \cap (B \cap C)$. Likewise, $A \cup B \cup C = (A \cup B) \cup C = A \cup (B \cup C)$.

Notice that in these examples, where the expression either contains only the symbol \cup or only the symbol \cap , the placement of the parentheses is irrelevant, so we are free to drop them. It is analogous to the situations in algebra involving expressions $(a+b)+c = a+(b+c)$ or $(a \cdot b) \cdot c = a \cdot (b \cdot c)$. We tend to drop the parentheses and write simply $a+b+c$ or $a \cdot b \cdot c$. By contrast, in an expression like $(a+b) \cdot c$ the parentheses are absolutely essential because $(a+b) \cdot c$ and $a+(b \cdot c)$ are generally not equal.

Now let's use Venn diagrams to help us understand the expressions $(A \cup B) \cap C$ and $A \cup (B \cap C)$, which use a mix of \cup and \cap . Figure 2.9 shows how to draw a Venn diagram for $(A \cup B) \cap C$. In the drawing on the left, the set $A \cup B$ is shaded with horizontal lines, while C is shaded with vertical lines. Thus the set $(A \cup B) \cap C$ is represented by the cross-hatched region where $A \cup B$ and C overlap. The superfluous shadings are omitted in the drawing on the right showing the set $(A \cup B) \cap C$.

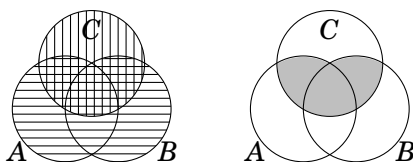


Figure 2.9. How to make a Venn diagram for $(A \cup B) \cap C$

Now think about $A \cup (B \cap C)$. In Figure 2.10 the set A is shaded with horizontal lines, and $B \cap C$ is shaded with vertical lines. The union $A \cup (B \cap C)$ is represented by the totality of all shaded regions, as shown on the right.

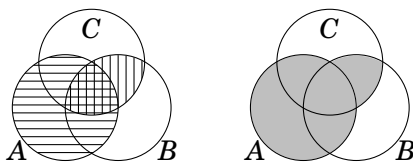


Figure 2.10. How to make a Venn diagram for $A \cup (B \cap C)$

Compare the diagrams for $(A \cup B) \cap C$ and $A \cup (B \cap C)$ in Figures 2.9 and 2.10. The fact that the diagrams are different indicates that $(A \cup B) \cap C \neq A \cup (B \cap C)$ in general. Thus an expression such as $A \cup B \cap C$ is absolutely meaningless because we can't tell whether it means $(A \cup B) \cap C$ or $A \cup (B \cap C)$. In summary, Venn diagrams have helped us understand the following.

Important Points:

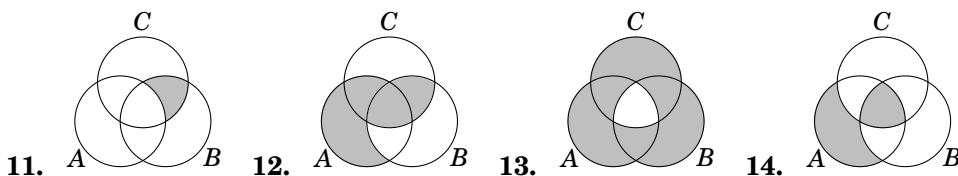
- If an expression involving sets uses only \cup , then parentheses are optional.
- If an expression involving sets uses only \cap , then parentheses are optional.
- If an expression uses both \cup and \cap , then parentheses are **essential**.

In the next section we will study types of expressions that use only \cup or only \cap . These expressions will not require the use of parentheses.

Exercises for Section 2.7

1. Draw a Venn diagram for \overline{A} .
2. Draw a Venn diagram for $B - A$.
3. Draw a Venn diagram for $(A - B) \cap C$.
4. Draw a Venn diagram for $(A \cup B) - C$.
5. Draw Venn diagrams for $A \cup (B \cap C)$ and $(A \cup B) \cap (A \cup C)$. Based on your drawings, do you think $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$?
6. Draw Venn diagrams for $A \cap (B \cup C)$ and $(A \cap B) \cup (A \cap C)$. Based on your drawings, do you think $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$?
7. Suppose sets A and B are in a universal set U . Draw Venn diagrams for $\overline{A \cap B}$ and $\overline{A} \cup \overline{B}$. Based on your drawings, do you think it's true that $\overline{A \cap B} = \overline{A} \cup \overline{B}$?
8. Suppose sets A and B are in a universal set U . Draw Venn diagrams for $\overline{A \cup B}$ and $\overline{A} \cap \overline{B}$. Based on your drawings, do you think it's true that $\overline{A \cup B} = \overline{A} \cap \overline{B}$?
9. Draw a Venn diagram for $(A \cap B) - C$.
10. Draw a Venn diagram for $(A - B) \cup C$.

Following are Venn diagrams for expressions involving sets A, B and C . Write the corresponding expression.



2.8 Indexed Sets

When a mathematical problem involves lots of sets, it is often convenient to keep track of them by using subscripts (also called indices). Thus instead of denoting three sets as A, B and C , we might instead write them as A_1, A_2 and A_3 . These are called **indexed sets**.

Although we defined union and intersection to be operations that combine two sets, you by now have no difficulty forming unions and intersections of three or more sets. (For instance, in the previous section we drew Venn diagrams for the intersection and union of three sets.) But let's take a moment to write down careful definitions. Given sets A_1, A_2, \dots, A_n , the set $A_1 \cup A_2 \cup A_3 \cup \dots \cup A_n$ consists of everything that is in *at least one* of the sets A_i . Likewise $A_1 \cap A_2 \cap A_3 \cap \dots \cap A_n$ consists of everything that is common to *all* of the sets A_i . Here is a careful definition.

Definition 2.7 Suppose A_1, A_2, \dots, A_n are sets. Then

$$A_1 \cup A_2 \cup A_3 \cup \dots \cup A_n = \{x : x \in A_i \text{ for at least one set } A_i, \text{ for } 1 \leq i \leq n\},$$

$$A_1 \cap A_2 \cap A_3 \cap \dots \cap A_n = \{x : x \in A_i \text{ for every set } A_i, \text{ for } 1 \leq i \leq n\}.$$

But if the number n of sets is large, these expressions can get messy. To overcome this, we now develop some notation akin to sigma notation. You already know that sigma notation is a convenient symbolism for expressing sums of many numbers. Given numbers $a_1, a_2, a_3, \dots, a_n$, then

$$\sum_{i=1}^n a_i = a_1 + a_2 + a_3 + \dots + a_n.$$

Even if the list of numbers is infinite, the sum

$$\sum_{i=1}^{\infty} a_i = a_1 + a_2 + a_3 + \dots + a_i + \dots$$

is often still meaningful. The notation we are about to introduce is very similar to this. Given sets $A_1, A_2, A_3, \dots, A_n$, we define

$$\bigcup_{i=1}^n A_i = A_1 \cup A_2 \cup A_3 \cup \dots \cup A_n \quad \text{and} \quad \bigcap_{i=1}^n A_i = A_1 \cap A_2 \cap A_3 \cap \dots \cap A_n.$$

Example 2.12 Suppose $A_1 = \{0, 2, 5\}$, $A_2 = \{1, 2, 5\}$ and $A_3 = \{2, 5, 7\}$. Then

$$\bigcup_{i=1}^3 A_i = A_1 \cup A_2 \cup A_3 = \{0, 1, 2, 5, 7\} \quad \text{and} \quad \bigcap_{i=1}^3 A_i = A_1 \cap A_2 \cap A_3 = \{2, 5\}. \quad \text{👉}$$


This notation is also used when the list of sets $A_1, A_2, A_3, A_4 \dots$ is infinite:

$$\bigcup_{i=1}^{\infty} A_i = A_1 \cup A_2 \cup A_3 \cup \dots = \{x : x \in A_i \text{ for at least one set } A_i \text{ with } 1 \leq i\}.$$

$$\bigcap_{i=1}^{\infty} A_i = A_1 \cap A_2 \cap A_3 \cap \dots = \{x : x \in A_i \text{ for every set } A_i \text{ with } 1 \leq i\}.$$

Example 2.13 This example involves the following infinite list of sets.

$$A_1 = \{-1, 0, 1\}, \quad A_2 = \{-2, 0, 2\}, \quad A_3 = \{-3, 0, 3\}, \quad \dots, \quad A_i = \{-i, 0, i\}, \quad \dots$$

Observe that $\bigcup_{i=1}^{\infty} A_i = \mathbb{Z}$, and $\bigcap_{i=1}^{\infty} A_i = \{0\}$. 

Here is a useful twist on our new notation. We can write

$$\bigcup_{i=1}^3 A_i = \bigcup_{i \in \{1, 2, 3\}} A_i,$$

as this takes the union of the sets A_i for $i = 1, 2, 3$. Likewise:

$$\bigcap_{i=1}^3 A_i = \bigcap_{i \in \{1, 2, 3\}} A_i$$

$$\bigcup_{i=1}^{\infty} A_i = \bigcup_{i \in \mathbb{N}} A_i$$

$$\bigcap_{i=1}^{\infty} A_i = \bigcap_{i \in \mathbb{N}} A_i$$

Here we are taking the union or intersection of a collection of sets A_i where i is an element of some set, be it $\{1, 2, 3\}$ or \mathbb{N} . In general, the way this works is that we will have a collection of sets A_i for $i \in I$, where I is the set of possible subscripts. The set I is called an **index set**.

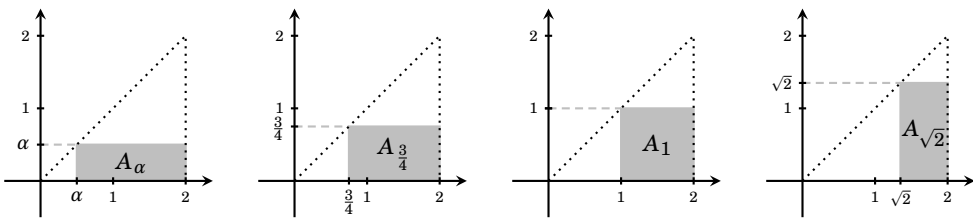
It is important to realize that the set I need not even consist of integers. (We could subscript with letters or real numbers, etc.) Since we are programmed to think of i as an integer, let's make a slight notational change: We use α , not i , to stand for an element of I . Thus we are dealing with a collection of sets A_α for $\alpha \in I$. This leads to the following definition.

Definition 2.8 If A_α is a set for every α in some index set I , then

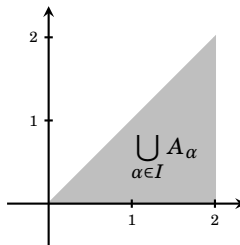
$$\bigcup_{\alpha \in I} A_\alpha = \{x : x \in A_\alpha \text{ for at least one set } A_\alpha \text{ with } \alpha \in I\}$$

$$\bigcap_{\alpha \in I} A_\alpha = \{x : x \in A_\alpha \text{ for every set } A_\alpha \text{ with } \alpha \in I\}.$$

Example 2.14 In this example, all sets A_α are all subsets of the plane \mathbb{R}^2 . Each α belongs to the index set $I = [0, 2] = \{x \in \mathbb{R} : 0 \leq x \leq 2\}$, which is the set of all real numbers between 0 and 2. For each number $\alpha \in I$, define A_α to be the set $A_\alpha = [\alpha, 2] \times [0, \alpha]$, which is the rectangle on the xy -plane whose base runs from α to 2 on the x -axis, and whose height is α . Some of these are shown shaded below. (The dotted diagonal line $y = x$ is not a part of any of the sets, but is shown for clarity, as the upper left corner of each A_α touches it.) Note that these sets are not indexed with just integers. For example, as $\sqrt{2} \in I$, there is a set $A_{\sqrt{2}}$, which is shown below on the right.



Now consider the infinite union $\bigcup_{\alpha \in I} A_\alpha$. It is the shaded triangle shown below, because any point (x, y) on this triangle belongs to the set A_x , and is therefore in the union.



Now let's work out the intersection $\bigcap_{\alpha \in I} A_\alpha$. Notice that the point $(2, 0)$ on the x -axis is the lower right corner of any set A_α , so $(2, 0) \in A_\alpha$ for any $\alpha \in I$. Therefore the point $(2, 0)$ is in the intersection of all the A_α . But any *other* point $(x, y) \neq (2, 0)$ on the triangle does not belong to all of the sets A_α . The reason is that if $x < 2$, then $(x, y) \notin A_\alpha$ for any $x < \alpha \leq 2$. (Check this.) And if $x = 2$, then $(x, y) \notin A_\alpha$ for any $0 < \alpha \leq y$. Consequently

$$\bigcap_{\alpha \in I} A_\alpha = \{(2, 0)\}.$$

This intersection consists of only one element, the point $(2, 0)$.



Exercises for Section 2.8

1. Suppose $A_1 = \{a, b, d, e, g, f\}$, $A_2 = \{a, b, c, d\}$, $A_3 = \{b, d, a\}$ and $A_4 = \{a, b, h\}$.

(a) $\bigcup_{i=1}^4 A_i =$

(b) $\bigcap_{i=1}^4 A_i =$

2. Suppose $\begin{cases} A_1 = \{0, 2, 4, 8, 10, 12, 14, 16, 18, 20, 22, 24\}, \\ A_2 = \{0, 3, 6, 9, 12, 15, 18, 21, 24\}, \\ A_3 = \{0, 4, 8, 12, 16, 20, 24\}. \end{cases}$

(a) $\bigcup_{i=1}^3 A_i =$

(b) $\bigcap_{i=1}^3 A_i =$

3. For each $n \in \mathbb{N}$, let $A_n = \{0, 1, 2, 3, \dots, n\}$.

(a) $\bigcup_{i \in \mathbb{N}} A_i =$

(b) $\bigcap_{i \in \mathbb{N}} A_i =$

4. For each $n \in \mathbb{N}$, let $A_n = \{-2n, 0, 2n\}$.

(a) $\bigcup_{i \in \mathbb{N}} A_i =$

(b) $\bigcap_{i \in \mathbb{N}} A_i =$

5. (a) $\bigcup_{i \in \mathbb{N}} [i, i+1] =$

(b) $\bigcap_{i \in \mathbb{N}} [i, i+1] =$

6. (a) $\bigcup_{i \in \mathbb{N}} [0, i+1] =$

(b) $\bigcap_{i \in \mathbb{N}} [0, i+1] =$

7. (a) $\bigcup_{i \in \mathbb{N}} \mathbb{R} \times [i, i+1] =$

(b) $\bigcap_{i \in \mathbb{N}} \mathbb{R} \times [i, i+1] =$

8. (a) $\bigcup_{\alpha \in \mathbb{R}} \{\alpha\} \times [0, 1] =$

(b) $\bigcap_{\alpha \in \mathbb{R}} \{\alpha\} \times [0, 1] =$

9. (a) $\bigcup_{X \in \mathcal{P}(\mathbb{N})} X =$

(b) $\bigcap_{X \in \mathcal{P}(\mathbb{N})} X =$

10. (a) $\bigcup_{x \in [0, 1]} [x, 1] \times [0, x^2] =$

(b) $\bigcap_{x \in [0, 1]} [x, 1] \times [0, x^2] =$

11. Is $\bigcap_{\alpha \in I} A_\alpha \subseteq \bigcup_{\alpha \in I} A_\alpha$ always true for any collection of sets A_α with index set I ?

12. If $\bigcap_{\alpha \in I} A_\alpha = \bigcup_{\alpha \in I} A_\alpha$, what do you think can be said about the relationships between the sets A_α ?

13. If $J \neq \emptyset$ and $J \subseteq I$, does it follow that $\bigcup_{\alpha \in J} A_\alpha \subseteq \bigcup_{\alpha \in I} A_\alpha$? What about $\bigcap_{\alpha \in J} A_\alpha \subseteq \bigcap_{\alpha \in I} A_\alpha$?

14. If $J \neq \emptyset$ and $J \subseteq I$, does it follow that $\bigcap_{\alpha \in I} A_\alpha \subseteq \bigcap_{\alpha \in J} A_\alpha$? Explain.

2.9 Sets that Are Number Systems

In practice, the sets we tend to be most interested in often have special properties and structures. For example, the sets \mathbb{Z} , \mathbb{Q} and \mathbb{R} are familiar number systems: Given such a set, any two of its elements can be added (or multiplied, etc.) together to produce another element in the set. These operations obey the familiar commutative, associative and distributive properties that we have dealt with for years. Such properties lead to the standard algebraic techniques for solving equations. Even though much of this book will be concerned with the idea of proof, we will not find it necessary to define or prove these properties and techniques; we will accept them as the ground rules upon which further deductions are based.

We also accept as fact the natural ordering of the elements of \mathbb{N} , \mathbb{Z} , \mathbb{Q} and \mathbb{R} , so that (for example) the meaning of “ $5 < 7$ ” is understood and does not need to be justified or explained. Similarly, if $x \leq y$ and $a \neq 0$, we know that $ax \leq ay$ or $ax \geq ay$, depending on whether a is positive or negative.

Another thing that our ingrained understanding of the ordering of numbers tells us is that any non-empty subset of \mathbb{N} has a smallest element. In other words, if $A \subseteq \mathbb{N}$ and $A \neq \emptyset$, then there is an element $x_0 \in A$ that is smaller than every other element of A . (To find it, start at 1, then move in increments to 2, 3, 4, etc., until you hit a number $x_0 \in A$; this is the smallest element of A .) Similarly, given an integer b , any non-empty subset $A \subseteq \{b, b+1, b+2, b+3, \dots\}$ has a smallest element. This fact is sometimes called the **well-ordering principle**. There is no need to remember this term, but do be aware that we will use this simple, intuitive idea often in proofs, usually without a second thought.

The well-ordering principle seems innocent enough, but it actually says something very fundamental and special about the positive integers \mathbb{N} . In fact, the corresponding statement about the positive real numbers is false: The subset $A = \{\frac{1}{n} : n \in \mathbb{N}\}$ of the positive reals has no smallest element because for any $x_0 = \frac{1}{n} \in A$ that we might pick, there is always a smaller element $\frac{1}{n+1} \in A$.

Despite the fact that we will scarcely mention it again in this book, the well-ordering principle plays a fundamental role in discrete mathematics. For example, imagine a loop in a computer program that continues to execute as long as some integer value x is positive. If each iteration of the loop decreases the value of x , then it is the well-ordering principle that assures us that the loop eventually terminates. This is because the set A of all values that x takes on is a subset of \mathbb{N} and therefore has a smallest element, namely the value of x in the last iteration of the loop.

2.10 Case Study: Russell's Paradox

This section contains some background information that may be interesting, but is not used in the remainder of the book.

The philosopher and mathematician Bertrand Russell (1872–1970) did groundbreaking work on the theory of sets and the foundations of mathematics. He was probably among the first to understand how the misuse of sets can lead to bizarre and paradoxical situations. He is famous for an idea that has come to be known as **Russell's paradox**.

Russell's paradox involves the following set of sets:

$$A = \{X : X \text{ is a set and } X \notin X\}. \quad (2.1)$$

In words, A is the set of all sets that do not include themselves as elements. Most sets we can think of are in A . The set \mathbb{Z} of integers is not an integer (i.e., $\mathbb{Z} \notin \mathbb{Z}$) and therefore $\mathbb{Z} \in A$. Also $\emptyset \in A$ because \emptyset is a set and $\emptyset \notin \emptyset$.

Is there a set that is not in A ? Consider $B = \{\underbrace{\{\{\{\dots\}\}\}}_B\}$. Think of B as a box containing a box, containing a box, containing a box, and so on, forever. Or a set of Russian dolls, nested one inside the other, endlessly. The curious thing about B is that it has just one element, namely B itself:

$$B = \{\underbrace{\{\{\{\dots\}\}\}}_B\}.$$

Thus $B \in B$. As B does not satisfy $B \notin B$, Equation (2.1) says $B \notin A$.

Russell's paradox arises from the question “*Is A an element of A ?*”

For a set X , Equation (2.1) says $X \in A$ means the same thing as $X \notin X$. So for $X = A$, the previous line says $A \in A$ means the same thing as $A \notin A$. Conclusion: if $A \in A$ is true, then it is false; if $A \in A$ is false, then it is true. This is Russell's paradox.

Initially Russell's paradox sparked a crisis among mathematicians. How could a mathematical statement be both true and false? This seemed to be in opposition to the very essence of mathematics.

The paradox instigated a very careful examination of set theory and an evaluation of what can and cannot be regarded as a set. Eventually mathematicians settled upon a collection of axioms for set theory—the so-called **Zermelo-Fraenkel axioms**. One of these axioms is the well-ordering principle of the previous section. Another, the axiom of foundation, states that no non-empty set X is allowed to have the property $X \cap x \neq \emptyset$ for all its elements x . This rules out such circularly defined “sets” as $B = \{B\}$ mentioned above. If we adhere to these axioms, then situations like Russell's

paradox disappear. Most mathematicians accept all this on faith and happily ignore the Zermelo-Fraenkel axioms. Paradoxes like Russell's do not tend to come up in everyday mathematics—you have to go out of your way to construct them.

Still, Russell's paradox reminds us that precision of thought and language is an important part of doing mathematics. The next chapter deals with the topic of logic, a codification of thought and language.

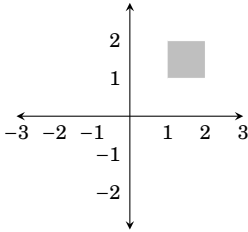
Additional Reading on Sets. For a lively account of Bertrand Russell's life and work (including his paradox), see the graphic novel *Logicomix: An Epic Search For Truth*, by Apostolos Doxiadis and Christos Papadimitriou. Also see cartoonist Jessica Hagy's online strip *Indexed*—it is based largely on Venn diagrams.

2.11 Solutions for Chapter 2

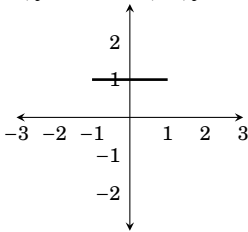
Section 2.1

1. $\{5x - 1 : x \in \mathbb{Z}\} = \{\dots - 11, -6, -1, 4, 9, 14, 19, 24, 29, \dots\}$
3. $\{x \in \mathbb{Z} : -2 \leq x < 7\} = \{-2, -1, 0, 1, 2, 3, 4, 5, 6\}$
5. $\{x \in \mathbb{R} : x^2 = 3\} = \{-\sqrt{3}, \sqrt{3}\}$
7. $\{x \in \mathbb{R} : x^2 + 5x = -6\} = \{-2, -3\}$
9. $\{x \in \mathbb{R} : \sin \pi x = 0\} = \{\dots, -2, -1, 0, 1, 2, 3, 4, \dots\} = \mathbb{Z}$
11. $\{x \in \mathbb{Z} : |x| < 5\} = \{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$
13. $\{x \in \mathbb{Z} : |6x| < 5\} = \{0\}$
15. $\{5a + 2b : a, b \in \mathbb{Z}\} = \{\dots, -2, -1, 0, 1, 2, 3, \dots\} = \mathbb{Z}$
17. $\{2, 4, 8, 16, 32, 64, \dots\} = \{2^x : x \in \mathbb{N}\}$
19. $\{\dots, -6, -3, 0, 3, 6, 9, 12, 15, \dots\} = \{3x : x \in \mathbb{Z}\}$
21. $\{0, 1, 4, 9, 16, 25, 36, \dots\} = \{x^2 : x \in \mathbb{Z}\}$
23. $\{3, 4, 5, 6, 7, 8\} = \{x \in \mathbb{Z} : 3 \leq x \leq 8\} = \{x \in \mathbb{N} : 3 \leq x \leq 8\}$
25. $\{\dots, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, \dots\} = \{2^n : n \in \mathbb{Z}\}$
27. $\{\dots, -\pi, -\frac{\pi}{2}, 0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}, 2\pi, \frac{5\pi}{2}, \dots\} = \{\frac{k\pi}{2} : k \in \mathbb{Z}\}$
29. $|\{\{1\}, \{2, \{3, 4\}\}, \emptyset\}| = 3$
33. $|\{x \in \mathbb{Z} : |x| < 10\}| = 19$
37. $|\{x \in \mathbb{N} : x^2 < 0\}| = 0$
31. $|\{\{\{1\}, \{2, \{3, 4\}\}, \emptyset\}\}| = 1$
35. $|\{x \in \mathbb{Z} : x^2 < 10\}| = 7$

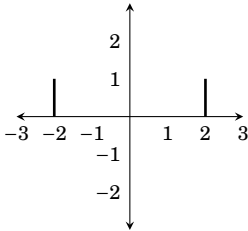
39. $\{(x, y) : x \in [1, 2], y \in [1, 2]\}$



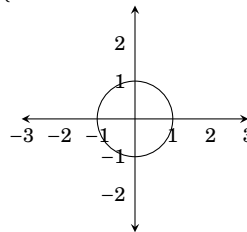
41. $\{(x, y) : x \in [-1, 1], y = 1\}$



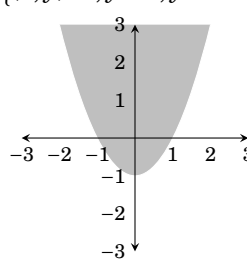
43. $\{(x, y) : |x| = 2, y \in [0, 1]\}$



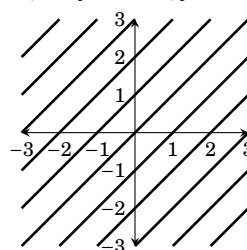
45. $\{(x, y) : x, y \in \mathbb{R}, x^2 + y^2 = 1\}$



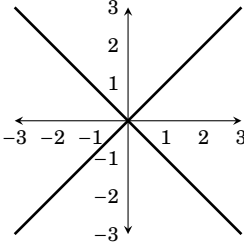
47. $\{(x, y) : x, y \in \mathbb{R}, y \geq x^2 - 1\}$



49. $\{(x, x + y) : x \in \mathbb{R}, y \in \mathbb{Z}\}$



51. $\{(x, y) \in \mathbb{R}^2 : (y - x)(y + x) = 0\}$



53. $\{x \in \mathbb{N} : 100 \leq x \leq 1011\} = \{100, 101, 110, 111, 1000, 1001, 1010, 1011\}$

55. $\{x \in \mathbb{N} : A \leq x \leq 20\} = \{A, B, C, D, E, F, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 1A, 1B, 1C, 1D, 1E, 1F, 20\}$

Section 2.2

1. Suppose $A = \{1, 2, 3, 4\}$ and $B = \{a, c\}$.

(a) $A \times B = \{(1, a), (1, c), (2, a), (2, c), (3, a), (3, c), (4, a), (4, c)\}$

(b) $B \times A = \{(a, 1), (a, 2), (a, 3), (a, 4), (c, 1), (c, 2), (c, 3), (c, 4)\}$

(c) $A \times A = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 1), (2, 2), (2, 3), (2, 4), (3, 1), (3, 2), (3, 3), (3, 4), (4, 1), (4, 2), (4, 3), (4, 4)\}$

(d) $B \times B = \{(a, a), (a, c), (c, a), (c, c)\}$

(e) $\emptyset \times B = \{(a, b) : a \in \emptyset, b \in B\} = \emptyset$ (There are no ordered pairs (a, b) with $a \in \emptyset$.)

(f) $(A \times B) \times B =$

$\{((1, a), a), ((1, c), a), ((2, a), a), ((2, c), a), ((3, a), a), ((3, c), a), ((4, a), a), ((4, c), a), ((1, a), c), ((1, c), c), ((2, a), c), ((2, c), c), ((3, a), c), ((3, c), c), ((4, a), c), ((4, c), c)\}$

(g) $A \times (B \times B) =$

$\{(1, (a, a)), (1, (a, c)), (1, (c, a)), (1, (c, c)), (2, (a, a)), (2, (a, c)), (2, (c, a)), (2, (c, c)), (3, (a, a)), (3, (a, c)), (3, (c, a)), (3, (c, c)), (4, (a, a)), (4, (a, c)), (4, (c, a)), (4, (c, c))\}$

(h) $B^3 = \{(a, a, a), (a, a, c), (a, c, a), (a, c, c), (c, a, a), (c, a, c), (c, c, a), (c, c, c)\}$

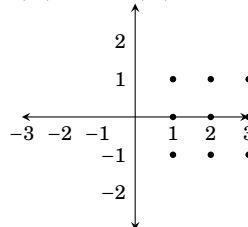
3. $\{x \in \mathbb{R} : x^2 = 2\} \times \{a, c, e\} = \{(-\sqrt{2}, a), (\sqrt{2}, a), (-\sqrt{2}, c), (\sqrt{2}, c), (-\sqrt{2}, e), (\sqrt{2}, e)\}$

5. $\{x \in \mathbb{R} : x^2 = 2\} \times \{x \in \mathbb{R} : |x| = 2\} = \{(-\sqrt{2}, -2), (\sqrt{2}, 2), (-\sqrt{2}, 2), (\sqrt{2}, -2)\}$

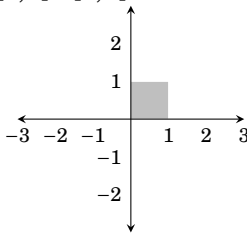
7. $\{\emptyset\} \times \{0, \emptyset\} \times \{0, 1\} = \{(\emptyset, 0, 0), (\emptyset, 0, 1), (\emptyset, \emptyset, 0), (\emptyset, \emptyset, 1)\}$

Sketch the following Cartesian products on the x - y plane.

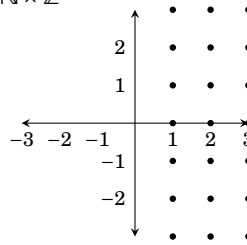
9. $\{1, 2, 3\} \times \{-1, 0, 1\}$



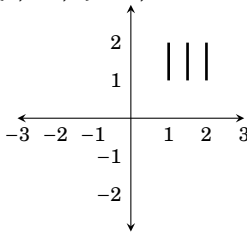
11. $[0, 1] \times [0, 1]$



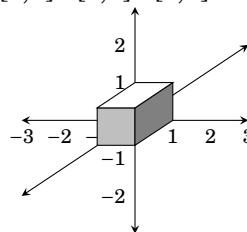
17. $\mathbb{N} \times \mathbb{Z}$



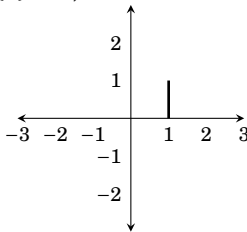
13. $\{1, 1.5, 2\} \times [1, 2]$



19. $[0, 1] \times [0, 1] \times [0, 1]$



15. $\{1\} \times [0, 1]$



Section 2.3

A. List all the subsets of the following sets.

- 1. The subsets of $\{1, 2, 3, 4\}$ are: $\{\}, \{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}, \{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}, \{2, 3, 4\}, \{1, 2, 3, 4\}$.
- 3. The subsets of $\{\{\mathbb{R}\}\}$ are: $\{\}$ and $\{\{\mathbb{R}\}\}$.
- 5. The subsets of $\{\emptyset\}$ are $\{\}$ and $\{\emptyset\}$.
- 7. The subsets of $\{\mathbb{R}, \{\mathbb{Q}, \mathbb{N}\}\}$ are $\{\}, \{\mathbb{R}\}, \{\{\mathbb{Q}, \mathbb{N}\}\}, \{\mathbb{R}, \{\mathbb{Q}, \mathbb{N}\}\}$.

B. Write out the following sets by listing their elements between braces.

- 9. $\{X : X \subseteq \{3, 2, a\} \text{ and } |X| = 2\} = \{\{3, 2\}, \{3, a\}, \{2, a\}\}$
- 11. $\{X : X \subseteq \{3, 2, a\} \text{ and } |X| = 4\} = \{\} = \emptyset$

C. Decide if the following statements are true or false.

- 13. $\mathbb{R}^3 \subseteq \mathbb{R}^3$ is **true** because any set is a subset of itself.
- 15. $\{(x, y) : x - 1 = 0\} \subseteq \{(x, y) : x^2 - x = 0\}$. This is true. (The even-numbered ones are both false. You have to explain why.)

Section 2.4

A. Find the indicated sets.

1. $\mathcal{P}(\{\{a, b\}, \{c\}\}) = \{\emptyset, \{\{a, b\}\}, \{\{c\}\}, \{\{a, b\}, \{c\}\}\}$
3. $\mathcal{P}(\{\{\emptyset\}, 5\}) = \{\emptyset, \{\{\emptyset\}\}, \{5\}, \{\{\emptyset\}, 5\}\}$
5. $\mathcal{P}(\mathcal{P}(\{2\})) = \{\emptyset, \{\emptyset\}, \{\{2\}\}, \{\emptyset, \{2\}\}\}$
7. $\mathcal{P}(\{a, b\}) \times \mathcal{P}(\{0, 1\}) =$

$$\left\{ \begin{array}{cccc} (\emptyset, \emptyset), & (\emptyset, \{0\}), & (\emptyset, \{1\}), & (\emptyset, \{0, 1\}), \\ (\{a\}, \emptyset), & (\{a\}, \{0\}), & (\{a\}, \{1\}), & (\{a\}, \{0, 1\}), \\ (\{b\}, \emptyset), & (\{b\}, \{0\}), & (\{b\}, \{1\}), & (\{b\}, \{0, 1\}), \\ (\{a, b\}, \emptyset), & (\{a, b\}, \{0\}), & (\{a, b\}, \{1\}), & (\{a, b\}, \{0, 1\}) \end{array} \right\}$$
9. $\mathcal{P}(\{a, b\} \times \{0\}) = \{\emptyset, \{(a, 0)\}, \{(b, 0)\}, \{(a, 0), (b, 0)\}\}$
11. $\{X \subseteq \mathcal{P}(\{1, 2, 3\}) : |X| \leq 1\} =$
 $\{\emptyset, \{\emptyset\}, \{\{1\}\}, \{\{2\}\}, \{\{3\}\}, \{\{1, 2\}\}, \{\{1, 3\}\}, \{\{2, 3\}\}, \{\{1, 2, 3\}\}\}$

B. Suppose that $|A| = m$ and $|B| = n$. Find the following cardinalities.

13. $|\mathcal{P}(\mathcal{P}(\mathcal{P}(A)))| = 2^{(2^{(2^m)})}$
15. $|\mathcal{P}(A \times B)| = 2^{mn}$
17. $|\{X \in \mathcal{P}(A) : |X| \leq 1\}| = m + 1$
19. $|\mathcal{P}(\mathcal{P}(\mathcal{P}(A \times \emptyset)))| = |\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset)))| = 4$

Section 2.5

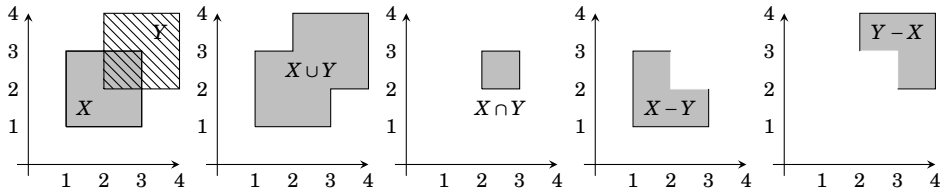
1. Suppose $A = \{4, 3, 6, 7, 1, 9\}$, $B = \{5, 6, 8, 4\}$ and $C = \{5, 8, 4\}$. Find:

- | | |
|--|--|
| (a) $A \cup B = \{1, 3, 4, 5, 6, 7, 8, 9\}$ | (f) $A \cap C = \{4\}$ |
| (b) $A \cap B = \{4, 6\}$ | (g) $B \cap C = \{5, 8, 4\}$ |
| (c) $A - B = \{3, 7, 1, 9\}$ | (h) $B \cup C = \{5, 6, 8, 4\}$ |
| (d) $A - C = \{3, 6, 7, 1, 9\}$ | (i) $C - B = \emptyset$ |
| (e) $B - A = \{5, 8\}$ | |

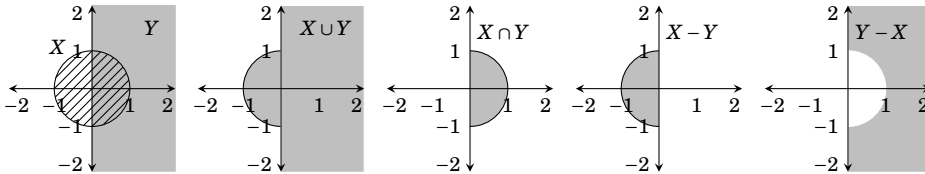
3. Suppose $A = \{0, 1\}$ and $B = \{1, 2\}$. Find:

- | | |
|--|--|
| (a) $(A \times B) \cap (B \times B) = \{(1, 1), (1, 2)\}$ | (f) $\mathcal{P}(A) \cap \mathcal{P}(B) = \{\emptyset, \{1\}\}$ |
| (b) $(A \times B) \cup (B \times B) = \{(0, 1), (0, 2), (1, 1), (1, 2), (2, 1), (2, 2)\}$ | (g) $\mathcal{P}(A) - \mathcal{P}(B) = \{\{0\}, \{0, 1\}\}$ |
| (c) $(A \times B) - (B \times B) = \{(0, 1), (0, 2)\}$ | (h) $\mathcal{P}(A \cap B) = \{\emptyset, \{1\}\}$ |
| (d) $(A \cap B) \times A = \{(1, 0), (1, 1)\}$ | |
| (e) $(A \times B) \cap B = \emptyset$ | |
- (i)** $\{\emptyset, \{(0, 1)\}, \{(0, 2)\}, \{(1, 1)\}, \{(1, 2)\}, \{(0, 1), (0, 2)\}, \{(0, 1), (1, 1)\}, \{(0, 1), (1, 2)\}, \{(0, 2), (1, 1)\}, \{(0, 2), (1, 2)\}, \{(1, 1), (1, 2)\}, \{(0, 2), (1, 1), (1, 2)\}, \{(0, 1), (1, 1), (1, 2)\}, \{(0, 1), (0, 2), (1, 2)\}, \{(0, 1), (0, 2), (1, 1)\}, \{(0, 1), (0, 2), (1, 1), (1, 2)\}\}$

5. Sketch the sets $X = [1, 3] \times [1, 3]$ and $Y = [2, 4] \times [2, 4]$ on the plane \mathbb{R}^2 . On separate drawings, shade in the sets $X \cup Y$, $X \cap Y$, $X - Y$ and $Y - X$. (Hint: X and Y are Cartesian products of intervals. You may wish to review how you drew sets like $[1, 3] \times [1, 3]$ in the Section 2.2.)



7. Sketch the sets $X = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 \leq 1\}$ and $Y = \{(x, y) \in \mathbb{R}^2 : x \geq 0\}$ on \mathbb{R}^2 . On separate drawings, shade in the sets $X \cup Y$, $X \cap Y$, $X - Y$ and $Y - X$.



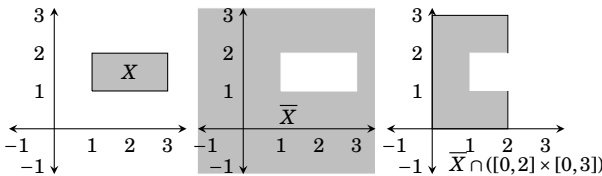
9. The first statement is true. (A picture should convince you; draw one if necessary.) The second statement is false: Notice for instance that $(0.5, 0.5)$ is in the right-hand set, but not the left-hand set.

Section 2.6

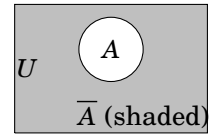
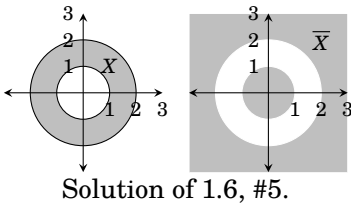
1. Suppose $A = \{4, 3, 6, 7, 1, 9\}$ and $B = \{5, 6, 8, 4\}$ have universal set $U = \{n \in \mathbb{Z} : 0 \leq n \leq 10\}$.

- (a) $\bar{A} = \{0, 2, 5, 8, 10\}$
- (b) $\bar{B} = \{0, 1, 2, 3, 7, 9, 10\}$
- (c) $A \cap \bar{A} = \emptyset$
- (d) $A \cup \bar{A} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} = U$
- (e) $A - \bar{A} = A$
- (f) $A - \bar{B} = \{4, 6\}$
- (g) $\bar{A} - \bar{B} = \{5, 8\}$
- (h) $\bar{A} \cap B = \{5, 8\}$
- (i) $\overline{\bar{A} \cap B} = \{0, 1, 2, 3, 4, 6, 7, 9, 10\}$

3. Sketch the set $X = [1, 3] \times [1, 2]$ on the plane \mathbb{R}^2 . On separate drawings, shade in the sets \bar{X} , and $\bar{X} \cap ([0, 2] \times [0, 3])$.



5. Sketch the set $X = \{(x, y) \in \mathbb{R}^2 : 1 \leq x^2 + y^2 \leq 4\}$ on the plane \mathbb{R}^2 . On a separate drawing, shade in the set \bar{X} .



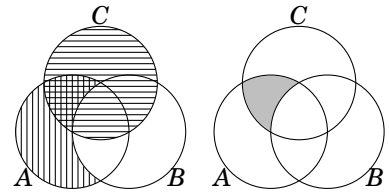
Solution of 1.7, #1.

Section 2.7

1. Draw a Venn diagram for \bar{A} . (Solution above right)

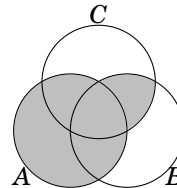
3. Draw a Venn diagram for $(A - B) \cap C$.

Scratch work is shown on the right. The set $A - B$ is indicated with vertical shading. The set C is indicated with horizontal shading. The intersection of $A - B$ and C is thus the overlapping region that is shaded with both vertical and horizontal lines. The final answer is drawn on the far right, where the set $(A - B) \cap C$ is shaded in gray.



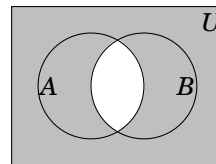
5. Draw Venn diagrams for $A \cup (B \cap C)$ and $(A \cup B) \cap (A \cup C)$. Based on your drawings, do you think $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$?

If you do the drawings carefully, you will find that your Venn diagrams are the same for both $A \cup (B \cap C)$ and $(A \cup B) \cap (A \cup C)$. Each looks as illustrated on the right. Based on this, we are inclined to say that the equation $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ holds for all sets A, B and C .

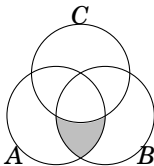


7. Suppose sets A and B are in a universal set U . Draw Venn diagrams for $\overline{A \cap B}$ and $\bar{A} \cup \bar{B}$. Based on your drawings, do you think it's true that $\overline{A \cap B} = \bar{A} \cup \bar{B}$?

The diagrams for $\overline{A \cap B}$ and $\bar{A} \cup \bar{B}$ look exactly alike. In either case the diagram is the shaded region illustrated on the right. Thus we would expect that the equation $\overline{A \cap B} = \bar{A} \cup \bar{B}$ is true for any sets A and B .



9. Draw a Venn diagram for $(A \cap B) - C$.



11. The simplest answer is $(B \cap C) - A$.

13. One answer is $(A \cup B \cup C) - (A \cap B \cap C)$.

Section 2.8

1. Suppose $A_1 = \{a, b, d, e, g, f\}$, $A_2 = \{a, b, c, d\}$, $A_3 = \{b, d, a\}$ and $A_4 = \{a, b, h\}$.

(a) $\bigcup_{i=1}^4 A_i = \{a, b, c, d, e, f, g, h\}$

(b) $\bigcap_{i=1}^4 A_i = \{a, b\}$

3. For each $n \in \mathbb{N}$, let $A_n = \{0, 1, 2, 3, \dots, n\}$.

(a) $\bigcup_{i \in \mathbb{N}} A_i = \{0\} \cup \mathbb{N}$

(b) $\bigcap_{i \in \mathbb{N}} A_i = \{0, 1\}$

5. (a) $\bigcup_{i \in \mathbb{N}} [i, i+1] = [1, \infty)$

(b) $\bigcap_{i \in \mathbb{N}} [i, i+1] = \emptyset$

7. (a) $\bigcup_{i \in \mathbb{N}} \mathbb{R} \times [i, i+1] = \{(x, y) : x, y \in \mathbb{R}, y \geq 1\}$

(b) $\bigcap_{i \in \mathbb{N}} \mathbb{R} \times [i, i+1] = \emptyset$

9. (a) $\bigcup_{X \in \mathcal{P}(\mathbb{N})} X = \mathbb{N}$

(b) $\bigcap_{X \in \mathcal{P}(\mathbb{N})} X = \emptyset$

11. Yes, this is always true.

13. The first is true, the second is false.

Logic

Logic is a systematic way of thinking that allows us to deduce new information from old information and to parse the meanings of sentences. We introduce logic now because it is the key to understanding certain words like “and,” “or,” and “if” that have special meanings in a mathematical context. Understanding these meanings is essential throughout this book, and beyond it. Logic becomes even more important Part II if this book, as we begin proving theorems and verifying mathematical truths.

You use logic informally in everyday life and certainly also in doing mathematics. For example, suppose you are working with a certain circle, call it “Circle X,” and you have available the following two pieces of information.

1. Circle X has radius equal to 3.
2. If any circle has radius r , then its area is πr^2 square units.

You have no trouble putting these two facts together to get:

3. Circle X has area 9π square units.

In doing this you are using logic to combine existing information to produce new information. Because deducing new information is central to mathematics, logic plays a fundamental role.

It is important to realize that logic is a process of deducing information correctly, *not* just deducing correct information. For example, suppose we were mistaken and Circle X actually had a radius of 4, not 3. Let’s look at our exact same argument again.

1. Circle X has radius equal to 3.
2. If any circle has radius r , then its area is πr^2 square units.

-
3. Circle X has area 9π square units.

The sentence “*Circle X has radius equal to 3.*” is now untrue, and so is our conclusion “*Circle X has area 9π square units.*” But the logic is perfectly correct; the information was combined correctly, even if some of it was false.

This distinction between correct logic and correct information is significant because it is often important to follow the consequences of an incorrect assumption. Ideally, we want both our logic *and* our information to be correct, but the point is that they are different things.

The study of logic begins with *statements*.

3.1 Statements

A **statement** is a sentence or a mathematical expression that is either definitely true or definitely false. You can think of statements as pieces of information that are either correct or incorrect. Thus statements are pieces of information that we might apply logic to in order to produce other pieces of information (which are also statements).

Example 3.1 Here are some examples of statements. They are all true.

If a circle has radius r , then its area is πr^2 square units.

Every even number is divisible by 2.

$$2 \in \mathbb{Z}$$

$$\sqrt{2} \notin \mathbb{Z}$$

$$\mathbb{N} \subseteq \mathbb{Z}$$

The set $\{0, 1, 2\}$ has three elements.

Some right triangles are isosceles. 

Example 3.2 Here are some additional statements. They are all false.

All right triangles are isosceles.

$$5 = 2$$

$$\sqrt{2} \notin \mathbb{R}$$

$$\mathbb{Z} \subseteq \mathbb{N}$$

$$\{0, 1, 2\} \cap \mathbb{N} = \emptyset$$
 

Example 3.3 Here we pair sentences or expressions that are not statements with similar expressions that *are* statements.

| NOT Statements: | Statements: |
|-------------------------------------|---|
| Add 5 to both sides. | Adding 5 to both sides of $x - 5 = 37$ gives $x = 42$. |
| \mathbb{Z} | $42 \in \mathbb{Z}$ |
| 42 | 42 is not a number. |
| What is the solution of $2x = 84$? | The solution of $2x = 84$ is 42. |

Example 3.4 We will often use the letters P , Q , R and S to stand for specific statements. When more letters are needed we can use subscripts. Here are more statements, designated with letters. You decide which of them are true and which are false.

P : For every integer $n > 1$, the number $2^n - 1$ is prime.

Q : Every polynomial of degree n has at most n roots.

R : The function $f(x) = x^2$ is continuous.

S_1 : $\mathbb{Z} \subseteq \emptyset$

S_2 : $\{0, -1, -2\} \cap \mathbb{N} = \emptyset$



Designating statements with letters (as was done above) is a very useful shorthand. In discussing a particular statement, such as “*The function $f(x) = x^2$ is continuous,*” it is convenient to just refer to it as R to avoid having to write or say it many times.

Statements can contain variables. Here is an example.

P : If an integer x is a multiple of 6, then x is even.

This is a sentence that is true. (All multiples of 6 are even, so no matter which multiple of 6 the integer x happens to be, it is even.) Since the sentence P is definitely true, it is a statement. When a sentence or statement P contains a variable such as x , we sometimes denote it as $P(x)$ to indicate that it is saying something about x . Thus the above statement can be denoted as

$P(x)$: If an integer x is a multiple of 6, then x is even.

A statement or sentence involving two variables might be denoted $P(x, y)$, and so on.

It is quite possible for a sentence containing variables to not be a statement. Consider the following example.

$Q(x)$: The integer x is even.

Is this a statement? Whether it is true or false depends on just which integer x is. It is true if $x = 4$ and false if $x = 7$, etc. But without any stipulations on the value of x it is impossible to say whether $Q(x)$ is true or false. Since it is neither definitely true nor definitely false, $Q(x)$ cannot be a statement. A sentence such as this, whose truth depends on the value of one or more variables, is called an **open sentence**. The variables in an open sentence (or statement) can represent any type of entity, not just numbers. Here is an open sentence where the variables are functions:

$R(f, g)$: The function f is the derivative of the function g .

This open sentence is true if $f(x) = 2x$ and $g(x) = x^2$. It is false if $f(x) = x^3$ and $g(x) = x^2$, etc. We point out that a sentence such as $R(f, g)$ (that involves variables) can be denoted either as $R(f, g)$ or just R . We use the expression $R(f, g)$ when we want to emphasize that the sentence involves variables.

We will have more to say about open sentences later, but for now let's return to statements.

Statements are everywhere in mathematics. Any result or theorem that has been proved true is a statement. The quadratic formula and the Pythagorean theorem are both statements:

P : The solutions of the equation $ax^2 + bx + c = 0$ are $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$.

Q : If a right triangle has legs of lengths a and b and hypotenuse of length c , then $a^2 + b^2 = c^2$.

Here is a very famous statement, so famous, in fact, that it has a name. It is called **Fermat's last theorem** after Pierre Fermat, a seventeenth-century French mathematician who scribbled it in the margin of a notebook.

R : For all numbers $a, b, c, n \in \mathbb{N}$ with $n > 2$, it is the case that $a^n + b^n \neq c^n$.

Fermat believed this statement was true. He noted that he could prove it was true, except his notebook's margin was too narrow to contain his proof. It is doubtful that he really had a correct proof in mind, for after his death generations of brilliant mathematicians tried unsuccessfully to prove that his statement was true (or false). Finally, in 1993, Andrew Wiles of Princeton University announced that he had devised a proof. Wiles had worked on the problem for over seven years, and his proof runs through hundreds of pages. The moral of this story is that some true statements are not obviously true.

Here is another statement famous enough to be named. It was first posed in the eighteenth century by the German mathematician Christian Goldbach, and thus is called the **Goldbach conjecture**:

S : Every even integer greater than 2 is a sum of two prime numbers.

You must agree that S is either true or false. It appears to be true, because when you examine even numbers that are bigger than 2, they seem to be sums of two primes: $4 = 2 + 2$, $6 = 3 + 3$, $8 = 3 + 5$, $10 = 5 + 5$, $12 = 5 + 7$,

$100 = 17 + 83$ and so on. But that's not to say there isn't some large even number that's not the sum of two primes. If such a number exists, then S is false. The thing is, in the over 260 years since Goldbach first posed this problem, no one has been able to determine whether it's true or false. But since it is clearly either true or false, S is a statement.

Much of this book is about the methods that can be used to prove that S (or any other statement) is true or false. To prove that a statement is true, we start with obvious statements (or other statements that have been proven true) and use logic to deduce more and more complex statements until finally we obtain a statement such as S . Of course some statements are more difficult to prove than others, and S appears to be notoriously difficult; we will concentrate on statements that are easier to prove.

But the point is this: In proving that statements are true, we use logic to help us understand statements and to combine pieces of information to produce new pieces of information. In the next several sections we explore some standard ways that statements can be combined to form new statements, or broken down into simpler statements.

Exercises for Section 3.1

Decide whether or not the following are statements. In the case of a statement, say if it is true or false, if possible.

1. Every real number is an even integer.
 2. Every even integer is a real number.
 3. If x and y are real numbers and $5x = 5y$, then $x = y$.
 4. Sets \mathbb{Z} and \mathbb{N} .
 5. Sets \mathbb{Z} and \mathbb{N} are infinite.
 6. Some sets are finite.
 7. The derivative of any polynomial of degree 5 is a polynomial of degree 6.
 8. $\mathbb{N} \notin \mathcal{P}(\mathbb{N})$.
 9. $\cos(x) = -1$
 10. $(\mathbb{R} \times \mathbb{N}) \cap (\mathbb{N} \times \mathbb{R}) = \mathbb{N} \times \mathbb{N}$
 11. The integer x is a multiple of 7.
 12. If the integer x is a multiple of 7, then it is divisible by 7.
 13. Either x is a multiple of 7, or it is not.
 14. Call me Ishmael.
 15. In the beginning, God created the heaven and the earth.
-

3.2 And, Or, Not

The word “and” can be used to combine two statements to form a new statement. Consider for example the following sentence.

R_1 : The number 2 is even **and** the number 3 is odd.

We recognize this as a true statement, based on our common-sense understanding of the meaning of the word “and.” Notice that R_1 is made up of two simpler statements:

P : The number 2 is even.

Q : The number 3 is odd.

These are joined together by the word “and” to form the more complex statement R_1 . The statement R_1 asserts that P and Q are both true. Since both P and Q are in fact true, the statement R_1 is also true.

Had one or both of P and Q been false, then R_1 would be false. For instance, each of the following statements is false.

R_2 : The number 1 is even **and** the number 3 is odd.

R_3 : The number 2 is even **and** the number 4 is odd.

R_4 : The number 3 is even **and** the number 2 is odd.

From these examples we see that any two statements P and Q can be combined to form a new statement “ P **and** Q .” In the spirit of using letters to denote statements, we now introduce the special symbol \wedge to stand for the word “and.” Thus if P and Q are statements, $P \wedge Q$ stands for the statement “ P **and** Q .” The statement $P \wedge Q$ is true if both P and Q are true; otherwise it is false. This is summarized in the following table, called a **truth table**.

| P | Q | $P \wedge Q$ |
|-----|-----|--------------|
| T | T | T |
| T | F | F |
| F | T | F |
| F | F | F |

In this table, T stands for “True,” and F stands for “False.” (T and F are called **truth values**.) Each line lists one of the four possible combinations or truth values for P and Q , and the column headed by $P \wedge Q$ tells whether the statement $P \wedge Q$ is true or false in each case.

Statements can also be combined using the word “or.” Consider the following four statements.

S_1 : The number 2 is even **or** the number 3 is odd.

S_2 : The number 1 is even **or** the number 3 is odd.

S_3 : The number 2 is even **or** the number 4 is odd.

S_4 : The number 3 is even **or** the number 2 is odd.

In mathematics, the assertion “ P **or** Q ” is always understood to mean that one *or both* of P and Q is true. Thus statements S_1 , S_2 , S_3 are all true, while S_4 is false. The symbol \vee is used to stand for the word “or.” So if P and Q are statements, $P \vee Q$ represents the statement “ P **or** Q .” Here is the truth table.

| P | Q | $P \vee Q$ |
|-----|-----|------------|
| T | T | T |
| T | F | T |
| F | T | T |
| F | F | F |

It is important to be aware that the meaning of “or” expressed in the above table differs from the way it is often used in everyday conversation. For example, suppose a university official makes the following threat:

You pay your tuition **or** you will be withdrawn from school.

You understand that this means that either you pay your tuition *or* you will be withdrawn from school, *but not both*. In mathematics we never use the word “or” in such a sense. For us “or” means exactly what is stated in the table for \vee . Thus $P \vee Q$ being true means *one or both* of P and Q is true. If we ever need to express the fact that exactly one of P and Q is true, we use one of the following constructions:

P or Q , but not both.

Either P or Q .

Exactly one of P or Q .

If the university official were a mathematician, he might have qualified his statement in one of the following ways.

Pay your tuition **or** you will be withdrawn from school, **but not both**.

Either you pay your tuition **or** you will be withdrawn from school.

To conclude this section, we mention another way of obtaining new statements from old ones. Given any statement P , we can form the new statement “**It is not true that P .**” For example, consider the following statement.

The number 2 is even.

This statement is true. Now change it by inserting the words “It is not true that” at the beginning:

It is not true that the number 2 is even.

This new statement is false.

For another example, starting with the false statement “ $2 \in \emptyset$,” we get the true statement “It is not true that $2 \in \emptyset$.”

We use the symbol \sim to stand for the words “It’s not true that,” so $\sim P$ means “**It’s not true that P .**” We often read $\sim P$ simply as “not P .” Unlike \wedge and \vee , which combine two statements, the symbol \sim just alters a single statement. Thus its truth table has just two lines, one for each possible truth value of P .

| | |
|-----|----------|
| P | $\sim P$ |
| T | F |
| F | T |

The statement $\sim P$ is called the **negation** of P . The negation of a specific statement can be expressed in numerous ways. Consider

P : The number 2 is even.

Here are several ways of expressing its negation.

$\sim P$: It’s not true that the number 2 is even.

$\sim P$: It is false that the number 2 is even.

$\sim P$: The number 2 is not even.

In this section we’ve learned how to combine or modify statements with the operations \wedge , \vee and \sim . Of course we can also apply these operations to open sentences or a mixture of open sentences and statements. For example, $(x \text{ is an even integer}) \wedge (3 \text{ is an odd integer})$ is an open sentence that is a combination of an open sentence and a statement.

Think of $P \Rightarrow Q$ as a promise that whenever P is true, Q will be true also. There is only one way this promise can be broken (i.e. be false) and that is if P is true but Q is false. Thus the truth table for the promise $P \Rightarrow Q$ is this:

| P | Q | $P \Rightarrow Q$ |
|-----|-----|-------------------|
| T | T | T |
| T | F | F |
| F | T | T |
| F | F | T |

Perhaps you are bothered by the fact that $P \Rightarrow Q$ is true in the last two lines of this table. Here's an example to convince you that the table is correct. Suppose your professor makes the following promise:

If you pass the final exam, **then** you will pass the course.

(You pass the exam) \Rightarrow (You pass the course).

Under what circumstances did she lie? There are four possible scenarios, depending on whether or not you passed the exam and whether or not you passed the course. These scenarios are tallied below.

| You pass exam | You pass course | (You pass exam) \Rightarrow (You pass course) |
|---------------|-----------------|---|
| T | T | T |
| T | F | F |
| F | T | T |
| F | F | T |

In the first line you pass the exam and you pass the course. Your professor kept her promise, and the T in the third column indicates she told the truth. In the second line, you passed the exam, but your professor gave you a failing grade in the course. In this case she broke her promise, and the F in the third column indicates that what she said was untrue.

Now consider the third row. In this scenario you failed the exam but still passed the course. How could that happen? Maybe your professor felt sorry for you. But that doesn't make her a liar. Her only promise was that if you passed the exam then you would pass the course. She did not say passing the exam was the *only way* to pass the course. Since she didn't lie, then she told the truth, so there is a T in the third column.

Finally look at the fourth row. In that scenario you failed the exam and you failed the course. Your professor did not lie; she did exactly what she said she would do. Hence the T in the third column.

Here is another example that explains why $P \Rightarrow Q$ is true whenever P is false. Consider the following statement.

If this month is September, **then** there is an equinox this month.

An *equinox* is a day for which there are equal hours of darkness and light. There are two equinoxes per year, one in September and the other in March. The above statement is thus unquestionably true, for it asserts correctly that if the current month is September, then an equinox will occur this month. In symbolic form, our statement is

(This month is September) \Rightarrow (There is an equinox this month).

This statement is always true, no matter the month in which we say it. It is true if we say it in September, and it is true if we say it in March, or May, or any other month. But the open sentences P : “*This month is September,*” and Q : “*There is an equinox this month,*” are either true or false, depending on what month it is. Still, $P \Rightarrow Q$ is always true. This is tallied below for six months. Remember that in this example $P \Rightarrow Q$ is always true, and notice how this can be so even when P is false.

| | This month is September | There is an equinox this month | $\left(\begin{array}{c} \text{This month} \\ \text{is September} \end{array} \right) \Rightarrow \left(\begin{array}{c} \text{There is an} \\ \text{equinox} \\ \text{this month} \end{array} \right)$ |
|-------|-------------------------|--------------------------------|--|
| Sept. | <i>T</i> | <i>T</i> | <i>T</i> |
| Oct. | <i>F</i> | <i>F</i> | <i>T</i> |
| Nov. | <i>F</i> | <i>F</i> | <i>T</i> |
| Dec. | <i>F</i> | <i>F</i> | <i>T</i> |
| Jan. | <i>F</i> | <i>F</i> | <i>T</i> |
| Feb. | <i>F</i> | <i>F</i> | <i>T</i> |
| March | <i>F</i> | <i>T</i> | <i>T</i> |

Here is a summary of what we have learned so far about conditional statements.

| <p>The truth table for $P \Rightarrow Q$ is shown on the right. In mathematics, the sentence “<i>If P, then Q</i>” means exactly what the truth table for $P \Rightarrow Q$ expresses. It promises that P being true will make Q true too. It promises nothing about what happens if P is false, so we cannot ever say that $P \Rightarrow Q$ is false when P is false. The only way $P \Rightarrow Q$ can be false is if P is true and Q is false.</p> | <table border="1"> <thead> <tr> <th>P</th> <th>Q</th> <th>$P \Rightarrow Q$</th> </tr> </thead> <tbody> <tr> <td><i>T</i></td> <td><i>T</i></td> <td><i>T</i></td> </tr> <tr> <td><i>T</i></td> <td><i>F</i></td> <td><i>F</i></td> </tr> <tr> <td><i>F</i></td> <td><i>T</i></td> <td><i>T</i></td> </tr> <tr> <td><i>F</i></td> <td><i>F</i></td> <td><i>T</i></td> </tr> </tbody> </table> | P | Q | $P \Rightarrow Q$ | <i>T</i> | <i>T</i> | <i>T</i> | <i>T</i> | <i>F</i> | <i>F</i> | <i>F</i> | <i>T</i> | <i>T</i> | <i>F</i> | <i>F</i> | <i>T</i> |
|---|--|-------------------|-----|-------------------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|
| P | Q | $P \Rightarrow Q$ | | | | | | | | | | | | | | |
| <i>T</i> | <i>T</i> | <i>T</i> | | | | | | | | | | | | | | |
| <i>T</i> | <i>F</i> | <i>F</i> | | | | | | | | | | | | | | |
| <i>F</i> | <i>T</i> | <i>T</i> | | | | | | | | | | | | | | |
| <i>F</i> | <i>F</i> | <i>T</i> | | | | | | | | | | | | | | |

Of course there are other grammatical constructions that mean exactly the same thing as $P \Rightarrow Q$. Here is a summary of the main ones.

| | | |
|---|---|-------------------|
| If P , then Q . | } | $P \Rightarrow Q$ |
| Q if P . | | |
| Q whenever P . | | |
| Q , provided that P . | | |
| Whenever P , then also Q . | | |
| P is a sufficient condition for Q . | | |
| For Q , it is sufficient that P . | | |
| Q is a necessary condition for P . | | |
| For P , it is necessary that Q . | | |
| P only if Q . | | |

These can all be used in the place of (and mean exactly the same thing as) “*If P , then Q .*” You should analyze the meaning of each one and convince yourself that it captures the meaning of $P \Rightarrow Q$. For example, $P \Rightarrow Q$ means the condition of P being true is enough (i.e., sufficient) to make Q true; hence “ *P is a sufficient condition for Q .*”

The wording can be tricky. Often an everyday situation involving a conditional statement can help clarify it. For example, consider your professor’s promise:

(You pass the exam) \Rightarrow (You pass the course)

This means that your passing the exam is a sufficient (though perhaps not necessary) condition for your passing the course. Thus your professor might just as well have phrased her promise in one of the following ways.

Passing the exam is a sufficient condition for passing the course.

For you to pass the course, it is sufficient that you pass the exam.

However, when we want to say “*If P , then Q* ” in everyday conversation, we do not normally express this as “ *Q is a necessary condition for P* ” or “ *P only if Q .*” But such constructions are not uncommon in mathematics. To understand why they make sense, notice that $P \Rightarrow Q$ being true means that it’s impossible that P is true but Q is false, so in order for P to be true it is necessary that Q is true; hence “ *Q is a necessary condition for P .*” And this means that P can only be true if Q is true, i.e., “ *P only if Q .*”

Exercises for Section 3.3

Without changing their meanings, convert each of the following sentences into a sentence having the form “If P , then Q .”

1. A matrix is invertible provided that its determinant is not zero.
2. For a function to be continuous, it is sufficient that it is differentiable.
3. For a function to be integrable, it is necessary that it is continuous.
4. A function is rational if it is a polynomial.
5. An integer is divisible by 8 only if it is divisible by 4.
6. Whenever a surface has only one side, it is non-orientable.
7. A series converges whenever it converges absolutely.
8. A geometric series with ratio r converges if $|r| < 1$.
9. A function is integrable provided the function is continuous.
10. The discriminant is negative only if the quadratic equation has no real solutions.
11. You fail only if you stop writing. (Ray Bradbury)
12. People will generally accept facts as truth only if the facts agree with what they already believe. (Andy Rooney)
13. Whenever people agree with me I feel I must be wrong. (Oscar Wilde)

3.4 Biconditional Statements

It is important to understand that $P \Rightarrow Q$ is not the same as $Q \Rightarrow P$. To see why, suppose that a is some integer and consider the statements

$$\begin{aligned}(a \text{ is a multiple of } 6) &\Rightarrow (a \text{ is divisible by } 2), \\(a \text{ is divisible by } 2) &\Rightarrow (a \text{ is a multiple of } 6).\end{aligned}$$

The first statement asserts that if a is a multiple of 6 then a is divisible by 2. This is clearly true, for any multiple of 6 is even and therefore divisible by 2. The second statement asserts that if a is divisible by 2 then it is a multiple of 6. This is not necessarily true, for $a = 4$ (for instance) is divisible by 2, yet not a multiple of 6. Therefore the meanings of $P \Rightarrow Q$ and $Q \Rightarrow P$ are in general quite different. The conditional statement $Q \Rightarrow P$ is called the **converse** of $P \Rightarrow Q$, so a conditional statement and its converse express entirely different things.

But sometimes, if P and Q are just the right statements, it can happen that $P \Rightarrow Q$ and $Q \Rightarrow P$ are both necessarily true. For example, consider the statements

$$\begin{aligned}(a \text{ is even}) &\Rightarrow (a \text{ is divisible by } 2), \\ (a \text{ is divisible by } 2) &\Rightarrow (a \text{ is even}).\end{aligned}$$

No matter what value a has, both of these statements are true. Since both $P \Rightarrow Q$ and $Q \Rightarrow P$ are true, it follows that $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$ is true.

We now introduce a new symbol \Leftrightarrow to express the meaning of the statement $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$. The expression $P \Leftrightarrow Q$ is understood to have exactly the same meaning as $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$. According to the previous section, $Q \Rightarrow P$ is read as “ P if Q ,” and $P \Rightarrow Q$ can be read as “ P only if Q .” Therefore we pronounce $P \Leftrightarrow Q$ as “ P if and only if Q .” For example, given an integer a , we have the true statement

$$(a \text{ is even}) \Leftrightarrow (a \text{ is divisible by } 2),$$

which we can read as “*Integer a is even if and only if a is divisible by 2.*”

The truth table for \Leftrightarrow is shown below. Notice that in the first and last rows, both $P \Rightarrow Q$ and $Q \Rightarrow P$ are true (according to the truth table for \Rightarrow), so $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$ is true, and hence $P \Leftrightarrow Q$ is true. However, in the middle two rows one of $P \Rightarrow Q$ or $Q \Rightarrow P$ is false, so $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$ is false, making $P \Leftrightarrow Q$ false.

| P | Q | $P \Leftrightarrow Q$ |
|-----|-----|-----------------------|
| T | T | T |
| T | F | F |
| F | T | F |
| F | F | T |

Compare the statement $R : (a \text{ is even}) \Leftrightarrow (a \text{ is divisible by } 2)$ with this truth table. If a is even then the two statements on either side of \Leftrightarrow are true, so according to the table R is true. If a is odd then the two statements on either side of \Leftrightarrow are false, and again according to the table R is true. Thus R is true no matter what value a has. In general, $P \Leftrightarrow Q$ being true means P and Q are both true or both false.

Not surprisingly, there are many ways of saying $P \Leftrightarrow Q$ in English. The following constructions all mean $P \Leftrightarrow Q$:

$$\left. \begin{array}{l} P \text{ if and only if } Q. \\ P \text{ is a necessary and sufficient condition for } Q. \\ \text{For } P \text{ it is necessary and sufficient that } Q. \\ \text{If } P, \text{ then } Q, \text{ and conversely.} \end{array} \right\} P \Leftrightarrow Q$$

The first three of these just combine constructions from the previous section to express that $P \Rightarrow Q$ and $Q \Rightarrow P$. In the last one, the words “...and conversely” mean that in addition to “If P , then Q ” being true, the converse statement “If Q , then P ” is also true.

Exercises for Section 3.4

Without changing their meanings, convert each of the following sentences into a sentence having the form “ P if and only if Q .”

1. For matrix A to be invertible, it is necessary and sufficient that $\det(A) \neq 0$.
2. If a function has a constant derivative then it is linear, and conversely.
3. If $xy = 0$ then $x = 0$ or $y = 0$, and conversely.
4. If $a \in \mathbb{Q}$ then $5a \in \mathbb{Q}$, and if $5a \in \mathbb{Q}$ then $a \in \mathbb{Q}$.
5. For an occurrence to become an adventure, it is necessary and sufficient for one to recount it. (Jean-Paul Sartre)

3.5 Truth Tables for Statements

You should now know the truth tables for \wedge , \vee , \sim , \Rightarrow and \Leftrightarrow . They should be *internalized* as well as memorized. You must understand the symbols thoroughly, for we now combine them to form more complex statements.

For example, suppose we want to convey that one or the other of P and Q is true but they are not both true. No single symbol expresses this, but we could combine them as

$$(P \vee Q) \wedge \sim (P \wedge Q),$$

which literally means:

P or Q is true, and it is not the case that both P and Q are true.

This statement will be true or false depending on the truth values of P and Q . In fact we can make a truth table for the entire statement. Begin as usual by listing the possible true/false combinations of P and Q on four lines. The statement $(P \vee Q) \wedge \sim (P \wedge Q)$ contains the individual statements $(P \vee Q)$ and $(P \wedge Q)$, so we next tally their truth values in the third and fourth columns. The fifth column lists values for $\sim (P \wedge Q)$, and these are just the opposites

of the corresponding entries in the fourth column. Finally, combining the third and fifth columns with \wedge , we get the values for $(P \vee Q) \wedge \sim(P \wedge Q)$ in the sixth column.

| P | Q | $(P \vee Q)$ | $(P \wedge Q)$ | $\sim(P \wedge Q)$ | $(P \vee Q) \wedge \sim(P \wedge Q)$ |
|-----|-----|--------------|----------------|--------------------|--------------------------------------|
| T | T | T | T | F | F |
| T | F | T | F | T | T |
| F | T | T | F | T | T |
| F | F | F | F | T | F |

This truth table tells us that $(P \vee Q) \wedge \sim(P \wedge Q)$ is true precisely when one but not both of P and Q are true, so it has the meaning we intended. (Notice that the middle three columns of our truth table are just “helper columns” and are not necessary parts of the table. In writing truth tables, you may choose to omit such columns if you are confident about your work.)

For another example, consider the following familiar statement concerning two real numbers x and y :

The product xy equals zero if and only if $x = 0$ or $y = 0$.

This can be modeled as $(xy = 0) \Leftrightarrow (x = 0 \vee y = 0)$. If we introduce letters P, Q and R for the statements $xy = 0, x = 0$ and $y = 0$, it becomes $P \Leftrightarrow (Q \vee R)$. Notice that the parentheses are necessary here, for without them we wouldn’t know whether to read the statement as $P \Leftrightarrow (Q \vee R)$ or $(P \Leftrightarrow Q) \vee R$.

Making a truth table for $P \Leftrightarrow (Q \vee R)$ entails a line for each T/F combination for the three statements P, Q and R . The eight possible combinations are tallied in the first three columns of the following table.

| P | Q | R | $Q \vee R$ | $P \Leftrightarrow (Q \vee R)$ |
|-----|-----|-----|------------|--------------------------------|
| T | T | T | T | T |
| T | T | F | T | T |
| T | F | T | T | T |
| T | F | F | F | F |
| F | T | T | T | F |
| F | T | F | T | F |
| F | F | T | T | F |
| F | F | F | F | T |

We fill in the fourth column using our knowledge of the truth table for \vee . Finally the fifth column is filled in by combining the first and fourth columns with our understanding of the truth table for \Leftrightarrow . The resulting table gives the true/false values of $P \Leftrightarrow (Q \vee R)$ for all values of P, Q and R .

Notice that when we plug in various values for x and y , the statements $P : xy = 0$, $Q : x = 0$ and $R : y = 0$ have various truth values, but the statement $P \Leftrightarrow (Q \vee R)$ is always true. For example, if $x = 2$ and $y = 3$, then P, Q and R are all false. This scenario is described in the last row of the table, and there we see that $P \Leftrightarrow (Q \vee R)$ is true. Likewise if $x = 0$ and $y = 7$, then P and Q are true and R is false, a scenario described in the second line of the table, where again $P \Leftrightarrow (Q \vee R)$ is true. There is a simple reason why $P \Leftrightarrow (Q \vee R)$ is true for any values of x and y : It is that $P \Leftrightarrow (Q \vee R)$ represents $(xy = 0) \Leftrightarrow (x = 0 \vee y = 0)$, which is a *true mathematical statement*. It is absolutely impossible for it to be false.

This may make you wonder about the lines in the table where $P \Leftrightarrow (Q \vee R)$ is false. Why are they there? The reason is that $P \Leftrightarrow (Q \vee R)$ can also represent a false statement. To see how, imagine that at the end of the semester your professor makes the following promise.

You pass the class if and only if you get an “A” on the final or you get a “B” on the final.

This promise has the form $P \Leftrightarrow (Q \vee R)$, so its truth values are tabulated in the above table. Imagine it turned out that you got an “A” on the exam but failed the course. Then surely your professor lied to you. In fact, P is false, Q is true and R is false. This scenario is reflected in the sixth line of the table, and indeed $P \Leftrightarrow (Q \vee R)$ is false (i.e., it is a lie).

The moral of this example is that people can lie, but true mathematical statements *never* lie.

We close this section with a word about the use of parentheses. The symbol \sim is analogous to the minus sign in algebra. It negates the expression it precedes. Thus $\sim P \vee Q$ means $(\sim P) \vee Q$, not $\sim (P \vee Q)$. In $\sim (P \vee Q)$, the value of the entire expression $P \vee Q$ is negated.

Exercises for Section 3.5

Write a truth table for the logical statements in problems 1–9:

- | | | |
|--|------------------------------------|--------------------------------------|
| 1. $P \vee (Q \Rightarrow R)$ | 4. $\sim (P \vee Q) \vee (\sim P)$ | 7. $(P \wedge \sim P) \Rightarrow Q$ |
| 2. $(Q \vee R) \Leftrightarrow (R \wedge Q)$ | 5. $(P \wedge \sim P) \vee Q$ | 8. $P \vee (Q \wedge \sim R)$ |
| 3. $\sim (P \Rightarrow Q)$ | 6. $(P \wedge \sim P) \wedge Q$ | 9. $\sim (\sim P \vee \sim Q)$ |
10. Suppose the statement $((P \wedge Q) \vee R) \Rightarrow (R \vee S)$ is false. Find the truth values of P, Q, R and S . (This can be done without a truth table.)
11. Suppose P is false and that the statement $(R \Rightarrow S) \Leftrightarrow (P \wedge Q)$ is true. Find the truth values of R and S . (This can be done without a truth table.)

3.6 Logical Equivalence

In contemplating the truth table for $P \Leftrightarrow Q$, you probably noticed that $P \Leftrightarrow Q$ is true exactly when P and Q are both true or both false. In other words, $P \Leftrightarrow Q$ is true precisely when at least one of the statements $P \wedge Q$ or $\sim P \wedge \sim Q$ is true. This may tempt us to say that $P \Leftrightarrow Q$ means the same thing as $(P \wedge Q) \vee (\sim P \wedge \sim Q)$.

To see if this is really so, we can write truth tables for $P \Leftrightarrow Q$ and $(P \wedge Q) \vee (\sim P \wedge \sim Q)$. In doing this, it is more efficient to put these two statements into the same table, as follows. (This table has helper columns for the intermediate expressions $\sim P$, $\sim Q$, $(P \wedge Q)$ and $(\sim P \wedge \sim Q)$.)

| P | Q | $\sim P$ | $\sim Q$ | $(P \wedge Q)$ | $(\sim P \wedge \sim Q)$ | $(P \wedge Q) \vee (\sim P \wedge \sim Q)$ | $P \Leftrightarrow Q$ |
|-----|-----|----------|----------|----------------|--------------------------|--|-----------------------|
| T | T | F | F | T | F | T | T |
| T | F | F | T | F | F | F | F |
| F | T | T | F | F | F | F | F |
| F | F | T | T | F | T | T | T |

The table shows that $P \Leftrightarrow Q$ and $(P \wedge Q) \vee (\sim P \wedge \sim Q)$ have the same truth value, no matter the values P and Q . It is as if $P \Leftrightarrow Q$ and $(P \wedge Q) \vee (\sim P \wedge \sim Q)$ are algebraic expressions that are equal no matter what is “plugged into” variables P and Q . We express this state of affairs by writing

$$P \Leftrightarrow Q = (P \wedge Q) \vee (\sim P \wedge \sim Q)$$

and saying that $P \Leftrightarrow Q$ and $(P \wedge Q) \vee (\sim P \wedge \sim Q)$ are **logically equivalent**.

In general, two statements are **logically equivalent** if their truth values match up line-for-line in a truth table.

Logical equivalence is important because it can give us different (and potentially useful) ways of looking at the same thing. As an example, the following table shows that $P \Rightarrow Q$ is logically equivalent to $(\sim Q) \Rightarrow (\sim P)$.

| P | Q | $\sim P$ | $\sim Q$ | $(\sim Q) \Rightarrow (\sim P)$ | $P \Rightarrow Q$ |
|-----|-----|----------|----------|---------------------------------|-------------------|
| T | T | F | F | T | T |
| T | F | F | T | F | F |
| F | T | T | F | T | T |
| F | F | T | T | T | T |

The fact that $P \Rightarrow Q = (\sim Q) \Rightarrow (\sim P)$ is useful because so many theorems have the form $P \Rightarrow Q$. As we will see in Chapter 5, proving such a theorem may be easier if we express it in the logically equivalent form $(\sim Q) \Rightarrow (\sim P)$.

There are two pairs of logically equivalent statements that come up again and again throughout this book and beyond. They are prevalent enough to be dignified by a special name: **DeMorgan's laws**.

Fact 3.1 (DeMorgan's Laws)

1. $\sim(P \wedge Q) = (\sim P) \vee (\sim Q)$
2. $\sim(P \vee Q) = (\sim P) \wedge (\sim Q)$

The first of DeMorgan's laws is verified by the following table. You are asked to verify the second in one of the exercises.

| P | Q | $\sim P$ | $\sim Q$ | $P \wedge Q$ | $\sim(P \wedge Q)$ | $(\sim P) \vee (\sim Q)$ |
|-----|-----|----------|----------|--------------|--------------------|--------------------------|
| T | T | F | F | T | F | F |
| T | F | F | T | F | T | T |
| F | T | T | F | F | T | T |
| F | F | T | T | F | T | T |

DeMorgan's laws are actually very natural and intuitive. Consider the statement $\sim(P \wedge Q)$, which we can interpret as meaning that *it is not the case that both P and Q are true*. If it is not the case that both P and Q are true, then at least one of P or Q is false, in which case $(\sim P) \vee (\sim Q)$ is true. Thus $\sim(P \wedge Q)$ means the same thing as $(\sim P) \vee (\sim Q)$.

DeMorgan's laws can be very useful. Suppose we happen to know that some statement having form $\sim(P \vee Q)$ is true. The second of DeMorgan's laws tells us that $(\sim Q) \wedge (\sim P)$ is also true, hence $\sim P$ and $\sim Q$ are both true as well. Being able to quickly obtain such additional pieces of information can be extremely useful.

Here is a summary of some significant logical equivalences. Those that are not immediately obvious can be verified with a truth table.

$$P \Rightarrow Q = (\sim Q) \Rightarrow (\sim P) \qquad \text{Contrapositive law} \qquad (3.1)$$

$$\left. \begin{aligned} \sim(P \wedge Q) &= \sim P \vee \sim Q \\ \sim(P \vee Q) &= \sim P \wedge \sim Q \end{aligned} \right\} \text{DeMorgan's laws} \qquad (3.2)$$

$$\left. \begin{aligned} P \wedge Q &= Q \wedge P \\ P \vee Q &= Q \vee P \end{aligned} \right\} \text{Commutative laws} \qquad (3.3)$$

$$\left. \begin{aligned} P \wedge (Q \vee R) &= (P \wedge Q) \vee (P \wedge R) \\ P \vee (Q \wedge R) &= (P \vee Q) \wedge (P \vee R) \end{aligned} \right\} \text{Distributive laws} \qquad (3.4)$$

$$\left. \begin{aligned} P \wedge (Q \wedge R) &= (P \wedge Q) \wedge R \\ P \vee (Q \vee R) &= (P \vee Q) \vee R \end{aligned} \right\} \text{Associative laws} \qquad (3.5)$$

Notice how the distributive law $P \wedge (Q \vee R) = (P \wedge Q) \vee (P \wedge R)$ has the same structure as the distributive law $p \cdot (q + r) = p \cdot q + p \cdot r$ from algebra. Concerning the associative laws, the fact that $P \wedge (Q \wedge R) = (P \wedge Q) \wedge R$ means that the position of the parentheses is irrelevant, and we can write this as $P \wedge Q \wedge R$ without ambiguity. Similarly, we may drop the parentheses in an expression such as $P \vee (Q \vee R)$.

But parentheses are essential when there is a mix of \wedge and \vee , as in $P \vee (Q \wedge R)$. Indeed, $P \vee (Q \wedge R)$ and $(P \vee Q) \wedge R$ are **not** logically equivalent. (See Exercise 13 for Section 3.6, below.)

Exercises for Section 3.6

A. Use truth tables to show that the following statements are logically equivalent.

- | | |
|---|--|
| 1. $P \wedge (Q \vee R) = (P \wedge Q) \vee (P \wedge R)$ | 5. $\sim(P \vee Q \vee R) = (\sim P) \wedge (\sim Q) \wedge (\sim R)$ |
| 2. $P \vee (Q \wedge R) = (P \vee Q) \wedge (P \vee R)$ | 6. $\sim(P \wedge Q \wedge R) = (\sim P) \vee (\sim Q) \vee (\sim R)$ |
| 3. $P \Rightarrow Q = (\sim P) \vee Q$ | 7. $P \Rightarrow Q = (P \wedge \sim Q) \Rightarrow (Q \wedge \sim Q)$ |
| 4. $\sim(P \vee Q) = (\sim P) \wedge (\sim Q)$ | 8. $\sim P \Leftrightarrow Q = (P \Rightarrow \sim Q) \wedge (\sim Q \Rightarrow P)$ |

B. Decide whether or not the following pairs of statements are logically equivalent.

- | | |
|--|---|
| 9. $P \wedge Q$ and $\sim(\sim P \vee \sim Q)$ | 12. $\sim(P \Rightarrow Q)$ and $P \wedge \sim Q$ |
| 10. $(P \Rightarrow Q) \vee R$ and $\sim((P \wedge \sim Q) \wedge \sim R)$ | 13. $P \vee (Q \wedge R)$ and $(P \vee Q) \wedge R$ |
| 11. $(\sim P) \wedge (P \Rightarrow Q)$ and $\sim(Q \Rightarrow P)$ | 14. $P \wedge (Q \vee \sim Q)$ and $(\sim P) \Rightarrow (Q \wedge \sim Q)$ |

3.7 Solutions for Chapter 3

Section 3.1

Decide whether or not the following are statements. In the case of a statement, say if it is true or false.

1. Every real number is an even integer. (Statement, False)
3. If x and y are real numbers and $5x = 5y$, then $x = y$. (Statement, True)
5. Sets \mathbb{Z} and \mathbb{N} are infinite. (Statement, True)
7. The derivative of any polynomial of degree 5 is a polynomial of degree 6. (Statement, False)
9. $\cos(x) = -1$
This is not a statement. It is an open sentence because whether it's true or false depends on the value of x .
11. The integer x is a multiple of 7.
This is an open sentence, and not a statement.
13. Either x is a multiple of 7, or it is not.
This is a statement, for the sentence is true no matter what x is.
15. In the beginning God created the heaven and the earth.
This is a statement, for it is either definitely true or definitely false. There is some controversy over whether it's true or false, but no one claims that it is neither true nor false.

Section 3.2

Express each statement as one of the forms $P \wedge Q$, $P \vee Q$, or $\sim P$. Be sure to also state exactly what statements P and Q stand for.

1. The number 8 is both even and a power of 2.
 $P \wedge Q$
 P : 8 is even
 Q : 8 is a power of 2
 Note: Do not say " Q : a power of 2," because that is not a statement.
3. $x \neq y$ $\sim (x = y)$ (Also $\sim P$ where $P : x = y$.)
5. $y \geq x$ $\sim (y < x)$ (Also $\sim P$ where $P : y < x$.)
7. The number x equals zero, but the number y does not.
 $P \wedge \sim Q$
 $P : x = 0$
 $Q : y = 0$
9. $x \in A - B$
 $(x \in A) \wedge \sim (x \in B)$

11. $A \in \{X \in \mathcal{P}(\mathbb{N}) : |\overline{X}| < \infty\}$
 $(A \subseteq \mathbb{N}) \wedge (|\overline{A}| < \infty).$
13. Human beings want to be good, but not too good, and not all the time.
 $P \wedge \sim Q \wedge \sim R$
 P : Human beings want to be good.
 Q : Human beings want to be too good.
 R : Human beings want to be good all the time.

Section 3.3

Without changing their meanings, convert each of the following sentences into a sentence having the form “*If P, then Q.*”

1. A matrix is invertible provided that its determinant is not zero.
Answer: If a matrix has a determinant not equal to zero, then it is invertible.
3. For a function to be integrable, it is necessary that it is continuous.
Answer: If a function is integrable, then it is continuous.
5. An integer is divisible by 8 only if it is divisible by 4.
Answer: If an integer is divisible by 8, then it is divisible by 4.
7. A series converges whenever it converges absolutely.
Answer: If a series converges absolutely, then it converges.
9. A function is integrable provided the function is continuous.
Answer: If a function is continuous, then that function is integrable.
11. You fail only if you stop writing.
Answer: If you fail, then you have stopped writing.
13. Whenever people agree with me I feel I must be wrong.
Answer: If people agree with me, then I feel I must be wrong.

Section 3.4

Without changing their meanings, convert each of the following sentences into a sentence having the form “*P if and only if Q.*”

1. For a matrix to be invertible, it is necessary and sufficient that its determinant is not zero.
Answer: A matrix is invertible if and only if its determinant is not zero.
3. If $xy = 0$ then $x = 0$ or $y = 0$, and conversely.
Answer: $xy = 0$ if and only if $x = 0$ or $y = 0$
5. For an occurrence to become an adventure, it is necessary and sufficient for one to recount it.
Answer: An occurrence becomes an adventure if and only if one recounts it.

Section 3.5

1. Write a truth table for $P \vee (Q \Rightarrow R)$

| P | Q | R | $Q \Rightarrow R$ | $P \vee (Q \Rightarrow R)$ |
|-----|-----|-----|-------------------|----------------------------|
| T | T | T | T | T |
| T | T | F | F | T |
| T | F | T | T | T |
| T | F | F | T | T |
| F | T | T | T | T |
| F | T | F | F | F |
| F | F | T | T | T |
| F | F | F | T | T |

5. Write a truth table for $(P \wedge \sim P) \vee Q$

| P | Q | $(P \wedge \sim P)$ | $(P \wedge \sim P) \vee Q$ |
|-----|-----|---------------------|----------------------------|
| T | T | F | T |
| T | F | F | F |
| F | T | F | T |
| F | F | F | F |

3. Write a truth table for $\sim(P \Rightarrow Q)$

| P | Q | $P \Rightarrow Q$ | $\sim(P \Rightarrow Q)$ |
|-----|-----|-------------------|-------------------------|
| T | T | T | F |
| T | F | F | T |
| F | T | T | F |
| F | F | T | F |

7. Write a truth table for $(P \wedge \sim P) \Rightarrow Q$

| P | Q | $(P \wedge \sim P)$ | $(P \wedge \sim P) \Rightarrow Q$ |
|-----|-----|---------------------|-----------------------------------|
| T | T | F | T |
| T | F | F | T |
| F | T | F | T |
| F | F | F | T |

9. Write a truth table for $\sim(\sim P \vee \sim Q)$.

| P | Q | $\sim P$ | $\sim Q$ | $\sim P \vee \sim Q$ | $\sim(\sim P \vee \sim Q)$ |
|-----|-----|----------|----------|----------------------|----------------------------|
| T | T | F | F | F | T |
| T | F | F | T | T | F |
| F | T | T | F | T | F |
| F | F | T | T | T | F |

11. Suppose P is false and that the statement $(R \Rightarrow S) \Leftrightarrow (P \wedge Q)$ is true. Find the truth values of R and S . (This can be done without a truth table.)

Answer: Since P is false, it follows that $(P \wedge Q)$ is false also. But then in order for $(R \Rightarrow S) \Leftrightarrow (P \wedge Q)$ to be true, it must be that $(R \Rightarrow S)$ is false. The only way for $(R \Rightarrow S)$ to be false is if R is true and S is false.

Section 3.6

A. Use truth tables to show that the following statements are logically equivalent.

1. $P \wedge (Q \vee R) = (P \wedge Q) \vee (P \wedge R)$

| <i>P</i> | <i>Q</i> | <i>R</i> | $Q \vee R$ | $P \wedge Q$ | $P \wedge R$ | $P \wedge (Q \vee R)$ | $(P \wedge Q) \vee (P \wedge R)$ |
|----------|----------|----------|------------|--------------|--------------|-----------------------|----------------------------------|
| <i>T</i> | <i>T</i> | <i>T</i> | <i>T</i> | <i>T</i> | <i>T</i> | T | T |
| <i>T</i> | <i>T</i> | <i>F</i> | <i>T</i> | <i>T</i> | <i>F</i> | T | T |
| <i>T</i> | <i>F</i> | <i>T</i> | <i>T</i> | <i>F</i> | <i>T</i> | T | T |
| <i>T</i> | <i>F</i> | <i>F</i> | <i>F</i> | <i>F</i> | <i>F</i> | F | F |
| <i>F</i> | <i>T</i> | <i>T</i> | <i>T</i> | <i>F</i> | <i>F</i> | F | F |
| <i>F</i> | <i>T</i> | <i>F</i> | <i>T</i> | <i>F</i> | <i>F</i> | F | F |
| <i>F</i> | <i>F</i> | <i>T</i> | <i>T</i> | <i>F</i> | <i>F</i> | F | F |
| <i>F</i> | <i>F</i> | <i>F</i> | <i>F</i> | <i>F</i> | <i>F</i> | F | F |

Thus since their columns agree, the two statements are logically equivalent.

3. $P \Rightarrow Q = (\sim P) \vee Q$

| <i>P</i> | <i>Q</i> | $\sim P$ | $(\sim P) \vee Q$ | $P \Rightarrow Q$ |
|----------|----------|----------|-------------------|-------------------|
| <i>T</i> | <i>T</i> | <i>F</i> | T | T |
| <i>T</i> | <i>F</i> | <i>F</i> | F | F |
| <i>F</i> | <i>T</i> | <i>T</i> | T | T |
| <i>F</i> | <i>F</i> | <i>T</i> | T | T |

Thus since their columns agree, the two statements are logically equivalent.

5. $\sim (P \vee Q \vee R) = (\sim P) \wedge (\sim Q) \wedge (\sim R)$

| <i>P</i> | <i>Q</i> | <i>R</i> | $P \vee Q \vee R$ | $\sim P$ | $\sim Q$ | $\sim R$ | $\sim (P \vee Q \vee R)$ | $(\sim P) \wedge (\sim Q) \wedge (\sim R)$ |
|----------|----------|----------|-------------------|----------|----------|----------|--------------------------|--|
| <i>T</i> | <i>T</i> | <i>T</i> | <i>T</i> | <i>F</i> | <i>F</i> | <i>F</i> | F | F |
| <i>T</i> | <i>T</i> | <i>F</i> | <i>T</i> | <i>F</i> | <i>F</i> | <i>T</i> | F | F |
| <i>T</i> | <i>F</i> | <i>T</i> | <i>T</i> | <i>F</i> | <i>T</i> | <i>F</i> | F | F |
| <i>T</i> | <i>F</i> | <i>F</i> | <i>T</i> | <i>F</i> | <i>T</i> | <i>T</i> | F | F |
| <i>F</i> | <i>T</i> | <i>T</i> | <i>T</i> | <i>T</i> | <i>F</i> | <i>F</i> | F | F |
| <i>F</i> | <i>T</i> | <i>F</i> | <i>T</i> | <i>T</i> | <i>F</i> | <i>T</i> | F | F |
| <i>F</i> | <i>F</i> | <i>T</i> | <i>T</i> | <i>T</i> | <i>T</i> | <i>F</i> | F | F |
| <i>F</i> | <i>F</i> | <i>F</i> | <i>F</i> | <i>T</i> | <i>T</i> | <i>T</i> | T | T |

Thus since their columns agree, the two statements are logically equivalent.

7. $P \Rightarrow Q = (P \wedge \sim Q) \Rightarrow (Q \wedge \sim Q)$

| <i>P</i> | <i>Q</i> | $\sim Q$ | $P \wedge \sim Q$ | $Q \wedge \sim Q$ | $(P \wedge \sim Q) \Rightarrow (Q \wedge \sim Q)$ | $P \Rightarrow Q$ |
|----------|----------|----------|-------------------|-------------------|---|-------------------|
| <i>T</i> | <i>T</i> | <i>F</i> | <i>F</i> | <i>F</i> | T | T |
| <i>T</i> | <i>F</i> | <i>T</i> | <i>T</i> | <i>F</i> | F | F |
| <i>F</i> | <i>T</i> | <i>F</i> | <i>F</i> | <i>F</i> | T | T |
| <i>F</i> | <i>F</i> | <i>T</i> | <i>F</i> | <i>F</i> | T | T |

Thus since their columns agree, the two statements are logically equivalent.

B. Decide whether or not the following pairs of statements are logically equivalent.

9. By DeMorgan's law, we have $\sim(\sim P \vee \sim Q) = \sim\sim P \wedge \sim\sim Q = P \wedge Q$. Thus the two statements are logically equivalent.

11. $(\sim P) \wedge (P \Rightarrow Q)$ and $\sim(Q \Rightarrow P)$

| P | Q | $\sim P$ | $P \Rightarrow Q$ | $Q \Rightarrow P$ | $(\sim P) \wedge (P \Rightarrow Q)$ | $\sim(Q \Rightarrow P)$ |
|-----|-----|----------|-------------------|-------------------|-------------------------------------|-------------------------|
| T | T | F | T | T | F | F |
| T | F | F | F | T | F | F |
| F | T | T | T | F | T | T |
| F | F | T | T | T | T | F |

The columns for the two statements do not quite agree, thus the two statements are **not logically equivalent**.

Part II

*Counting, Probability and
Algorithms*

Counting

At its most basic level, counting is a process of pointing to each object in a collection and calling off “one, two, three,…” until the quantity is determined. But this primitive approach to counting is inadequate for applications that demand us to count large quantities in complex situations. We might need to find how many steps an algorithm makes to process a certain input, in order to find whether it can complete its task in a reasonable duration, or to compare it to other algorithms. Or we might need to count the possible outcomes in some game or process in order to determine a winning strategy or compute the probability of success.

This chapter presents fundamental methods of sophisticated counting. Sets play a big role because the things we need to count are often naturally grouped together into a set. The concept of a *list* is also extremely useful.

4.1 Lists

A **list** is an ordered sequence of objects. A list is denoted by an opening parenthesis, followed by the objects, separated by commas, followed by a closing parenthesis. For example (a, b, c, d, e) is a list consisting of the first five letters of the English alphabet, in order. The objects a, b, c, d, e are called the **entries** of the list; the first entry is a , the second is b , and so on. If the entries are rearranged we get a different list, so, for instance,

$$(a, b, c, d, e) \neq (b, a, c, d, e).$$

A list is somewhat like a set, but instead of being a mere collection of objects, the entries of a list have a definite *order*. For sets we have

$$\{a, b, c, d, e\} = \{b, a, c, d, e\},$$

but—as noted above—the analogous equality for lists does not hold.

Unlike sets, lists can have repeated entries. Thus $(5, 3, 5, 4, 3, 3)$ is a perfectly acceptable list, as is (S, O, S) . The **length** of a list is its number of entries. So $(5, 3, 5, 4, 3, 3)$ has length six, and (S, O, S) has length three.

For more examples, $(a, 15)$ is a list of length two. And $(0, (0, 1, 1))$ is a list of length two whose second entry is a list of length three. Two lists are **equal** if they have exactly the same entries in exactly the same positions. Thus equal lists have the same number of entries. If two lists have different lengths, then they can not be equal. Thus $(0, 0, 0, 0, 0, 0) \neq (0, 0, 0, 0, 0)$. Also

$$(g, r, o, c, e, r, y, l, i, s, t) \neq \left(\begin{array}{|l} \text{bread} \\ \text{milk} \\ \text{eggs} \\ \text{bananas} \\ \text{coffee} \end{array} \right)$$

because the list on the left has length eleven but the list on the right has just one entry (a piece of paper with some words on it).

There is one very special list which has no entries at all. It is called the **empty list** and is denoted $()$. It is the only list whose length is zero.

For brevity we often write lists without parentheses, or even commas. For instance, we may write (S, O, S) as SOS if there is no risk of confusion. But be alert that doing this can lead to ambiguity: writing $(9, 10, 11)$ as $9\ 10\ 11$ may cause us to confuse it with $(9, 1, 0, 1, 1)$. Here it's best to retain the parenthesis/comma notation or at least write the list as $9, 10, 11$. A list of symbols written without parentheses and commas is called a **string**.

The process of tossing a coin ten times may be described by a string such as $HHTHTTTHHT$. Tossing it twice could lead to any of the outcomes HH , HT , TH or TT . Tossing it zero times is described by the empty list $()$.

Imagine rolling a dice five times and recording the outcomes. This might be described by the list $(\text{1}, \text{2}, \text{3}, \text{4}, \text{5})$, meaning that you rolled 1 first, then 2 , then 3 , etc. We might abbreviate this list as $\text{1}\text{2}\text{3}\text{4}\text{5}$, or $3, 5, 3, 1, 6$.

Now imagine rolling a pair of dice, one white and one black. A typical outcome might be modeled as a set like $\{\text{1}, \text{2}\}$. Rolling the pair six times might be described with a list of six such outcomes:

$$(\{\text{1}, \text{2}\}, \{\text{1}, \text{3}\}, \{\text{1}, \text{4}\}, \{\text{1}, \text{5}\}, \{\text{1}, \text{6}\}, \{\text{2}, \text{3}\})$$

We might abbreviate this list as $\text{1}\text{2}, \text{1}\text{3}, \text{1}\text{4}, \text{1}\text{5}, \text{1}\text{6}, \text{2}\text{3}$.

We study lists because many real-world phenomena can be described and understood in terms of them. Your phone number can be identified as a list of ten digits. (Order is essential, for rearranging the digits can produce a different phone number.) A *byte* is another important example of a list. A byte is simply a length-eight list of 0's and 1's. The world of information technology revolves around bytes. And the examples above show that multi-step processes (such as rolling a dice twice) can be modeled as lists.

We now explore methods of counting or enumerating lists and processes.

4.2 The Multiplication Principle

Many practical problems involve counting the number of possible lists that satisfy some condition or property.

For example, suppose we make a list of length three having the property that the first entry must be an element of the set $\{a, b, c\}$, the second entry must be in $\{5, 7\}$ and the third entry must be in $\{a, x\}$. Thus $(a, 5, a)$ and $(b, 5, a)$ are two such lists. How many such lists are there all together? To answer this question, imagine making the list by selecting the first entry, then the second and finally the third. This is described in Figure 4.1. The choices for the first list entry are a, b or c , and the left of the diagram branches out in three directions, one for each choice. Once this choice is made there are two choices (5 or 7) for the second entry, and this is described graphically by two branches from each of the three choices for the first entry. This pattern continues for the choice for the third entry, which is either a or x . Thus, in the diagram there are $3 \cdot 2 \cdot 2 = 12$ paths from left to right, each corresponding to a particular choice for each entry in the list. The corresponding lists are tallied at the far-right end of each path. So, to answer our original question, there are 12 possible lists with the stated properties.

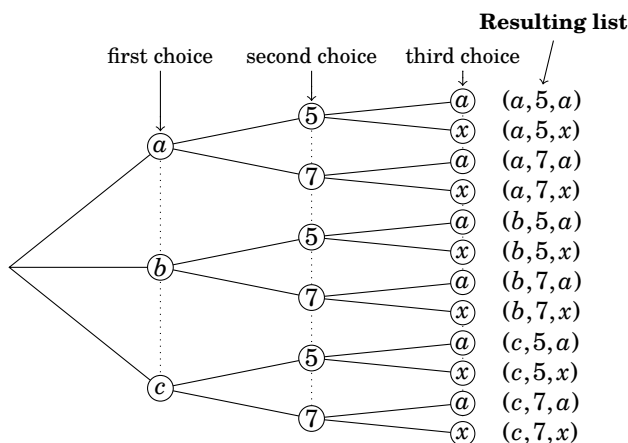


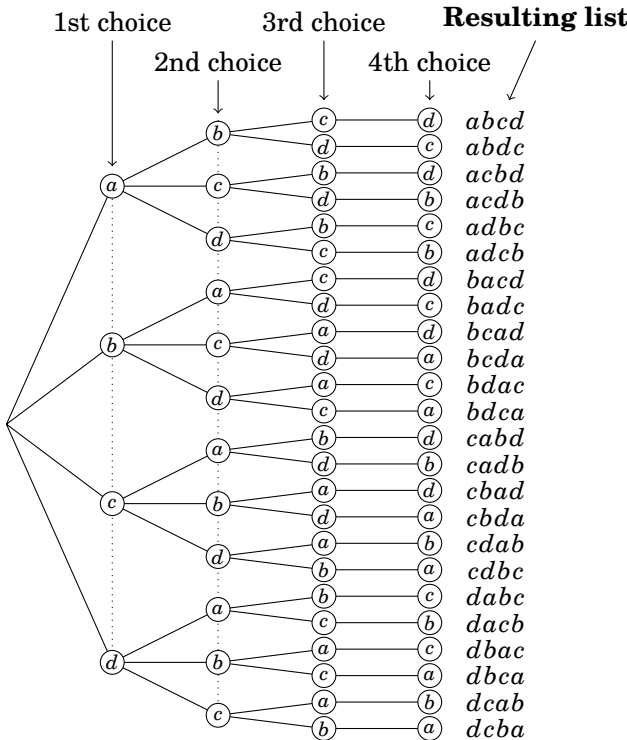
Figure 4.1. Constructing lists of length 3

In the above example there are 3 choices for the first entry, 2 choices for the second entry, and 2 for the third, and the total number of possible lists is the product of choices $3 \cdot 2 \cdot 2 = 12$. This kind of reasoning is an instance of what we will call the *multiplication principle*. We will do one more example before stating this important idea.

Consider making a list of length 4 from the four letters $\{a, b, c, d\}$, where the list is not allowed to have a repeated letter. For example, $abcd$ and $cadb$ are allowed, but $aabc$ and $cacb$ are not allowed. How many such lists are there?

Let's analyze this question with a tree representing the choices we have for each list entry. In making such a list we could start with the first entry: we have 4 choices for it, namely a, b, c or d , and the left side of the tree branches out to each of these choices. But once we've chosen a letter for the first entry, we can't use that letter in the list again, so there are only 3 choices for the second entry. And once we've chosen letters for the first and second entries we can't use these letters in the third entry, so there are just 2 choices for it. By the time we get to the fourth entry we are forced to use whatever letter we have left; there is only 1 choice.

The situation is described fully in the below tree showing how to make all allowable lists by choosing 4 letters for the first entry, 3 for the second entry, 2 for the third entry and 1 for the fourth entry. We see that the total number of lists is the product $4 \cdot 3 \cdot 2 \cdot 1 = 24$.




These trees show that the number of lists constructible by some specified process equals the product of the numbers of choices for each list entry. We summarize this kind of reasoning as an important fact.


Fact 4.1 (Multiplication Principle) Suppose in making a list of length n there are a_1 possible choices for the first entry, a_2 possible choices for the second entry, a_3 possible choices for the third entry, and so on. Then the total number of different lists that can be made this way is the product $a_1 \cdot a_2 \cdot a_3 \cdots a_n$.

In using the multiplication principle you **do not** need to draw a tree with $a_1 \cdot a_2 \cdots a_n$ branches. Just multiply the numbers!

Example 4.1 A standard license plate consists of three letters followed by four numbers. For example, *JRB-4412* and *MMX-8901* are two standard license plates. How many different standard license plates are possible?

Solution: A license plate such as *JRB-4412* corresponds to a length-7 list ($J, R, B, 4, 4, 1, 2$), so we just need to count how many such lists are possible. We use the multiplication principle. There are $a_1 = 26$ possibilities (one for each letter of the alphabet) for the first entry of the list. Similarly, there are $a_2 = 26$ possibilities for the second entry and $a_3 = 26$ possibilities for the third. There are $a_4 = 10$ possibilities for the fourth entry. Likewise $a_5 = a_6 = a_7 = 10$. So there is a total of $a_1 \cdot a_2 \cdot a_3 \cdot a_4 \cdot a_5 \cdot a_6 \cdot a_7 = 26 \cdot 26 \cdot 26 \cdot 10 \cdot 10 \cdot 10 \cdot 10 =$ **175,760,000 possible standard license plates.** 

Example 4.2 In ordering a café latte, you have a choice of whole, skim or soy milk; small, medium or large; and either one or two shots of espresso. How many choices do you have in ordering one drink?

Solution: Your choice is modeled by a list of form (milk, size, shots). There are 3 choices for the first entry, 3 for the second and 2 for the third. By the multiplication principle, the number of choices is $3 \cdot 3 \cdot 2 =$ **18.** 

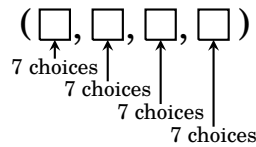
There are two types of list-counting problems. On one hand, there are situations in which list entries can be repeated, as in license plates or telephone numbers. The sequence *CCX-4144* is a perfectly valid license plate in which the symbols *C* and *4* appear more than once. On the other hand, for some lists repeated symbols do not make sense or are not allowed, as in the (milk, size, shots) list from Example 4.2. We say *repetition is allowed* in the first type of list and *repetition is not allowed* in the second kind of list. (We will call a list in which repetition is not allowed a **non-repetitive list**.) The next example illustrates the difference.

Example 4.3 Consider lists of length 4 made with symbols A, B, C, D, E, F, G .

- How many such lists are possible if repetition is allowed?
- How many such lists are possible if repetition is **not** allowed?
- How many are there if repetition is **not** allowed and the list has an E ?
- How many are there if repetition is allowed and the list has an E ?

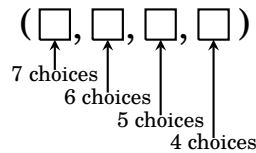
Solutions:

- Imagine the list as containing four boxes that we fill with selections from the letters A, B, C, D, E, F and G , as illustrated below.



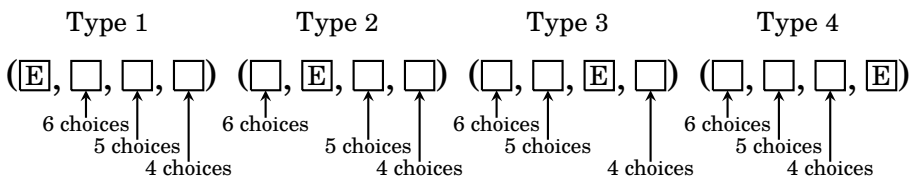
We have 7 choices in filling each box. The multiplication principle says the total number of lists that can be made this way is $7 \cdot 7 \cdot 7 \cdot 7 = 2401$.

- This problem is the same as the previous one except that repetition is not allowed. We have seven choices for the first box, but once it is filled we can no longer use the symbol that was placed in it. Hence there are only six possibilities for the second box. Once the second box has been filled we have used up two of our letters, and there are only five left to choose from in filling the third box. Finally, when the third box is filled we have only four possible letters for the last box.




Thus there are $7 \cdot 6 \cdot 5 \cdot 4 = 840$ lists in which repetition does not occur.

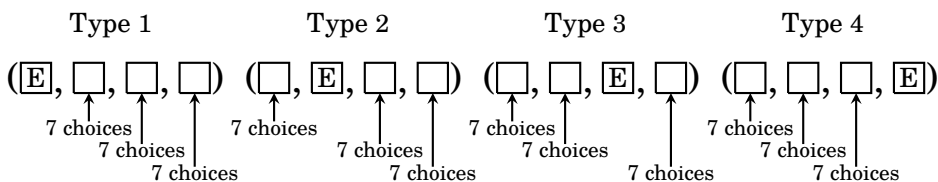
- We are asked to count the length-4 lists in which repetition is not allowed and the symbol E must appear somewhere in the list. Thus E occurs once and only once in each list. Let us divide these lists into four categories depending on whether the E occurs as the first, second, third or fourth entry. These four types of lists are illustrated below.



Consider lists of the first type, in which the E appears in the first entry. We have six remaining choices (A, B, C, D, F or G) for the second entry, five choices for the third entry and four choices for the fourth entry. Hence there are $6 \cdot 5 \cdot 4 = 120$ lists having an E in the first entry. As shown above, there are also $6 \cdot 5 \cdot 4 = 120$ lists having an E in the second, third or fourth entry. So there are $120 + 120 + 120 + 120 = 480$ lists with exactly one E .

- (d) Now we seek the number of length-4 lists where repetition is allowed and the list must contain an E . Here is our strategy: By Part (a) of this exercise there are $7 \cdot 7 \cdot 7 \cdot 7 = 7^4 = 2401$ lists with repetition allowed. Obviously this is not the answer to our current question, for many of these lists contain no E . We will subtract from 2401 the number of lists that **do not** contain an E . In making a list that does not contain an E , we have six choices for each list entry (because we can choose any one of the six letters A, B, C, D, F or G). Thus there are $6 \cdot 6 \cdot 6 \cdot 6 = 6^4 = 1296$ lists without an E . So the answer to our question is that there are $2401 - 1296 = 1105$ lists with repetition allowed that contain at least one E . 

Before moving on from Example 4.3, let's address an important point. Perhaps you wondered if Part (d) could be solved in the same way as Part (c). Let's try doing it that way. We want to count the length-4 lists (repetition allowed) that contain at least one E . The following diagram is adapted from Part (c). The only difference is that there are now seven choices in each slot because we are allowed to repeat any of the seven letters.

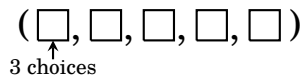


We get a total of $7^3 + 7^3 + 7^3 + 7^3 = 1372$ lists, an answer that is larger than the (correct) value of 1105 from our solution to Part (d) above. It is easy to see what went wrong. The list (E, E, A, B) is of type 1 and type 2, so it got counted *twice*. Similarly (E, E, C, E) is of type 1, 2 and 4, so it got counted three times. In fact, you can find many similar lists that were counted multiple times. In solving counting problems, we must always be careful to avoid this kind of double-counting or triple-counting, or worse.

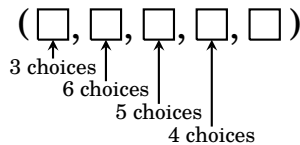
The next section presents two new counting principles that codify the kind of thinking we used in parts (c) and (d) above. Combined with the multiplication principle, they solve complex counting problems in ways that avoid the pitfalls of double counting. But first, one more example of the multiplication principle highlights another pitfall to be alert to.

Example 4.4 A non-repetitive list of length 5 is to be made from the symbols A, B, C, D, E, F, G . The first entry must be either a B, C or D , and the last entry must be a vowel. How many such lists are possible?

Solution: Start by making a list of five boxes. The first box must contain either B, C or D , so there are three choices for it.

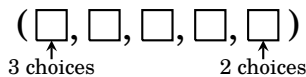


Now there are 6 letters left for the remaining 4 boxes. The knee-jerk action is to fill them in, one at a time, using up an additional letter each time.

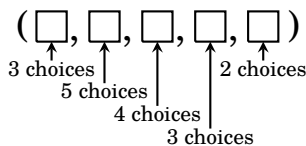



But when we get to the last box, there is a problem. It is supposed to contain a vowel, but for all we know we have already used up one or both vowels in the previous boxes. The multiplication principle breaks down because there is no way to tell how many choices there are for the last box.

The correct way to solve this problem is to fill in the first and last boxes (the ones that have restrictions) first.





Then fill the remaining middle boxes with the 5 remaining letters.



By the multiplication principle, there are $3 \cdot 5 \cdot 4 \cdot 3 \cdot 2 = \mathbf{360}$ lists. 

The new principles to be introduced in the next section are usually used in conjunction with the multiplication principle. So work a few exercises now to test your understanding of it.

Exercises for Section 4.2

1. Consider lists made from the letters T, H, E, O, R, Y , with repetition allowed.
 - (a) How many length-4 lists are there?
 - (b) How many length-4 lists are there that begin with T ?
 - (c) How many length-4 lists are there that do not begin with T ?
 2. Airports are identified with 3-letter codes. For example, Richmond, Virginia has the code RIC , and Memphis, Tennessee has MEM . How many different 3-letter codes are possible?
 3. How many lists of length 3 can be made from the symbols A, B, C, D, E, F if...
 - (a) ... repetition is allowed.
 - (b) ... repetition is not allowed.
 - (c) ... repetition is not allowed and the list must contain the letter A .
 - (d) ... repetition is allowed and the list must contain the letter A .
 4. In ordering coffee you have a choice of regular or decaf; small, medium or large; here or to go. How many different ways are there to order a coffee?
 5. This problem involves 8-digit binary strings such as 10011011 or 00001010 (i.e., 8-digit numbers composed of 0's and 1's).
 - (a) How many such strings are there?
 - (b) How many such strings end in 0?
 - (c) How many such strings have 1's for their second and fourth digits?
 - (d) How many such strings have 1's for their second **or** fourth digits?
 6. You toss a coin, then roll a dice, and then draw a card from a 52-card deck. How many different outcomes are there? How many outcomes are there in which the dice lands on 6? How many outcomes are there in which the dice lands on an odd number? How many outcomes are there in which the dice lands on an odd number and the card is a King?
 7. This problem concerns 4-letter codes made from the letters A, B, C, D, \dots, Z .
 - (a) How many such codes can be made?
 - (b) How many such codes have no two consecutive letters the same?
 8. A coin is tossed 10 times in a row. How many possible sequences of heads and tails are there?
 9. A new car comes in a choice of five colors, three engine sizes and two transmissions. How many different combinations are there?
 10. A dice is tossed four times in a row. There are many possible outcomes, such as  or . How many different outcomes are possible?
-

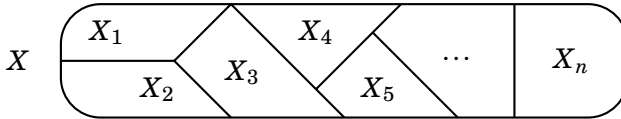
4.3 The Addition and Subtraction Principles

We now discuss two new counting principles, the addition and subtraction principles. Actually, they are not *entirely* new—you’ve used them intuitively for years. Here we give names to these two fundamental thought patterns, and phrase them in the language of sets. Doing this helps us recognize when we are using them, and, more importantly, it helps us see new situations in which they can be used.

The *addition principle* simply asserts that if a set can be broken into pieces, then the size of the set is the sum of the sizes of the pieces.

Fact 4.2 (Addition Principle)

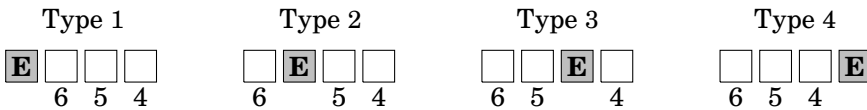
Suppose a finite set X can be decomposed as a union $X = X_1 \cup X_2 \cup \dots \cup X_n$, where $X_i \cap X_j = \emptyset$ whenever $i \neq j$. Then $|X| = |X_1| + |X_2| + \dots + |X_n|$.



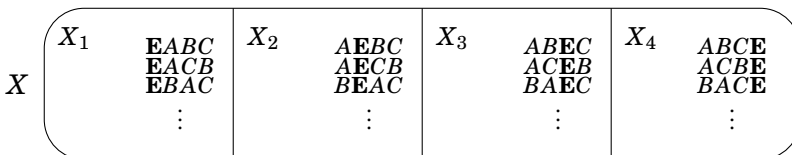
In our first example we will rework an instance where we used the addition principle naturally, without comment: in Part (c) of Example 4.3.

Example 4.5 How many length-4 non-repetitive lists can be made from the symbols A, B, C, D, E, F, G , if the list must contain an E ?


In Example 4.3 (c) our approach was to divide these lists into four types, depending on whether the E is in the first, second, third or fourth position.



Then we used the multiplication principle to count the lists of type 1. There are 6 choices for the second entry, 5 for the third, and 4 for the fourth. This is indicated above, where the number below a box is the number of choices we have for that position. The multiplication principle implies that there are $6 \cdot 5 \cdot 4 = 120$ lists of type 1. Similarly there are $6 \cdot 5 \cdot 4 = 120$ lists of types 2, 3, and 4.



We then used the addition principle intuitively, conceiving of the lists to be counted as the elements of a set X , broken up into parts X_1, X_2, X_3 and X_4 , which are the lists of types 1, 2, 3 and 4, respectively.

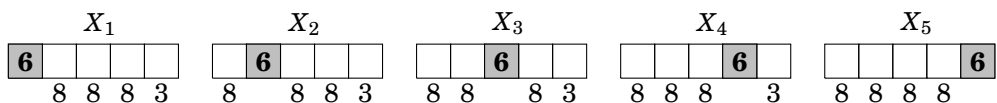
The addition principle says that the number of lists that contain an E is $|X| = |X_1| + |X_2| + |X_3| + |X_4| = 120 + 120 + 120 + 120 = \mathbf{480}$. 

We use the addition principle when we need to count the things in some set X . If we can find a way to break X up as $X = X_1 \cup X_2 \cup \dots \cup X_n$, where each X_i is easier to count than X , then the addition principle gives an answer of $|X| = |X_1| + |X_2| + |X_3| + \dots + |X_n|$.

But for this to work the intersection of any two pieces X_i must be \emptyset , as stated in Fact 4.2. For instance, if X_1 and X_2 shared an element, then that element would be counted once in $|X_1|$ and again in $|X_2|$, and we'd get $|X| < |X_1| + |X_2| + \dots + |X_n|$. (This is precisely the double counting issue mentioned after Example 4.3.)


Example 4.6 How many **even** 5-digit numbers are there for which no digit is 0, and the digit 6 appears exactly once? For instance, 55634 and 16118 are such numbers, but not 63304 (has a 0), nor 63364 (too many 6's), nor 55637 (not even).

Solution: Let X be the set of all such numbers. The answer will be $|X|$, so our task is to find $|X|$. Put $X = X_1 \cup X_2 \cup X_3 \cup X_4 \cup X_5$, where X_i is the set of those numbers in X whose i th digit is 6, as diagramed below. Note $X_i \cap X_j = \emptyset$ whenever $i \neq j$ because the numbers in X_i have their 6 in a different position than the numbers in X_j . Our plan is to use the multiplication principle to compute each $|X_i|$, and follow this with the addition principle.

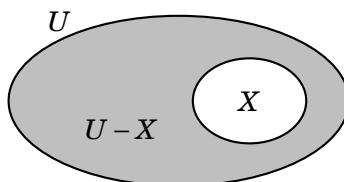


The first digit of any number in X_1 is 6, and the three digits following it can be any of the ten digits except 0 (not allowed) or 6 (already appears). Thus there are eight choices for each of three digits following the first 6. But because any number in X_1 is even, its final digit must be one of 2, 4 or 8, so there are just three choices for this final digit. By the multiplication principle, $|X_1| = 8 \cdot 8 \cdot 8 \cdot 3 = 1536$. Likewise $|X_2| = |X_3| = |X_4| = 8 \cdot 8 \cdot 8 \cdot 3 = 1536$.

But X_5 is slightly different because we do not choose the final digit, which is already 6. The multiplication principle gives $|X_5| = 8 \cdot 8 \cdot 8 \cdot 8 = 4096$.

The addition principle gives our final answer. The number of even 5-digit numbers with no 0's and one 6 is $|X| = |X_1| + |X_2| + |X_3| + |X_4| + |X_5| = 1536 + 1536 + 1536 + 1536 + 4096 = \mathbf{10,240}$. 

Now we introduce our next counting method, the *subtraction principle*. To set it up, imagine that a set X is a subset of a universal set U , as shown on the right. The complement $\bar{X} = U - X$ is shaded.



Suppose we wanted to count the things in this shaded region. Surely this is the number of things in U minus the number of things in X , which is to say $|U - X| = |U| - |X|$. That is the subtraction principle.

Fact 4.3 (Subtraction Principle)

If X is a subset of a finite set U , then $|\bar{X}| = |U| - |X|$.

In other words, if $X \subseteq U$ then $|U - X| = |U| - |X|$.


The subtraction principle is used in situations where it is easier to count the things in some set U that we wish to *exclude* from consideration than it is to count those things that *are* included. We have seen this kind of thinking before. We quietly and naturally used it in part (d) of Example 4.3. For convenience we repeat that example now, casting it into the language of the subtraction principle.

Example 4.7 How many length-4 lists can be made from the symbols A, B, C, D, E, F, G if the list has at least one E , and repetition is allowed?

Solution: Such a list might contain one, two, three or four E 's, which could occur in various positions. This is a fairly complex situation.

But it is very easy to count the set U of all lists of length 4 made from A, B, C, D, E, F, G if we don't care whether or not the lists have any E 's. The multiplication principle says $|U| = 7 \cdot 7 \cdot 7 \cdot 7 = 2401$.

It is equally easy to count the set X of those lists that *contain no* E 's. The multiplication principle says $|X| = 6 \cdot 6 \cdot 6 \cdot 6 = 1296$.

We are interested in those lists that have at least one E , and this is the set $U - X$. By the subtraction principle, the answer to our question is $|U - X| = |U| - |X| = 2401 - 1296 = \mathbf{1105}$. 

As we continue with counting we will have many opportunities to use the multiplication, addition and subtraction principles. Usually these will arise in the context of other counting principles that we have yet to explore. It is thus important that you solidify the current ideas now, by working some exercises before moving on.

Exercises for Section 4.3

1. Five cards are dealt off of a standard 52-card deck and lined up in a row. How many such lineups are there that have at least one red card? How many such lineups are there in which the cards are either all black or all hearts?
 2. Five cards are dealt off of a standard 52-card deck and lined up in a row. How many such lineups are there in which all 5 cards are of the same suit?
 3. Five cards are dealt off of a standard 52-card deck and lined up in a row. How many such lineups are there in which all 5 cards are of the same color (i.e., all black or all red)?
 4. Five cards are dealt off of a standard 52-card deck and lined up in a row. How many such lineups are there in which exactly one of the 5 cards is a queen?
 5. How many integers between 1 and 9999 have no repeated digits? How many have at least one repeated digit?
 6. Consider lists made from the symbols A, B, C, D, E , with repetition allowed.
 - (a) How many such length-5 lists have at least one letter repeated?
 - (b) How many such length-6 lists have at least one letter repeated?
 7. A password on a certain site must be five characters long, made from letters of the alphabet, and have at least one upper case letter. How many different passwords are there? What if there must be a mix of upper and lower case?
 8. This problem concerns lists made from the letters $A, B, C, D, E, F, G, H, I, J$.
 - (a) How many length-5 lists can be made from these letters if repetition is not allowed and the list must begin with a vowel?
 - (b) How many length-5 lists can be made from these letters if repetition is not allowed and the list must begin and end with a vowel?
 - (c) How many length-5 lists can be made from these letters if repetition is not allowed and the list must contain exactly one A ?
 9. Consider lists of length 6 made from the letters A, B, C, D, E, F, G, H . How many such lists are possible if repetition is not allowed and the list contains two consecutive vowels?
 10. Consider the lists of length six made with the symbols P, R, O, F, S , where repetition is allowed. (For example, the following is such a list: (P, R, O, O, F, S) .) How many such lists can be made if the list must end in an S and the symbol O is used more than once?
 11. How many integers between 1 and 1000 are divisible by 5? How many are not divisible by 5?
 12. Six math books, four physics books and three chemistry books are arranged on a shelf. How many arrangements are possible if all books of the same subject are grouped together?
-

4.4 Factorials and Permutations

In working examples from the previous two sections you may have noticed that we often need to count the number of non-repetitive lists of length n that are made from n symbols. This kind of problem occurs so often that a special idea, called a *factorial*, is used to handle it.

The table below motivates this. The first column lists successive integer values n , from 0 onward. The second contains a set $\{a, b, \dots\}$ of n symbols. The third column shows all the possible non-repetitive lists of length n that can be made from these symbols. Finally, the last column tallies up how many lists there are of that type. When $n = 0$ there is only one list of length 0 that can be made from 0 symbols, namely the empty list $()$. Thus the value 1 is entered in the last column of that row.

| n | Symbols | Non-repetitive lists of length n made from the symbols | $n!$ |
|----------|------------------|---|----------|
| 0 | $\{\}$ | $()$ | 1 |
| 1 | $\{a\}$ | a | 1 |
| 2 | $\{a, b\}$ | ab, ba | 2 |
| 3 | $\{a, b, c\}$ | $abc, acb, bac, bca, cab, cba$ | 6 |
| 4 | $\{a, b, c, d\}$ | $abcd, acbd, bacd, bcad, cabd, cbad,$ $abdc, acdb, badc, bcda, cadb, cbda,$ $adbc, adcb, bdac, bdca, cdab, cdba,$ $dabc, dacb, dbac, dbca, dcab, dcba$ | 24 |
| \vdots | \vdots | \vdots | \vdots |

For $n > 0$, the number that appears in the last column can be computed using the multiplication principle. The number of non-repetitive lists of length n that can be made from n symbols is $n(n-1)(n-2)\cdots 3\cdot 2\cdot 1$. Thus, for instance, the number in the last column of the row for $n = 4$ is $4\cdot 3\cdot 2\cdot 1 = 24$.

The number that appears in the last column of Row n is called the **factorial** of n . It is denoted with the special symbol $n!$, which we pronounce as "*n factorial*." Here is the definition:

Definition 4.1 If n is a non-negative integer, then $n!$ is the number of lists of length n that can be made from n symbols, without repetition. Thus $0! = 1$ and $1! = 1$. If $n > 1$, then $n! = n(n-1)(n-2)\cdots 3\cdot 2\cdot 1$.

It follows that

$$\begin{aligned}
 0! &= 1 \\
 1! &= 1 \\
 2! &= 2 \cdot 1 = 2 \\
 3! &= 3 \cdot 2 \cdot 1 = 6 \\
 4! &= 4 \cdot 3 \cdot 2 \cdot 1 = 24 \\
 5! &= 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120 \\
 6! &= 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 720, \quad \text{and so on.}
 \end{aligned}$$

Students are often tempted to say $0! = 0$, but this is wrong. The correct value is $0! = 1$, as the above definition and table show. Here is another way to see that $0!$ must equal 1: Notice that $5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 5 \cdot (4 \cdot 3 \cdot 2 \cdot 1) = 5 \cdot 4!$. Also $4! = 4 \cdot 3 \cdot 2 \cdot 1 = 4 \cdot (3 \cdot 2 \cdot 1) = 4 \cdot 3!$. Generalizing this, we get a formula.


$$n! = n \cdot (n - 1)! \quad (4.1)$$

Plugging in $n = 1$ gives $1! = 1 \cdot (1 - 1)! = 1 \cdot 0!$, that is, $1! = 1 \cdot 0!$. If we mistakenly thought $0!$ were 0, this would give the incorrect result $1! = 0$.

Example 4.8 This problem involves making lists of length seven from the letters a, b, c, d, e, f and g .

- How many such lists are there if repetition is not allowed?
- How many such lists are there if repetition is not allowed *and* the first two entries must be vowels?
- How many such lists are there in which repetition is allowed, and the list must contain at least one repeated letter?

To answer the first question, note that there are seven letters, so the number of lists is $7! = \mathbf{5040}$. To answer the second question, notice that the set $\{a, b, c, d, e, f, g\}$ contains two vowels and five consonants. Thus in making the list the first two entries must be filled by vowels and the final five must be filled with consonants. By the multiplication principle, the number of such lists is $2 \cdot 1 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 2!5! = \mathbf{240}$.

To answer part (c) we use the subtraction principle. Let U be the set of all lists made from a, b, c, d, e, f, g , with repetition allowed. The multiplication principle gives $|U| = 7 \cdot 7 \cdot 7 \cdot 7 \cdot 7 \cdot 7 \cdot 7 = 7^7 = 823,543$. Notice that U includes lists that are non-repetitive, like (a, g, f, b, d, c, e) , as well as lists that have some repetition, like (f, g, b, g, a, a, a) . We want to find the number of lists that have at least one repeated letter, so we will subtract away from U all those lists that have no repetition. Let $X \subseteq U$ be those lists that have no repetition, so $|X| = 7!$. Thus the answer to our question is $|U - X| = |U| - |X| = 7^7 - 7! = 823,543 - 5040 = \mathbf{818,503}$. 

In part (a) of Example 4.8 we counted the number of non-repetitive lists made from all seven of the symbols in the set $X = \{a, b, c, d, e, f, g\}$, and there were $7! = 5040$ such lists. Any such list, such as $bcedagf$, $gfedcba$ or $abcdefg$ is simply an arrangement of the elements of X in a row. There is a name for such an arrangement. It is called a *permutation* of X .

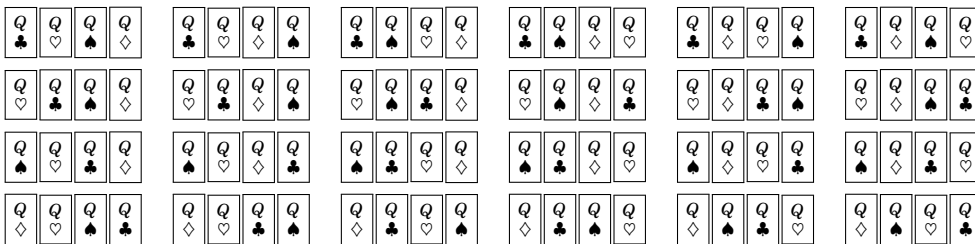
A **permutation** of a set is an arrangement of all of the set's elements in a row, that is, a list without repetition that uses every element of the set. For example, the permutations of the set $X = \{1, 2, 3\}$ are the six lists

123, 132, 213, 231, 312, 321.

That we get six different permutations of X is predicted by Definition 4.1, which says there are $3! = 3 \cdot 2 \cdot 1 = 6$ non-repetitive lists that can be made from the three symbols in X .

Think of the numbers 1, 2 and 3 as representing three books. The above shows that there are six ways to arrange them on a shelf.

From a deck of cards you take the four queens and lay them in a row. By the multiplication principle there are $4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$ ways to do this, that is, there are 24 permutations of the set of four Queen cards.



In general, a set with n elements will have $n!$ different permutations. Above, the set $\{1, 2, 3\}$ has $3! = 6$ permutations, while $\left\{ \begin{matrix} Q \\ \diamond \end{matrix}, \begin{matrix} Q \\ \heartsuit \end{matrix}, \begin{matrix} Q \\ \spadesuit \end{matrix}, \begin{matrix} Q \\ \clubsuit \end{matrix} \right\}$ has $4! = 24$ permutations. The set $\{a, b, c, d, e, f, g\}$ has $7! = 5040$ permutations, though there's not much point in listing them all out. The important thing is that the factorial counts the number of permutations.

In saying a permutation of a set is an arrangement of its elements in a *row*, we are speaking informally because sometimes the elements are not literally in a row. Imagine a classroom of 20 desks, in four rows of five desks each. Let X be a class (set) of 20 students. If the students walk in and seat themselves, one per desk, we can regard this as a permutation of the 20 students because we can number the desks $1, 2, 3, \dots, 20$ and in this sense the students have arranged themselves in a list of length 20. There are $20! = 2,432,902,008,176,640,000$ permutations of the students.

Now we discuss a variation of the idea of a permutation of a set X . Imagine taking some number $k \leq |X|$ of elements from the set X and then arranging *them* in a row. The result is what we call a k -permutation of X . A **permutation** of X is a non-repetitive list made from all elements of X . A **k -permutation** of X is a non-repetitive list made from k elements of X .

For example, take $X = \{a, b, c, d\}$. The 1-permutations of X are the lists we could make with just one element from X . There are only 4 such lists:

$$a \quad b \quad c \quad d.$$

The 2-permutations of X are the non-repetitive lists that we could make from two elements of X . There are 12 of them:

$$ab \quad ac \quad ad \quad ba \quad bc \quad bd \quad ca \quad cb \quad cd \quad da \quad db \quad dc.$$

Even before writing them all down, we'd know there are 12 of them because in making a non-repetitive length-2 list from X we have 4 choices for the first element, then 3 choices for the second, so by the multiplication principle the total number of 2-permutations of X is $4 \cdot 3 = 12$.

Now let's count the number of 3-permutations of X . They are the length-3 non-repetitive lists made from elements of X . The multiplication principle says there will be $4 \cdot 3 \cdot 2 = 24$ of them. Here they are:

$$\begin{array}{cccccc} abc & acb & bac & bca & cab & cba \\ abd & adb & bad & bda & dab & dba \\ acd & adc & cad & cda & dac & dca \\ bcd & bdc & cbd & cdb & dbc & dcb \end{array}$$

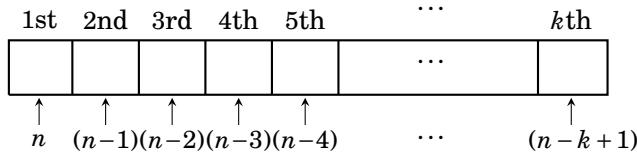
The 4-permutations of X are the non-repetitive lists made from all 4 elements of X . These are simply the $4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$ permutations of X .

Let's go back and think about the *0-permutations* of X . They are the non-repetitive lists of length 0 made from the elements of X . Of course there is only one such list, namely the empty list $()$.

Now we are going to introduce some notation. The expression $P(n, k)$ denotes the number of k -permutations of an n -element set. By the examples on this page we have $P(4, 0) = 1$, $P(4, 1) = 4$, $P(4, 2) = 12$, $P(4, 3) = 24$, and $P(4, 4) = 24$.

What about, say, $P(4, 5)$? This is the number of 5-permutations of a 4-element set, that is, the number of non-repetitive length-5 lists that can be made from 4 symbols. There is no such list, so $P(4, 5) = 0$.

If $n > 0$, then $P(n, k)$ can be computed with the multiplication principle. In making a non-repetitive length- k list from n symbols we have n choices for the 1st entry, $n - 1$ for the 2nd, $n - 2$ for the 3rd, and $n - 3$ for the 4th.



Notice that the number of choices for the i th position is $n - i + 1$. For example, the 5th position has $n - 5 + 1 = n - 4$ choices. Continuing in this pattern, the last (k th) entry has $n - k + 1$ choices. Therefore

$$P(n, k) = n(n - 1)(n - 2) \cdots (n - k + 1). \tag{4.2}$$

All together there are k factors in this product, so to compute $P(n, k)$ just perform $n(n - 1)(n - 2)(n - 3) \cdots$ until you've multiplied k numbers. Examples:

$$\begin{aligned} P(10, 1) &= 10 = 10 \\ P(10, 2) &= 10 \cdot 9 = 90 \\ P(10, 3) &= 10 \cdot 9 \cdot 8 = 720 \\ P(10, 4) &= 10 \cdot 9 \cdot 8 \cdot 7 = 5040 \\ &\vdots \quad \quad \quad \vdots \\ P(10, 10) &= 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 3,628,800 \\ P(10, 11) &= 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \cdot 0 = 0. \end{aligned}$$

Note $P(10, 11) = 0$, as the 11th factor in the product is 0. This makes sense because $P(10, 11)$ is the number of non-repetitive length-11 lists made from just 10 symbols. There are no such lists, so $P(10, 11) = 0$ is right. In fact you can check that Equation (4.2) gives $P(n, k) = 0$ whenever $k > n$.

Also notice above that $P(10, 10) = 10!$. In general $P(n, n) = n!$.

We now derive another formula for $P(n, k)$, one that works for $0 \leq k \leq n$. Using Equation (4.2) with cancellation and the definition of a factorial,

$$\begin{aligned} P(n, k) &= n(n - 1)(n - 2) \cdots (n - k + 1) \\ &= \frac{n(n - 1)(n - 2) \cdots (n - k + 1)(n - k)(n - k - 1) \cdots 3 \cdot 2 \cdot 1}{(n - k)(n - k - 1) \cdots 3 \cdot 2 \cdot 1} = \frac{n!}{(n - k)!}. \end{aligned}$$

To illustrate, let's find $P(8, 5)$ in two ways. Equation (4.2) says $P(8, 5) = 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 = 6720$. By the above formula, $P(8, 5) = \frac{8!}{(8 - 5)!} = \frac{8!}{3!} = \frac{40,320}{6} = 6720$.

We summarize these ideas in the following definition and fact.

Fact 4.4 A **k -permutation** of an n -element set is a non-repetitive length- k list made from elements of the set. Informally we think of a k -permutation as an arrangement of k of the set's elements in a row.


The number of k -permutations of an n -element set is denoted $P(n, k)$, and

$$P(n, k) = n(n-1)(n-2)\cdots(n-k+1).$$

If $0 \leq k \leq n$, then $P(n, k) = n(n-1)(n-2)\cdots(n-k+1) = \frac{n!}{(n-k)!}$.

Notice that $P(n, 0) = \frac{n!}{(n-0)!} = \frac{n!}{n!} = 1$, which makes sense because only one list of length 0 can be made from n symbols, namely the empty list. Also $P(0, 0) = \frac{0!}{(0-0)!} = \frac{0!}{0!} = \frac{1}{1} = 1$, which is to be expected because there is only one list of length 0 that can be made with 0 symbols, again the empty list.


Example 4.9 Ten contestants run a marathon. All finish, and there are no ties. How many different possible rankings are there for first-, second- and third-place?

Solution: Call the contestants $A, B, C, D, E, F, G, H, I$ and J . A ranking of winners can be regarded as a 3-permutation of the set of 10 contestants. For example, ECH means E in first-place, C in second-place and H in third. Thus there are $P(10, 3) = 10 \cdot 9 \cdot 8 = 720$ possible rankings. 

Example 4.10 You deal five cards off of a standard 52-card deck, and line them up in a row. How many such lineups are there that either consist of all red cards, or all clubs?

Solution: There are 26 red cards. The number of ways to line up five of them is $P(26, 5) = 26 \cdot 25 \cdot 24 \cdot 23 \cdot 22 = 7,893,600$.

There are 13 club cards (which are black). The number of ways to line up five of them is $P(13, 5) = 13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 = 154,440$.

By the addition principle, the answer to our question is that there are $P(26, 5) + P(13, 5) = 8,048,040$ lineups that are either all red cards, or all club cards. 

Notice that we do not need to use the notation $P(n, k)$ to solve the problems on this page. Straightforward applications of the multiplication and addition principles would suffice. However, the $P(n, k)$ notation often proves to be a convenient shorthand.

Exercises for Section 4.4

1. What is the smallest n for which $n!$ has more than 10 digits?
 2. For which values of n does $n!$ have n or fewer digits?
 3. How many 5-digit positive integers are there in which there are no repeated digits and all digits are odd?
 4. Using only pencil and paper, find the value of $\frac{100!}{95!}$.
 5. Using only pencil and paper, find the value of $\frac{120!}{118!}$.
 6. There are two 0's at the end of $10! = 3,628,800$. Using only pencil and paper, determine how many 0's are at the end of the number $100!$.
 7. Find how many 9-digit numbers can be made from the digits 1, 2, 3, 4, 5, 6, 7, 8, 9 if repetition is not allowed and all the odd digits occur first (on the left) followed by all the even digits (i.e., as in 137598264, but not 123456789).
 8. Compute how many 7-digit numbers can be made from the digits 1, 2, 3, 4, 5, 6, 7 if there is no repetition and the odd digits must appear in an unbroken sequence. (Examples: 3571264 or 2413576 or 2467531, etc., but **not** 7234615.)
 9. How many permutations of the letters A, B, C, D, E, F, G are there in which the three letters ABC appear consecutively, in alphabetical order?
 10. How many permutations of the digits 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 are there in which the digits alternate even and odd? (For example, 2183470965.)
 11. You deal 7 cards off of a 52-card deck and line them up in a row. How many possible lineups are there in which not all cards are red?
 12. You deal 7 cards off of a 52-card deck and line them up in a row. How many possible lineups are there in which no card is a club?
 13. How many lists of length six (with no repetition) can be made from the 26 letters of the English alphabet?
 14. Five of ten books are arranged on a shelf. In how many ways can this be done?
 15. In a club of 15 people, we need to choose a president, vice-president, secretary, and treasurer. In how many ways can this be done?
 16. How many 4-permutations are there of the set $\{A, B, C, D, E, F\}$ if whenever A appears in the permutation, it is followed by E ?
 17. Three people in a group of ten line up at a ticket counter to buy tickets. How many lineups are possible?
 18. There is a very interesting function $\Gamma : [0, \infty) \rightarrow \mathbb{R}$ called the **gamma function**. It is defined as $\Gamma(x) = \int_0^\infty t^{x-1} e^{-t} dt$. It has the remarkable property that if $x \in \mathbb{N}$, then $\Gamma(x) = (x-1)!$. Check that this is true for $x = 1, 2, 3, 4$.
Notice that this function provides a way of extending factorials to numbers other than integers. Since $\Gamma(n) = (n-1)!$ for all $n \in \mathbb{N}$, we have the formula $n! = \Gamma(n+1)$. But Γ can be evaluated at any number in $[0, \infty)$, not just at integers, so we have a formula for $n!$ for any real number $n \in [0, \infty)$. Extra credit: Compute $\pi!$.
-

4.5 Counting Subsets

The previous section dealt with counting lists made by selecting k entries from a set of n elements. We turn now to a related question: How many *subsets* can be made by selecting k elements from a set with n elements?

To see the difference between these two problems, take $A = \{a, b, c, d, e\}$. Consider the non-repetitive lists made from selecting two elements from A . Fact 4.4 says there are $P(5, 2) = 5 \cdot 4 = 20$ such lists, namely

- $(a, b), (a, c), (a, d), (a, e), (b, c), (b, d), (b, e), (c, d), (c, e), (d, e),$
 $(b, a), (c, a), (d, a), (e, a), (c, b), (d, b), (e, b), (d, c), (e, c), (e, d).$

But there are only ten 2-element *subsets* of A . They are

- $\{a, b\}, \{a, c\}, \{a, d\}, \{a, e\}, \{b, c\}, \{b, d\}, \{b, e\}, \{c, d\}, \{c, e\}, \{d, e\}.$

The reason that there are more lists than subsets is that changing the order of the entries of a list produces a different list, but changing the order of the elements of a set does not change the set. Using elements $a, b \in A$, we can make two lists (a, b) and (b, a) , but only one subset $\{a, b\}$.

This section is concerned with counting subsets, not lists. As noted above, the basic question is this: How many subsets can be made by choosing k elements from an n -element set? We begin with some notation that gives a name to the answer to this question.

Definition 4.2 If n and k are integers, then $\binom{n}{k}$ denotes the number of subsets that can be made by choosing k elements from an n -element set. We read $\binom{n}{k}$ as “ n choose k .” (Some textbooks write $C(n, k)$ instead of $\binom{n}{k}$.)

This is illustrated in the following table that tallies the k -element subsets of the 4-element set $A = \{a, b, c, d\}$, for various values of k .

| k | k -element subsets of $A = \{a, b, c, d\}$ | $\binom{4}{k}$ |
|-----|--|---------------------|
| -1 | | $\binom{4}{-1} = 0$ |
| 0 | \emptyset | $\binom{4}{0} = 1$ |
| 1 | $\{a\}, \{b\}, \{c\}, \{d\}$ | $\binom{4}{1} = 4$ |
| 2 | $\{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}, \{c, d\}$ | $\binom{4}{2} = 6$ |
| 3 | $\{a, b, c\}, \{a, b, d\}, \{a, c, d\}, \{b, c, d\}$ | $\binom{4}{3} = 4$ |
| 4 | $\{a, b, c, d\}$ | $\binom{4}{4} = 1$ |
| 5 | | $\binom{4}{5} = 0$ |

The values of k appear in the far-left column of the table. To the right of each k are all of the subsets (if any) of A of size k . For example, when $k = 1$, set A has four subsets of size k , namely $\{a\}$, $\{b\}$, $\{c\}$ and $\{d\}$. Therefore $\binom{4}{1} = 4$. When $k = 2$ there are six subsets of size k so $\binom{4}{2} = 6$.

When $k = 0$, there is only one subset of A that has cardinality k , namely the empty set, \emptyset . Therefore $\binom{4}{0} = 1$.

Notice that if k is negative or greater than $|A|$, then A has no subsets of cardinality k , so $\binom{4}{k} = 0$ in these cases. In general $\binom{n}{k} = 0$ whenever $k < 0$ or $k > n$. In particular this means $\binom{n}{k} = 0$ if n is negative.

Although it was not hard to work out the values of $\binom{4}{k}$ by writing out subsets in the above table, this method of actually listing sets would not be practical for computing $\binom{n}{k}$ when n and k are large. We need a formula. To find one, we will now carefully work out the value of $\binom{5}{3}$ in a way that highlights a pattern that points the way to a formula for any $\binom{n}{k}$.

To begin, note that $\binom{5}{3}$ is the number of 3-element subsets of $\{a, b, c, d, e\}$. These are listed in the top row of the table below, where we see $\binom{5}{3} = 10$. The column under each subset tallies the $3! = 6$ permutations of that subset. The first subset $\{a, b, c\}$ has $3! = 6$ permutations; these are listed below it. The second column tallies the permutations of $\{a, b, d\}$, and so on.

| | | | | | | | | | | | |
|-------|----|---|-------|-------|-------|-------|-------|-------|-------|-------|-------|
| | | ← $\binom{5}{3}$ → | | | | | | | | | |
| | | $\{a, b, c\}$ $\{a, b, d\}$ $\{a, b, e\}$ $\{a, c, d\}$ $\{a, c, e\}$ $\{a, d, e\}$ $\{b, c, d\}$ $\{b, c, e\}$ $\{b, d, e\}$ $\{c, d, e\}$ | | | | | | | | | |
| ↑ | 3! | abc | abd | abe | acd | ace | ade | bcd | bce | bde | cde |
| acb | | adb | aeb | adc | aec | aed | bdc | bec | bed | ced | |
| bac | | bad | bae | cad | cae | dae | cbd | cbe | dbe | dce | |
| bca | | bda | bea | cda | cea | dea | cdb | ceb | deb | dec | |
| cba | | dba | eba | dca | eca | eda | dcb | ecb | edb | edc | |
| cab | | dab | eab | dac | eac | ead | dbc | ebc | ebd | ecd | |

The body of this table has $\binom{5}{3}$ columns and $3!$ rows, so it has a total of $3! \binom{5}{3}$ lists. But notice also that the table consists of every 3-permutation of $\{a, b, c, d, e\}$. Fact 4.4 says that there are $P(5, 3) = \frac{5!}{(5-3)!}$ such 3-permutations. Thus the total number of lists in the table can be written as either $3! \binom{5}{3}$ or $\frac{5!}{(5-3)!}$, which is to say $3! \binom{5}{3} = \frac{5!}{(5-3)!}$. Dividing both sides by $3!$ yields

$$\binom{5}{3} = \frac{5!}{3!(5-3)!}$$

Working this out, you will find that it does give the correct value of 10.


But there was nothing special about the values 5 and 3. We could do the above analysis for any $\binom{n}{k}$ instead of $\binom{5}{3}$. The table would have $\binom{n}{k}$ columns and $k!$ rows. We would get

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$


We have established the following fact, which holds for all $k, n \in \mathbb{Z}$.

Fact 4.5 If $0 \leq k \leq n$, then $\binom{n}{k} = \frac{n!}{k!(n-k)!}$. Otherwise $\binom{n}{k} = 0$.

Let's now use our new knowledge to work some exercises.

Example 4.11 How many size-4 subsets does $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ have? The answer is $\binom{9}{4} = \frac{9!}{4!(9-4)!} = \frac{9!}{4!5!} = \frac{9 \cdot 8 \cdot 7 \cdot 6 \cdot 5!}{4!5!} = \frac{9 \cdot 8 \cdot 7 \cdot 6}{4!} = \frac{9 \cdot 8 \cdot 7 \cdot 6}{24} = \mathbf{126}$. 

Example 4.12 How many 5-element subsets of $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ have exactly two even elements?

Solution: Making a 5-element subset of A with exactly two even elements is a 2-step process. First select two of the four even elements from A . There are $\binom{4}{2} = 6$ ways to do this. Next, there are $\binom{5}{3} = 10$ ways select three of the five odd elements of A . By the multiplication principle, there are $\binom{4}{2} \binom{5}{3} = 6 \cdot 10 = 60$ ways to select two even and three odd elements from A . So there are **60** 5-element subsets of A with exactly two even elements. 


Example 4.13 A single 5-card hand is dealt off of a standard 52-card deck. How many different 5-card hands are possible?

Solution: Think of the deck as a set D of 52 cards. Then a 5-card hand is just a 5-element subset of D . There are many such subsets, such as

$$\left\{ \begin{array}{|c|} \hline 7 \\ \hline \spadesuit \\ \hline \end{array}, \begin{array}{|c|} \hline 2 \\ \hline \clubsuit \\ \hline \end{array}, \begin{array}{|c|} \hline 3 \\ \hline \heartsuit \\ \hline \end{array}, \begin{array}{|c|} \hline A \\ \hline \spadesuit \\ \hline \end{array}, \begin{array}{|c|} \hline 5 \\ \hline \diamondsuit \\ \hline \end{array} \right\}.$$

Thus the number of 5-card hands is the number of 5-element subsets of D , which is


$$\binom{52}{5} = \frac{52!}{5! \cdot 47!} = \frac{52 \cdot 51 \cdot 50 \cdot 49 \cdot 48 \cdot 47!}{5! \cdot 47!} = \frac{52 \cdot 51 \cdot 50 \cdot 49 \cdot 48}{5!} = 2,598,960.$$

Answer: There are **2,598,960** different five-card hands that can be dealt from a deck of 52 cards. 


Example 4.14 This problem concerns 5-card hands that can be dealt off of a 52-card deck. How many such hands are there in which two of the cards are clubs and three are hearts?

Solution: Such a hand is described by a list of length two of the form

$$\left(\left\{ \begin{array}{|c|} \hline * \\ \hline \clubsuit \\ \hline \end{array}, \begin{array}{|c|} \hline * \\ \hline \clubsuit \\ \hline \end{array} \right\}, \left\{ \begin{array}{|c|} \hline * \\ \hline \heartsuit \\ \hline \end{array}, \begin{array}{|c|} \hline * \\ \hline \heartsuit \\ \hline \end{array}, \begin{array}{|c|} \hline * \\ \hline \heartsuit \\ \hline \end{array} \right\} \right),$$

where the first entry is a 2-element subset of the set of 13 club cards, and the second entry is a 3-element subset of the set of 13 heart cards. There are $\binom{13}{2}$ choices for the first entry and $\binom{13}{3}$ choices for the second, so by the multiplication principle there are $\binom{13}{2}\binom{13}{3} = \frac{13!}{2!11!} \frac{13!}{3!10!} = 22,308$ such lists. Thus there are **22,308** such 5-card hands. 


Example 4.15 A lottery features a bucket of 36 balls numbered 1 through 36. Six balls will be drawn randomly. For \$1 you buy a ticket with six blanks: $\square\square\square\square\square\square$. You fill in the blanks with six different numbers between 1 and 36. You win \$1,000,000 if you chose the same numbers that are drawn, regardless of order. What are your chances of winning?

Solution: In filling out the ticket you are choosing six numbers from a set of 36 numbers. Thus there are $\binom{36}{6} = \frac{36!}{6!(36-6)!} = 1,947,792$ different combinations of numbers you might write. Only one of these will be a winner. **Your chances of winning are one in 1,947,792.** 

Example 4.16 How many 7-digit binary strings (0010100, 1101011, etc.) have an odd number of 1's?

Solution: Let A be the set of all 7-digit binary strings with an odd number of 1's, so the answer will be $|A|$. To find $|A|$, we break A into smaller parts. Notice any string in A will have either one, three, five or seven 1's. Let A_1 be the set of 7-digit binary strings with only one 1. Let A_3 be the set of 7-digit binary strings with three 1's. Let A_5 be the set of 7-digit binary strings with five 1's, and let A_7 be the set of 7-digit binary strings with seven 1's. Then $A = A_1 \cup A_3 \cup A_5 \cup A_7$. Any two of the sets A_i have empty intersection, so the addition principle gives $|A| = |A_1| + |A_3| + |A_5| + |A_7|$.

Now we must compute the individual terms of this sum. Take A_3 , the set of 7-digit binary strings with three 1's. Such a string can be formed by selecting three out of seven positions for the 1's and putting 0's in the other spaces. Thus $|A_3| = \binom{7}{3}$. Similarly $|A_1| = \binom{7}{1}$, $|A_5| = \binom{7}{5}$, and $|A_7| = \binom{7}{7}$.

Answer: $|A| = |A_1| + |A_3| + |A_5| + |A_7| = \binom{7}{1} + \binom{7}{3} + \binom{7}{5} + \binom{7}{7} = 7 + 35 + 21 + 1 = 64$. There are **64** 7-digit binary strings with an odd number of 1's. 

Exercises for Section 4.5

1. Suppose a set A has 37 elements. How many subsets of A have 10 elements? How many subsets have 30 elements? How many have 0 elements?
 2. Suppose A is a set for which $|A| = 100$. How many subsets of A have 5 elements? How many subsets have 10 elements? How many have 99 elements?
 3. A set X has exactly 56 subsets with 3 elements. What is the cardinality of X ?
 4. Suppose a set B has the property that $|\{X : X \in \mathcal{P}(B), |X| = 6\}| = 28$. Find $|B|$.
 5. How many 16-digit binary strings contain exactly seven 1's? (Examples of such strings include 0111000011110000 and 0011001100110010, etc.)
 6. $|\{X \in \mathcal{P}(\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}) : |X| = 4\}| =$
 7. $|\{X \in \mathcal{P}(\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}) : |X| < 4\}| =$
 8. This problem concerns lists made from the symbols $A, B, C, D, E, F, G, H, I$.
 - (a) How many length-5 lists can be made if there is no repetition and the list is in alphabetical order? (Example: $BDEFI$ or $ABCGH$, but not $BACGH$.)
 - (b) How many length-5 lists can be made if repetition is not allowed and the list is **not** in alphabetical order?
 9. This problem concerns lists of length 6 made from the letters A, B, C, D, E, F , without repetition. How many such lists have the property that the D occurs before the A ?
 10. A department consists of 5 men and 7 women. From this department you select a committee with 3 men and 2 women. In how many ways can you do this?
 11. How many positive 10-digit integers contain no 0's and exactly three 6's?
 12. Twenty-one people are to be divided into two teams, the Red Team and the Blue Team. There will be 10 people on Red Team and 11 people on Blue Team. In how many ways can this be done?
 13. Suppose $n, k \in \mathbb{Z}$, and $0 \leq k \leq n$. Use Fact 4.5, the formula $\binom{n}{k} = \frac{n!}{k!(n-k)!}$, to show that $\binom{n}{k} = \binom{n}{n-k}$.
 14. Suppose $n, k \in \mathbb{Z}$, and $0 \leq k \leq n$. Use Definition 4.2 alone (without using Fact 4.5) to show that $\binom{n}{k} = \binom{n}{n-k}$.
 15. How many 10-digit binary strings are there that do not have exactly four 1's?
 16. How many 6-element subsets of $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ have exactly three even elements? How many do not have exactly three even elements?
 17. How many 10-digit binary strings are there that have exactly four 1's or exactly five 1's? How many do not have exactly four 1's or exactly five 1's?
 18. How many 10-digit binary strings have an even number of 1's?
 19. A 5-card poker hand is called a *flush* if all cards are the same suit. How many different flushes are there?
-

4.6 Pascal's Triangle and the Binomial Theorem

There are some beautiful and significant patterns among the numbers $\binom{n}{k}$. We now investigate a pattern based on one equation in particular. It happens that

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k} \tag{4.3}$$

for any integers n and k with $1 \leq k \leq n$.

To see why this is true, notice that the left-hand side $\binom{n+1}{k}$ is the number of k -element subsets of the set $A = \{0, 1, 2, 3, \dots, n\}$, which has $n + 1$ elements. Such a subset either contains 0 or it does not. The $\binom{n}{k-1}$ on the right is the number of subsets of A that contain 0, because to make such a subset we can start with $\{0\}$ and append it an additional $k - 1$ numbers selected from $\{1, 2, 3, \dots, n\}$, and there are $\binom{n}{k-1}$ ways to do this. Also, the $\binom{n}{k}$ on the right is the number of subsets of A that **do not** contain 0, for it is the number of ways to select k elements from $\{1, 2, 3, \dots, n\}$. In light of all this, Equation (4.3) just states the obvious fact that the number of k -element subsets of A equals the number of k -element subsets that contain 0 plus the number of k -element subsets that do not contain 0.

Having seen why Equation (4.3) is true, we now highlight it by arranging the numbers $\binom{n}{k}$ in a triangular pattern. The left-hand side of Figure 4.3 shows the numbers $\binom{n}{k}$ arranged in a pyramid with $\binom{0}{0}$ at the apex, just above a row containing $\binom{1}{k}$ with $k = 0$ and $k = 1$. Below *this* is a row listing the values of $\binom{2}{k}$ for $k = 0, 1, 2$, and so on.

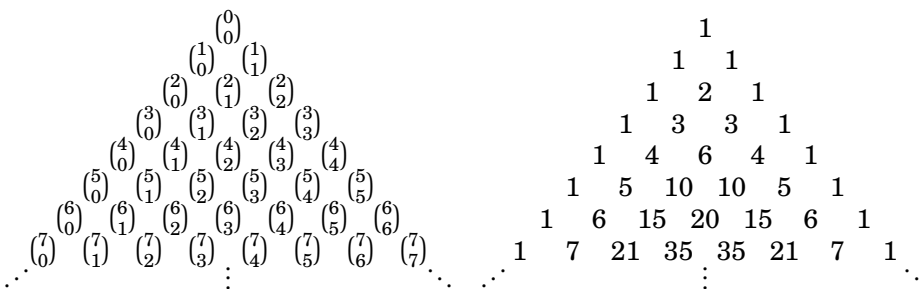


Figure 4.3. Pascal's triangle

Any number $\binom{n+1}{k}$ for $0 < k < n$ in this pyramid is just below and between the two numbers $\binom{n}{k-1}$ and $\binom{n}{k}$ in the previous row. But Equation (4.3) says $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$. Therefore any number (other than 1) in the pyramid is the sum of the two numbers immediately above it.

This pattern is especially evident on the right of Figure 4.3, where each $\binom{n}{k}$ is worked out. Notice how 21 is the sum of the numbers 6 and 15 above it. Similarly, 5 is the sum of the 1 and 4 above it and so on.

This arrangement is called **Pascal's triangle**, after Blaise Pascal, 1623–1662, a French philosopher and mathematician who discovered many of its properties. We've shown only the first eight rows, but the triangle extends downward forever. We can always add a new row at the bottom by placing a 1 at each end and obtaining each remaining number by adding the two numbers above its position. Doing this in Figure 4.3 (right) gives a new bottom row

$$1 \quad 8 \quad 28 \quad 56 \quad 70 \quad 56 \quad 28 \quad 8 \quad 1.$$

This row consists of the numbers $\binom{8}{k}$ for $0 \leq k \leq 8$, and we have computed them without the formula $\binom{8}{k} = \frac{8!}{k!(8-k)!}$. Any $\binom{n}{k}$ can be computed this way.

The very top row (containing only 1) of Pascal's triangle is called *Row 0*. Row 1 is the next down, followed by Row 2, then Row 3, etc. Thus Row n lists the numbers $\binom{n}{k}$ for $0 \leq k \leq n$. Exercises 4.5.13 and 4.5.14 established

$$\binom{n}{k} = \binom{n}{n-k}, \tag{4.4}$$

for each $0 \leq k \leq n$. In words, the k th entry of Row n of Pascal's triangle equals the $(n - k)$ th entry. This means that Pascal's triangle is symmetric with respect to the vertical line through its apex, as is evident in Figure 4.3.

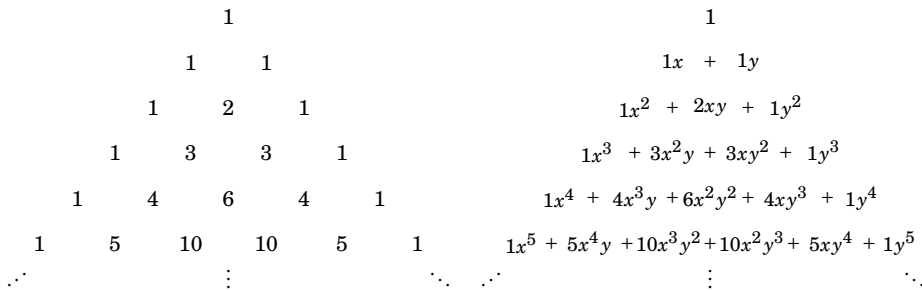


Figure 4.4. The n^{th} row of Pascal's triangle lists the coefficients of $(x + y)^n$

Notice that Row n appears to be a list of the coefficients of $(x + y)^n$. For example $(x + y)^2 = 1x^2 + 2xy + 1y^2$, and Row 2 lists the coefficients 1 2 1. Also $(x + y)^3 = 1x^3 + 3x^2y + 3xy^2 + 1y^3$, and Row 3 is 1 3 3 1. See Figure 4.4, which suggests that the numbers in Row n are the coefficients of $(x + y)^n$.

In fact this turns out to be true for every n . This fact is known as the **binomial theorem**, and it is worth mentioning here. It tells how to raise a binomial $x + y$ to a non-negative integer power n .

Theorem 4.1 (Binomial Theorem) If n is a non-negative integer, then $(x + y)^n = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \binom{n}{3}x^{n-3}y^3 + \cdots + \binom{n}{n-1}xy^{n-1} + \binom{n}{n}y^n$.

For now we will be content to accept the binomial theorem without proof. (You will be asked to prove it in an exercise in Chapter 14.) You may find it useful from time to time. For instance, you can use it if you ever need to expand an expression such as $(x + y)^7$. To do this, look at Row 7 of Pascal's triangle in Figure 4.3 and apply the binomial theorem to get

$$(x + y)^7 = x^7 + 7x^6y + 21x^5y^2 + 35x^4y^3 + 35x^3y^4 + 21x^2y^5 + 7xy^6 + y^7.$$

For another example,

$$\begin{aligned} (2a - b)^4 &= ((2a) + (-b))^4 \\ &= (2a)^4 + 4(2a)^3(-b) + 6(2a)^2(-b)^2 + 4(2a)(-b)^3 + (-b)^4 \\ &= 16a^4 - 32a^3b + 24a^2b^2 - 8ab^3 + b^4. \end{aligned}$$

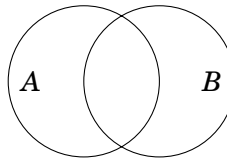
Exercises for Section 4.6

- Write out Row 11 of Pascal's triangle.
- Use the binomial theorem to find the coefficient of x^8y^5 in $(x + y)^{13}$.
- Use the binomial theorem to find the coefficient of x^8 in $(x + 2)^{13}$.
- Use the binomial theorem to find the coefficient of x^6y^3 in $(3x - 2y)^9$.
- Use the binomial theorem to show $\sum_{k=0}^n \binom{n}{k} = 2^n$.
- Use Definition 4.2 (page 99) and Fact 2.3 (page 25) to show $\sum_{k=0}^n \binom{n}{k} = 2^n$.
- Use the binomial theorem to show $\sum_{k=0}^n 3^k \binom{n}{k} = 4^n$.
- Use Fact 4.5 (page 101) to derive Equation 4.3 (page 104).
- Use the binomial theorem to show $\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \binom{n}{4} - \cdots + (-1)^n \binom{n}{n} = 0$, for $n > 0$.
- Show that the formula $k \binom{n}{k} = n \binom{n-1}{k-1}$ is true for all integers n, k with $0 \leq k \leq n$.
- Use the binomial theorem to show $9^n = \sum_{k=0}^n (-1)^k \binom{n}{k} 10^{n-k}$.
- Show that $\binom{n}{k} \binom{k}{m} = \binom{n}{m} \binom{n-m}{k-m}$.
- Show that $\binom{n}{3} = \binom{2}{2} + \binom{3}{2} + \binom{4}{2} + \binom{5}{2} + \cdots + \binom{n-1}{2}$.
- The first five rows of Pascal's triangle appear in the digits of powers of 11: $11^0 = 1$, $11^1 = 11$, $11^2 = 121$, $11^3 = 1331$ and $11^4 = 14641$. Why is this so? Why does the pattern not continue with 11^5 ?

4.7 The Inclusion-Exclusion Principle

Many counting problems involve computing the cardinality of a union $A \cup B$ of two finite sets. We examine this kind of problem now.

First we develop a formula for $|A \cup B|$. It is tempting to say that $|A \cup B|$ must equal $|A| + |B|$, but that is not quite right. If we count the elements of A and then count the elements of B and add the two figures together, we get $|A| + |B|$. But if A and B have some elements in common, then we have counted each element in $A \cap B$ *twice*.



Therefore $|A| + |B|$ exceeds $|A \cup B|$ by $|A \cap B|$, and consequently $|A \cup B| = |A| + |B| - |A \cap B|$. This can be a useful equation.

Fact 4.6 Inclusion-Exclusion Formula

If A and B are finite sets, then $|A \cup B| = |A| + |B| - |A \cap B|$.

Notice that the sets A , B and $A \cap B$ are all generally smaller than $A \cup B$, so Fact 4.6 has the potential of reducing the problem of determining $|A \cup B|$ to three simpler counting problems. It is called the *inclusion-exclusion* formula because elements in $A \cap B$ are included (twice) in $|A| + |B|$, then excluded when $|A \cap B|$ is subtracted. Notice that if $A \cap B = \emptyset$, then we do in fact get $|A \cup B| = |A| + |B|$. (This is an instance of the addition principle!) Conversely, if $|A \cup B| = |A| + |B|$, then it must be that $A \cap B = \emptyset$.

Example 4.17 A 3-card hand is dealt off of a standard 52-card deck. How many different such hands are there for which all three cards are red or all three cards are face cards?


Solution: Let A be the set of 3-card hands where all three cards are red (i.e., either \heartsuit or \diamondsuit). Let B be the set of 3-card hands in which all three cards are face cards (i.e., J, K or Q of any suit). These sets are illustrated below.

$$\begin{aligned}
 A &= \left\{ \left\{ \begin{array}{|c|} \hline 5 \\ \hline \heartsuit \\ \hline \end{array} \right\}, \left\{ \begin{array}{|c|} \hline K \\ \hline \diamondsuit \\ \hline \end{array} \right\}, \left\{ \begin{array}{|c|} \hline 2 \\ \hline \heartsuit \\ \hline \end{array} \right\}, \left\{ \begin{array}{|c|} \hline K \\ \hline \heartsuit \\ \hline \end{array} \right\}, \left\{ \begin{array}{|c|} \hline J \\ \hline \heartsuit \\ \hline \end{array} \right\}, \left\{ \begin{array}{|c|} \hline Q \\ \hline \heartsuit \\ \hline \end{array} \right\}, \left\{ \begin{array}{|c|} \hline A \\ \hline \diamondsuit \\ \hline \end{array} \right\}, \left\{ \begin{array}{|c|} \hline 6 \\ \hline \diamondsuit \\ \hline \end{array} \right\}, \left\{ \begin{array}{|c|} \hline 6 \\ \hline \heartsuit \\ \hline \end{array} \right\}, \dots \right\} & \text{(Red cards)} \\
 B &= \left\{ \left\{ \begin{array}{|c|} \hline K \\ \hline \spadesuit \\ \hline \end{array} \right\}, \left\{ \begin{array}{|c|} \hline K \\ \hline \diamondsuit \\ \hline \end{array} \right\}, \left\{ \begin{array}{|c|} \hline J \\ \hline \clubsuit \\ \hline \end{array} \right\}, \left\{ \begin{array}{|c|} \hline K \\ \hline \heartsuit \\ \hline \end{array} \right\}, \left\{ \begin{array}{|c|} \hline J \\ \hline \heartsuit \\ \hline \end{array} \right\}, \left\{ \begin{array}{|c|} \hline Q \\ \hline \heartsuit \\ \hline \end{array} \right\}, \left\{ \begin{array}{|c|} \hline Q \\ \hline \diamondsuit \\ \hline \end{array} \right\}, \left\{ \begin{array}{|c|} \hline Q \\ \hline \clubsuit \\ \hline \end{array} \right\}, \left\{ \begin{array}{|c|} \hline Q \\ \hline \heartsuit \\ \hline \end{array} \right\}, \dots \right\} & \text{(Face cards)}
 \end{aligned}$$


We seek the number of 3-card hands that are all red or all face cards, and this number is $|A \cup B|$. By Fact 4.6, $|A \cup B| = |A| + |B| - |A \cap B|$. Let's examine $|A|, |B|$ and $|A \cap B|$ separately. Any hand in A is formed by selecting three cards from the 26 red cards in the deck, so $|A| = \binom{26}{3}$. Similarly, any hand in B is formed by selecting three cards from the 12 face cards in the deck, so $|B| = \binom{12}{3}$. Now think about $A \cap B$. It contains all the 3-card hands made up of cards that are red face cards.

$$A \cap B = \left\{ \left\{ \begin{array}{|c|} \hline K \\ \hline \heartsuit \\ \hline \end{array} , \begin{array}{|c|} \hline K \\ \hline \diamondsuit \\ \hline \end{array} , \begin{array}{|c|} \hline J \\ \hline \heartsuit \\ \hline \end{array} \right\}, \left\{ \begin{array}{|c|} \hline K \\ \hline \heartsuit \\ \hline \end{array} , \begin{array}{|c|} \hline J \\ \hline \heartsuit \\ \hline \end{array} , \begin{array}{|c|} \hline Q \\ \hline \heartsuit \\ \hline \end{array} \right\}, \left\{ \begin{array}{|c|} \hline Q \\ \hline \diamondsuit \\ \hline \end{array} , \begin{array}{|c|} \hline J \\ \hline \diamondsuit \\ \hline \end{array} , \begin{array}{|c|} \hline Q \\ \hline \heartsuit \\ \hline \end{array} \right\}, \dots \right\} \quad \text{(Red face cards)}$$

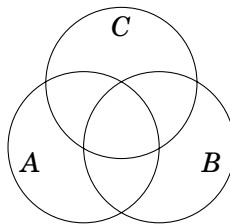
The deck has only 6 red face cards, so $|A \cap B| = \binom{6}{3}$.

Now we can answer our question. The number of 3-card hands that are all red or all face cards is $|A \cup B| = |A| + |B| - |A \cap B| = \binom{26}{3} + \binom{12}{3} - \binom{6}{3} = 2600 + 220 - 20 = \mathbf{2800}$. 

Example 4.18 A 3-card hand is dealt off of a standard 52-card deck. How many different such hands are there for which it is **not** the case that all 3 cards are red or all three cards are face cards?

Solution: We will use the subtraction principle combined with our answer to Example 4.17, above. The total number of 3-card hands is $\binom{52}{3} = \frac{52!}{3!(52-3)!} = \frac{52!}{3!49!} = \frac{52 \cdot 51 \cdot 50}{3!} = 26 \cdot 17 \cdot 50 = 22,100$. To get our answer, we must subtract from this the number of 3-card hands that are all red or all face cards, that is, we must subtract the answer from Example 4.17. Thus the answer to our question is $22,100 - 2800 = \mathbf{19,300}$. 

There is an analogue of Fact 4.6 that involves three sets. Consider three sets A, B and C , as represented in the following Venn Diagram.



Using the same kind of reasoning that resulted in Fact 4.6, you can convince yourself that

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|. \quad (4.5)$$

There's probably not much harm in ignoring this one for now, but if you find this kind of thing intriguing you should definitely take a course in combinatorics. (Ask your instructor!)

Exercises for Section 4.7

1. At a certain university 523 of the seniors are history majors or math majors (or both). There are 100 senior math majors, and 33 seniors are majoring in both history and math. How many seniors are majoring in history?
 2. How many 4-digit positive integers are there for which there are no repeated digits, or for which there may be repeated digits, but all digits are odd?
 3. How many 4-digit positive integers are there that are even or contain no 0's?
 4. This problem involves lists made from the letters T, H, E, O, R, Y , with repetition allowed.
 - (a) How many 4-letter lists are there that don't begin with T , or don't end in Y ?
 - (b) How many 4-letter lists are there in which the sequence of letters T, H, E appears consecutively (in that order)?
 - (c) How many 6-letter lists are there in which the sequence of letters T, H, E appears consecutively (in that order)?
 5. How many 7-digit binary strings begin in 1 or end in 1 or have exactly four 1's?
 6. Is the following statement true or false? Explain. If $A_1 \cap A_2 \cap A_3 = \emptyset$, then $|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3|$.
 7. Consider 4-card hands dealt off of a standard 52-card deck. How many hands are there for which all 4 cards are of the same suit or all 4 cards are red?
 8. Consider 4-card hands dealt off of a standard 52-card deck. How many hands are there for which all 4 cards are of different suits or all 4 cards are red?
 9. A 4-letter list is made from the letters L, I, S, T, E, D according to the following rule: Repetition is allowed, and the first two letters on the list are vowels or the list ends in D . How many such lists are possible?
 10. How many 6-digit numbers are even or are divisible by 5?
 11. How many 7-digit numbers are even or have exactly three digits equal to 0?
 12. How many 5-digit numbers are there in which three of the digits are 7, or two of the digits are 2?
 13. How many 8-digit binary strings end in 1 or have exactly four 1's?
 14. How many 3-card hands (from a standard 52-card deck) have the property that it is **not** the case that all cards are black or all cards are of the same suit?
 15. How many 10-digit binary strings begin in 1 or end in 1?
-

4.8 Counting Multisets

You have in your pocket four pennies, two nickels, a dime and two quarters. You might be tempted to regard this collection as a set

$$\{1, 1, 1, 1, 5, 5, 10, 25, 25\}.$$

But this is not a valid model of your collection of change, because a set cannot have repeated elements. To overcome this difficulty, we make a new construction called a **multiset**. A multiset is like a set, except that elements can be repeated. We will use square brackets $[]$ instead of braces $\{ \}$ to denote multisets. For example, your multiset of change is

$$[1, 1, 1, 1, 5, 5, 10, 25, 25].$$

A multiset is a hybrid of a set and a list; in a multiset, elements can be repeated, but order does not matter. For instance

$$\begin{aligned} [1, 1, 1, 1, 5, 5, 10, 25, 25] &= [25, 5, 1, 1, 10, 1, 1, 5, 25] \\ &= [25, 10, 25, 1, 5, 1, 5, 1, 1]. \end{aligned}$$

Given a multiset A , its **cardinality** $|A|$ is the number of elements it has, including repetition. So if $A = [1, 1, 1, 1, 5, 5, 10, 25, 25]$, then $|A| = 9$. The **multiplicity** of an element $x \in A$ is the number of times that x appears, so $1 \in A$ has multiplicity 4, while 5 and 25 each have multiplicity 2, and 10 has multiplicity 1. Notice that every set can be regarded as a multiset for which each element has multiplicity 1. In this sense we can think of $\emptyset = \{ \} = []$ as the multiset that has no elements.

To illustrate the idea of multisets, consider the multisets of cardinality 2 that can be made from the symbols $\{a, b, c, d\}$. They are

$$[a, a] \quad [a, b] \quad [a, c] \quad [a, d] \quad [b, b] \quad [b, c] \quad [b, d] \quad [c, c] \quad [c, d] \quad [d, d].$$

We have listed them so that the letters in each multiset are in alphabetical order (remember, we can order the elements of a multiset in any way we choose), and the 10 multisets are arranged in dictionary order.

For multisets of cardinality 3 made from $\{a, b, c, d\}$, we have

$$\begin{array}{cccccc} [a, a, a] & [a, a, b] & [a, a, c] & [a, a, d] & [a, b, b] \\ [a, b, c] & [a, b, d] & [a, c, c] & [a, c, d] & [a, d, d] \\ [b, b, b] & [b, b, c] & [b, b, d] & [b, c, c] & [b, c, d] \\ [b, d, d] & [c, c, c] & [c, c, d] & [c, d, d] & [d, d, d]. \end{array}$$

Though $X = \{a, b, c, d\}$ has no *subsets* of cardinality 5, there are many *multisets* of cardinality 5 made from these elements, including $[a, a, a, a, a]$, $[a, a, b, c, d]$ and $[b, c, c, d, d]$, and so on. Exactly how many are there?

This is the first question about multisets that we shall tackle: Given a finite set X , how many cardinality- k multisets can be made from X ?

Let's start by counting the cardinality-5 multisets made from symbols $X = \{a, b, c, d\}$. (Our approach will lead to a general formula.) We know we can write any such multiset with its letters in alphabetical order. Tweaking the notation slightly, we could write any such multiset with bars separating the groupings of a, b, c, d , as shown in the table below. Notice that if a symbol does not appear in the multiset, we still write the bar that would have separated it from the others.

| Multiset | with separating bars | encoding |
|-------------------|----------------------|------------|
| $[a, a, b, c, d]$ | $aa b c d$ | $** * * *$ |
| $[a, b, b, c, d]$ | $a bb c d$ | $* ** * *$ |
| $[a, b, c, c, d]$ | $a b cc d$ | $* * ** *$ |
| $[a, a, c, c, d]$ | $aa cc d$ | $** ** *$ |
| $[b, b, d, d, d]$ | $ bb ddd$ | $ ** ***$ |
| $[a, a, a, a, a]$ | $aaaaa $ | $***** $ |

This suggests that we can encode the multisets as lists made from the two symbols $*$ and $|$, with an $*$ for each element of the multiset, as follows.

$$\begin{array}{cccc}
 * \text{ for each } a & * \text{ for each } b & * \text{ for each } c & * \text{ for each } d \\
 \underbrace{*\dots*}_{} & | \underbrace{*\dots*}_{} & | \underbrace{*\dots*}_{} & | \underbrace{*\dots*}_{}
 \end{array}$$

For examples see the right-hand column of the table. Any such encoding is a list made from 5 stars and 3 bars, so the list has a total of 8 entries. How many such lists are there? We can form such a list by choosing 3 of the 8 positions for the bars, and filling the remaining three positions with stars. Therefore the number of such lists is $\binom{8}{3} = \frac{8!}{3!5!} = 56$.

That is our answer. **There are 56 cardinality-5 multisets** that can be made from the symbols in $X = \{a, b, c, d\}$.

If we wanted to count the cardinality-3 multisets made from X , then the exact same reasoning would apply, but with 3 stars instead of 5. We'd be counting the length-6 lists with 3 stars and 3 bars. There are $\binom{6}{3} = \frac{6!}{3!3!} = 20$ such lists. So there are 20 cardinality-3 multisets made from $X = \{a, b, c, d\}$. This agrees with our accounting on the previous page.

In general, given a set $X = \{x_1, x_2, \dots, x_n\}$ of n elements, any cardinality- k multiset made from its elements can be encoded in a star-and-bar list

$$\overbrace{*****}^{\text{* for each } x_1} \mid \overbrace{*****}^{\text{* for each } x_2} \mid \overbrace{*****}^{\text{* for each } x_3} \mid \dots \dots \mid \overbrace{*****}^{\text{* for each } x_n}.$$

Such a list has k stars (one for each element of the multiset) and $n - 1$ separating bars (a bar between each of the n groupings of stars). Therefore its length is $k + n - 1$. We can make such a list by selecting $n - 1$ list positions out of $k + n - 1$ positions for the bars and inserting stars in the left-over positions. Thus there are $\binom{k+n-1}{n-1}$ such lists. Alternatively we could choose k positions for the stars and fill in the remaining $n - k$ with bars, so there are $\binom{k+n-1}{k}$ such lists. Note that $\binom{k+n-1}{k} = \binom{k+n-1}{n-1}$ by Equation (4.4) on page 105.

Let's summarize our reckoning.

Fact 4.7 The number of k -element multisets that can be made from the elements of an n -element set $X = \{x_1, x_2, \dots, x_n\}$ is

$$\binom{k+n-1}{k} = \binom{k+n-1}{n-1}.$$

This works because any cardinality- k multiset made from the n elements of X can be encoded in a star-and-bar list of length $k + n - 1$, having form

$$\overbrace{*****}^{\text{* for each } x_1} \mid \overbrace{*****}^{\text{* for each } x_2} \mid \overbrace{*****}^{\text{* for each } x_3} \mid \dots \dots \mid \overbrace{*****}^{\text{* for each } x_n}$$

with k stars and $n - 1$ bars separating the n groupings of stars. Such a list can be made by selecting $n - 1$ positions for the bars, and filling the remaining positions with stars, and there are $\binom{k+n-1}{n-1}$ ways to do this.

For example, the number of 2-element multisets that can be made from the 4-element set $X = \{a, b, c, d\}$ is $\binom{2+4-1}{2} = \binom{5}{2} = 10$. This agrees with our accounting of them on page 110. The number of 3-element multisets that can be made from the elements of X is $\binom{3+4-1}{3} = \binom{6}{3} = 20$. Again this agrees with our list of them on page 110.

The number of 1-element multisets made from X is $\binom{1+4-1}{1} = \binom{4}{1} = 4$. Indeed, the four multisets are $[a], [b], [c]$ and $[d]$. The number of 0-element multisets made from X is $\binom{0+4-1}{0} = \binom{3}{0} = 1$. This is right, because there is only one such multiset, namely \emptyset .


Example 4.19 A bag contains 20 identical red marbles, 20 identical green marbles, and 20 identical blue marbles. You reach in and grab 20 marbles. There are many possible outcomes. You could have 11 reds, 4 greens and 5 blues. Or you could have 20 reds, 0 greens and 0 blues, etc. All together, how many outcomes are possible?

Solution: Each outcome can be thought of as a 20-element multiset made from the elements of the 3-element set $X = \{R, G, B\}$. For example, 11 reds, 4 greens and 5 blues would correspond to the multiset

$$[R, R, R, R, R, R, R, R, R, R, R, G, G, G, G, B, B, B, B, B].$$

The outcome consisting of 10 reds and 10 blues corresponds to the multiset

$$[R, R, R, R, R, R, R, R, R, R, B, B, B, B, B, B, B, B, B, B].$$

Thus the total number of outcomes is the number of 20-element multisets made from the elements of the 3-element set $X = \{R, G, B\}$. By Fact 4.7, the answer is $\binom{20+3-1}{20} = \binom{22}{20} = \mathbf{231}$ possible outcomes. 

Rather than remembering the formula in Fact 4.7, it is probably best to work out a new stars-and-bars model as needed. This is because it is often easy to see how a particular problem can be modeled with stars and bars, and once they have been set up, the formula in Fact 4.7 falls out automatically.

For instance, we could solve Example 4.19 by noting that each outcome has a star-and-bar encoding using 20 stars and 2 bars. (The outcome $[R, R, R, R, R, R, R, R, R, R, R, G, G, G, G, B, B, B, B, B]$ can be encoded in stars and bars as $*****|*****|*****$, etc.) We can form such a list by choosing 2 out of 22 slots for bars and filling the remaining 20 slots with stars. There are $\binom{22}{2} = 231$ ways of doing this.

Our next example involves counting the number of *non-negative* integer solutions of the equation $w + x + y + z = 20$. By a *non-negative integer solution* to the equation, we mean an assignment of non-negative integers to the variables that makes the equation true. For example, one solution is $w = 7, x = 3, y = 5, z = 5$. We can write this solution compactly as $(w, x, y, z) = (7, 3, 5, 5)$. Two other solutions are $(w, x, y, z) = (1, 3, 1, 15)$ and $(w, x, y, z) = (0, 20, 0, 0)$. We would not include $(w, x, y, z) = (1, -1, 10, 10)$ as a solution because even though it satisfies the equation, the value of x is negative. How many solutions are there all together? The next example presents a way of solving this type of question.

Example 4.20 How many non-negative integer solutions does the equation $w + x + y + z = 20$ have?


Solution: We can model a solution with stars and bars. For example, encode the solution $(w, x, y, z) = (3, 4, 5, 8)$ as

$$\overbrace{***}^3 \mid \overbrace{****}^4 \mid \overbrace{*****}^5 \mid \overbrace{*****}^8.$$

In general, any solution $(w, x, y, z) = (a, b, c, d)$ gets encoded as

$$\overbrace{***\dots*}^{a \text{ stars}} \mid \overbrace{***\dots*}^{b \text{ stars}} \mid \overbrace{***\dots*}^{c \text{ stars}} \mid \overbrace{***\dots*}^{d \text{ stars}},$$

where all together there are 20 stars and 3 bars. So, for instance the solution $(w, x, y, z) = (0, 0, 10, 10)$ gets encoded as $||*****|*****$, and the solution $(w, x, y, z) = (7, 3, 5, 5)$ is encoded as $*****|***|*****|*****$. Thus we can describe any non-negative integer solution to the equation as a list of length $20 + 3 = 23$ that has 20 stars and 3 bars. We can make any such list by choosing 3 out of 23 spots for the bars, and filling the remaining 20 spots with stars. The number of ways to do this is $\binom{23}{3} = \frac{23!}{3!20!} = \frac{23 \cdot 22 \cdot 21}{3 \cdot 2} = 23 \cdot 11 \cdot 7 = 1771$. Thus there are **1771** non-negative integer solutions of $w + x + y + z = 20$.

For another approach to this example, model solutions of $w + x + y + z = 20$ as 20-element multisets made from the elements of $\{w, x, y, z\}$. For example, solution $(5, 5, 4, 6)$ corresponds to $[w, w, w, w, w, x, x, x, x, x, y, y, y, y, z, z, z, z, z, z]$. By Fact 4.7, there are $\binom{20+4-1}{20} = \binom{23}{20} = 1771$ such multisets, so this is the number of solutions to $w + x + y + z = 20$. 


Example 4.21 This problem concerns the lists (w, x, y, z) of integers with the property that $0 \leq w \leq x \leq y \leq z \leq 10$. That is, each entry is an integer between 0 and 10, and the entries are ordered from smallest to largest. For example, $(0, 3, 3, 7)$, $(1, 1, 1, 1)$ and $(2, 3, 6, 9)$ have this property, but $(2, 3, 6, 4)$ does not. How many such lists are there?

Solution: We can encode such a list with 10 stars and 4 bars, where w is the number of stars to the left of the first bar, x is the number of stars to the left of the second bar, y is the number of stars to the left of the third bar, and z is the number of stars to the left of the fourth bar.

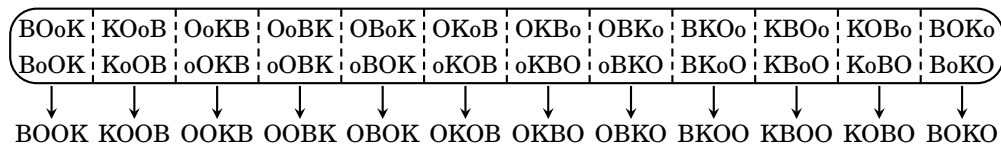
For example, $(2, 3, 6, 9)$ is encoded as $**|*|***|***|*$, and $(1, 2, 3, 4)$ is encoded as $*|*|*|*|*****$.

Here are some other examples of lists paired with their encodings.

(0, 3, 3, 7) | * * * | | * * * * | * * *
 (1, 1, 1, 1) * | | | | * * * * * * * * * *
 (9, 9, 9, 10) * * * * * * * * * * | | | * |

Such encodings are lists of length 14, with 10 stars and 4 bars. We can make such a list by choosing 4 of the 14 slots for the bars and filling the remaining slots with stars. The number of ways to do this is $\binom{14}{4} = 1001$. Answer: There are **1001** such lists. 

We will examine one more type of multiset problem. To motivate it, consider the permutations of the letters of the word “BOOK.” At first glance there are 4 letters, so we should get $4! = 24$ permutations. But this is not quite right because two of the letters are identical. We could interchange the two O’s but still have the same permutation. To get a grip on the problem, let’s make one of the letters lower case: BOoK. Now our 24 permutations are listed below in the oval.



The columns in the oval correspond to the same permutation of the letters of BOOK, as indicated in the row below the oval. Thus there are actually $\frac{4!}{2} = \frac{24}{2} = 12$ permutations of the letters of BOOK.

This is actually a problem about multisets. The letters in “BOOK” form a multiset [B,O,O,K], and we have determined that there are 12 permutations of this multiset.

For another motivational example, consider the permutations of the letters of the word BANANA. Here there are two N’s and three A’s. Though some of the letters look identical, think of them as distinct physical objects that we can permute into different orderings. It helps to subscript the letters to emphasize that they are actually six distinct objects:

$$B A_1 N_1 A_2 N_2 A_3.$$

Now, there are $6! = 720$ permutations of these six letters. It’s not practical to write out all of them, but we can get a sense of the problem by making a partial listing in the box below.

| | | | |
|--|--|-----|---|
| B A ₁ N ₁ A ₂ N ₂ A ₃ | A ₁ B N ₁ A ₂ N ₂ A ₃ | ... | 720 permutations of B A ₁ N ₁ A ₂ N ₂ A ₃ |
| B A ₁ N ₁ A ₃ N ₂ A ₂ | A ₁ B N ₁ A ₃ N ₂ A ₂ | ... | |
| B A ₂ N ₁ A ₁ N ₂ A ₃ | A ₂ B N ₁ A ₁ N ₂ A ₃ | ... | |
| B A ₂ N ₁ A ₃ N ₂ A ₁ | A ₂ B N ₁ A ₃ N ₂ A ₁ | ... | |
| B A ₃ N ₁ A ₂ N ₂ A ₁ | A ₃ B N ₁ A ₂ N ₂ A ₁ | ... | |
| B A ₃ N ₁ A ₁ N ₂ A ₂ | A ₃ B N ₁ A ₁ N ₂ A ₂ | ... | |
| B A ₁ N ₂ A ₂ N ₁ A ₃ | A ₁ B N ₂ A ₂ N ₁ A ₃ | ... | |
| B A ₁ N ₂ A ₃ N ₁ A ₂ | A ₁ B N ₂ A ₃ N ₁ A ₂ | ... | |
| B A ₂ N ₂ A ₁ N ₁ A ₃ | A ₂ B N ₂ A ₁ N ₁ A ₃ | ... | |
| B A ₂ N ₂ A ₃ N ₁ A ₁ | A ₂ B N ₂ A ₃ N ₁ A ₁ | ... | |
| B A ₃ N ₂ A ₂ N ₁ A ₁ | A ₃ B N ₂ A ₂ N ₁ A ₁ | ... | |
| B A ₃ N ₂ A ₁ N ₁ A ₂ | A ₃ B N ₂ A ₁ N ₁ A ₂ | ... | |
| ↓ | ↓ | | |
| BANANA | ABNANA | | |

The first column lists the permutations of B A₁ N₁ A₂ N₂ A₃ corresponding to the word BANANA. By the multiplication principle, the column has 3!2! = 12 permutations because the three A_i's can be permuted in 3! ways within their positions, and the two N_i's can be permuted in 2! ways. Similarly, the second column lists the 3!2! = 12 permutations corresponding to the “word” ABNANA.

All together there are 6! = 720 permutations of B A₁ N₁ A₂ N₂ A₃, and groupings of 12 of them correspond to particular permutations of BANANA. Therefore the total number of permutations of BANANA is $\frac{6!}{3!2!} = \frac{720}{12} = 60$.

The kind of reasoning used here generalizes to the following fact.

Fact 4.8 Suppose a multiset A has n elements, with multiplicities p_1, p_2, \dots, p_k . Then the total number of permutations of A is

$$\frac{n!}{p_1! p_2! \cdots p_k!}.$$

Example 4.22 Count the permutations of the letters in MISSISSIPPI.

Solution: Think of this word as an 11-element multiset with one M, four I's, four S's and two P's. By Fact 4.8, it has $\frac{11!}{1!4!4!2!} = 34,650$ permutations.

Example 4.23 Determine the number of permutations of the multiset $[1, 1, 1, 1, 5, 5, 10, 25, 25]$.

Solution: By Fact 4.8 the answer is $\frac{9!}{4!2!1!2!} = 3780$.

Exercises for Section 4.8

1. How many 10-element multisets can be made from the symbols $\{1, 2, 3, 4\}$?
 2. How many 2-element multisets can be made from the 26 letters of the alphabet?
 3. You have a dollar in pennies, a dollar in nickels, a dollar in dimes, and a dollar in quarters. You give a friend four coins. How many ways can this be done?
 4. A bag contains 20 identical red balls, 20 identical blue balls, 20 identical green balls, and 20 identical white balls. You reach in and grab 15 balls. How many different outcomes are possible?
 5. A bag contains 20 identical red balls, 20 identical blue balls, 20 identical green balls, and **one** white ball. You reach in and grab 15 balls. How many different outcomes are possible?
 6. A bag contains 20 identical red balls, 20 identical blue balls, 20 identical green balls, one white ball, and one black ball. You reach in and grab 20 balls. How many different outcomes are possible?
 7. In how many ways can you place 20 identical balls into five different boxes?
 8. How many lists (x, y, z) of three integers are there with $0 \leq x \leq y \leq z \leq 100$?
 9. A bag contains 50 pennies, 50 nickels, 50 dimes and 50 quarters. You reach in and grab 30 coins. How many different outcomes are possible?
 10. How many non-negative integer solutions does $u + v + w + x + y + z = 90$ have?
 11. How many integer solutions does the equation $w + x + y + z = 100$ have if $w \geq 4$, $x \geq 2$, $y \geq 0$ and $z \geq 0$?
 12. How many integer solutions does the equation $w + x + y + z = 100$ have if $w \geq 7$, $x \geq 0$, $y \geq 5$ and $z \geq 4$?
 13. How many length-6 lists can be made from the symbols $\{A, B, C, D, E, F, G\}$, if repetition is allowed and the list is in alphabetical order? (Examples: BBCEGG, but not BBBAGG.)
 14. How many permutations are there of the letters in the word "PEPPERMINT"?
 15. How many permutations are there of the letters in the word "TENNESSEE"?
 16. A community in Canada's Northwest Territories is known in the local language as "TUKTUYAAQTUUQ." How many permutations does this name have?
 17. You roll a dice six times in a row. How many possible outcomes are there that have two 1's three 5's and one 6?
 18. Flip a coin ten times in a row. How many outcomes have 3 heads and 7 tails?
 19. In how many ways can you place 15 identical balls into 20 different boxes if each box can hold at most one ball?
 20. You distribute 25 identical pieces of candy among five children. In how many ways can this be done?
 21. How many numbers between 10,000 and 99,999 contain one or more of the digits 3, 4 and 8, but no others?
-

4.9 The Division and Pigeonhole Principles

Our final fundamental counting principle is called the **division principle**. Before discussing it, we need some notation. Given a number x , its **floor** $\lfloor x \rfloor$ is x rounded down to the nearest integer. Thus $\lfloor \frac{10}{4} \rfloor = 2$, and $\lfloor 9.31 \rfloor = 9$, and $\lfloor 7 \rfloor = 7$, etc. The **ceiling** of x , denoted $\lceil x \rceil$, is x rounded up to the nearest integer. Thus $\lceil \frac{10}{4} \rceil = 3$, and $\lceil 9.31 \rceil = 10$, and $\lceil 7 \rceil = 7$.

The division principle is often illustrated by a simple situation involving pigeons. Imagine n pigeons that live in k pigeonholes, or boxes. (Possibly $n \neq k$.) At night all the pigeons fly into the boxes. When this happens, some of the k boxes may contain more than one pigeon, and some may be empty. But no matter what, the average number of pigeons per box is $\frac{n}{k}$. Obviously, at least one of the boxes contains $\frac{n}{k}$ or more pigeons. (Because not all the boxes can contain fewer than the average number of pigeons per box.) And because a box must contain a whole number of pigeons, we round up to conclude that at least one box contains $\lceil \frac{n}{k} \rceil$ or more pigeons.

Similarly, at least one box must contain $\frac{n}{k}$ or fewer pigeons, because not all boxes can contain more than the average number of pigeons per box. Rounding down, at least one box contains $\lfloor \frac{n}{k} \rfloor$ or fewer pigeons.

We call this line of reasoning the *division principle*. (Some texts call it the *strong form of the pigeonhole principle*.)

Fact 4.9 (Division Principle)

Suppose n objects are placed into k boxes.

Then at least one box contains $\lceil \frac{n}{k} \rceil$ or more objects,
and at least one box contains $\lfloor \frac{n}{k} \rfloor$ or fewer objects.

This has a useful variant. If $n > k$, then $\frac{n}{k} > 1$, so $\lceil \frac{n}{k} \rceil > 1$, and this means some box contains more than one object. On the other hand, if $n < k$ then $\frac{n}{k} < 1$, so $\lfloor \frac{n}{k} \rfloor < 1$, meaning at least one box is empty. Thus the division principle yields the following consequence, called the *pigeonhole principle*.

Fact 4.10 (Pigeonhole Principle)

Suppose n objects are placed into k boxes.

If $n > k$, then at least one box contains more than one object.

If $n < k$, then at least one box is empty.

The pigeonhole principle is named for the scenario in which n pigeons fly into k pigeonholes (or boxes). If there are more pigeons than boxes ($n > k$)

then some box gets more than one pigeon. And if there are fewer pigeons than boxes ($n < k$) then there must be at least one empty box.

Like the multiplication, addition and subtraction principles, the division and pigeonhole principles are intuitive and obvious, but they can prove things that are not obvious. The challenge is seeing where and how to apply them. Our examples will start simple and get progressively more complex.

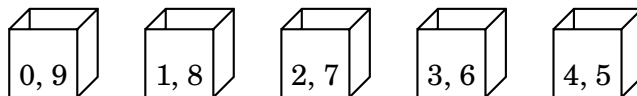
For an extremely simple application, notice that in any group of 13 people, at least two of them were born on the same month. Although this is obvious, it really does follow from the pigeonhole principle. Think of the 13 people as objects, and put each person in the “box” that is his birth month. As there are more people than boxes (months), at least one box (month) has two or more people in it, meaning at least two of the 13 people were born in the same month.


Further, for any group of 100 people, the division principle says that there is a month in which $\lceil \frac{100}{12} \rceil = 9$ or more of the people were born. It also guarantees a month in which $\lfloor \frac{100}{12} \rfloor = 8$ or fewer of the people were born.

Example 4.24 Pick six integers between 0 and 9 (inclusive). Show that two of them must add up to 9.

For example, suppose you picked 0, 1, 3, 5, 7 and 8. Then $1 + 8 = 9$. If you picked 4, 5, 6, 7, 8, 9. then $4 + 5 = 9$. The problem asks us to show that this happens no matter how we pick the numbers.

Solution: Pick six numbers between 0 and 9. Here’s why two of them sum to 9: Imagine five boxes, each marked with two numbers, as shown below. Each box is labeled so that the two numbers written on it sum to 9.

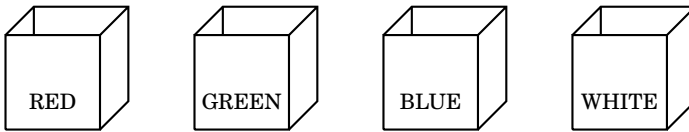


For each number that was picked, put it in the box having that number written on it. For example, if we picked 7, it goes in the box labeled “2, 7.” (The number 2, if picked, would go in that box too.) In this way we place the six chosen numbers in five boxes. As there are more numbers than boxes, the pigeonhole principle says that some box has more than one (hence two) of the picked numbers in it. Those two numbers sum to 9. 

Notice that if we picked only five numbers from 0 to 9, then it’s possible that no two sum to 9: we could be unlucky and pick 0, 1, 2, 3, 4. But the pigeonhole principle ensures that if *six* are picked then two do sum to 9.


Example 4.25 A store has a gumball machine containing a large number of red, green, blue and white gumballs. You get one gumball for each nickel you put into the machine. The store offers the following deal: You agree to buy some number of gumballs, and if 13 or more of them have the same color you get \$5. What is the fewest number of gumballs you need to buy to be 100% certain that you will make money on the deal?

Solution: Let n be the number of gumballs that you buy. Imagine sorting your n gumballs into four boxes labeled RED, GREEN, BLUE, and WHITE. (That is, red balls go in the red box, green balls go in the green box, etc.)



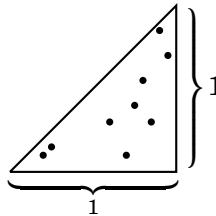
The division principle says that one box contains $\lceil \frac{n}{4} \rceil$ or more gumballs. Provided $\lceil \frac{n}{4} \rceil \geq 13$, you will know you have 13 gumballs of the same color. This happens if $\frac{n}{4} > 12$ (so the ceiling of $\frac{n}{4}$ rounds to a value larger than 12). Therefore you need $n > 4 \cdot 12 = 48$, so if $n = 49$ you know you have at least $\lceil \frac{49}{4} \rceil = \lceil 12.25 \rceil = 13$ gumballs of the same color.

Answer: Buy 49 gumballs for 49 nickels, which is \$2.45. You get \$5, and therefore have made \$2.55.

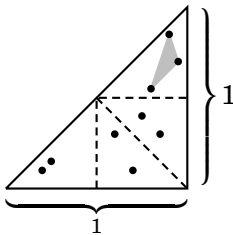
Note that if you bought just 48 gumballs, you might win, but there is a chance that you'd get 12 gumballs of each color and miss out on the \$5. And if you bought more than 49, you'd still get the \$5, but you would have spent more nickels. 


Explicitly mentioning the boxes in the above solution is not necessary. Some people prefer to draw a conclusion based averaging alone. They might solve the problem by letting n be the number of gumballs bought, so $n = r + g + b + w$, where r is the number of them that are red, g is the number that are green, b is the number of blues and w is the number of whites. Then the average number of gumballs of a particular color is $\frac{r + g + b + w}{4} = \frac{n}{4}$. We need this to be greater than 12 to ensure 13 of the same color, and the smallest number that does the job is $n = 49$. This is still the division principle, in a pure form.

Example 4.26 Nine points are randomly placed on the right triangle shown below. Show that three of these points form a triangle whose area is $\frac{1}{8}$ square unit or less. (We allow triangles with zero area, in which case the three points lie on a line.)



Solution: Divide the triangle into four smaller triangles, as indicated by the dashed lines below. Each of these four triangles has an area of



$\frac{1}{2}bh = \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{8}$ square units. Think of these smaller triangles as “boxes.” So we have placed 9 points in 4 boxes. (If one of the 9 points happens to be on a dashed line, say it belongs to the box below or to its left.) The division principle says one of the boxes has at least $\lceil \frac{9}{4} \rceil = 3$ of the points in it. Those three points form a triangle whose area is no larger than the area of the “box” that it is in. Thus these three points form a triangle whose area is $\frac{1}{8}$ or less. 

Exercises for Section 4.9

1. Show that if six numbers are chosen at random, then at least two of them will have the same remainder when divided by 5.
2. You deal a pile of cards, face down, from a standard 52-card deck. What is the least number of cards the pile must have before you can be assured that it contains at least five cards of the same suit?
3. What is the fewest number of times you must roll a six-sided dice before you can be assured that 10 or more of the rolls resulted in the same number?
4. Select any five points on a square whose side-length is one unit. Show that at least two of these points are within $\frac{\sqrt{2}}{2}$ units of each other.
5. Prove that any set of seven distinct natural numbers contains a pair of numbers whose sum or difference is divisible by 10.
6. Given a sphere S , a *great circle* of S is the intersection of S with a plane through its center. Every great circle divides S into two parts. A *hemisphere* is the union of the great circle and one of these two parts. Show that if five points are placed arbitrarily on S , then there is a hemisphere that contains four of them.

4.10 Combinatorial Proof

Combinatorial proof is a method of proving two different expressions are equal by showing that they are both answers to the same counting question. We have already used combinatorial proof (without *calling* it combinatorial proof) in proving Pascal's formula $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$ on page 104.


There we argued that the left-hand side $\binom{n+1}{k}$ is, by definition, the number of k -element subsets of the set $S = \{0, 1, 2, \dots, n\}$ with $|S| = n + 1$. But the right-hand side also gives the number of k -element subsets of S , because such a subset either contains 0 or it does not. We can make any k -element subset of S that contains 0 by starting with 0 and selecting $k - 1$ other elements from $\{1, 2, \dots, n\}$, in $\binom{n}{k-1}$ ways. We can make any k -element subset that does not contain 0 by selecting k elements from $\{1, 2, \dots, n\}$, and there are $\binom{n}{k}$ ways to do this. Thus,

$$\underbrace{\binom{n+1}{k}}_{\substack{\text{number of} \\ k\text{-element} \\ \text{subsets of} \\ S = \{0, 1, \dots, n\}}} = \underbrace{\binom{n}{k-1}}_{\substack{\text{number of} \\ k\text{-element} \\ \text{subsets of} \\ S \text{ with } 0}} + \underbrace{\binom{n}{k}}_{\substack{\text{number of} \\ k\text{-element} \\ \text{subsets of} \\ S \text{ without } 0}}.$$

Both sides count the number of k -element subsets of S , so they are equal. This is combinatorial proof.

Example 4.27 Use combinatorial proof to show $\binom{n}{k} = \binom{n}{n-k}$.

Solution. First, by definition, if $k < 0$ or $k > n$, then both sides are 0, and thus equal. Therefore for the rest of the proof we can assume $0 \leq k \leq n$.

The left-hand side $\binom{n}{k}$ is the number of k -element subsets of $S = \{1, 2, \dots, n\}$. Every k -element subset $X \subseteq S$ pairs with a unique $(n-k)$ -element subset $\bar{X} = S - X \subseteq S$. Thus the number of k -element subsets of S equals the number of $(n-k)$ -element subsets of S , which is to say $\binom{n}{k} = \binom{n}{n-k}$. 

We could also derive $\binom{n}{k} = \binom{n}{n-k}$ by using the formula for $\binom{n}{k}$ and quickly get

$$\binom{n}{n-k} = \frac{n!}{(n-k)!(n-(n-k))!} = \frac{n!}{(n-k)!k!} = \frac{n!}{k!(n-k)!} = \binom{n}{k}.$$

But you may feel that the combinatorial proof is “slicker” because it uses the *meanings* of the terms. Often it is flat-out easier than using formulas, as in the next example.

Our next example will prove that $\sum_{k=0}^n \binom{n}{k}^2 = \binom{2n}{n}$, for any positive integer n , which is to say that $\binom{n}{0}^2 + \binom{n}{1}^2 + \binom{n}{2}^2 + \dots + \binom{n}{n}^2 = \binom{2n}{n}$. For example, if $n = 5$, this statement asserts $\binom{5}{0}^2 + \binom{5}{1}^2 + \binom{5}{2}^2 + \binom{5}{3}^2 + \binom{5}{4}^2 + \binom{5}{5}^2 = \binom{2 \cdot 5}{5}$, that is,

$$1^2 + 5^2 + 10^2 + 10^2 + 5^2 + 1^2 = \binom{10}{5},$$

which is true, as both sides equal 252. In general, the statement says that the squares of the entries in the n th row of Pascal's triangle add up to $\binom{2n}{n}$.

Example 4.28 Use a combinatorial proof to show that $\sum_{k=0}^n \binom{n}{k}^2 = \binom{2n}{n}$.

Solution. First, the right-hand side $\binom{2n}{n}$ is the number of ways to select n things from a set S that has $2n$ elements.

Now let's count this a different way. Divide S into two equal-sized parts, $S = A \cup B$, where $|A| = n$ and $|B| = n$, and $A \cap B = \emptyset$.


For any fixed k with $0 \leq k \leq n$, we can select n things from S by taking k things from A and $n - k$ things from B for a total of $k + (n - k) = n$ things. By the multiplication principle, we get $\binom{n}{k} \binom{n}{n-k}$ n -element subsets of S this way.

As k could be any number from 0 to n , the number of ways to select n things from S is thus

$$\underbrace{\binom{n}{0}}_{\substack{0 \text{ from } A \\ n \text{ from } B}} + \underbrace{\binom{n}{1} \binom{n}{n-1}}_{\substack{1 \text{ from } A \\ n-1 \text{ from } B}} + \underbrace{\binom{n}{2} \binom{n}{n-2}}_{\substack{2 \text{ from } A \\ n-2 \text{ from } B}} + \underbrace{\binom{n}{3} \binom{n}{n-3}}_{\substack{3 \text{ from } A \\ n-3 \text{ from } B}} + \dots + \underbrace{\binom{n}{n} \binom{n}{0}}_{\substack{n \text{ from } A \\ 0 \text{ from } B}}.$$

But because $\binom{n}{n-k} = \binom{n}{k}$, this expression equals $\binom{n}{0} \binom{n}{0} + \binom{n}{1} \binom{n}{1} + \binom{n}{2} \binom{n}{2} + \dots + \binom{n}{n} \binom{n}{n}$, which is $\binom{n}{0}^2 + \binom{n}{1}^2 + \binom{n}{2}^2 + \dots + \binom{n}{n}^2 = \sum_{k=0}^n \binom{n}{k}^2$.

In summary, we've counted the ways to choose n elements from the set S with two methods. One method gives $\binom{2n}{n}$, and the other gives $\sum_{k=0}^n \binom{n}{k}^2$.

Therefore $\sum_{k=0}^n \binom{n}{k}^2 = \binom{2n}{n}$. 

Be on the lookout for opportunities to use combinatorial proof, and watch for it in your readings outside of this course. Also, try some of the exercises below. Sometimes it takes some creative thinking and false starts before you hit on an idea that works, but once you find it the solution is usually remarkably simple.

Exercises for Section 4.10

Use combinatorial proof to solve the following problems. You may assume that any variables m, n, k and p are non-negative integers.

1. Show that $1(n-0) + 2(n-1) + 3(n-2) + 4(n-3) + \cdots + (n-1)2 + (n-0)1 = \binom{n+2}{3}$.
2. Show that $1 + 2 + 3 + \cdots + n = \binom{n+1}{2}$.
3. Show that $\binom{n}{2} \binom{n-2}{k-2} = \binom{n}{k} \binom{k}{2}$.
4. Show that $P(n, k) = P(n-1, k) + k \cdot P(n-1, k-1)$.
5. Show that $\binom{2n}{2} = 2\binom{n}{2} + n^2$.
6. Show that $\binom{3n}{3} = 3\binom{n}{3} + 6n\binom{n}{2} + n^3$.
7. Show that $\sum_{k=0}^p \binom{m}{k} \binom{n}{p-k} = \binom{m+n}{p}$.
8. Show that $\sum_{k=0}^m \binom{m}{k} \binom{n}{p+k} = \binom{m+n}{m+p}$.
9. Show that $\sum_{k=m}^n \binom{k}{m} = \binom{n+1}{m+1}$.
10. Show that $\sum_{k=1}^n k \binom{n}{k} = n2^{n-1}$.
11. Show that $\sum_{k=0}^n 2^k \binom{n}{k} = 3^n$.
12. Show that $\sum_{k=0}^n \binom{n}{k} \binom{k}{m} = \binom{n}{m} 2^{n-m}$.

4.11 Solutions for Chapter 4

Section 4.2

- Consider lists made from the letters T, H, E, O, R, Y , with repetition allowed.
 - How many length-4 lists are there? Answer: $6 \cdot 6 \cdot 6 \cdot 6 = \mathbf{1296}$.
 - How many length-4 lists are there that begin with T ?
Answer: $1 \cdot 6 \cdot 6 \cdot 6 = \mathbf{216}$.
 - How many length-4 lists are there that do not begin with T ?
Answer: $5 \cdot 6 \cdot 6 \cdot 6 = \mathbf{1080}$.
- How many ways can you make a list of length 3 from symbols A, B, C, D, E, F if...
 - ... repetition is allowed. Answer: $6 \cdot 6 \cdot 6 = \mathbf{216}$.
 - ... repetition is not allowed. Answer: $6 \cdot 5 \cdot 4 = \mathbf{120}$.
 - ... repetition is not allowed and the list must contain the letter A .
Answer: $5 \cdot 4 + 5 \cdot 4 + 5 \cdot 4 = \mathbf{60}$.
 - ... repetition is allowed and the list must contain the letter A .
Answer: $6 \cdot 6 \cdot 6 - 5 \cdot 5 \cdot 5 = \mathbf{91}$.

(Note: See Example 4.3 if a more detailed explanation is required.)
- This problem involves 8-digit binary strings such as 10011011 or 00001010. (i.e., 8-digit numbers composed of 0's and 1's.)
 - How many such strings are there? Answer: $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = \mathbf{256}$.
 - How many such strings end in 0? Answer: $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 1 = \mathbf{128}$.
 - How many such strings have the property that their second and fourth digits are 1's? Answer: $2 \cdot 1 \cdot 2 \cdot 1 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = \mathbf{64}$.
 - How many such strings are such that their second **or** fourth digits are 1's?
Solution: These strings can be divided into three types. Type 1 consists of those strings of form $*1*0****$, Type 2 consist of strings of form $*0*1****$, and Type 3 consists of those of form $*1*1****$. By the multiplication principle there are $2^6 = 64$ strings of each type, so **there are $3 \cdot 64 = 192$ 8-digit binary strings whose second or fourth digits are 1's.**
- This problem concerns 4-letter codes made from the letters A, B, C, D, \dots, Z .
 - How many such codes can be made? Answer: $26 \cdot 26 \cdot 26 \cdot 26 = \mathbf{456,976}$
 - How many such codes have no two consecutive letters the same?
Solution: We use the multiplication principle. There are 26 choices for the first letter. The second letter can't be the same as the first letter, so there are only 25 choices for it. The third letter can't be the same as the second letter, so there are only 25 choices for it. The fourth letter can't be the same as the third letter, so there are only 25 choices for it. **Thus there are $26 \cdot 25 \cdot 25 \cdot 25 = 406,250$ codes with no two consecutive letters the same.**
- A new car comes in a choice of five colors, three engine sizes and two transmissions. How many different combinations are there? Answer $5 \cdot 3 \cdot 2 = 30$.

Section 4.3

1. Five cards are dealt off of a standard 52-card deck and lined up in a row. How many such lineups are there that have at least one red card?

Solution: All together there are $52 \cdot 51 \cdot 50 \cdot 49 \cdot 48 = 311875200$ possible lineups. The number of lineups that **do not** have any red cards (i.e. are made up only of black cards) is $26 \cdot 25 \cdot 24 \cdot 23 \cdot 22 = 7,893,600$. By the subtraction principle, the answer to the question is $311,875,200 - 7,893,600 = \mathbf{303,981,600}$.

How many such lineups are there in which the cards are all black or all hearts?

Solution: The number of lineups that are all black is $26 \cdot 25 \cdot 24 \cdot 23 \cdot 22 = 7,893,600$. The number of lineups that are hearts (which are red) is $13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 = 154,440$. By the addition principle, the answer to the question is $7,893,600 + 154,440 = \mathbf{8,048,040}$.

3. Five cards are dealt off of a standard 52-card deck and lined up in a row. How many such lineups are there in which all 5 cards are of the same color (i.e., all black or all red)?

Solution: There are $26 \cdot 25 \cdot 24 \cdot 23 \cdot 22 = 7,893,600$ possible black-card lineups and $26 \cdot 25 \cdot 24 \cdot 23 \cdot 22 = 7,893,600$ possible red-card lineups, so by the addition principle the answer is $7,893,600 + 7,893,600 = \mathbf{15,787,200}$.

5. How many integers between 1 and 9999 have no repeated digits?

Solution: Consider the 1-digit, 2-digit, 3-digit and 4-digit number separately. The number of 1-digit numbers that have no repeated digits is 9 (i.e., all of them). The number of 2-digit numbers that have no repeated digits is $9 \cdot 9 = 81$. (The number can't begin in 0, so there are only 9 choices for its first digit.) The number of 3-digit numbers that have no repeated digits is $9 \cdot 9 \cdot 8 = 648$. The number of 4-digit numbers that have no repeated digits is $9 \cdot 9 \cdot 8 \cdot 7 = 4536$. By the addition principle, the answer to the question is $9 + 81 + 648 + 4536 = \mathbf{5274}$.

How many integers between 1 and 9999 have at least one repeated digit?

Solution: The total number of integers between 1 and 9999 is 9999. Using the subtraction principle, we can subtract from this the number of digits that have *no* repeated digits, which is 5274, as above. Therefore the answer to the question is $9999 - 5274 = \mathbf{4725}$.

7. A password on a certain site must have five characters made from letters of the alphabet, and there must be at least one upper case letter. How many different passwords are there?

Solution: Let U be the set of all possible passwords made from a choice of upper and lower case letters. Let X be the set of all possible passwords made from lower case letters. Then $U - X$ is the set of passwords that have at least one lower case letter. By the subtraction principle our answer will be $|U - X| = |U| - |X|$.

All together, there are $26 + 26 = 52$ upper and lower case letters, so by the multiplication principle $|U| = 52 \cdot 52 \cdot 52 \cdot 52 \cdot 52 = 52^5 = 380,204,032$.

Likewise $|X| = 26 \cdot 26 \cdot 26 \cdot 26 \cdot 26 = 26^5 = 11,881,376$.

Thus the answer is $|U| - |X| = 380,204,032 - 11,881,376 = \mathbf{368,322,656}$.

Section 4.5

1. Suppose a set A has 37 elements. How many subsets of A have 10 elements? How many subsets have 30 elements? How many have 0 elements?
 Answers: $\binom{37}{10} = \mathbf{348,330,136}$; $\binom{37}{30} = \mathbf{10,295,472}$; $\binom{37}{0} = \mathbf{1}$.
3. A set X has exactly 56 subsets with 3 elements. What is the cardinality of X ?
 Solution: The answer will be the n for which $\binom{n}{3} = 56$. After some trial and error, you will discover $\binom{8}{3} = 56$, so $|X| = 8$.
5. How many 16-digit binary strings contain exactly seven 1's?
 Solution: Make such a string as follows. Start with a list of 16 blank spots. Choose 7 of the blank spots for the 1's and put 0's in the other spots. There are $\binom{16}{7} = \mathbf{11,440}$ ways to do this.
7. $|\{X \in \mathcal{P}(\{0,1,2,3,4,5,6,7,8,9\}) : |X| < 4\}| = \binom{10}{0} + \binom{10}{1} + \binom{10}{2} + \binom{10}{3} = 1 + 10 + 45 + 120 = \mathbf{176}$.
9. This problem concerns lists of length six made from the letters A, B, C, D, E, F , without repetition. How many such lists have the property that the D occurs before the A ?
 Solution: Make such a list as follows. Begin with six blank spaces and select two of these spaces. Put the D in the first selected space and the A in the second. There are $\binom{6}{2} = 15$ ways of doing this. For each of these 15 choices there are $4! = 24$ ways of filling in the remaining spaces. Thus the answer to the question is $15 \times 24 = \mathbf{360}$ such lists.
11. How many 10-digit integers contain no 0's and exactly three 6's?
 Solution: Make such a number as follows: Start with 10 blank spaces and choose three of these spaces for the 6's. There are $\binom{10}{3} = 120$ ways of doing this. For each of these 120 choices we can fill in the remaining seven blanks with choices from the digits 1, 2, 3, 4, 5, 7, 8, 9, and there are 8^7 to do this. Thus the answer to the question is $\binom{10}{3} \cdot 8^7 = \mathbf{251,658,240}$.
13. Assume $n, k \in \mathbb{Z}$ with $0 \leq k \leq n$. Then $\binom{n}{k} = \frac{n!}{(n-k)!k!} = \frac{n!}{k!(n-k)!} = \frac{n!}{(n-(n-k))!(n-k)!} = \binom{n}{n-k}$.
15. How many 10-digit binary strings are there that do not have exactly four 1's?
 Solution: All together, there are 2^{10} different binary strings. The number of 10-digit binary strings with exactly four 1's is $\binom{10}{4}$, because to make one we need to choose 4 out of 10 positions for the 1's and fill the rest in with 0's. By the subtraction principle, the answer to our questions is $2^{10} - \binom{10}{4}$.
17. How many 10-digit binary numbers are there that have exactly four 1's or exactly five 1's?
 Solution: By the addition principle the answer is $\binom{10}{4} + \binom{10}{5}$.
 How many do not have exactly four 1's or exactly five 1's?
 Solution: By the subtraction principle combined with the answer to the first part of this problem, the answer is $2^{10} - \binom{10}{4} - \binom{10}{5}$.
19. A 5-card poker hand is called a *flush* if all cards are the same suit. How many different flushes are there?

Solution: There are $\binom{13}{5} = 1287$ 5-card hands that are all hearts. Similarly, there are $\binom{13}{5} = 1287$ 5-card hands that are all diamonds, or all clubs, or all spades. By the addition principle, there are then $1287 + 1287 + 1287 + 1287 = \mathbf{5148}$ flushes.

Section 4.6

- Write out Row 11 of Pascal's triangle.
Answer: 1 11 55 165 330 462 462 330 165 55 11 1
- Use the binomial theorem to find the coefficient of x^8 in $(x+2)^{13}$.
Answer: According to the binomial theorem, the coefficient of x^8y^5 in $(x+y)^{13}$ is $\binom{13}{5}x^8y^5 = 1287x^8y^5$. Now plug in $y=2$ to get the final answer of $41184x^8$.
- Use the binomial theorem to show $\sum_{k=0}^n \binom{n}{k} = 2^n$. Hint: Observe that $2^n = (1+1)^n$. Now use the binomial theorem to work out $(x+y)^n$ and plug in $x=1$ and $y=1$.
- Use the binomial theorem to show $\sum_{k=0}^n 3^k \binom{n}{k} = 4^n$.
Hint: Observe that $4^n = (1+3)^n$. Now look at the hint for the previous problem.
- Use the binomial theorem to show $\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \binom{n}{4} - \binom{n}{5} + \dots \pm \binom{n}{n} = 0$. Hint: Observe that $0 = 0^n = (1+(-1))^n$. Now use the binomial theorem.
- Use the binomial theorem to show $9^n = \sum_{k=0}^n (-1)^k \binom{n}{k} 10^{n-k}$.
Hint: Observe that $9^n = (10+(-1))^n$. Now use the binomial theorem.
- Assume $n \geq 3$. Then $\binom{n}{3} = \binom{n-1}{3} + \binom{n-1}{2} = \binom{n-2}{3} + \binom{n-2}{2} + \binom{n-1}{2} = \dots = \binom{2}{2} + \binom{3}{2} + \dots + \binom{n-1}{2}$.

Section 4.7

- At a certain university 523 of the seniors are history majors or math majors (or both). There are 100 senior math majors, and 33 seniors are majoring in both history and math. How many seniors are majoring in history?
Solution: Let A be the set of senior math majors and B be the set of senior history majors. From $|A \cup B| = |A| + |B| - |A \cap B|$ we get $523 = 100 + |B| - 33$, so $|B| = 523 + 33 - 100 = 456$. **There are 456 history majors.**
- How many 4-digit positive integers are there that are even or contain no 0's?
Solution: Let A be the set of 4-digit even positive integers, and let B be the set of 4-digit positive integers that contain no 0's. We seek $|A \cup B|$. By the multiplication principle $|A| = 9 \cdot 10 \cdot 10 \cdot 5 = 4500$. (Note the first digit cannot be 0 and the last digit must be even.) Also $|B| = 9 \cdot 9 \cdot 9 \cdot 9 = 6561$. Further, $A \cap B$ consists of all even 4-digit integers that have no 0's. It follows that $|A \cap B| = 9 \cdot 9 \cdot 9 \cdot 4 = 2916$. Then the answer to our question is $|A \cup B| = |A| + |B| - |A \cap B| = 4500 + 6561 - 2916 = \mathbf{8145}$.
- How many 7-digit binary strings begin in 1 or end in 1 or have exactly four 1's?
Solution: Let A be the set of such strings that begin in 1. Let B be the set of such strings that end in 1. Let C be the set of such strings that have exactly four 1's. Then the answer to our question is $|A \cup B \cup C|$. Using Equation (4.5) to compute this number, we have $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C| = 2^6 + 2^6 + \binom{7}{4} - 2^5 - \binom{6}{3} - \binom{6}{3} + \binom{5}{2} = 64 + 64 + 35 - 32 - 20 - 20 + 10 = \mathbf{101}$.
- This problem concerns 4-card hands dealt off of a standard 52-card deck. How many 4-card hands are there for which all four cards are of the same suit or all four cards are red?

Solution: Let A be the set of 4-card hands for which all four cards are of the same suit. Let B be the set of 4-card hands for which all four cards are red. Then $A \cap B$ is the set of 4-card hands for which the four cards are either all hearts or all diamonds. The answer to our question is $|A \cup B| = |A| + |B| - |A \cap B| = 4 \binom{13}{4} + \binom{26}{4} - 2 \binom{13}{4} = 2 \binom{13}{4} + \binom{26}{4} = 1430 + 14,950 = \mathbf{16,380}$.

9. A 4-letter list is made from the letters L, I, S, T, E, D according to the following rule: Repetition is allowed, and the first two letters on the list are vowels or the list ends in D . How many such lists are possible?

Solution: Let A be the set of such lists for which the first two letters are vowels, so $|A| = 2 \cdot 2 \cdot 6 \cdot 6 = 144$. Let B be the set of such lists that end in D , so $|B| = 6 \cdot 6 \cdot 6 \cdot 1 = 216$. Then $A \cap B$ is the set of such lists for which the first two entries are vowels and the list ends in D . Thus $|A \cap B| = 2 \cdot 2 \cdot 6 \cdot 1 = 24$. The answer to our question is $|A \cup B| = |A| + |B| - |A \cap B| = 144 + 216 - 24 = \mathbf{336}$.

11. How many 7-digit numbers are even or have exactly three digits equal to 0?

Solution: Let A be the set of 7-digit numbers that are even. By the multiplication principle, $|A| = 9 \cdot 10 \cdot 10 \cdot 10 \cdot 10 \cdot 10 \cdot 5 = 4,500,000$. Let B be the set of 7-digit numbers that have exactly three digits equal to 0. Then $|B| = 9 \cdot \binom{6}{3} \cdot 9 \cdot 9 \cdot 9$. (First digit is anything but 0. Then choose 3 of 6 of the remaining places in the number for the 0's. Finally the remaining 3 places can be anything but 0.)

Note $A \cap B$ is the set of 7-digit numbers that are even and contain exactly three 0's. We can compute $|A \cap B|$ with the addition principle, by dividing $A \cap B$ into two parts: the even 7-digit numbers with three digits 0 and the last digit **is not** 0, and the even 7-digit numbers with three digits 0 and the last digit **is** 0. The first part has $9 \cdot \binom{5}{3} \cdot 9 \cdot 9 \cdot 4$ elements. The second part has $9 \cdot \binom{5}{2} \cdot 9 \cdot 9 \cdot 9 \cdot 1$ elements. Thus $|A \cap B| = 9 \cdot \binom{5}{3} \cdot 9 \cdot 9 \cdot 4 + 9 \cdot \binom{5}{2} \cdot 9 \cdot 9 \cdot 9$.

By the inclusion-exclusion formula, the answer to our question is $|A \cup B| = |A| + |B| - |A \cap B| = 4,500,000 + 9^4 \binom{6}{3} - 9^3 \binom{5}{3} \cdot 4 - 9^4 \binom{5}{2} = 4,536,450$.

13. How many 8-digit binary strings end in 1 or have exactly four 1's?

Solution: Let A be the set of strings that end in 1. By the multiplication principle $|A| = 2^7$. Let B be the number of strings with exactly four 1's. Then $|B| = \binom{8}{4}$ because we can make such a string by choosing 4 of 8 spots for the 1's and filling the remaining spots with 0's. Then $A \cap B$ is the set of strings that end with 1 and have exactly four 1's. Note that $|A \cap B| = \binom{7}{4}$ (make the last entry a 1 and choose 3 of the remaining 7 spots for 1's). By the inclusion-exclusion formula, the number 8-digit binary strings that end in 1 or have exactly four 1's is $|A \cup B| = |A| + |B| - |A \cap B| = 2^7 + \binom{8}{4} - \binom{7}{4} = 163$.

15. How many 10-digit binary strings begin in 1 or end in 1?

Solution: Let A be the set of strings that begin with 1. By the multiplication principle $|A| = 2^9$. Let B be the number of strings that end with 1. By the multiplication principle $|B| = 2^9$. Then $A \cap B$ is the set of strings that begin and end with 1. By the multiplication principle $|A \cap B| = 2^8$. By the inclusion-exclusion formula, the number 10-digit binary strings begin in 1 or end in 1 is $|A \cup B| = |A| + |B| - |A \cap B| = 2^9 + 2^9 - 2^8 = 768$.

Section 4.8

1. How many 10-element multisets can be made from the symbols $\{1, 2, 3, 4\}$?

Answer: $\binom{10+4-1}{10} = \binom{13}{10} = \mathbf{286}$.

3. You have a dollar in pennies, a dollar in nickels, a dollar in dimes and a dollar in quarters. You give four coins to a friend. In how many ways can this be done?

Solution: In giving your friend four coins, you are giving her a 4-element multiset made from elements in $\{1, 5, 10, 25\}$. There are $\binom{4+4-1}{4} = \binom{7}{4} = \mathbf{35}$ such multisets.

5. A bag contains 20 identical red balls, 20 identical blue balls, 20 identical green balls, and one white ball. You reach in and grab 15 balls. How many different outcomes are possible?

Solution: First we count the number of outcomes that don't have a white ball. Modeling this with stars and bars, we are looking at length-17 lists of the form

$$\overbrace{***\cdots*}^{\text{red}} \mid \overbrace{***\cdots*}^{\text{blue}} \mid \overbrace{***\cdots*}^{\text{green}},$$

where there are 15 stars and two bars. Therefore there are $\binom{17}{15}$ outcomes without the white ball. Next we count the outcomes that do have the white ball. Then there are 14 remaining balls in the grab. In counting the ways that they can be selected we can use the same stars-and-bars model above, but this time the list is of length 16 and has 14 stars. There are $\binom{16}{14}$ outcomes. Finally, by the addition principle, the answer to the question is $\binom{17}{15} + \binom{16}{14} = \mathbf{256}$.

7. In how many ways can you place 20 identical balls into five different boxes?

Solution: Let's model this with stars and bars. Doing this we get a list of length 24 with 20 stars and 4 bars, where the first grouping of stars has as many stars as balls in Box 1, the second grouping has as many stars as balls in Box 2, and so on.

$$\overbrace{***\cdots*}^{\text{Box 1}} \mid \overbrace{***\cdots*}^{\text{Box 2}} \mid \overbrace{***\cdots*}^{\text{Box 3}} \mid \overbrace{***\cdots*}^{\text{Box 4}} \mid \overbrace{***\cdots*}^{\text{Box 5}},$$

The number of ways to place 20 balls in the five boxes equals the number of such lists, which is $\binom{24}{20} = \mathbf{10,626}$.

9. A bag contains 50 pennies, 50 nickels, 50 dimes and 50 quarters. You reach in and grab 30 coins. How many different outcomes are possible?

Solution: The stars-and-bars model is

$$\overbrace{***\cdots*}^{\text{pennies}} \mid \overbrace{***\cdots*}^{\text{nickels}} \mid \overbrace{***\cdots*}^{\text{dimes}} \mid \overbrace{***\cdots*}^{\text{quarters}},$$

so there are $\binom{33}{30} = \mathbf{5456}$ outcomes.

11. How many integer solutions does the equation $w + x + y + z = 100$ have if $w \geq 4$, $x \geq 2$, $y \geq 0$ and $z \geq 0$?

Solution: Imagine a bag containing 100 red balls, 100 blue balls, 100 green balls and 100 white balls. Each solution of the equation corresponds to an outcome in selecting 100 balls from the bag, where the selection includes $w \geq 4$ red balls, $x \geq 2$ blue balls, $y \geq 0$ green balls and $z \geq 0$ white balls.

Now let's consider making such a selection. Pre-select 4 red balls and 2 blue balls, so 94 balls remain in the bag. Next the remaining 94 balls are selected. We can calculate the number of ways that this selection can be made with stars and bars, where there are 94 stars and 3 bars, so the list's length is 97.

$$\underbrace{\text{red}}_{*****} \mid \underbrace{\text{blue}}_{*****} \mid \underbrace{\text{green}}_{*****} \mid \underbrace{\text{white}}_{*****},$$

The number of outcomes is thus $\binom{97}{3} = \mathbf{147,440}$.

13. How many length-6 lists can be made from the symbols {A, B, C, D, E, F, G}, if repetition is allowed and the list is in alphabetical order?

Solution: Any such list corresponds to a 6-element multiset made from the symbols {A, B, C, D, E, F, G}. For example, the list AACDDG corresponds to the multiset [A, A, C, D, D, G]. Thus the number of lists equals the number of multisets, which is $\binom{6+7-1}{6} = \binom{12}{6} = \mathbf{924}$.

15. How many permutations are there of the letters in the word "TENNESSEE"?

Solution: By Fact 4.8, the answer is $\frac{9!}{4!2!2!} = \mathbf{3,780}$.

17. You roll a dice six times in a row. How many possible outcomes are there that have two 1's three 5's and one 6?

Solution: This is the number of permutations of the "word" $\square \square \square \square \square \square$. By Fact 4.8, the answer is $\frac{6!}{2!3!1!} = \mathbf{60}$.

19. In how many ways can you place 15 identical balls into 20 different boxes if each box can hold at most one ball?

Solution: Regard each such distribution as a binary string of length 20, where there is a 1 in the i th position precisely if the i th box contains a ball (and zeros elsewhere). The answer is the number of permutations of such a string, which by Fact 4.8 is $\frac{20!}{15!5!} = \mathbf{15,504}$. Alternatively, the answer is the number of ways to choose 15 positions out of 20, which is $\binom{20}{15} = \mathbf{15,504}$.

21. How many numbers between 10,000 and 99,999 contain one or more of the digits 3, 4 and 8, but no others?

Solution: First count the numbers that have three 3's, one 4, and one 8, like 33,348. By Fact 4.8, the number of permutations of this is $\frac{5!}{3!1!1!} = \mathbf{20}$.

By the same reasoning there are 20 numbers that contain three 4's, one 3, and one 8, and 20 numbers that contain three 8's, one 3, and one 4.

Next, consider the numbers that have two 3's, two 4's and one 8, like 33,448. By Fact 4.8, the number of permutations of this is $\frac{5!}{2!2!1!} = \mathbf{30}$.

By the same reasoning there are 30 numbers that contain two 3's, two 8's and one 4, and 30 numbers that contain two 4's, two 8's and one 3. This exhausts all possibilities. By the addition principle the answer is $20+20+20+30+30+30 = \mathbf{150}$.

Section 4.9

1. Show that if 6 integers are chosen at random, at least two will have the same remainder when divided by 5.

Solution: Pick six integers n_1, n_2, n_3, n_4, n_5 and n_6 at random. Imagine five boxes, labeled Box 0, Box 1, Box 2, Box 3, Box 4. Each of the picked integers has a remainder when divided by 5, and that remainder is 0, 1, 2, 3 or 4. For each n_i , let r_i be its remainder when divided by 5. Put n_i in Box r_i . We have now put six numbers in five boxes, so by the pigeonhole principle one of the boxes has two or more of the picked numbers in it. Those two numbers have the same remainder when divided by 5.

3. What is the fewest number of times you must roll a six-sided dice before you can be assured that 10 or more of the rolls resulted in the same number?

Solution: Imagine six boxes, labeled 1 through 6. Every time you roll a \square , put an object in Box 1. Every time you roll a \square , put an object in Box 2, etc. After n rolls, the division principle says that one box contains $\lceil \frac{n}{6} \rceil$ objects, and this means you rolled the same number $\lceil \frac{n}{6} \rceil$ times. We seek the smallest n for which $\lceil \frac{n}{6} \rceil \geq 10$. This is the smallest n for which $\frac{n}{6} > 9$, that is $n > 9 \cdot 6 = 54$. Thus the answer is $n = 55$. You need to roll the dice 55 times.

5. Prove that any set of 7 distinct natural numbers contains a pair of numbers whose sum or difference is divisible by 10.

Solution: Let $S = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7\}$ be any set of 7 natural numbers. Let's say that $a_1 < a_2 < a_3 < \dots < a_7$. Consider the set

$$A = \{a_1 - a_2, a_1 - a_3, a_1 - a_4, a_1 - a_5, a_1 - a_6, a_1 - a_7, \\ a_1 + a_2, a_1 + a_3, a_1 + a_4, a_1 + a_5, a_1 + a_6, a_1 + a_7\}$$

Thus $|A| = 12$. Now imagine 10 boxes numbered 0, 1, 2, ..., 9. For each number $a_1 \pm a_i \in A$, put it in the box whose number is the one's digit of $a_1 \pm a_i$. (For example, if $a_1 \pm a_i = 4$, put it in Box 4. If $a_1 \pm a_i = 8$, put it in Box 8, etc.) Now we have placed the 12 numbers in A into 10 boxes, so the pigeonhole principle says at least one box contains two elements $a_1 \pm a_i$ and $a_1 \pm a_j$ from A . This means the last digit of $a_1 \pm a_i$ is the same as the last digit of $a_1 \pm a_j$. Thus the last digit of the difference $(a_1 \pm a_i) - (a_1 \pm a_j) = \pm a_i \pm a_j$ is 0. Hence $\pm a_i \pm a_j$ is a sum or difference of elements of S that is divisible by 10.

Section 4.10

1. Show that $1(n-0) + 2(n-1) + 3(n-2) + 4(n-3) + \dots + (n-1)2 + (n-0)1 = \binom{n+2}{3}$.

Solution: Let $S = \{0, 1, 2, 3, \dots, n, n+1\}$, which is a set with $n+2$ elements. The right-hand side $\binom{n+2}{3}$ of our equations is the number of 3-element subsets of S .

Let's now count these 3-element subsets in a different way. Any such subset X can be written as $X = \{j, k, \ell\}$, where $0 \leq j < k < \ell \leq n+1$. Note that this forces the middle element k to be in the range $1 \leq k \leq n$. Given a fixed middle element k ,

there are k choices for the smallest element j and $n + 1 - k$ choices for the largest element ℓ .

$$\underbrace{0 \quad 1 \quad 2 \quad \cdots \quad k-1}_{k \text{ choices for } j} \quad \begin{array}{c} k \\ \uparrow \\ \text{middle} \end{array} \quad \underbrace{k+1 \quad k+2 \quad k+3 \quad \cdots \quad n \quad n+1}_{n+1-k \text{ choices for } \ell}$$

By the multiplication principle, there are $k(n + 1 - k)$ possible 3-element sets X with middle element k . For example, if $k = 1$, there are $1(n - 0)$ sets X with middle element 1. If $k = 2$, there are $2(n - 1)$ sets X with middle element 2. If $k = 3$, there are $3(n - 2)$ sets X with middle element 3. Thus the left-hand side of our equation counts up the number of 3-element subsets of S , so it is equal to the right-hand side.

3. Show that $\binom{n}{2}\binom{n-2}{k-2} = \binom{n}{k}\binom{k}{2}$.

Solution: Consider the following problem. From a group of n people, you need to select k people to serve on a committee, and you also need to select 2 of these k people to lead the committee's discussion. In how many ways can this be done?

One approach is to first select k people from n , and then select 2 of these k people to lead the discussion. By the multiplication principle, there are $\binom{n}{k}\binom{k}{2}$ ways to make this selection.

Another approach is to first select 2 of the n people to be the discussion leaders, and there are $\binom{n}{2}$ ways to do this. Next we need to fill out the committee by selecting $k - 2$ people from the remaining $n - 2$ people, and there are $\binom{n-2}{k-2}$ ways to do this. By the multiplication principle, there are $\binom{n}{2}\binom{n-2}{k-2}$ ways to make the selection.

By the previous two paragraphs, $\binom{n}{2}\binom{n-2}{k-2}$ and $\binom{n}{k}\binom{k}{2}$ are both answers to the same counting problem, so they are equal.

5. Show that $\binom{2n}{2} = 2\binom{n}{2} + n^2$.

Solution: Let S be a set with $2n$ elements. Then the left-hand side counts the number of 2-element subsets of S .

Let's now count this in a different way. Split S as $S = A \cup B$, where $|A| = n = |B|$. We can choose a 2-element subset of S in three ways: We could choose both elements from A , and there are $\binom{n}{2}$ ways to do this. We could choose both elements from B , and there are $\binom{n}{2}$ ways to do this. Or we could choose one element from A and then another element from B , and by the multiplication principle there are $n \cdot n = n^2$ ways to do this. Thus the number of 2-element subsets of S is $\binom{n}{2} + \binom{n}{2} + n^2 = 2\binom{n}{2} + n^2$, and this is the right-hand side. Therefore the equation holds because both sides count the same thing.

7. Show that $\sum_{k=0}^p \binom{m}{k}\binom{n}{p-k} = \binom{m+n}{p}$.

Solution: Take three non-negative integers m, n and p . Let S be a set with $|S| = m + n$, so the right-hand side counts the number of p -element subsets of S .

Now let's count this in a different way. Split S as $S = A \cup B$, where $|A| = m$ and $|B| = n$. We can make any p -element subset of S by choosing k of its elements from A in and $p - k$ of its elements from B , for any $0 \leq k \leq p$. There are $\binom{m}{k}$ ways to choose k elements from A , and $\binom{n}{p-k}$ ways to choose $p - k$ elements from B , so there are $\binom{m}{k}\binom{n}{p-k}$ ways to make a p -element subset of S that has k elements from A . As k could be any number between 0 and p , the left-hand side of our equation counts up the p -element subsets of S . Thus the left- and right-hand sides count the same thing, so they are equal.

9. Show that $\sum_{k=m}^n \binom{k}{m} = \binom{n+1}{m+1}$.

Solution: Let $S = \{0, 1, 2, \dots, n\}$, so $|S| = n + 1$. The right-hand side of our equation is the number of subsets X of S with $m + 1$ elements.

Now let's think of a way to make such an $X \subseteq S$ with $|X| = m + 1$. We could begin by selecting a largest element k for X . Now, once we have chosen k , there are k elements in S to the left of k , and we need to choose m of them to go in X (so these, along with k , form the set X).

$$S = \{ \underbrace{0, 1, 2, 3, 4, 5, \dots, k-1}_{\text{choose } m \text{ of these } k \text{ numbers for } X}, \underset{\substack{\uparrow \\ \text{largest} \\ \text{number} \\ \text{in } X}}}{k}, k+1, k+2, k+3, \dots, n \}$$

There are $\binom{k}{m}$ ways to choose these m numbers, so there are $\binom{k}{m}$ subsets of S whose largest element is k . Notice that we must have $m \leq k \leq n$. (The largest element k of X cannot be smaller than m because we need at least m elements on its left.) Summing over all possible largest values in X , we see that $\sum_{k=m}^n \binom{k}{m}$ equals the number of subsets of S with $m + 1$ elements.

The previous two paragraphs show that $\sum_{k=m}^n \binom{k}{m}$ and $\binom{n+1}{m+1}$ are answers to the same counting question, so they are equal.

11. Show that $\sum_{k=0}^n 2^k \binom{n}{k} = 3^n$.

Solution: Consider the problem of counting the number of length- n lists made from the symbols $\{a, b, c\}$, with repetition allowed. There are 3^n such lists, so the right-hand side counts the number of such lists.

On the other hand, given k with $0 \leq k \leq n$, let's count the lists that have exactly k entries unequal to a . There are $2^k \binom{n}{k}$ such lists. (First choose k of n list positions to be filled with b or c , in $\binom{n}{k}$ ways. Then fill these k positions with b 's and c 's in 2^k ways. Fill any remaining positions with a 's.) As k could be any number between 0 and n , the left-hand side of our equation counts up the number of length- n lists made from the symbols $\{a, b, c\}$. Thus the right- and left-hand sides count the same thing, so they are equal.

Discrete Probability

An urban legend has it that one Friday a weatherman announced “*There’s a 50% chance of rain on Saturday, and a 50% chance of rain on Sunday, so there’s a 100% chance of rain this weekend.*” Obviously he was wrong, because under the circumstances there’s still a chance of no rain at all over the weekend. But what is the correct answer?

Here is one approach to the answer. Make a set of four length-2 lists:

$$S = \{RR, RN, NR, NN\}.$$

This set encodes the four possible outcomes for the weather over the weekend. The first letter of each list is either R or N depending on whether there is rain or no-rain on Saturday. The second letter is either R or N depending on whether or not there is rain on Sunday. Thus RN means rain on Saturday and no rain on Sunday; NR means no rain on Saturday but rain on Sunday; RR means rain both days; and NN means no rain over the weekend.

The information suggests that each outcome RR, RN, NR and NN is equally likely to occur: There is a 25% chance of RR, a 25% chance of RN, a 25% chance of NR, and a 25% chance of NN.

We want to determine the chance of rain over the weekend. The event of rain over the weekend corresponds to the subset $\{RR, RN, NR\} \subseteq S$.

$$S = \{RR, RN, NR, NN\}$$

Thus rain over the weekend will occur in three out of four equally likely outcomes, so the weatherman should have said there is a $\frac{3}{4} = 75\%$ chance of rain over the weekend.

This chapter is about probability and computing the probabilities of events. The above example sets up the main ideas and definitions that are needed. Given a situation with a finite number of possible outcomes (like whether or not there’s rain over the weekend), its *sample space* is the set S of all possible outcomes, and an *event* (like rain over the weekend) is a subset of S . Let’s set up these ideas carefully.

5.1 Sample Spaces, Events and Probability

In the study of probability, an **experiment** is an activity that produces one of a number of different outcomes that cannot be determined in advance. The **sample space** of the experiment is the set S of all possible outcomes. An **event** is a subset $E \subseteq S$. We say the **event occurs** if the experiment is performed and the outcome is an element of E .

One example of an experiment was described on the previous page: Observe whether it rains on each day of a weekend, and record the result as one of RR, RN, NR or NN. The sample space of this experiment is the set $S = \{\text{RR}, \text{RN}, \text{NR}, \text{NN}\}$. The event of rain over the weekend is the subset $E = \{\text{RR}, \text{RN}, \text{NR}\} \subseteq S$. If we perform the experiment and the outcome is one RR, RN or NR, in E , then we say the event E occurs.

There are numerous other events associated with this experiment. The event of rain on Saturday is the subset $E' = \{\text{RR}, \text{RN}\} \subseteq S$. Here are some other events $E \subseteq S = \{\text{RR}, \text{RN}, \text{NR}, \text{NN}\}$ for this experiment.

| Event | probability of event |
|---|--|
| Rain over the weekend: $E = \{\text{RR}, \text{RN}, \text{NR}\}$ | $p(E) = \frac{ E }{ S } = \frac{3}{4} = 75\%$ |
| Rain on Sunday: $E = \{\text{RR}, \text{NR}\}$ | $p(E) = \frac{ E }{ S } = \frac{2}{4} = 50\%$ |
| No rain over weekend: $E = \{\text{NN}\}$ | $p(E) = \frac{ E }{ S } = \frac{1}{4} = 25\%$ |
| Rain on just one day: $E = \{\text{RN}, \text{NR}\}$ | $p(E) = \frac{ E }{ S } = \frac{1}{2} = 50\%$ |
| Nothing happens: $E = \emptyset$ | $p(E) = \frac{ E }{ S } = \frac{0}{4} = 0\%$ |
| Something happens: $E = \{\text{RR}, \text{RN}, \text{NR}, \text{NN}\}$ | $p(E) = \frac{ E }{ S } = \frac{4}{4} = 100\%$ |

The **probability** or **chance** of an event is the likelihood of its occurring when the experiment is performed. The probability of an event is a number from 0 to 1 (that is, from a 0% chance of occurring to a 100% chance of occurring). We denote the probability of E as $p(E)$. Thus, the experiment of recording the weather over the weekend when there is a 50% chance of rain on each day, the probability of the event $E = \{\text{RR}, \text{RN}, \text{NR}\}$ is $p(E) = 75\%$, as calculated on the previous page.

In many cases, all outcomes in a sample space are equally likely to occur. This is the case in the above weekend weather experiment, where each outcome RR, RN, NR, or NN has a 25% chance of occurring. In such a situation, an event E occurs in $|E|$ out of $|S|$ equally likely outcomes, so its probability is $p(E) = \frac{|E|}{|S|}$. See the right-hand column of the above table.

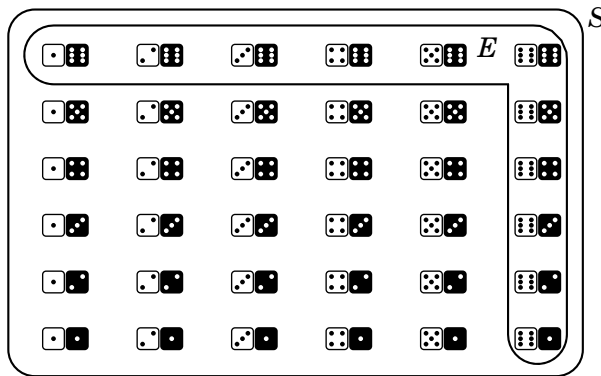
This type of reasoning leads to a formula for the probability of an event when all outcomes in a sample space are equally likely to occur.

Fact 5.1 In an experiment where all outcomes in the sample space S are equally likely to occur, the probability of an event $E \subseteq S$ is

$$p(E) = \frac{|E|}{|S|}.$$

Example 5.1 You have two dice, a white one and a black one. You roll both of them. What is the probability that at least one of them will be a six?

Solution. The sample space S is drawn below, showing the 36 equally likely outcomes. The event $E \subseteq S$ of at least one six is also shown.



Note that you will get at least one six in $|E| = 11$ out of $|S| = 36$ equally likely outcomes, so Fact 5.1 says the probability of getting at least one six is

$$p(E) = \frac{|E|}{|S|} = \frac{11}{36} = 0.30\bar{5} = 30.\bar{5}\%.$$


This means that if you roll the pair of dice, say, 100 times, you should expect to get at least one six on about 30 of the rolls. Try it.

Fact 5.1 applies only to situations in which all outcomes in a sample space are equally likely to occur. For an example of an experiment that does not meet this criterion, imagine that one of the dice in Example 5.1 was weighted so that it was more likely to land on six. Then the outcome $\{6,6\}$ would be more likely than the outcome (say) $\{1,1\}$, and Fact 5.1 would not apply. In such a case $p(E)$ would be greater than $30.\bar{5}\%$. We will treat this kind of situation in Section 5.4. Until then, all of our experiments will have outcomes that are equally likely, and we will use Fact 5.1 freely.

Example 5.2 You toss a coin three times in a row. What is the probability of getting at least one tail?

Solution. Denote a typical outcome as a length-3 list such as HTH, which means you rolled a head first, then a tail, and then a head. Here is the sample space S and the event E of at least one tail:

$$S = \{ \text{HHH}, \overbrace{\{ \text{HHT}, \text{HTH}, \text{HTT}, \text{THH}, \text{THT}, \text{TTH}, \text{TTT} \}}^E \}$$

The chance of getting at least one tail is $p(E) = \frac{|E|}{|S|} = \frac{7}{8} = 0.875 = \mathbf{87.5\%}$. 

Example 5.3 You deal a 5-card hand from a shuffled deck of 52 cards. What is the probability that all five cards are of the same suit?

Solution. The sample space S consists of all possible 5-card hands. Such a hand is a 5-element subset of the set of 52 cards, so we could begin writing out S as something like

$$S = \left\{ \left\{ \begin{array}{c} 7 \\ \clubsuit \end{array} \right\}, \left\{ \begin{array}{c} 2 \\ \clubsuit \end{array} \right\}, \left\{ \begin{array}{c} 3 \\ \heartsuit \end{array} \right\}, \left\{ \begin{array}{c} A \\ \spadesuit \end{array} \right\}, \left\{ \begin{array}{c} 5 \\ \diamondsuit \end{array} \right\} \right\}, \left\{ \begin{array}{c} 8 \\ \heartsuit \end{array} \right\}, \left\{ \begin{array}{c} 2 \\ \heartsuit \end{array} \right\}, \left\{ \begin{array}{c} K \\ \heartsuit \end{array} \right\}, \left\{ \begin{array}{c} A \\ \heartsuit \end{array} \right\}, \left\{ \begin{array}{c} 5 \\ \heartsuit \end{array} \right\} \right\}, \dots \dots \left. \right\}.$$


However, this is too big to write out conveniently in its entirety. But note that $|S|$ is the number of ways to select 5 cards from 52 cards, so

$$|S| = \binom{52}{5} = \frac{52!}{5!(52-5)!} = \frac{52 \cdot 51 \cdot 50 \cdot 49 \cdot 48}{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1} = 2,598,960.$$

Now consider the event $E \subseteq S$ consisting of all 5-card hands in S that are of the same suit. We can compute $|E|$ using the addition principle (Fact 4.2 on page 88). The set E can be divided into four parts: the hands that are all hearts, the hands that are all diamonds, the hands that are all clubs and the hands that are all spades.

As the deck has 13 heart cards, the number of 5-card hands that are all hearts is $\binom{13}{5} = \frac{13 \cdot 12 \cdot 11 \cdot 10 \cdot 9}{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1} = 1287$. For the same reason, the number of 5-card hands that are all diamonds is also 1287. This is also the number of 5-card hands that are all clubs, and the number of 5-card hands that are all spades. By the addition principle, $|E| = 1287 + 1287 + 1287 + 1287 = 5148$.

Thus the probability that all cards in the hand are of the same suit is thus $p(E) = \frac{|E|}{|S|} = \frac{5148}{2,598,960} \approx 0.00198 = \mathbf{0.198\%}$.

So in playing cards, you should expect to be dealt a 5-card hand of the same suit only approximately 2 out of 1000 times. 

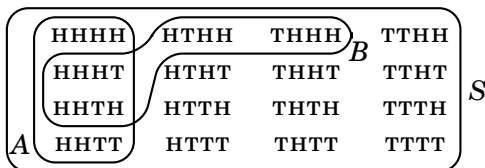
Exercises for Section 5.1

For each problem, write out the sample space S (or describe it if it's too big to write out) and find $|S|$. Then write out or describe the relevant event E . Find $p(E) = \frac{|E|}{|S|}$. You may need to use various counting techniques from Chapter 4

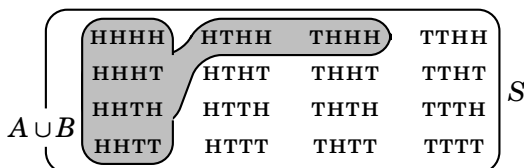
1. A card is randomly selected from a deck of 52 cards. What is the chance that the card is red or a king?
 2. A card is randomly selected from a deck of 52 cards. What is the chance that the card is red but not a king?
 3. Toss a dice 5 times in a row. What is the probability that you don't get any 6's?
 4. Toss a dice 6 times in a row. What is the probability that exactly three of the tosses are even?
 5. Toss a dice 5 times in a row. What is the probability that you will get the same number on each roll? (i.e. $\square\square\square\square\square$ or $\square\square\square\square\square$, etc.)
 6. Toss a dice 5 times in a row. What is the probability that every roll is a different number?
 7. You have a pair of dice, a white one and a black one. Toss them both. What is the probability that they show the same number?
 8. You have a pair of dice, a white one and a black one. Toss them both. What is the probability that the numbers add up to 7?
 9. You have a pair of dice, a white one and a black one. Toss them both. What is the probability that both show even numbers?
 10. Toss a coin 8 times. What is the probability of getting exactly two heads?
 11. Toss a coin 8 times. Find the probability that the first and last tosses are heads.
 12. A hand of four cards is dealt off of a shuffled 52-card deck. What is the probability that all four cards are of the same color? (All red or all black.)
 13. Five cards are dealt from a shuffled 52-card deck. What is the probability of getting three red cards and two clubs?
 14. A coin is tossed 7 times. What is the probability that there are more tails than heads? What if it is tossed 8 times?
 15. Alice and Bob each randomly pick an integer from 0 to 9. What is the probability that they pick the same number? What is the probability that they pick different numbers?
 16. Alice and Bob each randomly pick an integer from 0 to 9. What is the probability that Alice picks an even number and Bob picks an odd number?
 17. What is the probability that a 5-card hand dealt off a shuffled 52-card deck does not contain an ace?
 18. What is the probability that a 5-card hand dealt off a shuffled 52-card deck does not contain any red cards?
-

5.2 Combining Events

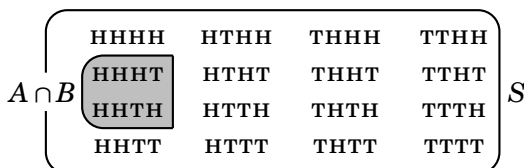
Now we begin combining events. To illustrate this, imagine tossing a coin four times in a row. Let A be the event “*The first two tosses are heads,*” and let B be the event “*There are exactly three heads.*” The sample space S is shown below, along with the events A and B . Note that $p(A) = \frac{|A|}{|S|} = \frac{4}{16} = 25\%$ and $p(B) = \frac{|B|}{|S|} = \frac{4}{16} = 25\%$.



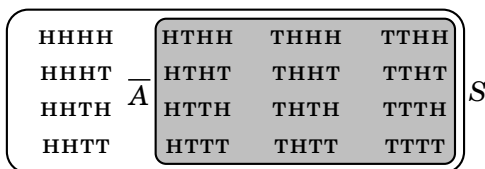
Now, the union $A \cup B$ is a subset of S , so it is an event. Think of it as the event “*The first two tosses are heads or there are exactly three heads.*” This is diagramed below, and we see that $p(A \cup B) = \frac{|A \cup B|}{|S|} = \frac{6}{16} = 37.5\%$.



Also, the intersection $A \cap B$ is a subset of S , so it is an event. It is the event “*The first two tosses are heads and there are exactly three heads.*” This is diagramed below. Note that $p(A \cap B) = \frac{|A \cap B|}{|S|} = \frac{2}{16} = 12.5\%$.



Finally, regard S as a universal set and consider the complement $\bar{A} \subseteq S$, drawn below. This is yet another event. It is the event “*It is not the case that the first two tosses are heads.*” We have $p(\bar{A}) = \frac{|\bar{A}|}{|S|} = \frac{12}{16} = 75\%$.

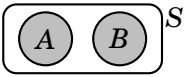


In general, if A and B are events in a sample space, then:

$A \cup B$ is the event “ A **or** B occurs,”
 $A \cap B$ is the event “ A **and** B occur,”
 \bar{A} is the event “ A **does not** occur.”

This section develops formulas for $p(A \cup B)$ and $p(\bar{A})$, while the next section treats $p(A \cap B)$. These formulas will be useful because often a complex event has form $E = A \cup B$ or $E = \bar{A}$, where A and B (or \bar{A}) are easier to deal with than E . In such cases formulas for $p(A \cup B)$ and $p(\bar{A})$ can be handy. But before stating them, we need to lay out a definition.

Definition 5.1 Two events A and B in a sample space S are **mutually exclusive** if $A \cap B = \emptyset$.



Mutually exclusive events have no outcomes in common: If one of them occurs, then the other does not occur. On any trial of the experiment, one of them may occur, or the other, or neither, but *never both*.

Events A and B from the previous page are *not* mutually exclusive, as $A \cap B = \{\text{HHHT}, \text{HHTH}\} \neq \emptyset$. You can toss a coin four times and have both events A : *First two tosses are heads*, and B : *Exactly three heads* occur.

Again, toss a coin four times. Say A is the event “*Exactly three tails*,” and B is “*Exactly three heads*.” These events are mutually exclusive. You could get three heads, or three tails, or neither (HHTT), but you cannot get three heads **and** three tails in the same four tosses.

Also, if E is any event in a sample space, then E and \bar{E} are mutually exclusive, as $E \cap \bar{E} = \emptyset$. An event E cannot both happen and not happen.

Now we are ready to derive our formula for $p(A \cup B)$. We will get it using Fact 5.1 and the inclusion-exclusion principle (Fact 4.6 on page 107) that states $|A \cup B| = |A| + |B| - |A \cap B|$. Simply observe that

$$\begin{aligned}
 p(A \cup B) &= \frac{|A \cup B|}{|S|} = \frac{|A| + |B| - |A \cap B|}{|S|} = \frac{|A|}{|S|} + \frac{|B|}{|S|} - \frac{|A \cap B|}{|S|} \\
 &= \boxed{p(A) + p(B) - p(A \cap B)}.
 \end{aligned}$$

Note that if A and B happen to be mutually exclusive, then $|A \cap B| = |\emptyset| = 0$, and we get simply $p(A \cup B) = p(A) + p(B)$.

For the formula for $p(\bar{A})$, use $\bar{A} = S - A$ and note that

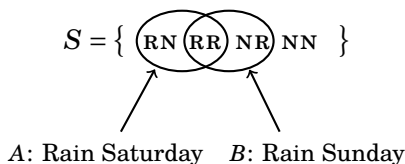
$$p(\bar{A}) = \frac{|\bar{A}|}{|S|} = \frac{|S - A|}{|S|} = \frac{|S| - |A|}{|S|} = \frac{|S|}{|S|} - \frac{|A|}{|S|} = \boxed{1 - p(A)}.$$

Rearranging $p(\bar{A}) = 1 - p(A)$ gives $p(A) = 1 - p(\bar{A})$, also a useful formula. In summary, we have deduced the following facts.

Fact 5.2 Suppose A and B are events in a sample space S . Then:

1. $p(A \cup B) = p(A) + p(B) - p(A \cap B)$
2. $p(A \cup B) = p(A) + p(B)$ if A and B are mutually exclusive
3. $p(\bar{A}) = 1 - p(A)$
4. $p(A) = 1 - p(\bar{A})$

Recall our weatherman that we began the chapter with, the one who said that because there was a 50% chance of rain on Saturday and a 50% chance of rain on Sunday, then there was a 100% chance of rain over the weekend. He had only a hazy understanding of the events A : *Rain on Saturday*, and B : *Rain on Sunday*, and their union $A \cup B$: *Rain over the weekend*.



From the data $p(A) = 50\%$ and $p(B) = 50\%$ he concluded $p(A \cup B) = p(A) + p(B) = 50\% + 50\% = 100\%$. The problem is that A and B are not mutually exclusive, as $A \cap B = \{\text{RR}\} \neq \emptyset$. In essence he was using Formula 2 of Fact 5.2, above, when he should have used Formula 1. The correct chance of rain over the weekend, as given by Formula 1, is

$$p(A \cup B) = p(A) + p(B) - p(A \cap B) = \frac{|A|}{|S|} + \frac{|B|}{|S|} - \frac{|\{\text{RR}\}|}{|S|} = \frac{2}{4} + \frac{2}{4} - \frac{1}{4} = \frac{3}{4} = 75\%.$$

Of course we can also get this answer without the aid of the formula $p(A \cup B) = p(A) + p(B) - p(A \cap B)$. Just let $E = A \cup B$ be the event of rain over the weekend. Fact 5.1, which states $p(E) = \frac{|E|}{|S|}$, says $p(E) = \frac{3}{4} = 75\%$. But a word of caution is in order. Recall that Fact 5.1 is only valid in situations in which all outcomes in S are equally likely to occur. Such is the case in this rain-over-the-weekend example (and all other examples in the next three sections), so we do not get into trouble. But the point is that the formulas from Fact 5.2 turn out to hold even if not all outcomes in S are equally likely (even though we derived them under that assumption on the previous page). We will investigate this thoroughly in Section 5.4.

For now, let's do some examples involving Fact 5.2.

Example 5.4 Two cards are dealt from a shuffled deck of 52 cards. What is the probability that both cards are red or both cards are clubs.

Solution. Regard a 2-card hand as a 2-element subset of the set of 52 cards. So the sample space is the set S of 2-element subsets of the 52 cards.

$$S = \left\{ \left\{ \begin{array}{|c|} \hline 7 \\ \hline \spadesuit \\ \hline \end{array}, \begin{array}{|c|} \hline 2 \\ \hline \clubsuit \\ \hline \end{array} \right\}, \left\{ \begin{array}{|c|} \hline 8 \\ \hline \heartsuit \\ \hline \end{array}, \begin{array}{|c|} \hline 2 \\ \hline \heartsuit \\ \hline \end{array} \right\}, \left\{ \begin{array}{|c|} \hline K \\ \hline \spadesuit \\ \hline \end{array}, \begin{array}{|c|} \hline 2 \\ \hline \heartsuit \\ \hline \end{array} \right\}, \left\{ \begin{array}{|c|} \hline K \\ \hline \clubsuit \\ \hline \end{array}, \begin{array}{|c|} \hline 2 \\ \hline \heartsuit \\ \hline \end{array} \right\}, \dots \right\}.$$

Though this is too large to write out, we can compute $|S| = \binom{52}{2} = \frac{52 \cdot 51}{2} = 1326$.

We are asked to compute $p(E)$ where E is the event

E : Both cards are red **or** both cards are clubs.

We can decompose E as $E = A \cup B$ where A and B are the events

A : Both cards are red

B : Both cards are clubs

Thus $A = \left\{ \left\{ \begin{array}{|c|} \hline K \\ \hline \heartsuit \\ \hline \end{array}, \begin{array}{|c|} \hline K \\ \hline \diamondsuit \\ \hline \end{array} \right\}, \left\{ \begin{array}{|c|} \hline K \\ \hline \heartsuit \\ \hline \end{array}, \begin{array}{|c|} \hline 2 \\ \hline \heartsuit \\ \hline \end{array} \right\}, \left\{ \begin{array}{|c|} \hline 8 \\ \hline \diamondsuit \\ \hline \end{array}, \begin{array}{|c|} \hline 2 \\ \hline \heartsuit \\ \hline \end{array} \right\}, \left\{ \begin{array}{|c|} \hline Q \\ \hline \diamondsuit \\ \hline \end{array}, \begin{array}{|c|} \hline K \\ \hline \diamondsuit \\ \hline \end{array} \right\}, \dots \right\} \subseteq S$,

and $B = \left\{ \left\{ \begin{array}{|c|} \hline K \\ \hline \clubsuit \\ \hline \end{array}, \begin{array}{|c|} \hline 5 \\ \hline \clubsuit \\ \hline \end{array} \right\}, \left\{ \begin{array}{|c|} \hline 7 \\ \hline \clubsuit \\ \hline \end{array}, \begin{array}{|c|} \hline 8 \\ \hline \clubsuit \\ \hline \end{array} \right\}, \left\{ \begin{array}{|c|} \hline J \\ \hline \clubsuit \\ \hline \end{array}, \begin{array}{|c|} \hline Q \\ \hline \clubsuit \\ \hline \end{array} \right\}, \left\{ \begin{array}{|c|} \hline J \\ \hline \clubsuit \\ \hline \end{array}, \begin{array}{|c|} \hline 7 \\ \hline \clubsuit \\ \hline \end{array} \right\}, \dots \right\} \subseteq S$.

Note that these two events are mutually exclusive, as club cards are black. Further, $|A| = \binom{26}{2} = 325$ because to make a 2-card hand of red cards we have to choose 2 of the 26 red cards. Also, $|B| = \binom{13}{2} = 78$ because to make a 2-card hand of club cards we have to choose 2 of the 13 clubs. Using Formula 2 from Fact 5.2 as well as Fact 5.1 (page 138), our answer is

$$\begin{aligned} p(E) &= p(A \cup B) = p(A) + p(B) = \frac{|A|}{|S|} + \frac{|B|}{|S|} \\ &= \frac{325}{1326} + \frac{78}{1326} = \frac{403}{1326} \approx 0.3039 = \mathbf{30.39\%}. \quad \blacktriangleleft \end{aligned}$$

You may prefer to solve this example without using Fact 5.2. Instead you can use Fact 5.1 combined with the addition principle, $|A \cup B| = |A| + |B|$, which holds when $A \cap B = \emptyset$ (as is the case here because A and B are mutually exclusive). Then compute the answer as

$$p(E) = p(A \cup B) = \frac{|A \cup B|}{|S|} = \frac{|A| + |B|}{|S|} = \frac{325 + 78}{1326} = \frac{403}{1326} \approx \mathbf{30.39\%}.$$

But as noted on the previous page, there will be situations where Fact 5.2 is unavoidable. So it is not advisable to always bypass it. For now your best strategy is to become accustomed to it, but at the same time be on the lookout for alternate methods.

Example 5.5 Two cards are dealt from a shuffled deck of 52 cards. What is the probability both cards are red or both cards are face cards (J, K, Q)?

Solution. As before, the sample space is the set S of 2-element subsets of the 52 cards, and $|S| = \binom{52}{2} = 1326$:

$$S = \left\{ \left\{ \begin{array}{|c|} \hline 7 \\ \hline \clubsuit \\ \hline \end{array}, \begin{array}{|c|} \hline 2 \\ \hline \clubsuit \\ \hline \end{array} \right\}, \left\{ \begin{array}{|c|} \hline 8 \\ \hline \heartsuit \\ \hline \end{array}, \begin{array}{|c|} \hline 2 \\ \hline \heartsuit \\ \hline \end{array} \right\}, \left\{ \begin{array}{|c|} \hline K \\ \hline \spadesuit \\ \hline \end{array}, \begin{array}{|c|} \hline 2 \\ \hline \heartsuit \\ \hline \end{array} \right\}, \left\{ \begin{array}{|c|} \hline K \\ \hline \clubsuit \\ \hline \end{array}, \begin{array}{|c|} \hline 2 \\ \hline \heartsuit \\ \hline \end{array} \right\}, \dots \right\}.$$

We are asked to compute $p(E)$ where E is the event

E: Both cards are red or both cards are clubs.

We can decompose E as $E = A \cup B$ where A and B are the events

A: Both cards are red

B: Both cards are face cards

Let's take a moment to diagram these two events, and their intersection.

$$\begin{aligned} A &= \left\{ \left\{ \begin{array}{|c|} \hline K \\ \hline \heartsuit \\ \hline \end{array}, \begin{array}{|c|} \hline K \\ \hline \diamondsuit \\ \hline \end{array} \right\}, \left\{ \begin{array}{|c|} \hline K \\ \hline \heartsuit \\ \hline \end{array}, \begin{array}{|c|} \hline 2 \\ \hline \heartsuit \\ \hline \end{array} \right\}, \left\{ \begin{array}{|c|} \hline 8 \\ \hline \diamondsuit \\ \hline \end{array}, \begin{array}{|c|} \hline 2 \\ \hline \heartsuit \\ \hline \end{array} \right\}, \left\{ \begin{array}{|c|} \hline Q \\ \hline \diamondsuit \\ \hline \end{array}, \begin{array}{|c|} \hline K \\ \hline \diamondsuit \\ \hline \end{array} \right\}, \dots \right\} \subseteq S. \\ B &= \left\{ \left\{ \begin{array}{|c|} \hline K \\ \hline \heartsuit \\ \hline \end{array}, \begin{array}{|c|} \hline K \\ \hline \diamondsuit \\ \hline \end{array} \right\}, \left\{ \begin{array}{|c|} \hline K \\ \hline \spadesuit \\ \hline \end{array}, \begin{array}{|c|} \hline J \\ \hline \spadesuit \\ \hline \end{array} \right\}, \left\{ \begin{array}{|c|} \hline J \\ \hline \diamondsuit \\ \hline \end{array}, \begin{array}{|c|} \hline Q \\ \hline \heartsuit \\ \hline \end{array} \right\}, \left\{ \begin{array}{|c|} \hline Q \\ \hline \diamondsuit \\ \hline \end{array}, \begin{array}{|c|} \hline J \\ \hline \clubsuit \\ \hline \end{array} \right\}, \dots \right\} \subseteq S. \\ A \cap B &= \left\{ \left\{ \begin{array}{|c|} \hline K \\ \hline \heartsuit \\ \hline \end{array}, \begin{array}{|c|} \hline K \\ \hline \diamondsuit \\ \hline \end{array} \right\}, \left\{ \begin{array}{|c|} \hline K \\ \hline \diamondsuit \\ \hline \end{array}, \begin{array}{|c|} \hline Q \\ \hline \diamondsuit \\ \hline \end{array} \right\}, \left\{ \begin{array}{|c|} \hline J \\ \hline \diamondsuit \\ \hline \end{array}, \begin{array}{|c|} \hline Q \\ \hline \heartsuit \\ \hline \end{array} \right\}, \left\{ \begin{array}{|c|} \hline Q \\ \hline \diamondsuit \\ \hline \end{array}, \begin{array}{|c|} \hline J \\ \hline \diamondsuit \\ \hline \end{array} \right\}, \dots \right\} \subseteq S. \end{aligned}$$

Note that A and B are not mutually exclusive, because $A \cap B \neq \emptyset$. (It is possible for the two cards to be *both red and both face cards*.) Also,

$$|A| = \binom{26}{2} = \frac{26 \cdot 25}{2} = 325 \quad (\text{choose 2 out of 26 red cards})$$

$$|B| = \binom{12}{2} = \frac{12 \cdot 11}{2} = 66 \quad (\text{choose 2 out of 12 face cards})$$

$$|A \cap B| = \binom{6}{2} = \frac{6 \cdot 5}{2} = 15 \quad (\text{choose 2 out of 6 red face cards})$$

Using Fact 5.2, we get

$$\begin{aligned} p(E) &= p(A \cup B) = p(A) + p(B) - p(A \cap B) = \frac{|A|}{|S|} + \frac{|B|}{|S|} - \frac{|A \cap B|}{|S|} \\ &= \frac{325}{1326} + \frac{66}{1326} - \frac{15}{1326} = \frac{376}{1326} \approx 0.2835 = \mathbf{28.35\%}. \end{aligned}$$

Example 5.6 Two cards from dealt off a shuffled deck of 52 cards. What is the probability they are not both red?

Solution. The sample space is the set S of 2-element subsets of the 52 cards, and $|S| = \binom{52}{2} = 1326$:

$$S = \left\{ \underbrace{\left\{ \begin{array}{|c|} \hline 7 \\ \hline \clubsuit \end{array}, \begin{array}{|c|} \hline 2 \\ \hline \clubsuit \end{array} \right\}, \left\{ \begin{array}{|c|} \hline K \\ \hline \spadesuit \end{array}, \begin{array}{|c|} \hline 2 \\ \hline \heartsuit \end{array} \right\}, \left\{ \begin{array}{|c|} \hline 8 \\ \hline \heartsuit \end{array}, \begin{array}{|c|} \hline 2 \\ \hline \spadesuit \end{array} \right\} \cdots \left\{ \begin{array}{|c|} \hline K \\ \hline \heartsuit \end{array}, \begin{array}{|c|} \hline 2 \\ \hline \heartsuit \end{array} \right\}, \left\{ \begin{array}{|c|} \hline K \\ \hline \diamondsuit \end{array}, \begin{array}{|c|} \hline 2 \\ \hline \heartsuit \end{array} \right\} \cdots \right\}_{\substack{E: \text{Not both red} \\ \bar{E}: \text{Both red}}}$$


We need to compute the probability of the event E : *Not both cards are red*. This event contains pairs of cards that are both black, as well as those for which one card is red and the other is black. The event \bar{E} is simpler. It is the set of all elements of S for which it is not the case that not both cards are red. In other words, \bar{E} is the event \bar{E} : *Both cards are red*.

It is easy to compute the cardinality of \bar{E} . It is $|\bar{E}| = \binom{26}{2} = 325$, the number of ways to choose 2 cards from the 26 red cards. Fact 5.2 now gives our solution:

$$p(E) = 1 - p(\bar{E}) = 1 - \frac{|\bar{E}|}{|S|} = 1 - \frac{325}{1326} = \frac{1326 - 325}{1326} = \frac{1001}{1326} \approx 0.7549 = \mathbf{75.49\%}.$$

That is the answer, but before moving on, let's redo the problem using a different approach. The event E is the union of the mutually exclusive events A : *Both cards are black*, and B : *One card is black and the other is red*. Here $|A| = \binom{26}{2} = 325$, the number of ways to choose 2 cards from the 26 blacks, while the multiplication principle says $|B| = 26 \cdot 26 = 676$ (chose a black card and then choose a red one). Fact 5.2 gives

$$p(E) = p(A \cup B) = p(A) + p(B) = \frac{|A|}{|S|} + \frac{|B|}{|S|} = \frac{325}{1326} + \frac{676}{1326} = \frac{1001}{1326} = \mathbf{75.49\%}.$$

Shuffle a 52-card deck; deal two cards, put them back. Repeat 100 times. On about 75 of the trials, not both cards will be red. 

But what if you shuffled the deck, dealt two cards, *but did not put them back*. Then you deal two cards from the remaining 50 cards. Is there still a 75.49% chance of not getting two reds? Does the outcome of the first trial affect the probability of the second? The next section investigates this kind of question.

Exercises for Section 5.2

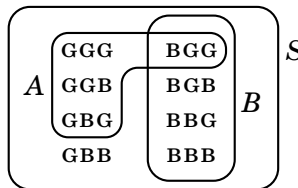
1. A card is taken off the top of a shuffled 52-card deck. What is the probability that it is black or an ace?
 2. What is the probability that a 5-card hand dealt off a shuffled 52-card deck contains at least one ace?
 3. What is the probability that a 5-card hand dealt off a shuffled 52-card deck contains at least one red card?
 4. A hand of five cards is dealt off a shuffled 52-card deck. What is the probability that the five cards are not all of the same suit?
 5. You toss a fair coin 8 times. What is the probability that you do not get 4 heads?
 6. A 4-card hand is dealt off a shuffled 52-card deck. What is the probability that the cards are all of the same color (i.e. all red or all black)?
 7. Two cards are dealt off a shuffled 52-card deck. What is the probability that the cards are both red or both aces?
 8. A coin is tossed six times. What is the probability that the first two tosses are heads or the last toss is a head?
 9. A dice is tossed six times. You win \$1 if the first toss is a five or the last toss is even. What are your chances of winning?
 10. A box contains 3 red balls, 3 blue balls, and 3 green ball. You reach in and grab 2 balls. What is the probability that they have the same color?
 11. A dice is rolled 5 times. Find the probability that not all of the tosses are even.
 12. Two cards are dealt off a well-shuffled deck. You win \$1 if either both cards are red or both cards are black. Find the probability of your winning.
 13. Two cards are dealt off a well-shuffled deck. You win \$1 if the two cards are of different suits. Find the probability of your winning?
 14. A dice is tossed six times. You win \$1 if there is at least one \square . Find the probability of winning.
 15. A coin is tossed 5 times. What is the probability that the first toss is a head or exactly 2 out of the five tosses are heads?
 16. In a shuffled 52-card deck, what is the probability that the top card is black or the bottom card is a heart?
 17. In a shuffled 52-card deck, what is the probability that neither the top nor bottom card is a heart?
 18. A bag contains 20 red marbles, 20 green marbles and 20 blue marbles. You reach in and grab 15 marbles. What is the probability of getting 5 of each color?
 19. A bag contains 20 red marbles, 20 green marbles and 20 blue marbles. You reach in and grab 15 marbles. What is the probability that they are all the same color?
-

5.3 Conditional Probability and Independent Events

Sometimes the probability of one event A will change if we know that another event B has occurred. This is what is known as *conditional probability*. Here is an illustration.

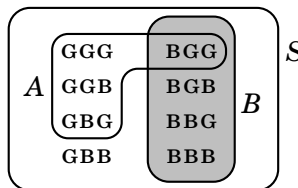
Imagine starting a family of three children. Assume the probability of having a boy is 50% and the probability of having a girl is 50%. What is more likely: the family has more girls than boys, or the oldest is a boy?

To decide, we write out the sample space for the family, listing the possible outcomes of having three children. Let G mean a girl was born first, then a boy, and then another boy. Likewise, B means a boy was born first, then a girl, then a boy, etc. The 8 equally-likely outcomes are shown below, with events A : *More girls than boys*, and B : *Oldest is a boy*.



Note $p(A) = \frac{|A|}{|S|} = \frac{4}{8} = 50\%$, and $p(B) = \frac{|B|}{|S|} = \frac{4}{8} = 50\%$, so more girls than boys is just as likely as the oldest being a boy.

But now imagine that the event B has occurred, so the oldest is a boy. *Now* what is the probability of more girls than boys? That is, what is $p(A)$? There are just four outcomes in event B , and for only one of them are there more girls than boys. Thus, given this new information (oldest is a boy) $p(A)$ has changed value to $p(A) = \frac{1}{4} = 25\%$.



So we have a situation in which $p(A) = 50\%$, but under the condition that B has occurred, then $p(A) = 25\%$. We express this as $p(A|B) = 25\%$, which we read as “*the conditional probability of A given that B has occurred is 25%*,” or just “*the conditional probability of A given B is 25%*.”

Definition 5.2 If A and B are two events in a sample space, then the **conditional probability of A given B**, written $P(A|B)$, is the probability that A will occur if B has already occurred.

Example 5.7 Toss a coin once. The sample space is $S = \{H, T\}$. Consider the events $A = \{H\}$ of getting a head and $B = \{T\}$ of getting a tail. Then $p(A) = p(B) = 50\%$, but $p(A|B) = 0$ because if B (tails) has happened, then A (heads) will not happen. Also $p(B|A) = 0$. Note that $p(A|A) = 1 = 100\%$. \blacktriangleleft

Example 5.8 Take one card from a shuffled deck, and then take another. Now you have two cards. Consider the following events.

A : The first card is a heart C : The second card is a heart
 B : The first card is black D : The second card is red

Find $p(A)$, $p(B)$, $p(D)$, $p(C|A)$, $p(A|C)$, $p(A|B)$, $p(D|C)$ and $p(C|D)$.

Solution. All answers can be found without considering the sample space S . For example, $p(A) = \frac{13}{52} = \frac{1}{4}$ because in taking the first card there are 13 hearts among the 52 equally-likely cards. But to be clear, note that S is the set of all non-repetitive length-2 lists whose entries are cards in the deck. The first list entry is the first card drawn; the second entry is the second card. Taking $7\clubsuit$ and then $2\clubsuit$ is a different outcome than $2\clubsuit$ and then $7\clubsuit$.

$$S = \left\{ \begin{array}{|c|c|} \hline 7 & 2 \\ \hline \clubsuit & \clubsuit \\ \hline \end{array}, \begin{array}{|c|c|} \hline 2 & 7 \\ \hline \clubsuit & \clubsuit \\ \hline \end{array}, \begin{array}{|c|c|} \hline K & 8 \\ \hline \spadesuit & \heartsuit \\ \hline \end{array}, \begin{array}{|c|c|} \hline 5 & 2 \\ \hline \clubsuit & \heartsuit \\ \hline \end{array}, \begin{array}{|c|c|} \hline 5 & 2 \\ \hline \clubsuit & \heartsuit \\ \hline \end{array}, \dots \right\}$$

Compare this to Example 5.6, where the outcomes were 2-element sets, not lists. In the present case $|S| = P(52, 2) = 52 \cdot 51 = 2652$.

As noted above, $p(A) = \frac{13}{52} = \frac{1}{4}$ because in dealing the first card there are 13 hearts in the 52 cards. Alternatively, the event $A \subseteq S$ consists of all the 2-elements lists whose first entry is a heart. There are 13 choices for the first entry, and then 51 of the remaining cards can be selected for the second entry. Thus $|A| = 13 \cdot 51$, and $p(A) = \frac{|A|}{|S|} = \frac{13 \cdot 51}{52 \cdot 51} = \frac{1}{4}$.


Similarly, $p(B) = \frac{26}{52} = \frac{1}{2}$ because in drawing the first card, there are 26 black cards out of 52. This could also be done by computing $|B|$, as above.

Evidently, $p(D) = \frac{1}{2}$, as half the cards are red. Alternatively, D consists of all the lists in S whose second entry is red, so by the multiplication principle, $|D| = 51 \cdot 26$. (Fill in the red second entry first, and then put one of the remaining 51 cards in the first entry.) Then $p(D) = \frac{|D|}{|S|} = \frac{51 \cdot 26}{52 \cdot 51} = \frac{1}{2}$.

Note $p(C|A) = \frac{12}{51}$ because if A has occurred, then a heart was drawn first, and there are 12 remaining hearts out of 51 cards for the second draw.

For $p(A|C)$, imagine the two cards have been dealt, one after the other, face down. The second card is turned over, and it is a heart. Event C has occurred. Now what is the chance that A occurred? That is, what is the chance that first card—when turned over—is a heart? It is not the second

card, and there are 51 other cards, and 12 of them are hearts. Thus the chance that the first card is a heart is $\frac{12}{51}$, so $p(A|C) = \frac{12}{51}$.

Also, $p(A|B) = 0$ because if B occurs (first card black), then A (first card heart) is impossible. Finally, $p(D|C) = 100\%$, but $p(C|D) = 50\%$ because if the second card is red, there is a one in two chance that it is a heart. 

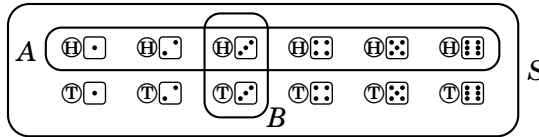
We will soon derive formulas for conditional probability, but they involve a definition that is motivated by the next example of two events having no bearing on one another.

Example 5.9 Toss a coin and roll a dice. Consider the following events.

$$A : \text{Coin is heads} \quad B : \text{Dice is } \heartsuit$$


Find $p(A)$, $p(B)$, $p(A|B)$ and $p(B|A)$.

Solution. Common sense says $p(A) = \frac{1}{2}$ and $p(B) = \frac{1}{6}$. Also, getting \heartsuit has no bearing the coin's outcome, and vice versa, so $P(A|B) = \frac{1}{2}$ and $p(B|A) = \frac{1}{6}$. Nonetheless, let's work it out carefully. The sample space S and events A and B are diagrammed below.



We see that $P(A) = \frac{|A|}{|S|} = \frac{6}{12} = \frac{1}{2}$ and $P(B) = \frac{|B|}{|S|} = \frac{2}{12} = \frac{1}{6}$.

To find $p(A|B)$, imagine that B has occurred. Now what is the chance that A occurs? Only one of the two outcomes in B is heads, so $p(A|B) = \frac{1}{2}$.

To find $p(B|A)$, imagine that A has occurred. Now what is the chance that B occurs? Only 1 of the 6 outcomes in A has \heartsuit , so $p(B|A) = \frac{1}{6}$. 

In the above example, whether or not B happens has no bearing on the probability of A , and vice versa. We say that events A and B are *independent*.

Definition 5.3 Two events A and B are **independent** if one happening does not change the probability of the other happening, that is, if $p(A) = p(A|B)$ and $p(B) = p(B|A)$. Otherwise they are **dependent**.

Thus events A and B in Example 5.9 are independent.

In Example 5.8 we dealt two cards off a deck. For events A : *First card* \heartsuit , and B : *First card black*, we saw $p(A) = \frac{1}{4}$ and $p(A|B) = 0$. Because $\frac{1}{4} \neq 0$, A and B are dependent. (In fact, they also happen to be mutually exclusive.)

We began this section showing that in a family of three children, the event A : *More girls than boys* has $p(A) = 50\%$. But if B : *Oldest is a boy* occurs, then $p(A|B) = 25\%$. Here A and B are dependent. (But note that they are not mutually exclusive).

Example 5.10 A box contains six tickets, three white and three gray, and marked as shown below. You reach in and grab a ticket at random.



Consider events A : *Ticket is gray*, and B : *Ticket has a star on it*. Are these events independent or dependent?

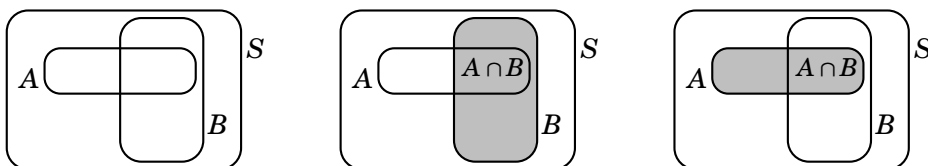
Solution. The chance of getting a gray ticket is $p(A) = \frac{3}{6} = \frac{1}{2}$. The chance of getting a star is $p(B) = \frac{4}{6} = \frac{2}{3}$.

If B occurs, then one of the four tickets with a star has been drawn. Half of these are gray, so $p(A|B) = \frac{1}{2}$, and this equals $p(A)$.

If A occurs, then one of the three gray tickets has been drawn. Two of these have stars, so $p(B|A) = \frac{2}{3}$, and this equals $p(B)$.

Thus A and B are independent. One of them happening does not change the probability of the other happening.

Now we are going to derive general formulas for $p(A|B)$ and $p(B|A)$. Let A and B be two events in a sample space S , as shown below on the left.



If B occurs (shown shaded in the middle drawing) then any outcome in the shaded region could occur, so the shaded set B is like a new sample space. Now if also A occurs, this means some outcome in $A \cap B$ occurs. Note that $A \cap B \subseteq B$ is an event in B , so Fact 5.1 gives

$$p(A|B) = \frac{|A \cap B|}{|B|} = \frac{|A \cap B|}{|B|} \cdot \frac{\frac{1}{|S|}}{\frac{1}{|S|}} = \frac{\frac{|A \cap B|}{|S|}}{\frac{|B|}{|S|}} = \frac{p(A \cap B)}{p(B)}.$$

Thus $p(A|B) = \frac{p(A \cap B)}{p(B)}$. Reversing the roles of A and B (and referring to the drawing on the above right) we also get $p(B|A) = \frac{p(A \cap B)}{p(A)}$. Cross-multiplying gives $p(A \cap B) = p(A|B) \cdot p(B)$ and $p(A \cap B) = p(A) \cdot p(B|A)$.


Thus we have formulas for not only $p(A|B)$ and $p(B|A)$, but also one for $p(A \cap B)$. Moreover, if A and B happen to be independent, then $p(A|B) = p(A)$, so the equation $p(A \cap B) = p(A|B) \cdot p(B)$ simplifies to $p(A \cap B) = p(A) \cdot p(B)$.

Fact 5.3 Suppose A and B are events in a sample space. Then:

1. $p(A|B) = \frac{p(A \cap B)}{p(B)}$
2. $p(B|A) = \frac{p(A \cap B)}{p(A)}$
3. $p(A \cap B) = p(A|B) \cdot p(B) = p(A) \cdot p(B|A)$
4. $p(A \cap B) = p(A) \cdot p(B)$ if A and B are independent.


In the earlier examples in this section, we found conditional probabilities $p(A|B)$ and $p(B|A)$ without the aid of the above formulas. In fact, it turns out that the above formulas 1 and 2 are of relatively limited use. But their consequences, formulas 3 and 4 are very useful, as they provide a method of computing $p(A \cap B)$, the probability that A and B both occur.

Example 5.11 Two cards are dealt off a deck. You win \$1 if the first card is red and the second card is black. What are your chances of winning?

Solution. Let A be the event “*The first card is red,*” and let B be the event “*The second card is black.*” We seek $p(A \text{ and } B)$, which is $p(A \cap B)$. Formula 3 above gives $p(A \cap B) = p(A) \cdot p(B|A) = \frac{1}{2} \cdot \frac{26}{51} = \frac{13}{51} \approx 0.2549 = 25.49\%$. 

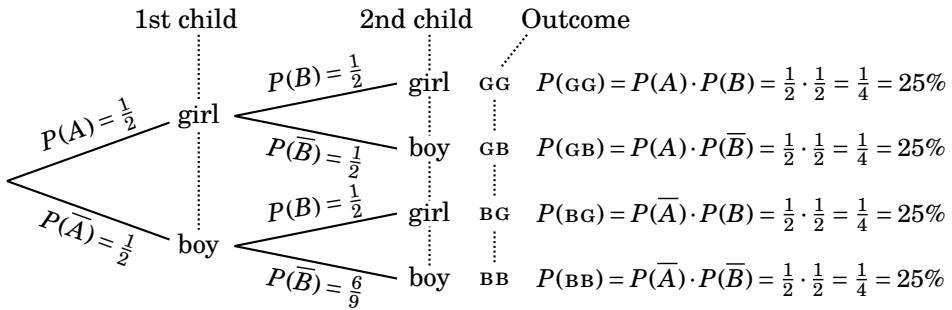
Example 5.12 A dice is rolled twice. You win \$1 if neither roll is \square . What are your chances are winning?

Solution. Let A be the event “*The first roll is not \square ,*” so $p(A) = \frac{5}{6}$. Let B be the event “*The second roll is not \square ,*” so $p(B) = \frac{5}{6}$. We seek $p(A \text{ and } B)$.

Events A and B are independent, because the result of the first roll does not influence the second. Formula 4 above gives $p(A \text{ and } B) = p(A \cap B) = p(A) \cdot p(B) = \frac{5}{6} \cdot \frac{5}{6} = \frac{25}{36} = 69.\bar{4}\%$. 

Questions about conditional probability can sometimes be answered by a so-called **probability tree**. To illustrate this, suppose (as we assume in this chapter) that there is a 50-50 chance of a child being born a boy or a girl. Suppose a woman has two children. The events A : *First child is a girl*, and B : *Second child is a girl* are independent; whether or not the first child is a girl does not change the probability that the second child is a girl. Thus the chance that both children are girls is $p(A \cap B) = p(A) \cdot p(B) = \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4} = 25\%$.

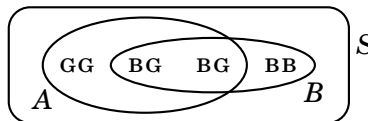
Notice that in this example the complements of A and B are the events \bar{A} : *First child is a boy*, and \bar{B} : *Second child is a boy*. The probability of the outcome GB (first child is a girl and the second is a boy) is thus $p(GG) = p(A \cap \bar{B}) = p(A) \cdot p(\bar{B}) = \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4} = 25\%$. Similarly, we can find the probabilities of all four outcomes in the branches of the following tree.



This confirms our intuitive supposition that each outcome in the sample space $S = \{GG, GB, BG, BB\}$ has a 25% chance of occurring.

Example 5.13 You meet a woman and a girl. The woman tells you that she has two children, one of whom is the girl. What are the chances that her other child is a boy?

Solution. Most of us would jump to the conclusion that the answer is 50%. But this is wrong. To see why, consider the sample space S , below, for the “experiment” of having two children.



Let A be the event of there being at least one girl. We met a daughter, so A has occurred. Let B be the event of there being a boy in the family. The problem thus asks for the probability of B given that A has occurred. Looking at the above diagram, we see that B occurs in 2 out of the 3 equally likely outcomes in A , so the answer to the question is $p(B|A) = \frac{2}{3} = 66.6\%$.

Alternatively, we can use Formula 2 from Fact 5.3 to get the answer as

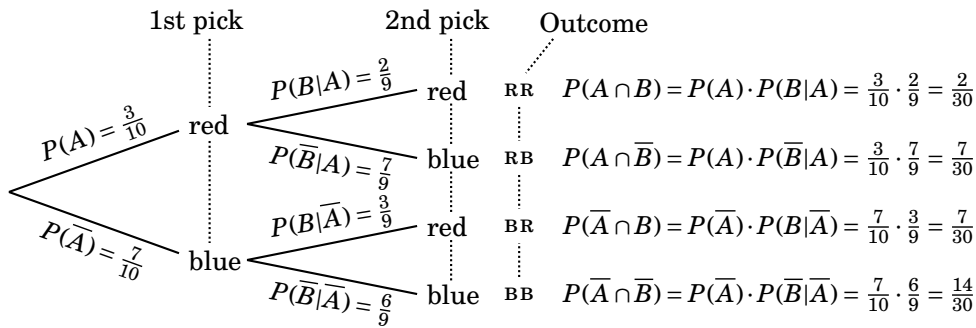
$$p(B|A) = \frac{p(A \cap B)}{p(A)} = \frac{\frac{|A \cap B|}{|S|}}{\frac{|A|}{|S|}} = \frac{\frac{2}{4}}{\frac{3}{4}} = \frac{2}{3} = 66.6\%.$$

Our next example involves an experiment with a sample space in which not all outcomes are equally likely.

Example 5.14 A jar contains 3 red balls and 7 blue balls. You reach in, pick a ball at random, and remove it. Then you randomly remove a second ball. Thus the sample space for this experiment $S = \{RR, RB, BR, BB\}$. Find the probability of each outcome in S .

Solution. Form the events A : *First pick is red*, and B : *Second pick is red*. Then we have \bar{A} : *First pick is blue*, and \bar{B} : *Second pick is blue*.

The probability of the first pick is red is $p(A) = \frac{3}{10}$, as there are 3 out of 10 red balls that we could have picked. Once this has happened, there are 9 balls left, two of which are red, so $p(B|A) = \frac{2}{9}$. So the probability that both picks are red is $p(RR) = p(A \cap B) = p(A) \cdot p(B|A) = \frac{3}{10} \cdot \frac{2}{9} = \frac{2}{30}$. This is tallied in the top branch of the following tree.



Likewise, $p(RB) = p(A \cap \bar{B}) = p(A) \cdot p(\bar{B}|A)$. To find $p(\bar{B}|A)$, note that if A has occurred, then there are 9 balls left in the jar, and 7 of them are blue, so $p(A \cap \bar{B}) = \frac{7}{9}$. Thus $p(RB) = p(A \cap \bar{B}) = p(A) \cdot p(\bar{B}|A) = \frac{3}{10} \cdot \frac{7}{9} = \frac{7}{30}$, and this is shown in the second-from-the-top branch of the tree.

Similar computations for the probabilities of the remaining two outcomes are shown on the bottom branches. Check that you understand them. From this tree we see that the probabilities of the various outcomes in S are

$$S = \left\{ \begin{array}{cccc} RR, & RB, & BR, & BB \\ 6.\bar{6}\% & 23.\bar{3}\% & 23.\bar{3}\% & 46.\bar{6}\% \end{array} \right\} \quad \blacktriangleright$$

If in the above Example 5.14, we had been asked for the probability of the event $E = \{RB, BR\}$ of the two picks being different colors, we would surmise that $p(E) = p(RB) + p(BR) = 23.\bar{3}\% + 23.\bar{3}\% = 46.\bar{6}\%$.

The next section is a further exploration of situations such as this one, in which not all outcomes in a sample space are equally likely.

Exercises for Section 5.3

1. A box contains six tickets:

| | | | | | |
|---|---|---|---|---|---|
| A | A | B | B | B | E |
|---|---|---|---|---|---|

. You remove two tickets, one after the other. What is the probability that the first ticket is an A and the second is a B?
 2. A box contains six tickets:

| | | | | | |
|---|---|---|---|---|---|
| A | A | B | B | B | E |
|---|---|---|---|---|---|

. You remove two tickets, one after the other. What is the probability that both tickets are vowels?
 3. In a shuffled 52-card deck, what is the probability that the top card is red and the bottom card is a heart?
 4. A card is drawn off a 52-card deck. Let A be the event "The card is a heart." Let B be the event "The card is a queen." Are these two events independent or dependent?
 5. Suppose A and B are events, and $P(A) = \frac{1}{2}$, $P(B) = \frac{1}{3}$, and $P(A \cap B) = \frac{1}{6}$. Are A and B independent, dependent, or is there not enough information to say for sure?
 6. Suppose A and B are events, and $P(A) = \frac{1}{2}$, $P(B) = \frac{1}{3}$, and $P(A \cup B) = \frac{2}{3}$. Are A and B independent, dependent, or is there not enough information to say for sure?
 7. Say A and B are events with $P(A) = \frac{2}{3}$, $P(A|B) = \frac{3}{4}$, and $P(B|A) = \frac{1}{2}$. Find $p(B)$.
 8. A box contains 2 red balls, 3 blue balls, and 1 green ball. You remove two balls, one after the other. Find the probability that both balls are red. Find the probability that both balls are blue. Find the probability that both balls have the same color.
 9. A box contains 2 red balls, 3 black balls, and 4 white balls. One is removed, and then another is removed. What is the probability that no black balls were drawn?
 10. A coin is flipped 5 times. What is the probability of all 5 tosses being tails? If there were more tails than heads, then what is the probability that all 5 tosses were tails?
 11. A coin is flipped 5 times, and there are more tails than heads. What is the probability that the first flip was a tail?
 12. Suppose events A and B are independent, $p(A) = \frac{1}{3}$, and $p(A \cup B) = \frac{2}{3}$. Find $p(B)$.
 13. A 5-card hand is dealt from a shuffled 52-card deck. Exactly 2 of the cards in the hand are hearts. Find the probability that all the cards in the hand are red.
 14. A 5-card hand is dealt from a shuffled 52-card deck. Exactly 2 of the cards in the hand are red. Find the probability that all the cards in the hand are hearts.
-

5.4 Probability Distributions and Probability Trees

Except for Example 5.14 on the previous page, we have, until now, assumed that any two outcomes in a sample space are equally likely to occur. This is reasonable in many situations, such as tossing an unbiased coin or dice, or dealing a hand from a shuffled deck.

But in reality, things are not always so uniform. Suppose the spots of a dice are hollowed out, and when tossed it is more likely to land with a lighter side up (one with more spots). Toss the dice once. The probabilities of the six outcomes in the sample space might be something like this:

$$S = \left\{ \begin{array}{cccccc} \square, & \square, & \square, & \square, & \square, & \square \\ 15\% & 15\% & 16\% & 16\% & 18\% & 20\% \end{array} \right\}$$

(Of course it's unlikely the percentages would be whole numbers; this is just an illustration.) Note that the probabilities of all outcomes sum to 1:

$$p(\square) + p(\square) + p(\square) + p(\square) + p(\square) + p(\square) = 1,$$

because if tossed, the probability of its landing on one of its six faces is 100%. The probability of an event such as $E = \{\square, \square, \square\}$ (*lands on even*) is

$$p(\square) + p(\square) + p(\square) = 15 + 16 + 20 = 51\%.$$

Formula 5.1 does not apply here because the outcomes are not all equally likely. In fact it gives the incorrect probability $p(E) = \frac{|E|}{|S|} = \frac{3}{6} = 50\%$.

These ideas motivate the main definition of this section.

Definition 5.4 For an experiment with sample space $S = \{x_1, x_2, \dots, x_n\}$, a **probability distribution** is a function p that assigns to each outcome $x_i \in S$ a probability $p(x_i)$ with $0 \leq p(x_i) \leq 1$, and for which

$$p(x_1) + p(x_2) + \dots + p(x_n) = 1.$$

The **probability** $p(E)$ of an event $E \subseteq S$ is the sum of the probabilities of the elements of E .

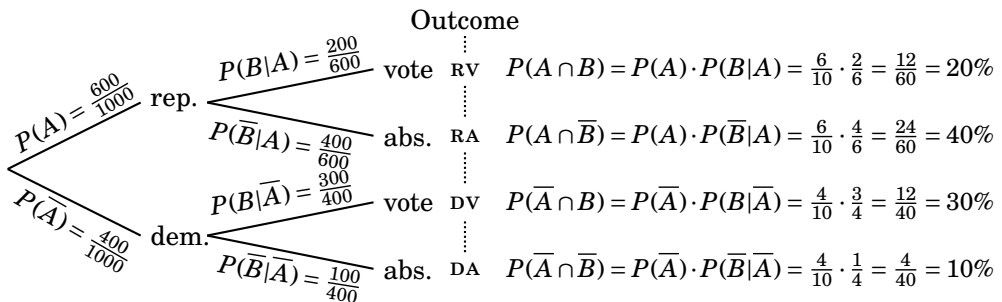
In the case where all outcomes are equally likely, any outcome $x_i \in S$ has probability $p(x_i) = \frac{1}{|S|}$. This is a probability distribution, by Definition 5.4. It is called the **uniform distribution** on S . For the uniform distribution we have the formula $p(E) = \frac{|E|}{|S|}$, but, as noted above, this may not hold for non-uniform probability distributions.

Example 5.15 A certain voting precinct has 1000 voters, 600 of whom are republicans and 400 of whom are democrats. In a recent election, 200 republicans voted and 300 democrats voted. You randomly select a member of the precinct and record whether they are republican or democrat, and whether or not they voted. Thus the sample space for the experiment is $S = \{RV, RA, DV, DA\}$, where RV means your selection was a republican who voted, whereas RA indicates a republican who abstained from voting, etc.

Find the probability distribution for S . Also, find the probability that your selection was a republican who voted or a democrat who didn't.

Solution. The chance that you picked a republican is $\frac{600}{1000} = 60\%$, and the chance that you picked a democrat is $\frac{400}{1000} = 40\%$. If you picked a republican, the conditional probability that this person voted is $\frac{200}{600}$, and the conditional probability that they didn't vote is $\frac{400}{600}$. If you picked a democrat, the conditional probability that this person voted is $\frac{300}{400}$, and the conditional probability that they didn't vote is $\frac{100}{400}$.

Here is the probability tree, where $A = \{RV, RA\}$ is the event of picking a republican and $B = \{RV, DV\}$ is the event of picking a voter.



Thus the probability distribution is

$$S = \left\{ \begin{array}{cccc} RV, & RA, & DV, & DA \\ 20\% & 40\% & 30\% & 10\% \end{array} \right\}$$

The probability that you picked a republican who voted or a democrat who didn't is $p(\{RV, DA\}) = p(RV) + p(DA) = 20\% + 10\% = 30\%$. ✍️

If p is a probability distribution on a sample space S , then Definition 5.4 implies $p(S) = 1$ (because the probabilities of the elements of S sum to 1). Also, for mutually exclusive events $A, B \subseteq S$, we have $p(A \cup B) = p(A) + p(B)$, because Definition 5.4 says $p(A \cup B)$ is the sum probabilities of elements of A , plus those for B . And $S = A \cup \bar{A}$, so $1 = p(S) = p(A \cup \bar{A}) = p(A) + p(\bar{A})$.

This implies $p(A) = 1 - p(\bar{A})$ and $p(\bar{A}) = 1 - p(A)$. Therefore the formulas 2, 3 and 4 of Fact 5.2 (page 143) hold for arbitrary probability distributions, even though we derived them earlier only for uniform distributions.

Similar reasoning gives the following facts, which can be taken as a summary of all probability formulas in this chapter so far.

Probability Summary

Suppose p is a probability distribution for a sample space S of some experiment. Then the probability of an event $E = \{x_1, x_2, \dots, x_k\} \subseteq S$ is $p(E) = p(x_1) + p(x_2) + \dots + p(x_k)$. Thus $p(S) = 1$ and $p(\emptyset) = 0$.

If $A, B \subseteq S$ are arbitrary arbitrary events, then

- $E = A \cup B$ is the event "A occurs **or** B occurs,"
- $E = A \cap B$ is the event "A occurs **and** B occurs,"
- $E = \bar{A}$ is the event "A **does not** occur."

Events A and B are **mutually exclusive** if $A \cap B = \emptyset$, meaning $p(A \cap B) = p(\emptyset) = 0$, that is, A and B cannot both happen at the same time. In general:

1. $p(A \cup B) = p(A) + p(B) - p(A \cap B)$
2. $p(A \cup B) = p(A) + p(B)$ if A and B are mutually exclusive
3. $p(\bar{A}) = 1 - p(A)$
4. $p(A) = 1 - p(\bar{A})$.

The **conditional probability** of A given B , denoted $p(A|B)$, is the probability of A , given that B has occurred. Events A and B are **independent** if $p(A|B) = p(A)$ and $p(B|A) = p(B)$, that is, if one happening does not change the probability that the other will happen.

5. $p(A|B) = \frac{p(A \cap B)}{p(B)}$
6. $p(B|A) = \frac{p(A \cap B)}{p(A)}$
7. $p(A \cap B) = p(A|B) \cdot p(B) = p(A) \cdot p(B|A)$
8. $p(A \cap B) = p(A) \cdot p(B)$ if A and B are independent

If p is the uniform distribution, then

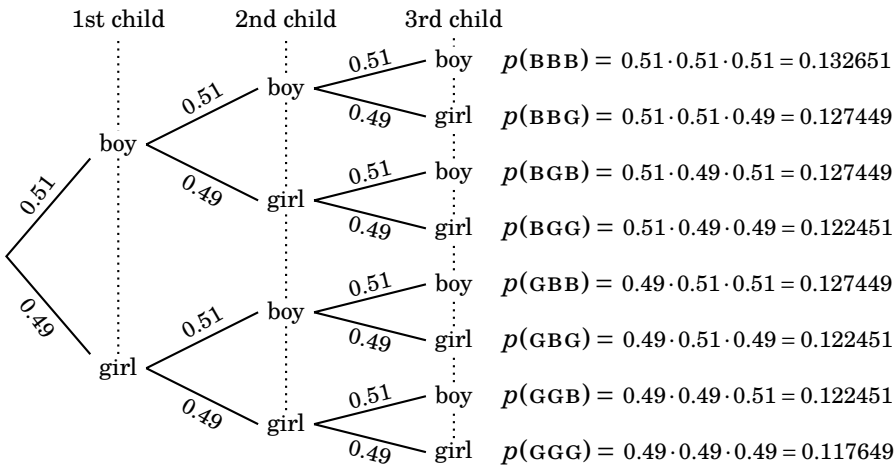
9. $p(A) = \frac{|A|}{|S|}$ if p is the uniform distribution.

At the beginning of Section 5.3 we calculated the probability that, for a family of three children, more girls than boys is just as likely as the oldest child being a boy. This was based on the assumption that there is a 50-50 chance of each child being a boy or a girl.

In reality, there is about a 51% chance of a child being born a boy, versus 49% for a girl. (Though the mortality rate for boys is higher, so this statistic is somewhat equalized in adulthood.) Let's revisit our question.

Example 5.16 Assume that there is 51% chance of a child being born a boy, versus 49% of being born a girl. For a family of three children, consider events A : *There are more girls than boys*, and B : *The oldest child is a boy*. Find $p(A)$ and $p(B)$.

Solution. The sample space is $S = \{BBB, BBG, BGB, BGG, GBB, GBG, GGB, GGG\}$. The following probability tree computes the probability of each outcome. (We assume that gender of births are independent, that is, the gender of one child does not influence the gender of the next child born.)



The probability $p(A)$ of more girls than boys is

$$\begin{aligned}
 p(\{BGG, GBG, GGB, GGG\}) &= p(BGG) + p(GBG) + p(GBG) + p(GGG) \\
 &= 0.122451 + 0.122451 + 0.122451 + 0.117649 \approx \mathbf{48.5\%}.
 \end{aligned}$$

The probability $p(B)$ of the oldest being a boy is

$$\begin{aligned}
 p(\{BBB, BBG, BGB, BGG\}) &= p(BGG) + p(GBG) + p(GBG) + p(GGG) \\
 &= 0.132651 + 0.127449 + 0.127449 + 0.122451 = 0.51 = \mathbf{51\%}.
 \end{aligned}$$

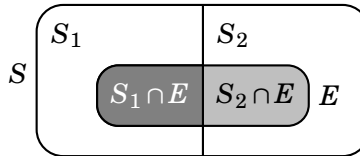
(This makes sense, as the chance of the firstborn being a boy is 51%.)

Exercises for Section 5.4

1. There is a 40% chance of rain on Saturday and a 25% chance of rain on Sunday. What is the probability that it will rain on at least one day of the weekend? (You may assume that the events “Rain on Saturday” and “Rain on Sunday” are independent events.)
 2. There is an 80% chance that there will be rain over the weekend, and a 50% chance of rain on Saturday. What is the chance of rain on Sunday? (You may assume that the events “Rain on Saturday” and “Rain on Sunday” are independent events.)
 3. A club consists of 60 men and 40 women. To fairly choose a president and a secretary, names of all members are put into a hat and two names are drawn. The first name drawn is the president, and the second name drawn is the secretary. What is the probability that the president and the secretary have the same gender?
 4. At a certain college, 40% of the students are male, and 60% are female. Also, 20% of the males are smokers, and 10% of the females are smokers. A student is chosen at random. What is the probability that the student is a male nonsmoker?
 5. At a certain college, 30% of the students are freshmen. Also, 80% of the freshmen live on campus, while only 60% of the non-freshman students live on campus. A student is chosen at random. What is the probability that the student is a freshman who lives off campus?
 6. Suppose events A and B are both independent *and* mutually exclusive. What can you say about $p(A)$ and $p(B)$?
-

5.5 Bayes' Formula

We are going to learn one final probability formula, *Bayes' formula*, named for its discoverer, Thomas Bayes (1702–1761). His formula gives an answer to the following question: Suppose a sample space S for an experiment is a union $S = S_1 \cup S_2$, with $S_1 \cap S_2 = \emptyset$, and $E \subseteq S$ is an event. If E occurs, then what is the probability that S_1 has occurred? That is, what is $p(S_1 | E)$?



A short computation gives the answer.

$$\begin{aligned}
 p(S_1 | E) &= \frac{p(S_1 \cap E)}{p(E)} && \text{by formula 5 on page 158} \\
 &= \frac{p(S_1) \cdot p(E | S_1)}{p(E)} && \text{by formula 7 on page 158} \\
 &= \frac{p(S_1) \cdot p(E | S_1)}{p((S_1 \cap E) \cup (S_2 \cap E))} && \text{as } E = (S_1 \cap E) \cup (S_2 \cap E) \\
 &= \frac{p(S_1) \cdot p(E | S_1)}{p(S_1 \cap E) + p(S_2 \cap E)} && \text{because } S_1 \cap E \text{ and } S_2 \cap E \\
 & && \text{are mutually exclusive} \\
 &= \frac{p(S_1) \cdot p(E | S_1)}{p(S_1) \cdot p(E | S_1) + p(S_2) \cdot p(E | S_2)}. && \text{by formula 7 on page 158}
 \end{aligned}$$

The same steps give $p(S_2 | E) = \frac{p(S_2) \cdot p(E | S_2)}{p(S_1) \cdot p(E | S_1) + p(S_2) \cdot p(E | S_2)}$.

Fact 5.4 Bayes' Formula

Suppose a sample space S for an experiment is a union $S = S_1 \cup S_2$, with $S_1 \cap S_2 = \emptyset$. Suppose also that $E \subseteq S$ is an event.

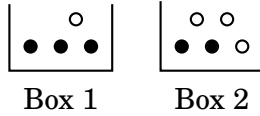
Then $p(S_1 | E) = \frac{p(S_1) \cdot p(E | S_1)}{p(S_1) \cdot p(E | S_1) + p(S_2) \cdot p(E | S_2)}$

and $p(S_2 | E) = \frac{p(S_2) \cdot p(E | S_2)}{p(S_1) \cdot p(E | S_1) + p(S_2) \cdot p(E | S_2)}$.

Though we will not use it here, we mention that Bayes' formula extends to situations in which S decomposes into more than two parts. If $S = S_1 \cup S_2 \cup \dots \cup S_n$, and $S_i \cap S_j = \emptyset$ whenever $1 \leq i < j \leq n$, then for any S_i ,

$$p(S_i | E) = \frac{p(S_i) \cdot p(E | S_i)}{p(S_1) \cdot p(E | S_1) + p(S_2) \cdot p(E | S_2) + \dots + p(S_n) \cdot p(E | S_n)}. \tag{5.1}$$

Example 5.17 There are two boxes. Box 1 contains three black balls and one white ball. Box 2 contains two black balls and three white balls.



Someone chooses a box at random and then randomly takes a ball from it. The ball is white. What is the probability that the ball is from Box 1?

Solution. The sample space is $S = \{1B, 1W, 2B, 2W\}$, where the number refers to the box the selected ball came from, and the letter designates whether the ball is black or white.

Let $S_1 = \{1B, 1W\}$ be the event S_1 : *The ball came from Box 1.*

Let $S_2 = \{2B, 2W\}$ be the event S_2 : *The ball came from Box 2.*

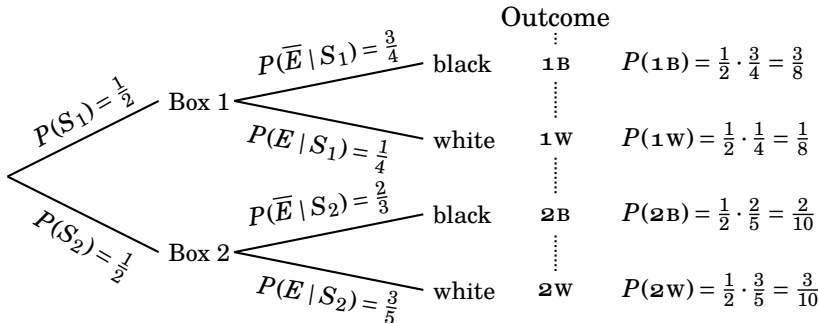
Let $E = \{1W, 2W\}$ be the event E : *The ball is white.*

The answer to the question is thus $p(S_1 | E)$. As $S = S_1 \cup S_2$ and $S_1 \cap S_2 = \emptyset$, Bayes' formula applies, and it gives

$$\begin{aligned}
 p(S_1 | E) &= \frac{p(S_1) \cdot p(E | S_1)}{p(S_1) \cdot p(E | S_1) + p(S_2) \cdot p(E | S_2)} \\
 &= \frac{\frac{1}{2} \cdot \frac{1}{4}}{\frac{1}{2} \cdot \frac{1}{4} + \frac{1}{2} \cdot \frac{3}{5}} = \frac{\frac{1}{8}}{\frac{1}{8} + \frac{3}{10}} = \frac{\frac{10}{80}}{\frac{34}{80}} = \frac{10}{34} \approx 29.4\%.
 \end{aligned}$$

So there's a 29.4% chance that the selected white ball came from Box 1. 🐦

For full disclosure, let it be noted that we could bypass Bayes' formula and solve this problem with a probability tree. Note that $\bar{E} = \{1B, 2B\}$ is the event of a black ball being chosen. Consider the following probability tree.



Applying Formula 5 from page 158 to these figures, our answer is

$$p(S_1 | E) = \frac{p(S_1 \cap E)}{p(E)} = \frac{p(\{1W\})}{p(\{1W, 2W\})} = \frac{p(1W)}{p(1W) + p(2W)} = \frac{\frac{1}{8}}{\frac{1}{8} + \frac{3}{10}} = \frac{10}{34} \approx 29.4\%.$$

Example 5.18 A certain disease occurs in only 1% of the population. A pharmaceutical company develops a test for this disease. They make the following claims about their test's accuracy in the event a subject is tested:

If you have the disease, then there is a 99% chance you will test positive.

If you don't have the disease, there is a 99% chance you will test negative.

You take the test and you test positive. Assuming that the pharmaceutical company's claims are accurate, what is the chance that you have the disease?

Solution: Given the data, you may suspect that there is a high probability that you have the disease. However, this is not so, and Baye's formula can give the exact answer. We can set up the problem as an experiment: You take the test. There are four possible outcomes:

HP (you Have the disease and test Positive);

HN (you Have the disease and test Negative);

DP (you Don't have the disease and test Positive);

DN (you Don't have the disease and test Negative);

Consequently the sample space is

$$S = \{ \underbrace{HP, HN}_{S_1}, \underbrace{DP, DN}_{S_2} \},$$

where $S_1 = \{HP, HN\}$ is the event of having the disease and $S_2 = \{DP, DN\}$ is the event of not having it. Further, $E = \{HP, DP\}$ is the event of testing positive for the disease.

We seek the probability that you have the disease given that you tested positive, that is, we seek $p(S_1 | E)$. Note $S = S_1 \cup S_2$ and $S_1 \cap S_2 = \emptyset$, so we have the set-up for Baye's formula. The formula says our answer will be

$$p(S_1 | E) = \frac{p(S_1) \cdot p(E | S_1)}{p(S_1) \cdot p(E | S_1) + p(S_2) \cdot p(E | S_2)}.$$

Note that, $p(S_1) = 0.01$ because only 1% of the population has the disease. Similarly, $p(S_2) = 0.99$ because 99% of the population does not have it. The pharmaceutical company said that there is a 99% chance that you will test positive if you have the disease, which is to say $p(E | S_1) = 99\%$. They also said that there is a 99% chance you will test negative if you don't have the disease, and from this we infer that there is a 1% chance that you will test *positive* if you don't have the disease; this means $p(E | S_2) = 1\%$. Thus

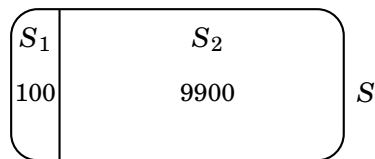
$$p(S_1 | E) = \frac{0.01 \cdot 0.99}{0.01 \cdot 0.99 + 0.99 \cdot 0.01} = \frac{0.0099}{0.0099 + 0.0099} = 0.5 = 50\%.$$

So if you test positive, there is a **50%** chance that you have the disease. 🐼

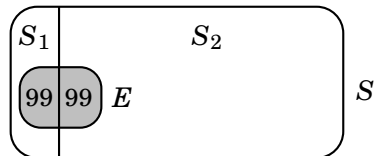
Example 5.18 is a cautionary tale about the risks of jumping to a reasonable-looking (but incorrect) conclusion based on a hasty analysis of data. If you tested positive, then—given the claims about the test’s accuracy—it seems as if you would be very likely to have the disease. Yet the chance is only 50%. This may seem somehow paradoxical.

To see that the answer really makes sense, let’s analyze the problem in a different way, as a scaled-down thought experiment. Imagine that we have a population of 10,000 people, and they all get tested for the disease. The experiment will involve picking a person at random, so the sample space S is the set of all people. Let $S_1 \subseteq S$ be the set of people that have the disease, and let $S_2 \subseteq S$ be the set of people that do not have it.

Only 1% of S has the disease, and thus $|S_1| = 0.01 \cdot 10,000 = 100$ people. And because 99% of the population is disease-free, we know $|S_2| = 0.99 \cdot 10,000 = 9900$ people. We record this in the Venn diagram on the right. (For clarity, the diagram is not quite to scale, as technically S_1 should be 1% of the area enclosed by S , a tiny sliver.)



Next, let E be the set of people who tested positive for the disease. The part of E that overlaps S_1 consists of the people who have the disease and tested positive for it. The pharmaceutical company stated that 99% of the 100 people in S_1 (who have the disease)



will test positive, so $|S_1 \cap E| = 99$. On the other hand, the part of E that overlaps S_2 consists of the people who *do not have* the disease and tested positive for it. Because 99% of people who do not have the disease will test negative, only 1% of them will test positive. This means that the part of E that overlaps S_2 contains 1% of the 9900 people in S_2 , which is 99 people.

Consequently, the set E of those who tested positive consists of 99 people who have the disease and 99 people who do not have it. So if we randomly select a person who tested positive, then that person is just as likely to have the disease (i.e., to be in S_1) as not have it (i.e., to be in S_2).

Thus the unexpected answer to Example 5.18 comes from the fact that the disease is very rare, so S_1 is a tiny fraction of S . It happens that 99% of S_1 is equal to 1% of S_2 , so the number of people who tested positive and have the disease equals the number who tested positive and do not have it.

So the claims about the test’s accuracy are misleading: if you tested positive, then there is only a 50% that you actually have the disease.

Exercises for Section 5.5

1. At a certain college, 40% of the students are male, and 60% are female. Also, 20% of the males are smokers, and 10% of the females are smokers. A student is chosen at random. If the student is a smoker, what is the probability that the student is female?
 2. At a certain college, 30% of the students are freshmen. Also, 80% of the freshmen live on campus, while only 60% of the non-freshman students live on campus. A student is chosen at random. If the student lives on campus, what is the probability that the student is a freshman?
 3. A jar contains 4 red balls and 5 white balls. A random ball is removed, and then another is removed. If the second ball was red, what is the probability that the first ball was red?
-

5.6 Solutions for Chapter 5

Section 5.1

1. A card is randomly selected from a deck of 52 cards. What is the chance that the card is red or a king?

Solution: The sample space S is the set of 52 cards. The experiment is drawing one card. The event $E \subseteq S$ is the set of the cards that are red or kings. This is the set of 26 red cards, plus the king of spades and the king of clubs. Therefore $|E| = 28$, and $p(E) = \frac{|E|}{|S|} = \frac{28}{52} \approx 53.8\%$.

3. Toss a dice 5 times in a row. What is the probability that you don't get any 6's?

Solution: The sample space S is the set of all length-5 lists (repetition allowed) whose entries are the numbers 1, 2, 3, 4, 5, 6. There are $6^5 = 7776$ such lists, so $|S| = 7776$. The event E consists of those lists in S that do not contain a 6. There are $5^5 = 3125$ of them, so $p(E) = \frac{|E|}{|S|} = \frac{3125}{7776} \approx 40.187\%$.

5. Toss a dice 5 times in a row. What is the probability that you will get the same number on each roll? (i.e. $\square\square\square\square\square$ or $\square\square\square\square\square$, etc.)

Solution: The sample space S is the set of all length-5 lists (repetition allowed) whose entries are the numbers 1, 2, 3, 4, 5, 6. There are $6^5 = 7776$ such lists, so $|S| = 7776$. Note that $E = \{11111, 22222, 33333, 44444, 55555, 66666\}$, so $|E| = 6$, and $p(E) = \frac{|E|}{|S|} = \frac{6}{7776} \approx 0.077\%$.

7. You have a pair of dice, a white one and a black one. Toss them both. What is the probability that they show the same number?

Solution: The sample space S is shown in Example 5.1 on page 138. You can see that $|S| = 36$ and the event E of both dice showing the same number has cardinality 6, so $p(E) = \frac{|E|}{|S|} = \frac{6}{36} = 16.\bar{6}\%$.

9. You have a pair of dice, a white one and a black one. Toss them both. What is the probability that both show even numbers?

Solution: The sample space S is shown in Example 5.1 on page 138. Note that $E = \{\square\square, \square\square, \square\square, \square\square, \square\square, \square\square, \square\square, \square\square, \square\square\}$. Thus $p(E) = \frac{|E|}{|S|} = \frac{9}{36} = 25\%$.

11. Toss a coin 8 times. Find the probability that the first and last tosses are heads.

Solution: The sample space S is the set of all length-8 lists made from the two symbols H and T. Thus $|S| = 2^8$. The event E of the first and last tosses being heads consists of all those outcomes in S that have the form $(H, \square, \square, \square, \square, \square, \square, H)$ where there are two choices for each box. Thus $|E| = 2^6$, and so $p(E) = \frac{|E|}{|S|} = \frac{2^6}{2^8} = \frac{1}{2^2} = 25\%$.

13. Five cards are dealt from a shuffled 52-card deck. What is the probability of getting three red cards and two clubs?

Solution: The sample space S is the set of all possible 5-card hands that can be made from the 52 cards in the deck, so $|S| = \binom{52}{5} = 2,598,960$. There are $\binom{26}{3}$ ways to get 3 red cards and $\binom{13}{2}$ ways to get 2 clubs, so by the multiplication principle there are $\binom{26}{3}\binom{13}{2} = 202,800$ different 5-card hands that have 3 red cards and 2 clubs. Therefore $p(E) = \frac{|E|}{|S|} = \frac{202,800}{2,598,960} \approx 12.81\%$.

15. Alice and Bob each randomly pick an integer from 0 to 9. What is the probability that they pick the same number? What is the probability that they pick different numbers?

Solution: Lets put $S = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : 0 \leq a, b \leq 9\} = \{(0, 0), (0, 1), (0, 2), \dots, (9, 9)\}$ where a ordered pair (a, b) means Alice picked a and Bob picked b . Then $S = 10 \cdot 10 = 100$. The event of their both picking the same number is $E = \{(0, 0), (1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (6, 6), (7, 7), (8, 8), (9, 9)\}$, so $|E| = 10$. Then the probability of their picking the same number is $p(E) = \frac{|E|}{|S|} = \frac{10}{100} = 10\%$. The event of their picking different numbers is $\bar{E} = S - E$, so the probability of their picking different numbers is $p(\bar{E}) = \frac{|\bar{E}|}{|S|} = \frac{90}{100} = 90\%$.

17. What is the probability that a 5-card hand dealt off a shuffled 52-card deck does not contain an ace?

Solution: The sample space S is the set of all possible 5-card hands that can be made from the 52 cards in the deck, so $|S| = \binom{52}{5} = 2,598,960$. To make a 5-card hand that contains no ace, we have to choose 5 cards from the 48 non-ace cards, so there are $\binom{48}{5} = 1,712,304$ hands that contain no aces. Thus the probability of the event E of no aces in the hand is $p(E) = \frac{|E|}{|S|} = \frac{1,712,304}{2,598,960} \approx 65.88\%$.

Section 5.2

1. A card is taken off the top of a shuffled 52-card deck. What is the probability that it is black or an ace?

Solution: Let A be the event of the card being an ace, and let B be the event of its being black. Then $p(A) = \frac{4}{52}$, and $p(B) = \frac{26}{52}$. The event $A \cap B$ is the event of the card being either the ace of spades or the ace of clubs. Thus $|A \cap B| = 2$, and $p(A \cap B) = \frac{2}{52}$. The answer we seek is $p(A \cup B) = p(A) + p(B) - p(A \cap B) = \frac{4}{52} + \frac{26}{52} - \frac{2}{52} = \frac{28}{52} \approx 53.8\%$.

3. What is the probability that a 5-card hand dealt off a shuffled 52-card deck contains at least one red card?

Solution: The sample space S is the set of all 5-card hands, so $|S| = \binom{52}{5} = 2,598,960$. Let E be the event of a 5-card hand without any red cards. Then $|E| = \binom{26}{5} = 65,780$ (choose 5 cards from the 26 black cards). Note that the complement \bar{E} is the event of at least one red card, so the answer we seek is $p(\bar{E}) = 1 - p(E) = 1 - \frac{|E|}{|S|} = 1 - \frac{65,780}{2,598,960} \approx 97.46\%$.

5. You toss a fair coin 8 times. What is the probability that you do not get 4 heads?

Solution: The sample space S is the set of all length-8 lists made from the symbols H and T . Thus $|S| = 2^8$. Now let E be the event of getting exactly 4 heads, so $|E| = \binom{8}{4} = 70$. (Choose 4 of 8 positions for H and fill the rest with T .) Then \bar{E} is the event of not getting four heads. Our answer is then $p(\bar{E}) = 1 - p(E) = 1 - \frac{|E|}{|S|} = 1 - \frac{70}{2^8} \approx 72.65\%$.

7. Two cards are dealt off a shuffled 52-card deck. What is the probability that the cards are both red or both aces?

Solution: The sample space S consists of all possible 2-card hands, so $|S| = \binom{52}{2} = 1326$. Let A be the event of both cards being aces, so $|A| = \binom{4}{2} = 6$. Let B be the event that both cards are red, so $|B| = \binom{26}{2} = 325$. Then the event $A \cap B$ consists on only one hand, namely the 2-card hand consisting of the ace of hearts and the ace of diamonds. The answer to our question is $p(A \cup B) = p(A) + p(B) - p(A \cap B) = \frac{|A|}{|S|} + \frac{|B|}{|S|} - \frac{|A \cap B|}{|S|} = \frac{6}{1326} + \frac{325}{1326} - \frac{1}{1326} \approx 24.88\%$.

9. A dice is tossed six times. You win \$1 if the first toss is a five or the last toss is even. What are your chances of winning?

Solution: The sample space S is the set of all length-6 lists made from the symbols 1, 2, 3, 4, 5 and 6. Thus $|S| = 6^6$. Let A be the event of the first toss being a five. By the multiplication principle, $|A| = 6^5$. Let B be the event of the last toss being even, that is, 2, 4 or 6. Then $|B| = 6^5 \cdot 3$. Note that $A \cap B$ is the set of all lists in S whose first entry is 5 and whose last entry is even. By the multiplication principle, $|A \cap B| = 6^4 \cdot 3$. The probability that the first toss is a five and the last is even is $p(A \cup B) = p(A) + p(B) - p(A \cap B) = \frac{|A|}{|S|} + \frac{|B|}{|S|} - \frac{|A \cap B|}{|S|} = \frac{6^5}{6^6} + \frac{6^5 \cdot 3}{6^6} - \frac{6^4 \cdot 3}{6^6} = \frac{1}{6} + \frac{3}{6} - \frac{3}{36} = \frac{21}{36} \approx 58.33\%$. So you have a reasonably good chance of winning.

11. A dice is rolled 5 times. Find the probability that not all of the tosses are even.

Solution: Think of the sample space as being the set of all length-5 lists made from the numbers 1, 2, 3, 4, 5 and 6, where the first entry is the result of the first roll, the second entry is the result of the second roll, etc. Thus $|S| = 6^5$. Now let E be the event of all rolls being even. Then E is the set of all length-5 lists made from the numbers 2, 4 and 6, so $|E| = 3^5$. We are interested in the probability of the event of not all rolls being even, that is, the probability of \overline{E} . Thus our answer is $p(\overline{E}) = 1 - p(E) = 1 - \frac{|E|}{|S|} = 1 - \frac{3^5}{6^5} \approx 96.875\%$.

13. Two cards are dealt off a well-shuffled deck. You win \$1 if the two cards are of different suits. Find the probability of your winning.

Solution: The sample space S is the set of all possible 2-card hands, so $|S| = \binom{52}{2} = 1326$. There are $\binom{13}{2} = 78$ 2-card hands with both cards hearts, and similarly 78 hands with both cards diamonds, 78 hands with both cards clubs, and 78 hands with both cards spades. By the addition principle there are $78 + 78 + 78 + 78 = 312$ hands in S for which both cards are of the same suit. So there are $|S| - 312 = 1014$ hands in S for which the cards are of different suits. Thus the probability of the two cards being the same suit is $\frac{312}{|S|} = \frac{1014}{1326} \approx 76.47\%$.

15. A coin is tossed 5 times. What is the probability that the first toss is a head or exactly 2 out of the five tosses are heads?

Solution: The sample space S is the set of length-5 lists made from the symbols H and T, so $|S| = 2^5 = 32$. The event $A \subseteq S$ of the first toss being a head is the set of all lists in S of form H□□□□, so $|A| = 2^4 = 16$. The event B of exactly two heads has cardinality $|B| = \binom{5}{2} = 10$. (Choose two of 5 positions for H, and fill the rest with T's.) Finally, $A \cap B$ is the set of lists in S whose first entry is H and exactly one of the four remaining entries is an H, so $|A \cap B| = 4$. So the

probability of the first toss being a head or exactly two tosses being heads is $p(A \cap B) = p(A) + p(B) - p(A \cup B) = \frac{|A|}{|S|} + \frac{|B|}{|S|} - \frac{|A \cup B|}{|S|} = \frac{16}{32} + \frac{10}{32} - \frac{4}{32} = \frac{22}{32} = 68.75\%$.

17. In a shuffled 52-card deck, what is the probability that neither the top nor bottom card is a heart?

Solution: Regard the sample space as the set of 2-element lists (no repetition) whose entries are the cards in the deck. The first entry represents the top card and the second entry represents the bottom card. Then $|S| = 52 \cdot 51 = 2652$. Now let E be the event that neither the top nor bottom card is a heart. So E consists of those lists in S for which neither entry is a heart. As there are 39 non-heart cards, $|E| = 39 \cdot 38 = 1482$. The answer is thus $p(E) = \frac{|E|}{|S|} = \frac{1482}{2652} \approx 55.88\%$.

19. A bag contains 20 red marbles, 20 green marbles and 20 blue marbles. You reach in and grab 15 marbles. What is the probability that they are all the same color?

Solution: An outcome for this experiment is a 15-element multiset made from the symbols $\{r, g, b\}$. Thus the sample space S is the set of all such multisets. Encode the elements of S as stars and bars, so a typical element of S is a list of length $15 + 2 = 17$, made from 15 stars and 2 bars.

$$\underbrace{** \cdots **}_{* \text{ for each } r} \mid \underbrace{** \cdots **}_{* \text{ for each } g} \mid \underbrace{** \cdots **}_{* \text{ for each } b}$$

Then $|S| = \binom{17}{2} = 136$. Also the event E of all balls being the same color is $E = \{***** \mid \mid, |***** \mid, \mid*****\}$, so $|E| = 3$. Finally, $p(E) = \frac{|E|}{|S|} = \frac{3}{136} \approx 2.2\%$.

Section 5.3

1. A box contains six tickets:

| | | | | | |
|---|---|---|---|---|---|
| A | A | B | B | B | E |
|---|---|---|---|---|---|

. You remove two tickets, one after the other. What is the probability that the first ticket is an A and the second is a B?

Solution: Let A be the event of the first draw being an A and let B be the event of the second draw being a B. With the help of Fact 5.3, the answer to this question is $p(A \cap B) = p(A) \cdot P(B|A) = \frac{2}{6} \cdot \frac{2}{5} = \frac{2}{15} = 13.\bar{3}\%$.

3. In a shuffled 52-card deck, what is the probability that the top card is red and the bottom card is a heart?

Solution: Let A be the event of the top card being red, and let B be the event of the bottom card being a heart. With the help of Fact 5.3, the answer to this question is $p(A \cap B) = p(B) \cdot P(A|B) = \frac{13}{52} \cdot \frac{25}{26} = \frac{25}{104} \approx 20.16\%$. (Notice that if you used the formula $p(A \cap B) = p(A) \cdot p(B|A)$, then the problem is somewhat harder to think about.)

5. Suppose A and B are events, and $P(A) = \frac{1}{2}$, $P(B) = \frac{1}{3}$, and $P(A \cap B) = \frac{1}{6}$. Are A and B independent, dependent, or is there not enough information to say for sure?

Solution: Using the information given, and Fact 5.3, we get $\frac{1}{6} = p(A \cap B) = p(A) \cdot p(B|A) = \frac{1}{2}p(B|A)$, which yields $p(B|A) = \frac{1}{3}$, so $p(B|A) = p(B)$. Also, $\frac{1}{6} = p(A \cap B) = p(B) \cdot p(A|B) = \frac{1}{3}p(A|B)$, which yields $p(A|B) = \frac{1}{2}$, so $p(A) = p(A|B)$. This means A and B are independent.

7. Say A and B are events with $P(A) = \frac{2}{3}$, $P(A|B) = \frac{3}{4}$, and $P(B|A) = \frac{1}{2}$. Find $p(B)$.

Solution: Fact 5.3 says $p(A) \cdot p(B|A) = p(A \cap B) = p(B) \cdot p(A|B)$. Plugging in the given information, this becomes $\frac{2}{3} \cdot \frac{1}{2} = p(B) \cdot \frac{3}{4}$. Solving, $p(B) = \frac{4}{9}$.

9. A box contains 2 red balls, 3 black balls, and 4 white balls. One is removed, and then another is removed. What is the probability that no black balls were drawn?

Let A be the event of no black ball on the first draw. Let B be the event of no black ball drawn on the second draw. Then $p(A) = \frac{6}{9}$, because 6 of the 9 balls are not black. If A has occurred, then 5 of the remaining 8 balls are not black, so $p(B|A) = \frac{5}{8}$. The probability that no black ball was drawn is then $p(A \cap B) = p(A) \cdot p(B|A) = \frac{6}{9} \cdot \frac{5}{8} = \frac{5}{12} = 41.6\%$.

11. A coin is flipped 5 times, and there are more tails than heads. What is the probability that the first flip was a tail?

Solution: The sample space S is the set of length-5 lists made from symbols H and T , so $|S| = 2^5 = 32$. Let A be the event of there being more tails than heads, and let B be the event of the first flip being a tail. Thus the answer to the question will be $p(B|A)$. Fact 5.3 says $p(B|A) = \frac{p(A \cap B)}{p(A)}$, so we need to calculate $p(A \cap B)$ and $p(A)$. Note that $A \cap B$ is the event of more tails than heads **and** the first flip is a tail. If the first flip is a tail, and there are to be more tails than heads, then 2, 3 or 4 of the remaining 4 flips must be tails. The number of ways for this to happen is $\binom{4}{2} + \binom{4}{3} + \binom{4}{4} = 6 + 4 + 1 = 11$, so $|A \cap B| = 11$. Considering $|A|$, to have more tails than heads, 3, 4 or 5 of the flips must be tails, and it follows that $|A| = \binom{5}{3} + \binom{5}{4} + \binom{5}{5} = 10 + 5 + 1 = 16$. To get our final answer, we have

$$p(B|A) = \frac{p(A \cap B)}{p(A)} = \frac{\frac{|A \cap B|}{|S|}}{\frac{|A|}{|S|}} = \frac{|A \cap B|}{|A|} = \frac{11}{16} = 68.75\%.$$

13. A 5-card hand is dealt from a shuffled 52-card deck. Exactly 2 of the cards in the hand are hearts. Find the probability that all the cards in the hand are red.

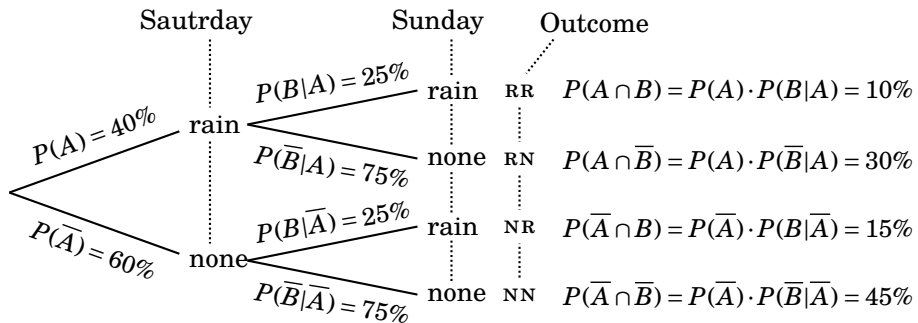
Solution: Let A be the event of getting exactly 2 hearts in the hand. Let B be the event of all cards in the hand being red. Thus the answer to the question will be $p(B|A)$. Fact 5.3 says $p(B|A) = \frac{p(A \cap B)}{p(A)}$, so we need to calculate $p(A \cap B)$ and $p(A)$. Note that $A \cap B$ is the event of getting a 5-card hand that has 2 hearts and 3 diamonds. Thus $|A \cap B| = \binom{13}{2} \binom{13}{3}$. Also $|A| = \binom{13}{2} \binom{39}{3}$ (choose 2 hearts and 3 non-hearts). To get our final answer, we have

$$p(B|A) = \frac{p(A \cap B)}{p(A)} = \frac{\frac{|A \cap B|}{|S|}}{\frac{|A|}{|S|}} = \frac{|A \cap B|}{|A|} = \frac{\binom{13}{2} \binom{13}{3}}{\binom{13}{2} \binom{39}{3}} = \frac{\binom{13}{3}}{\binom{39}{3}} = \frac{13 \cdot 12 \cdot 11}{39 \cdot 38 \cdot 37} \approx 3.13\%.$$

Section 5.4

1. There is a 40% chance of rain on Saturday and a 25% chance of rain on Sunday. What is the probability that it will rain on at least one day of the weekend? (You may assume that the events “Rain on Saturday” and “Rain on Sunday” are independent events.)

Solution: Say A is the event of rain on Saturday and B is the event of rain on Sunday. Then our sample space is $S = \{RR, RN, NR, NN\}$, and $A = \{RR, RN\}$ and $B = \{RR, NR\}$. Here is a probability tree for this.



From this, the probability of rain over the weekend is $10\% + 30\% + 15\% = 55\%$.

If you got the answer without drawing a probability tree, then that is good. Another solution would be to calculate the probability of no rain over the weekend, which is $p(\bar{A}) \cdot p(\bar{B}|\bar{A}) = p(\bar{A}) \cdot p(\bar{B}) = 0.6 \cdot 0.75 = 45\%$. Then the probability of rain over the weekend is $1 - 0.45 = 55\%$.

3. A club consists of 60 men and 40 women. To fairly choose a president and a secretary, names of all members are put into a hat and two names are drawn. The first name drawn is the president, and the second name drawn is the secretary. What is the probability that the president and the secretary have the same gender?

Solution: Say the sample space is $S = \{MM, MW, WM, ww\}$ where the first letter indicates the gender of the first draw, and the second letter indicates the gender of the second draw. Then $p(MM) = \frac{60}{100} \cdot \frac{59}{99} = \frac{3540}{9900}$ and $p(ww) = \frac{40}{100} \cdot \frac{39}{99} = \frac{1560}{9900}$. Thus the probability of both offices being the same gender is $p(\{MM, ww\}) = \frac{3540}{9900} + \frac{1560}{9900} = \frac{5100}{9900} = 51.51\%$.

5. At a certain college, 30% of the students are freshmen. Also, 80% of the freshmen live on campus, while only 60% of the non-freshman students live on campus. A student is chosen at random. What is the probability that the student is a freshman who lives off campus?

Solution: Let A be the event of choosing a freshman. Let B be the event of choosing someone who lives on campus. The given information states that $p(A) = 30\%$ and $p(\bar{B}|A) = 20\%$. (If you chose a freshman, there is an 80% chance he or she lives on campus, so there is a 20% chance he or she lives off campus.)

The problem is asking for $p(A \cap \bar{B})$. Now, $p(A \cap \bar{B}) = p(A) \cdot p(\bar{B}|A) = 0.30 \cdot 0.20 = 6\%$. Thus there is a 6% chance of choosing a freshman who lives off campus.

Section 5.5

1. At a certain college, 40% of the students are male, and 60% are female. Also, 20% of the males are smokers, and 10% of the females are smokers. A student is chosen at random. If the student is a smoker, what is the probability that the student is female?

Solution: Let S be the set of all students, S_1 be the set of female students, and S_2 be the set of male students. Then $S = S_1 \cup S_2$ and $S_1 \cap S_2 = \emptyset$. Let $E \subseteq S$ be the set of smokers. The problem asks for $p(S_1|E)$. Bayes' theorem applies and we get

$$p(S_1|E) = \frac{p(S_1) \cdot p(E|S_1)}{p(S_1) \cdot p(E|S_1) + p(S_2) \cdot p(E|S_2)} = \frac{0.60 \cdot 0.10}{0.60 \cdot 0.10 + 0.40 \cdot 0.20} = \frac{0.6}{0.8} = 75\%.$$

3. A jar contains 4 red balls and 5 white balls. A random ball is removed, and then another is removed. If the second ball was red, what is the probability that the first ball was red?

Solution: The sample space is $S = \{RR, RW, WR, WW\}$, where the first letter is the color of the first ball and the second letter is the color of the second ball. Let $S_1 = \{RR, RW\}$ be the event of the first ball being red. Let $S_2 = \{WR, WW\}$ be the event of the first ball being white. Let $E = \{RR, WR\}$ be the event of the second ball being red. The answer to the question is thus $p(S_1|E)$. As $S = S_1 \cup S_2$ and $S_1 \cap S_2 = \emptyset$, Bayes' formula applies, and it gives

$$\begin{aligned} p(S_1|E) &= \frac{p(S_1) \cdot p(E|S_1)}{p(S_1) \cdot p(E|S_1) + p(S_2) \cdot p(E|S_2)} \\ &= \frac{\frac{4}{9} \cdot \frac{3}{8}}{\frac{4}{9} \cdot \frac{3}{8} + \frac{5}{9} \cdot \frac{4}{8}} = \frac{\frac{1}{6}}{\frac{3}{18} + \frac{5}{18}} = \frac{\frac{1}{6}}{\frac{4}{9}} = \frac{3}{8} = 37.5\%. \end{aligned}$$

So there's a 37.5% chance that the first ball was red if the second is red.

Algorithms

The idea of an *algorithm* is of fundamental importance in computer science and discrete mathematics. Broadly speaking, an algorithm is a sequence of commands that, if followed, result in some desirable outcome. In this sense a recipe for baking a cake is an algorithm. If you follow the instructions you get a cake. A typical algorithm has what we call *input*, that is, material or data that the algorithm uses, and *output*, which is the end result of the algorithm. In following the recipe for a cake, the ingredients are the input. The recipe (algorithm) tells what to do with the ingredients, and the output is a cake.

For another example, the instructions for making an origami swan from a piece of paper is an algorithm. The input is the paper, the algorithm is a sequence of instructions telling how to fold the paper, and the output is a (paper) swan. Different input (in color, size, etc.) leads to different output.

To *run* or *execute* an algorithm means to apply it to input and obtain output. Running or executing the swan algorithm produces a swan as output. We freely use the words “input” and “output” as both nouns and a verbs. The algorithm *inputs* a piece of paper and *outputs* a swan.

Today the word “algorithm” almost always refers to a sequence of steps written in a computer language and executed by a computer, and the input and output are information or data. Doing a Google search causes an algorithm to run. The “Google Algorithm” takes as input a word or phrase, and outputs a list of web pages that contain the word or phrase. When we do a Google search we type in the input. Pressing the Return key causes the algorithm to run, and then the output is presented on the screen.

Running such an algorithm is effortless because the computer does all the steps. But someone (actually, a group of people) designed and implemented it, and this required very specialized knowledge and skills. This chapter is an introduction to these skills. Though our treatment is elementary, the ideas presented here—if taken further—can be applied to designing quite complex and significant algorithms.

In practice, algorithms may have complex “feedback” relationships between input and output. Input might involve our clicking on a certain icon or button, and based on this choice the algorithm might prompt us to enter further information, or even upload files. Output could be as varied as an email sent to some recipient or an object produced by a 3D printer.

For simplicity we will concentrate on algorithms that simply start with input information, act on it, and produce output information at the end. To further simplify our discussion, the input and output information will be mostly numeric or alphanumeric. This is not as limiting as it may sound. Any algorithm—no matter how complex—can be decomposed into such simple “building-block algorithms.”

Although all of our algorithms could be implemented on a computer, we will not express them any particular computer language. Instead we will develop a kind of *pseudocode* that has the basic features of any high-level computer language. Understanding this pseudocode makes mastering any computer language easier. Conversely, if you already know a programming language, then you may find this chapter relatively easy reading.

Our exploration begins with *variables*.

6.1 Variables and the Assignment Command

In an algorithm, a **variable** is a symbol that can be assigned various values. As in algebra, we use letters a, b, c, \dots, z as variables. If convenient, we may subscript our variables, so x_1, x_2 and x_3 are three different variables.

Though there is no harm in thinking of a variable as a name or symbol that represents a number, in programming languages a variable actually represents a location in the computer’s memory that can hold different quantities (i.e., values) at different times. But it can hold only one value at any specific time. As an algorithm runs, it can assign various values to a variable at different points in time.

An algorithm is a sequence of instructions or *commands*. The command that says the variable x is to be assigned the value of 2 is expressed as

$$x := 2,$$

which we read as “ x is assigned the value 2” or “ x gets 2.” Once this command is executed, x stands for the number 2, at least until it is assigned some other value. If a later command is

$$x := 7,$$

then x stands for the value 7. If the next command in the algorithm is

$$y := 2 \cdot x + 1,$$

then the variable y stands for the number 15. If the next command is

$$y := y + 2,$$

then once it executes y has the value $15 + 2 = 17$.

In the context of algorithms, the term *variable* has a slightly different meaning than in algebra. In an algorithm a variable represents a specific value at any point in time, and that value can change over time. But in algebra a variable is a (possibly) indefinite quantity. The difference is highlighted in the algorithm *command* $y := y + 2$, which means y gets a new value that is its previous value plus 2. By contrast, in algebra the *equation* $y = y + 2$ has no solution.

In an algorithm there is a difference between $y := 2$ and $y = 2$. In an algorithm, an expression like $y = 2$ is interpreted as an open sentence that is either true or false. Suppose an algorithm issues the command $y := 2$. Then, afterwards, the expression $y = 2$ has the value True (T), and $y = 3$ has the value False (F). Similarly, $y = y + 2$ is F , no matter the value of y .

6.2 Loops and Algorithm Notation

Programming languages employ certain kinds of *loops* that execute sequences of commands multiple times. One of the most basic kinds of loops is called a **while loop**. It is a special command to execute a sequence of commands as long as (or *while*) an open sentence $P(x)$ involving some variable x is true. A while loop has the following structure. It begins with the word **while** and ends with the word **end**, and these two words enclose a sequence of commands. The vertical bar is just a visual reminder that the commands are all grouped together within the while loop.

```

while  $P(x)$  do
  | Command 1
  | Command 2
  |   ⋮
  | Command  $n$ 
end

```

When the while loop begins running, the variable x has a certain value. If $P(x)$ is true, then the while loop executes Commands 1 through n , which may change the value of x . Then, if $P(x)$ is still true the loop executes Commands 1 through n again. It continues to execute Commands 1 through n until $P(x)$ is false. At that point the loop is finished and the algorithm moves on to whatever command comes after the while loop.

The first time the while loop executes the list of commands is called the **first iteration** of the loop. The second time it executes them is called the **second iteration**, and so on.

In summary, the while loop executes the sequence of commands $1-n$ over and over until $P(x)$ is false. If it happens that $P(x)$ is already false when the while loop begins, then the while loop does nothing.

Let's look at some examples. These will use the command **output** x , which outputs whatever value x has when the command is executed.

Consider the while loop on the right, after the line $x := 1$. It assigns $y := 2 \cdot x$, outputs y , replaces x with $x + 1$, and continues doing this as long as $x \leq 6$. We can keep track of this with a table. After the first iteration of the loop, we have $y = 2 \cdot 1 = 2$ and $x = 1 + 1 = 2$, as shown in the table. In any successive iteration, y is twice what x was at the end of the previous iteration, and x is one more than it was, as reflected in the table. At the end of the 6th iteration, $x = 7$, so $x \leq 6$ is no longer true, so the loop makes no further iterations. From the table we can see that the output is the list of numbers 2, 4, 6, 8, 10, 12

```
x := 1
while x ≤ 6 do
  y := 2 · x
  output y
  x := x + 1
end
```

| iteration | 1 | 2 | 3 | 4 | 5 | 6 |
|-----------|---|---|---|---|----|----|
| x | 2 | 3 | 4 | 5 | 6 | 7 |
| y | 2 | 4 | 6 | 8 | 10 | 12 |

Now let's tweak this example by moving the **output** command from *inside* the loop, to *after* it. This time there is no output until the while loop finishes. The table still applies, and it shows that $y = 12$ after the last iteration, so the output is the single number 12.

```
x := 1
while x ≤ 6 do
  y := 2 · x
  x := x + 1
end
output y
```

Next, consider the example on the right. It is the same as the previous example, except it has $x := x - 1$ instead of $x := x + 1$. Thus x gets smaller with each iteration, and $x \leq 6$ is *always true*, so the while loop continues forever, never stopping. This is what is called an **infinite loop**.

```
x := 1
while x ≤ 6 do
  y := 2 · x
  x := x - 1
end
output y
```

We regard an algorithm as a set of commands that completes a task in a finite number of steps. Therefore infinite loops are to be avoided. The potential for an infinite loop is seen as a mistake or flaw in an algorithm.

Now that we understand assignment commands and while loops, we can begin writing some complete algorithms. For clarity we will use a systematic notation. An algorithm will begin with a header with the word "Algorithm," followed by a brief description of what the algorithm does. Next, the input

and the output is described. Finally comes the **body** of the algorithm, a list of commands enclosed between the words **begin** and **end**. For clarity we write one command per line. We may insert comments on the right margin, preceded by a row of dots. These comments are to help a reader (and sometimes the writer!) understand how the algorithm works; they are *not* themselves commands. (If the algorithm were written in a computer language and run on a computer, the computer would ignore the comments.)

To illustrate this, here is an algorithm whose input is a positive integer n , and whose output is the first n positive even integers. If, for example, the input is 6, the output is the list 2, 4, 6, 8, 10, 12. (Clearly this is not the most impressive algorithm. It is intentionally simple because its purpose is to illustrate algorithm commands and notation.)

Algorithm 1: computes the first n positive even integers

Input: A positive integer n (Tells reader what the
Output: The first n positive even integers input & output is.)
begin
 $x := 1$
 while $x \leq n$ **do**
 $y := 2 \cdot x$ y is the x th even integer
 output y
 $x := x + 1$ increase x by 1
 end
end

In addition to while loops, most programming languages feature a so-called **for loop**, whose syntax is as follows. Here i is a variable, and m and n are integers with $m \leq n$.

for $i := m$ **to** n **do**
 Command
 Command
 :
 Command
end

In its first iteration the for loop sets $i := m$, and executes the list of commands between its first and last lines. In the next iteration it sets $i := m + 1$ and executes the commands again. Then it sets $i := m + 2$ and executes the commands, and so on, increasing i by 1 and executing the commands in each iteration. Finally, it reaches $i := n$ in the last iteration and the commands are executed a final time. None of the commands can alter i , m and n .

To illustrate this, let's rewrite Algorithm 1 with a for loop.

Algorithm 2: computes the first n positive even integers

Input: A positive integer n

Output: The first n positive even integers

begin

for $i := 1$ **to** n **do**

$y := 2 \cdot i$ y is the i th even integer

output y

end

end

6.3 Logical Operators in Algorithms

There is an inseparable connection between algorithms and logic. A while loop continues to execute as long as some open sentence $P(x)$ is true. This open sentence may even involve several variables and be made up of other open sentences joined with logical operators. For example, the following loop executes the list of commands as long as $P(x) \vee \sim Q(y)$ is true.

while $P(x) \vee \sim Q(y)$ **do**

 Command

 Command

\vdots

end

The list of commands must change the values of x or y , so $P(x) \vee \sim Q(y)$ is eventually false, or otherwise we may be stuck in an infinite loop.

Another way that algorithms can employ logic is with what is known as the **if-then** construction. Its syntax is as follows.

if $P(x)$ **then**

 Command

 Command

\vdots

end

If $P(x)$ is true, then this executes the list of commands between the **then** and the **end**. If $P(x)$ is false it does nothing, and the algorithm continues on to whatever commands come after the closing **end**. Of course the open sentence $P(x)$ could also be a compound sentence like $P(x) \vee \sim Q(y)$, etc.

A variation on the **if-then** command is the **if-then-else** command:

```

if  $P(x)$  then
  | Command
  | Command
  |   ⋮
else
  | Command
  |   ⋮
end
    
```

If $P(x)$ is true, this executes the first set of commands, between the **then** and the **else**. And if $P(x)$ is false it executes the second set of commands, between the **else** and the **end**.

Let's use these new ideas to write an algorithm whose input is n and whose output is $n!$. Recall that if $n = 0$, then $n! = 1$ and otherwise $n! = 1 \cdot 2 \cdot 3 \cdot 4 \cdots n$. Thus our algorithm should have the following structure.

```

if  $n = 0$  then
  | output 1 ..... because  $0! = 1$ 
else
  | Compute  $y := n!$  ..... (we need to add the lines that do this)
  | output  $y$ 
end
    
```

To finish it, we need to add in the lines that compute $y = 1 \cdot 2 \cdot 3 \cdot 4 \cdots n$. We do this by first setting $y = 1$ and then use a for loop to multiply y by 1, then by 2, then by 3, and so on, up to a final multiplication by n .

Algorithm 3: computes $n!$

Input: A non-negative integer n
Output: $n!$
begin
 | **if** $n = 0$ **then**
 | | **output** 1because $0! = 1$
 | **else**
 | | $y := 1$
 | | **for** $i := 1$ **to** n **do**
 | | | $y := y \cdot i$
 | | **end**
 | | **output** y because now $y = n!$
 | **end**
end

Lists often occur in algorithms. A list typically has multiple entries, so when stored in a computer's memory it's not stored in single memory location, but rather multiple locations. A list such as $X = (2, 4, 7, 4, 3)$, of length five, might be stored in six successive locations, with the first one (called X) containing the length of X :

| | | | | | |
|-----|-------|-------|-------|-------|-------|
| 5 | 2 | 4 | 7 | 4 | 3 |
| X | x_1 | x_2 | x_3 | x_4 | x_5 |

The memory location X contains the number 5, which indicates that the next five locations store the five entries of the list X . We denote by x_1 the location immediately following X , and the one after that is x_2 , and so on.

If an algorithm issues the command $X := (2, 4, 7, 4, 3)$, it has created a list with first entry $x_1 = 2$, second entry $x_2 = 4$, and so on. If a later command is (say) $x_3 := 1$, then we have $X = (2, 4, 1, 4, 3)$. If we then issued the for loop

```

for  $i := 2$  to 5 do
  |  $x_i := 0$ 
end

```

the list becomes $X = (4, 0, 0, 0, 0)$, etc.

We use uppercase letters to denote lists, while their entries are denoted by a same letter in lowercase, subscripted. Thus if $A = (7, 6, 5, 4, 3, 2, 1)$, then $a_1 = 7$, $a_2 = 6$, etc. The command $X := A$ results in $X = (7, 6, 5, 4, 3, 2, 1)$.

The next algorithm illustrates these ideas. It finds the largest entry of a list. We will deviate from our tendency to use letters to stand for variables, and use the word *biggest* as a variable. The algorithm starts by setting *biggest* equal to the first list entry. Then it traverses the list, replacing *biggest* with any larger entry it finds.

Algorithm 4: finds the largest entry of a list

Input: A list $X = (x_1, x_2, \dots, x_n)$

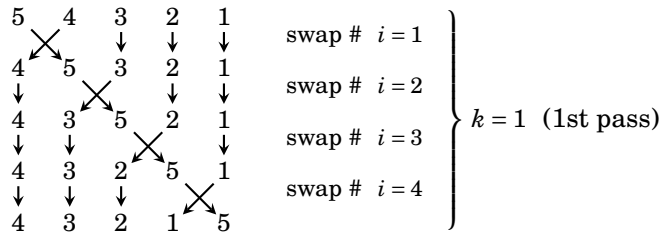
Output: The largest entry in the list

```

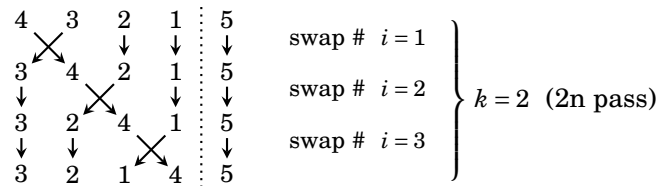
begin
  |  $biggest := x_1$  ..... this is the largest value found so far
  | for  $i := 1$  to  $n$  do
  |   | if  $biggest < x_i$  then
  |   |   |  $biggest := x_i$  ..... this is the largest value found so far
  |   |   end
  |   end
  | end
  | output  $biggest$ 
end

```

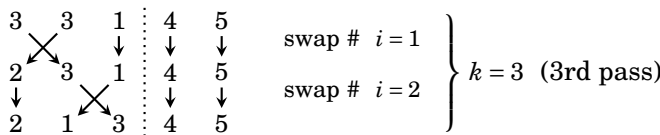
Next we create an algorithm that sorts a list into numerical order. For example, if the input is $X = (4, 5, 1, 2, 1, 3)$, the output will be $X = (1, 1, 2, 3, 4, 5)$. To illustrate the idea, take a very disordered list $X = (5, 4, 3, 2, 1)$. Starting at the first entry, it and the second entry are out of order, so swap them to get a new list $X = (4, 5, 3, 2, 1)$, shown on the second row below. Then move to the second entry of this new X . It and the third entry are out of order, so swap them. Now $X = (4, 3, 5, 2, 1)$ as on the third row below. Continue, in this pattern, moving left to right. For this particular list, four swaps occur.



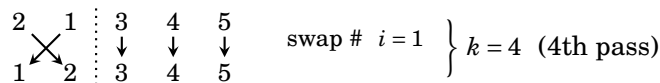
Now the last entry is in correct position, but those to its left are not. Make a second pass through the list, swapping any out of order pairs. But we can stop just before reaching the last entry, as it is placed correctly:



Now the last two entries are in their correct places. Make another pass through the list, this time stopping two positions from the left:



Now the last *three* entries are correct. We need only swap the first two.



This final list is in numeric order. Note that in this example the input list $X = (5, 4, 3, 2, 1)$ was totally out of order, and we had two swap every pair we encountered. In general, if a pair happens not to be out of order, we simply don't swap it. Our next algorithm implements this plan.

In sorting the example list of length $n = 5$ on the previous page, we had to make $n - 1$ passes through the list, numbered $k = 1, 2, 3, \dots, n - 1$. In the k th pass, we compared and swapped $i = n - k$ consecutive pairs of list entries (one less swap each time k increases). Our algorithm carries out this pattern with a for loop letting k run from 1 to $n - 1$. Inside this loop is another for loop that lets i run from 1 to $n - k$, and on each iteration comparing x_i to x_{i+1} and swapping if the first is larger than the second.

Algorithm 5: (Bubble Sort) sorts a list

Input: A list $X = (x_1, x_2, \dots, x_n)$ of numbers

Output: The list sorted into numeric order

```

begin
  for  $k := 1$  to  $n - 1$  do
    for  $i := 1$  to  $n - k$  do
      if  $x_i > x_{i+1}$  then
         $temp := x_i$  ..... temporarily holds value of  $x_i$ 
         $x_i := x_{i+1}$ 
         $x_{i+1} := temp$  ..... now  $x_i$  and  $x_{i+1}$  are swapped
      end
    end
  end
  output  $X$  ..... now  $X$  is sorted
end

```

Computer scientists call Algorithm 5 the **bubble sort** algorithm, because smaller numbers “bubble up” to the front of the list. It is not the most efficient sorting algorithm (In Chapter 20 we’ll see one that takes far fewer steps), but it gets the job done.

Our bubble sort algorithm has a for loop inside of another for loop. In programming, loops inside of loops are said to be **nested**. Nested loops are very common in the design of algorithms.

For full disclosure, Algorithm 5 has a minor flaw. You may have noticed it. What if the input list had length $n = 1$, like $X = (3)$? Then the first for loop would try to execute “**for** $k := 1$ **to** 0 **do**.” This makes no sense, or could lead to an infinite loop. The same problem happens X is the empty list. It would be easy to insert an if-else statement to handle this possibility. In the interest of simplicity (and pedagogy) we did not do this. The purpose of our Algorithm 5 is really to illustrate the idea of bubble sort, and not to sort any real-life lists. But professional programmers must be absolutely certain that their algorithms are robust enough to handle any input.

Exercises for Sections 6.1, 6.2 and 6.3

1. Find the output.

```

x := 1
y := 10
while x2 < y do
    | y := y + x
    | x := x + 1
end
output x
output y
    
```

2. Find the output.

```

s := 0
t := 0
for i := 1 to 4 do
    | s := s + t
    | t := t + i
end
output s
output t
    
```

3. Find the output.

```

a := 0
b := 3
for i := 1 to 8 do
    | if a < b then
    | | a := a + i
    | else
    | | b := b + a
    | end
end
output a
output b
    
```

4. Find the output if the input is $X = (3, 6, 4, 9, 5, 1, 6, 2, 5, 7)$.

Algorithm

```

Input:  $X = (x_1, x_2, \dots, x_n)$ 
begin
    for i := 2 to n do
        | z := xi-1
        | xi-1 := xi
        | xi := z
    end
    output X
end
    
```

5. Input is a list of even length. Find the output for input $X = (3, 5, 8, 4, 6, 8, 7, 4, 2, 3)$.

Algorithm

```

Input:  $X = (x_1, x_2, \dots, x_n)$ 
begin
    for i := 1 to  $\frac{n}{2}$  do
        | k := 2i
        | xk := xk + 1
    end
    for j := 1 to  $\frac{n}{2}$  do
        | k := 2j - 1
        | xk := xk - 1
    end
    output X
end
    
```

6. The following algorithm accepts a list X of numbers as input. What does the algorithm do?

Algorithm

```

Input:  $X = (x_1, x_2, \dots, x_n)$ 
Output: ?
begin
    x := 0
    for i = 1 to n do
        | x := x + xi
    end
    output  $\frac{x}{n}$ 
end
    
```

7. The **Fibonacci sequence** is the sequence $1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \dots$ whose first two terms are 1 and 1, and thereafter any term is the sum of the previous two terms. The numbers in this sequence are called **Fibonacci numbers**. Write an algorithm whose input is an integer n and whose output is the first n Fibonacci numbers.
 8. A **geometric sequence** with ratio r is a sequence of numbers for which any term is r times the previous term. For example, $5, 10, 20, 40, 80, 160, \dots$ is a geometric sequence with ratio 2. Write an algorithm whose input is three numbers $a, r \in \mathbb{R}$, and $n \in \mathbb{N}$, and whose output is the first n terms of the geometric sequence with first term a and ratio r .
 9. Write an algorithm whose input is two integers n and k , and whose output is $\binom{n}{k}$.
 10. Write an algorithm whose input is a list of numbers (x_1, x_2, \dots, x_n) , and whose output is the smallest number in the list.
 11. Write an algorithm whose input is a list of numbers (x_1, x_2, \dots, x_n) , and whose output is the word "YES" if the list has any repeated entries, and "NO" otherwise.
 12. Write an algorithm whose input is two integers n, k and whose output is $P(n, k)$ (as defined in Fact 4.4 on page 97).
 13. Write an algorithm whose input is two positive integers n, k , and whose output is the number of non-negative integer solutions of the equation $x_1 + x_2 + x_3 + \dots + x_k = n$. (See Section 4.8.)
 14. Write an algorithm whose input is a list $X = (x_1, x_2, \dots, x_n)$ and whose output is the word "YES" if $x_1 \leq x_2 \leq \dots \leq x_n$, or "NO" otherwise.
 15. As noted at the bottom of page 182, our Algorithm 5 does not work on lists of length 1 or 0. Modify it so that it does.
 16. Write an algorithm whose input is a list $X = (x_1, \dots, x_n)$, and whose output is the list X in reverse order. (For example input $(1, 3, 2, 3)$ yields output $(3, 2, 3, 1)$.)
 17. Write an algorithm whose input is an integer n , and whose output is the n th row of Pascal's triangle.
-

6.4 The Division Algorithm

Many times in this book we will need to use the basic fact that any integer a can be divided by an integer $b > 0$, resulting in a quotient q and remainder r , for which $0 \leq r < b$. In other words, given any two integers a and $b > 0$, we can find two integers q and r for which

$$a = qb + r, \quad \text{and} \quad 0 \leq r < b.$$

As an example, $b = 3$ goes into $a = 17$ $q = 5$ times with remainder $r = 2$. In symbols, $17 = 5 \cdot 3 + 2$, or $a = qb + r$.

We are now going to write an algorithm whose input is two integers $a \geq 0$ and $b > 0$, and whose output is the two numbers q and r , for which $a = qb + r$ and $0 \leq r < b$. That is, the output is the quotient and remainder that results in dividing a by b .

To see how to proceed, notice that if $a = qb + r$, then

$$a = \underbrace{b + b + b + \cdots + b}_{q \text{ times}} + r,$$

where the remainder r is less than b . This means that we can get r by continually subtracting b from a until we get a non-negative number r that is smaller than b . And then q is the number of times we had to subtract b . Our algorithm does just this. It keeps subtracting b from a until it gets an answer that is smaller than b (at which point no further b 's can be subtracted). A variable q simply counts how many b 's have been subtracted.

Algorithm 6: The division algorithm

Input: Integers $a \geq 0$ and $b > 0$

Output: Integers q and r for which $a = qb + r$ and $0 \leq r < b$

begin

$q := 0$ so far we have subtracted b from a zero times

while $a \geq b$ **do**

$a := a - b$ subtract b from a until $a \geq b$ is no longer true

$q := q + 1$ q increases by 1 each time a b is subtracted

end

$r := a$ a now equals its original value, minus q b 's

output q

output r

end

The division algorithm is actually quite old, and its origins are unclear. It goes back at least as far as ancient Egypt and Babylonia. Obviously it was not originally something that would be implemented on a computer. It was just a set of instructions for finding a quotient and remainder.

It has survived because it is so fundamental and useful. Actually, in mathematics the term *division algorithm* is usually understood to be the statement that any two integers a and $b > 0$ have a quotient and remainder. It is this statement that will be most useful for us later in this course.

Fact 6.1 (The Division Algorithm) Given integers a and b with $b > 0$, there exist integers q and r for which $a = qb + r$ and $0 \leq r < b$.

This will be very useful for proving many theorems about numbers and mathematical structures and systems, as we will see later in the course.

Notice that Fact 6.1 does not require $a \geq 0$, as our algorithm on the previous page did. In fact, the division algorithm in general works for any value of a , positive or negative. For example, if $a = -17$ and $b = 3$, then

$$a = qb + r$$

is achieved as

$$-17 = -6 \cdot 3 + 1,$$

that is, $b = 3$ goes into $a = -17$ $q = -6$ times, with a remainder of $r = 1$. Notice that indeed $0 \leq r \leq b$. Exercise 6.12 asks us to adapt Algorithm 6 so that it works for both positive and negative values of a .

6.5 Procedures and Recursion

In writing an algorithm, we may have to reuse certain blocks of code numerous times. Imagine an algorithm that has to sort two or more lists. For each sort, we'd have to insert code for a separate bubble sort. Rewriting code like this is cumbersome, inefficient and annoying.

To overcome this problem, most programming languages allow creation of *procedures*, which are mini-algorithms that accomplish some task. In general, a procedure is like a function $f(x)$ or $g(x, y)$ that we plug values into and get a result in return.

We will first illustrate this with a concrete example, and afterwards we will define the syntax for general procedures. Here is a procedure that computes $n!$.

Procedure $\text{Fac}(n)$

```

begin
  if  $n = 0$  then
    | return 1 ..... because  $0! = 1$ 
  else
    |  $y := 1$ 
    | for  $i := 1$  to  $n$  do
    |   |  $y := y \cdot i$ 
    |   end
    | return  $y$  ..... now  $y = n!$ 
  end
end

```

This procedure now acts as a function called Fac . It takes as input a number n and returns the value $y = n!$, as specified in the **return** command on the last line. For example $\text{Fac}(3) = 6$, $\text{Fac}(4) = 24$, and $\text{Fac}(5) = 120$. Now that we have defined it we could use it in (say) an algorithm to compute $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.

Algorithm 7: to compute $\binom{n}{k}$

```

Input: Integers  $n$  and  $k$ , with  $n \geq 0$ 
Output:  $\binom{n}{k}$ 
begin
  if  $(k < 0) \vee (k > n)$  then
    | output 0 ..... in this case  $\binom{n}{k} = 0$ 
  else
    | output  $\frac{\text{Fac}(n)}{\text{Fac}(k) \cdot \text{Fac}(n-k)}$  ..... procedure  $\text{Fac}$  is called here
  end
end

```

If an algorithm (like the one above) uses a previously-defined procedure, we say the algorithm **calls** the procedure.

In general, a procedure named (say) *Name* has the following syntax. The first line declares the name of the procedure, followed by a list of variables that it takes as input. The body of the procedure has a list of commands, including the **return** statement, saying what value the procedure returns.

Procedure *Name*(list of variables)

```

begin
  command
  :
  return value
end

```

Our next example is a procedure called `Largest`. Its input is a list (x_1, x_2, \dots, x_n) of numbers, and it returns the largest entry. For example, `Largest(7, 2, 3, 8, 4) = 8`. It is just a recasting of Algorithm 4 into a procedure.

Procedure `Largest` $(x_1, x_2, x_3, \dots, x_n)$

```

begin
  biggest :=  $x_1$  ..... this is the largest value found so far
  for  $i := 1$  to  $n$  do
    if  $biggest < x_i$  then
      | biggest :=  $x_i$  ..... this is the largest value found so far
    end
  end
  return biggest
end

```

To conclude the section, we explore a significant idea called *recursion*. Although this is a far-reaching idea, it will not be used extensively in the remainder of this book. But it is a fascinating topic, even mind-boggling.

We have seen that a procedure is a set of instructions for completing some task. We also know that algorithms may call procedures, and you can imagine writing a procedure that calls another procedure. But under certain circumstances it makes sense for a procedure to call *itself*. Such a procedure is called a **recursive procedure**.

Here is an example. We will call it `RFac` (for RecursiveFactorial). It is our second procedure for computing a factorial, that is, $\text{RFac}(n) = n!$. It uses the fact that $n! = n \cdot (n - 1)!$, which is to say $\text{RFac}(n) = n \cdot \text{RFac}(n - 1)$.

Procedure `RFac` (n)

```

begin
  if  $n = 0$  then
    | return 1 ..... because  $0! = 1$ 
  else
    | return  $n \cdot \text{RFac}(n - 1)$  ..... because  $n! = n \cdot (n - 1)!$ 
  end
end

```

To understand how it works, consider what happens when we run, say, `RFac(5)`. Because $5 \neq 0$, the procedure's code says it needs to return $5 \cdot \text{RFac}(4)$. But before doing *this*, it needs to run `RFac(4)`. But `RFac(4)` needs to return $4 \cdot \text{RFac}(3)$, and `RFac(3)` needs to run `RFac(2)`, and so on.

Figure 6.1 helps keep track of this. Each call to `RFac` is indicated by a shaded rectangle. The rectangles are nested, one within another, reflecting the pattern in which calls to `RFac` occur within other calls to `RFac`.

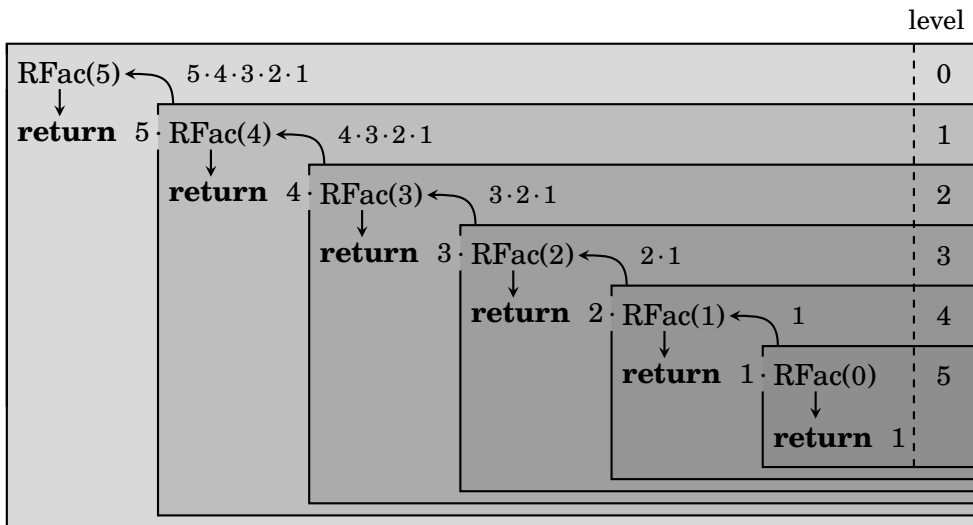


Figure 6.1. Running `RFac(5)`: First `RFac(5)` needs to return $5 \cdot \text{RFac}(4)$. Before returning this value, `RFac(4)` must be run. Now, `RFac(4)` must return $4 \cdot \text{RFac}(3)$, so it runs `RFac(3)` and waits for the result. Then `RFac(3)` must return $3 \cdot \text{RFac}(2)$, so it runs `RFac(2)` and waits for the result. Then `RFac(2)` must return $2 \cdot \text{RFac}(1)$, so it runs `RFac(1)` and wait for the result. Then `RFac(1)` must return $1 \cdot \text{RFac}(0)$. Here the pattern stops, as `RFac(0)` simply returns 1 (according to the procedure’s code). At this point, none of the calls `RFac(5)`, `RFac(4)`, `RFac(3)`, `RFac(2)`, and `RFac(1)` is finished, because each is waiting for the next one to finish. Now `RFac(1)` returns $1 \cdot \text{RFac}(0) = 1 \cdot 1 = 1$ to `RFac(2)`, which is waiting for that value. Next `RFac(2)` returns $2 \cdot \text{RFac}(1) = 2 \cdot 1$ to `RFac(3)`, and `RFac(3)` returns $3 \cdot \text{RFac}(2) = 3 \cdot 2 \cdot 1$ to `RFac(4)`. Finally, `RFac(4)` returns $4 \cdot \text{RFac}(3) = 4 \cdot 3 \cdot 2 \cdot 1$ to `RFac(5)`. At last `RFac(5)` returns to correct vlaue of $5 \cdot \text{RFac}(4) = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$.

A procedure that calls itself is a **recursive procedure**. The situation in which a procedure calls itself (i.e., runs a copy of itself) is called **recursion**.

Some mental energy may be necessary in order to fully grasp recursion, but practice and experience will bring you to the point that you can design programs that use it. We will see recursion in several other places in this text. Section 14.2 will introduce a method of *proving* that recursion really works. In Section 20.4 designs a recursive sorting algorithm that is much quicker and more efficient than bubble sort.

Exercises for Sections 6.4 and 6.5

1. Write a procedure whose input is a list of numbers $X = (x_1, x_2, \dots, x_n)$, and whose output is the list in reverse order.
 2. Write a procedure whose input is two positive numbers n and k , and whose output is $P(n, k)$ (as defined in Fact 4.4 on page 97).
 3. Write a procedure whose input is a list of numbers $X = (x_1, x_2, \dots, x_n)$, and whose output is “YES” if X is in numeric order (i.e., $x_1 \leq x_2 \leq \dots \leq x_n$), and “NO” otherwise.
 4. Write a procedure whose input is a list of numbers $X = (x_1, x_2, \dots, x_n)$, and whose output is the number of entries that are negative.
 5. Write a procedure whose input is a list $X = (0, 0, 1, 0, 1, \dots, 1)$ of 0’s and 1’s, of length n . The procedure returns the number of 1’s in X .
 6. Write a procedure whose input is a list of numbers $X = (x_1, x_2, \dots, x_n)$, and whose output is the average of all the entries.
 7. Write a procedure whose input is a list of numbers $X = (x_1, x_2, \dots, x_n)$, and whose output is the product of $x_1 x_2 \dots x_n$ of all the entries.
 8. Write a procedure whose input is a list of numbers $X = (x_1, x_2, \dots, x_n)$, and whose output is the list $(x_1, 2x_2, 3x_3, \dots, nx_n)$.
 9. Write a procedure whose input is two lists of numbers $X = (x_1, x_2, \dots, x_n)$ and $Y = (y_1, y_2, \dots, y_n)$, and whose output is the list $Z = (x_1, x_2, x_3, \dots, x_n, y_n, \dots, y_3, y_2, y_1)$.
 10. Write a procedure whose input is two lists of numbers $X = (x_1, x_2, \dots, x_n)$ and $Y = (y_1, y_2, \dots, y_n)$, and whose output is the merged list $Z = (x_1, y_1, x_2, y_2, x_3, y_3, \dots, x_n, y_n)$.
 11. Write a procedure whose input is two lists of numbers $X = (x_1, x_2, \dots, x_n)$ and $Y = (y_1, y_2, \dots, y_n)$, and whose output is the list $Z = (x_1 + y_1, x_2 + y_2, x_3 + y_3, \dots, x_n + y_n)$.
 12. Algorithm 6 is written so that it requires $a > 0$. Rewrite it so that it works for all values of a , both positive and negative. (But still assume $b > 0$.)
 13. The **Fibonacci sequence** is 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, The first two terms are 1, and thereafter any term is the sum of the previous two terms. The numbers in this sequence are called **Fibonacci numbers**. Write a *recursive* procedure whose input is an integer n and whose output is the n th Fibonacci number.
 14. A **geometric sequence** with ratio r is a sequence of numbers for which any term is r times the previous term. For example, 5, 10, 20, 40, 80, 160, ... is a geometric sequence with ratio 2. Write an *recursive* procedure whose input is three numbers $a, r \in \mathbb{R}$, and $n \in \mathbb{N}$, and whose output is the n th term of the geometric sequence with first term a and ratio r .
 15. An **arithmetic sequence** with difference d is a sequence of numbers for which any term is d plus the previous term. For example, 5, 8, 11, 14, 17, 20, ... is an arithmetic sequence with difference 3. Write an *recursive* procedure whose input is three numbers $a, d \in \mathbb{R}$, and $n \in \mathbb{N}$, and whose output is the n th term of the arithmetic sequence whose first term is a and whose difference is d .
-

6.6 Counting Steps in Algorithms

Computer scientists are attentive to algorithm *efficiency*. An algorithm should complete its task in the shortest amount of time possible, with the fewest number of steps. Of course the number of steps needed probably depends on what the input is. Thus a significant question is

How many steps does Algorithm X have to make to process input Y?

To get started, suppose an algorithm has the following piece of code, where n has been assigned an integer value in some previous line.

```

for  $i := 1$  to  $3n$  do
  | Command 1
  | Command 2
end
Command 3
for  $j := 1$  to  $n$  do
  | for  $k := 1$  to  $n$  do
  | | Command 4
  | end
end

```

In all, how many commands are executed? The first for loop makes $3n$ iterations, each issuing two commands, so it makes $3n \cdot 2 = 6n$ commands. Then a single command (Command 3) is executed. Next comes a nested for loop, where Command 4 is executed once for each pair (i, k) with $1 \leq j, k \leq n$. By the multiplication principle, there are $n \cdot n = n^2$ such pairs, so Command 4 is executed n^2 times. So in all, $6n + 1 + n^2$ commands are executed.

Now let's count the steps in this chunk of code:

```

for  $i := 0$  to  $n$  do
  | for  $j := 0$  to  $i$  do
  | | for  $k := 0$  to  $j$  do
  | | | Command 1
  | | end
  | end
end

```

Command 1 is executed for each combination of i, j, k with $0 \leq k \leq j \leq i \leq n$. Each combination corresponds to a list of n stars and 3 bars `***|**|*|**...*` where k is the number of stars to the left of the first bar, j is the number of stars to the left of the second bar, and i is the number of stars to the left of the third bar. Such a list has length $n + 3$, and we can make it by choosing 3 out of $n + 3$ spots for the bars and filling the rest with stars.

There are $\binom{n+3}{3}$ such lists, so the number of times Command 1 is executed is $\binom{n+3}{3} = \frac{n(n-1)(n-2)}{3!} = \frac{n^3-3n^2+2n}{6} = \frac{1}{6}n^3 - \frac{1}{2}n^2 + \frac{1}{3}n$.

We finish the chapter by comparing two different algorithms that do the same task, namely search through a sorted list of numbers to determine if a particular number appears. We will see that the second (somewhat more complex) algorithm is vastly more efficient in terms of commands executed.

Each algorithm takes as input a number z and a list $X = \{x_1, x_2, \dots, x_n\}$ of numbers in numeric order, that is, $x_1 \leq x_2 \leq \dots \leq x_n$. The output is the word “YES” if z equals some list entry; otherwise it returns the word “NO.”

The first algorithm, called **sequential search**, simply traverses the list from left to right, stopping either when it finds $z = x_k$, or when it goes past the end of the list without ever finding such an x_k . A variable *found* equals either the word “YES” or the word “NO.” The algorithm starts by assigning *found* := NO, and changes it to “YES” only when and if it finds a k for which $z = x_k$. It has a while loop that continues running as long as *found* := NO (no match found yet) and $k \leq n$ (it hasn’t run past the end of the list).

Algorithm 8: sequential search

Input: A number z and a sorted list $X = (x_1, x_2, \dots, x_n)$ of numbers

Output: “YES” if z appears in X ; otherwise “NO”

begin

found := NO means z not yet found in X

$k := 0$ k is subscript for list entries x_k

while (*found* = NO) \wedge ($k < n$) **do**

$k := k + 1$ go to next list entry

if $z = x_k$ **then**

 | *found* := YES the number z appears in X

end

end

output *found*

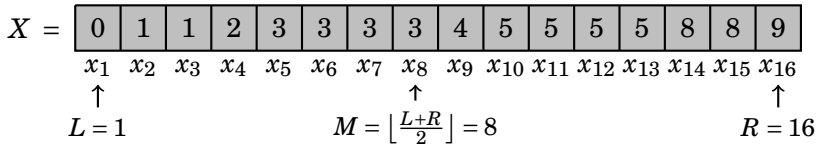
end

Two comments. First, we could opt to also output k at the end of the algorithm, to tell which which list entry x_k equals z in the event of YES. Second, the sequential search algorithm also works just as well when X is not in numeric order. (But this will not be the case with our next algorithm.)

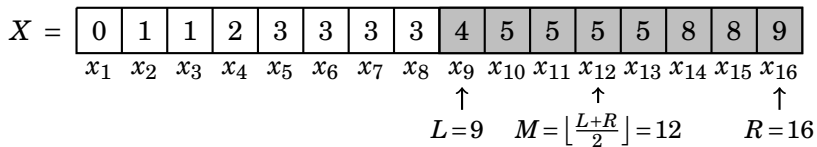
Counting steps, Algorithm 8 has two commands prior to the while loop. Then the while loop does at most n iterations, each with two commands. So it searches a list of length n in at most $2 + 2n$ steps. This is a worst-case scenario, in which z is not found, or it is found at the very end of the list. At the other extreme, if $x_1 = z$, then the algorithm stops after 4 steps.

Next we design an algorithm that takes a different approach to searching a list. Unlike sequential search, which examines every list entry, this new method ignores almost all entries but still returns the correct result.

To illustrate the idea, suppose we need to decide if $z = 4$ is in the list $X = (0, 1, 1, 2, 3, 3, 3, 3, 4, 5, 5, 5, 5, 8, 8, 9)$. If z is in the list, it is in the shaded area between the left-most position $L = 1$ and the right-most position $R = 16$.

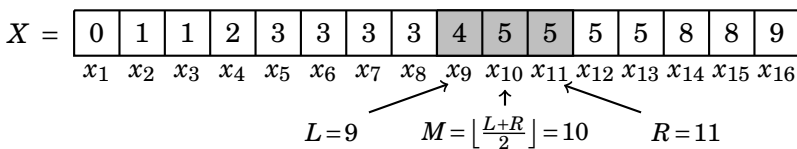


Jump to a middle position $M = \lfloor \frac{L+R}{2} \rfloor = 8$, the average of L and R , rounded down (if necessary) to an integer. The number $z = 4$ we are searching for is greater than $x_M = 3$, so it is to the right of x_8 , in the shaded area below.

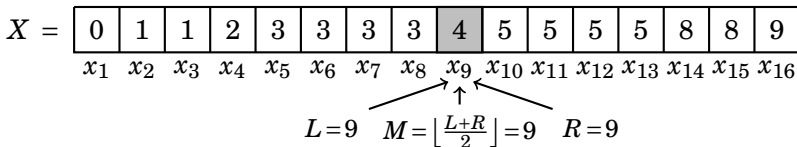


So update $L := M + 1$ and form a new middle $M := \lfloor \frac{L+R}{2} \rfloor = 12$ (shown above).

Now $x_M = 5$, and the number $z = 4$ we seek is less than x_M , so it is in the shaded area below. So update $R := M - 1$. Form a new middle $M := \lfloor \frac{L+R}{2} \rfloor = 10$.



Again, $x_M = 5$, and the number $z = 4$ we seek is less than x_M , so it is in the shaded area below. Update $R := M - 1$ and form a new middle $M := \lfloor \frac{L+R}{2} \rfloor = 9$.



Now $L = R$, and we have zeroed in at $x_M = 4$, the number sought, and having ignored most entries of the list.

This new search strategy is called **binary search**. Binary search works by continually maintaining two list positions L (left) and R (right) that the searched-for entry z must be between. In each iteration, a middle M is computed. If $x_M = z$, we have found z . If $x_M < z$, then z is to the right of M , so $M + 1$ becomes the new L . If $x_M > z$, then z is to the left of M , so $M - 1$ becomes the new R . In this way, L and R get closer and closer to each other, trapping z between them (if indeed X contains z). If z is not in X , then eventually $L = R$. At this point the algorithm terminates and reports that z is not in X .

Algorithm 9: binary search

Input: A number z , and a sorted list $X = (x_1, x_2, \dots, x_n)$ of numbers

Output: “YES” if z appears in X ; otherwise “NO”

begin

$found := \text{NO}$ this means z has not yet been found in X

$L := 1$ left end of search area is x_1

$R := n$ right end of search area is x_n

while $(found = \text{NO}) \wedge (L < R)$ **do**

$M := \left\lfloor \frac{L + R}{2} \right\rfloor$ M is middle of search area

if $z = x_M$ **then**

$found := \text{YES}$ the number z appears in X

else

if $z < x_M$ **then**

$R := M - 1$ if z is in X , it's between x_L and x_M

else

$L := M + 1$ if z is in X , it's between x_M and x_R

end

end

end

output $found$

end

Let's analyze the number of steps needed perform a binary search on a list of length n . Algorithm 9 starts with 3 commands, initializing $found$, L and R . Then comes the while loop, which iterates until $found = \text{YES}$ or $L = R$. How many iterations could this be? Before the first iteration, the distance between L and R is $n - 1$. At each iteration, the distance between L and R is at least halved.

Thus, after the first iteration the distance between L and R is less than $\frac{n}{2}$. After the second iteration the distance between them is less than $\frac{1}{2} \cdot \frac{n}{2} = \frac{n}{2^2}$. After the third iteration the distance between them is less than $\frac{1}{2} \cdot \frac{n}{2^2} = \frac{n}{2^3}$. Thus, after i iterations, the distance between L and R is less than $\frac{n}{2^i}$.

So in the worse case, the while loop keeps running, for i iterations, until

$$\frac{n}{2^i} \leq 1 < \frac{n}{2^{i-1}},$$

which is the smallest i for which we can be confident that the distance between R and L is less than 1 (and hence 0). Multiplying this by 2^i yields

$$n \leq 2^i < 2n.$$

We can isolate the number of iterations i by taking \log_2 , and using various logarithm properties.¹

$$\begin{aligned} \log_2(n) &\leq \log_2(2^i) < \log_2(2n) \\ \log_2(n) &\leq i < \log_2(2) + \log_2(n) \\ \log_2(n) &\leq i < 1 + \log_2(n). \end{aligned}$$

So the number of iterations i is an integer that is between $\log_2(n)$ and $1 + \log_2(n)$, which means $i = \lceil \log_2(n) \rceil$. (Generally $\log_2(n)$ is not an integer, unless $n = 2^k$ is an integer power of 2, in which case $\log_2(n) = \log_2(2^k) = k$.)

In summary, the binary search algorithm (Algorithm 9) issues 3 commands, followed by a while loop that makes at most $\lceil \log_2(n) \rceil$ iterations. Each iteration executes 2 commands: the assignment of $M = \lfloor \frac{L+R}{2} \rfloor$, followed by an if-else statement. Thus the binary search algorithm does a total of at most $3 + 2\lceil \log_2(n) \rceil$ steps to search a list of length n .

By contrast, we saw that sequential search (Algorithm 8) needs at most $2 + 2n$ steps to search a list of length n . Figure 6.2 compares the graphs of $y = 2 + 2n$ with $y = 3 + 2\log_2(n)$, showing that in general binary search involves far fewer steps than sequential search. This is especially pronounced for long lists. For example, if a list X has length $n = 2^{15} = 32768$, a sequential search could take as many as $2 + 2 \cdot 32768 = 65538$ steps, but a binary search is guaranteed to finish in no more than $3 + 2\log_2(32768) = 3 + 2 \cdot 15 = 33$ steps.

This case study illustrates a very important point. An algorithm that cannot finish quickly is of limited use, at best. In our technological world, it is often not acceptable to have to wait seconds, minutes, or hours for an

¹If your logarithm skills are rusty, we will review logarithms in Chapter 19. They will not be used in a substantial way until Chapter 20.

algorithm to complete a critical task. Programmers need to compare the relative efficiencies of different algorithm designs, and to create algorithms that run quickly. The ability to do this rests on the foundation of the counting techniques developed in Chapter 4. We will take up this topic again, in Chapter 20, and push it further.

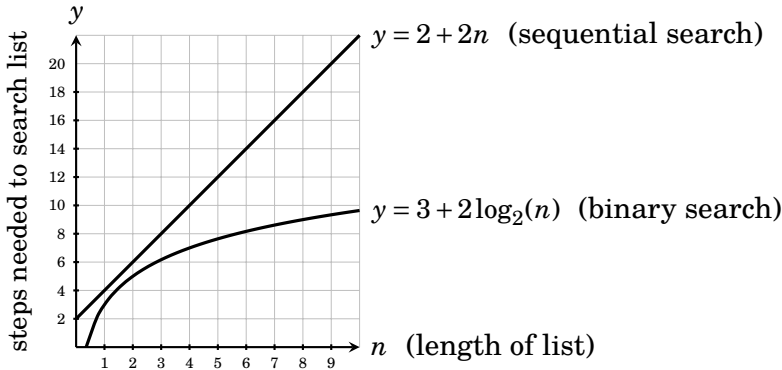


Figure 6.2. A comparison of the worst-case performance of sequential versus binary search, for lists of length n .

Exercises for Section 6.6

1. Count how many times Command is executed.

```

for  $i := 1$  to 60 do
  | for  $j := 1$  to  $i$  do
  | | Command
  | end
end

```

2. Count how many times Command is executed.

```

for  $i := 1$  to 60 do
  | for  $j := 1$  to  $i$  do
  | | Command
  | end
end

```

3. Let n be a positive integer. How many times is Command executed? (The answer depends on n .)

```

for  $i := 0$  to  $n$  do
  | for  $j := 0$  to  $i$  do
  | | for  $k := 0$  to  $j$  do
  | | | for  $\ell := 0$  to  $k$  do
  | | | | Command
  | | | | end
  | | | end
  | | end
  | end
end

```

4. Suppose n is a positive integer. How many times is Command executed? (The answer depends on n .)

```

for  $i := 1$  to  $n$  do
  | for  $j := 1$  to  $n$  do
  | | for  $k := 1$  to  $n$  do
  | | | for  $\ell := 1$  to  $n$  do
  | | | | Command
  | | | | end
  | | | end
  | | end
  | end
end

```

5. Count how many times Command is executed.

```

for  $i := 1$  to 2017 do
  | if  $i$  is even then
  | | Command
  | else
  | | Command
  | | Command
  | end
end

```

6. Count how many times Command is executed.

```

for  $i := 0$  to 4 do
  | for  $j := 0$  to 40 do
  | | for  $k := 0$  to 400 do
  | | | Command
  | | end
  | end
end

```

7. How many steps does the bubble sort algorithm (Algorithm 5 on page 182) take if its input list $X = (x_1, x_2, \dots, x_n)$ is already sorted?
8. Find a formula for the number of steps that Algorithm 1 (page 177) executes for an input of n .
9. Find a formula for the number of steps that Algorithm 2 (page 178) executes for an input of n .
10. Find a formula for the number of steps that Algorithm 3 (page 179) executes for an input of $n > 0$.
11. Find a formula for the number of steps that Algorithm 4 (page 180) executes when the input is a list of length n .
12. Find a formula for the worst-case number of steps that the bubble sort algorithm (Algorithm 5 on page 182) executes when the input is a list of length n .
13. Find a formula for the number of steps that The division algorithm (Algorithm 6 on page 185) executes when the input is two positive integers a and b . (The answer will depend on a and b .)
-

6.7 Solutions for Chapter 6

Sections 6.1, 6.2 and 6.3

1. Find the output.

```

x := 1
y := 10
while x2 < y do
  | y := y + x
  | x := x + 1
end
output x
output y

```

Solution The following table tallies the values of x and y initially, and at the end of each iteration of the while loop.

| iteration | | 1 | 2 | 3 |
|-----------|----|----|----|----|
| x | 1 | 2 | 3 | 4 |
| y | 10 | 11 | 13 | 16 |

The final values (which are the output) are $x = 4$ and $y = 16$.

3. Find the output.

```

a := 0
b := 3
for i := 1 to 8 do
  | if a < b then
  | | a := a + i
  | else
  | | b := b + a
  | end
end
output a
output b

```

Solution The following table tallies the values of a and b initially, and at the end of each iteration (i) of the for loop.

| iteration (i) | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|-------------------|---|---|---|---|---|----|----|----|----|
| a | 0 | 1 | 3 | 3 | 7 | 7 | 13 | 13 | 21 |
| b | 3 | 3 | 3 | 6 | 6 | 13 | 13 | 26 | 26 |

The final values (which are the output) are $a = 21$ and $b = 26$.

5. The input of the following algorithm is a list X of even length. Find the output for input $X = (3, 5, 8, 4, 6, 8, 7, 4, 2, 3)$.

Algorithm

```

Input:  $X = (x_1, x_2, \dots, x_n)$ 
begin
  for  $i := 1$  to  $\frac{n}{2}$  do
    |  $k := 2i$ 
    |  $x_k := x_k + 1$ 
  end
  for  $j := 1$  to  $\frac{n}{2}$  do
    |  $k := 2j - 1$ 
    |  $x_k := x_k - 1$ 
  end
  output  $X$ 
end

```

Solution The first for loop adds 1 to each list entry x_k for which the index k is even. In other words, it adds 1 to the entries x_2, x_4, x_6, x_8 and x_{10} .

The second for loop subtracts 1 from each list entry x_k for which the index k is odd. In other words, it subtracts 1 from the entries x_1, x_3, x_5, x_7 and x_9 .

Therefore the output is
 $X = (2, 6, 7, 5, 5, 9, 6, 5, 1, 4)$.

7. Write an algorithm whose input is an integer n and whose output is the first n Fibonacci numbers.

Algorithm: to compute the first n Fibonacci numbers

Input: An integer n for which $n \geq 2$

Output: The first n Fibonacci numbers

begin

$x := 1$ x is the 1st Fibonacci number

$y := 1$ y is the 2nd Fibonacci number

output x output 1st Fibonacci number

output y output 2nd Fibonacci number

$i := 2$ i is # of Fibonacci numbers outputted so far

while $i < n$ **do**

$z := x + y$ z is most recent Fibonacci number

output z output most recent Fibonacci number

$i := i + 1$ update i

$x := y$ x now second-most-recent Fibonacci number

$y := z$ y now most recent Fibonacci number

end

end

9. Write an algorithm whose input is two integers n and k , and whose output is $\binom{n}{k}$.

Solution: Recall that $\binom{n}{k} = 0$ if $n \leq 0$, or if $n > 0$ but $k < 0$ or $k > n$. Also $\binom{n}{k} = 1$ when $k = 0$ or $k = n$. Otherwise, Fact 4.5 (page 101) says

$$\begin{aligned} \binom{n}{k} &= \frac{n!}{k!(n-k)!} = \frac{n(n-1)(n-2)\cdots(n-k+3)(n-k+2)(n-k+1)}{k!} \\ &= \frac{(n-k+1)(n-k+2)(n-k+3)\cdots(n-2)(n-1)n}{1 \cdot 2 \cdot 3 \cdots (k-2)(k-1)k}. \end{aligned}$$

Our algorithm will carry out this arithmetic by first putting $y := 1$, then using a for loop to multiply y by $(n - k + 1)$, then by $(n - k + 2)$, then $(n - k + 3)$, and so on, working its way up to multiplying by n . Then a second for loop will divide by 1, then by 2, then by 3, and so on, until finally dividing by k .

Algorithm: computes $\binom{n}{k}$

Input: Integers n and k , with $n \geq 0$

Output: $\binom{n}{k}$

begin

if $(n \leq 0) \vee ((k < 0) \vee (k > n))$ **then**

output 0 in this case $\binom{n}{k} = 0$

else

if $(k = 0) \vee (k = n)$ **then**

output 1 in this case $\binom{n}{k} = 1$

else

$y := 1$ y is initially 1

for $i := n - k + 1$ **to** n **do**

$y := y \cdot i$ multiply y by i , for each $n - k + 1 \leq i \leq n$

end

for $i := 1$ **to** k **do**

$y := \frac{y}{i}$ divide y by i , for each $1 \leq i \leq k$

end

output y now $y = \binom{n}{k}$

end

end

end

11. Write an algorithm whose input is a list of numbers (x_1, x_2, \dots, x_n) , and whose output is the word "YES" if the list has any repeated entries, and "NO" if there are no repeated entries.

Solution: For each x_i up to x_{n-1} we check if it equals an x_k later on the list.

Algorithm

Input: A list of numbers $x_1, x_2, x_3, \dots, x_n$

Output: "YES" if the list has repetition, otherwise "NO"

begin

$match := \text{NO}$

for $i := 1$ **to** $n - 1$ **do**

for $k = i + 1$ **to** n **do**

if $x_i = x_k$ **then**

$match := \text{YES}$

end

end

end

end

output $match$

13. Write an algorithm whose input is two positive integers n, k , and whose output is the number of non-negative integer solutions of $x_1 + x_2 + x_3 + \dots + x_k = n$. (See Section 4.8.)

Solution: As in Section 4.8 we can model the solutions with stars-and-bars lists

$$\overbrace{***\dots*}^{x_1} \mid \overbrace{***\dots*}^{x_2} \mid \overbrace{***\dots*}^{x_3} \mid \dots \mid \overbrace{***\dots*}^{x_k},$$

having n stars and $k - 1$ bars. Such a list has length $n + k - 1$, and can be made by choosing n positions for stars and filling the remaining $k - 1$ with bars. Thus there are $\binom{n+k-1}{n}$ such lists, so this is also the number of solutions to the equation. Thus our algorithm must simply compute $\binom{n+k-1}{n}$. For this we can adapt the algorithm for $\binom{n}{k}$ in Exercise 9 above.

Algorithm: computes $\binom{n+k-1}{n}$

Input: Positive integers n and k

Output: $\binom{n+k-1}{n}$

```

begin
  y := 1 ..... y is initially 1
  for i := k to n + k - 1 do
    | y := y · i ..... multiply y by i, for each k ≤ i ≤ n + k - 1
  end
  for i := 1 to k do
    | y := y / i ..... divide y by i, for each 1 ≤ i ≤ k
  end
  output y ..... now y =  $\binom{n+k-1}{n}$ 
end

```

15. Fix BubbleSort.

(Better Bubble Sort) sorts any list

Input: A list $X = (x_1, x_2, \dots, x_n)$ of numbers

Output: The list sorted into numeric order

```

begin
  if 0 ≤ n ≤ 1 then
    | output X ..... X is already sorted
  else
    for k := 1 to n - 1 do
      | for i := 1 to n - k do
        | | if xi > xi+1 then
          | | | temp := xi ..... temporarily holds value of xi
          | | | xi := xi+1
          | | | xi+1 := temp ..... now xi and xi+1 are swapped
          | | end
        | | end
      | end
    output X ..... now X is sorted
  end
end

```

17. Design and algorithm whose input is an integer $n \geq 0$ and whose output is the n th row of Pascal's triangle.

For an input of n , the output will be the sequence

$$\binom{n}{0}, \binom{n}{1}, \binom{n}{2}, \binom{n}{3}, \dots, \binom{n}{n}$$

of $n + 1$ numbers. How could we write such an algorithm? To begin the design, we would need a for loop with the following structure.

```

for  $k := 0$  to  $n$  do
  |  $y := \binom{n}{k}$ 
  | output  $y$ 
end
    
```

To finish it we just need to add in the lines that compute $y := \binom{n}{k}$. For this we can reuse our code from Algorithm 10 in our solution of Exercise 9. Actually, the above for loop makes k go from 1 to n , so we don't even need the lines of Algorithm 10 that deal with the cases $n \leq 0 \vee ((k < 0) \vee (k > n))$, for which $\binom{n}{k} = 0$. Here is our algorithm.

Algorithm: computes the n th row of Pascal's triangle

```

Input: Integer  $n$  with  $n \geq 0$ 
Output:  $n$ th row of Pascal's triangle
begin
  | for  $k := 0$  to  $n$  do
  | | if  $(k = 0) \vee (k = n)$  then
  | | | output 1 .....in this case  $\binom{n}{k} = 1$ 
  | | else
  | | |  $y := 1$  .....  $y$  is initially 1
  | | | for  $i := n - k + 1$  to  $n$  do
  | | | |  $y := y \cdot i$ 
  | | | | end
  | | | | for  $i := 1$  to  $k$  do
  | | | | |  $y := \frac{y}{i}$ 
  | | | | end
  | | | output  $y$  ..... now  $y = \binom{n}{k}$ 
  | | end
  | end
end
    
```

Sections 6.4 and 6.5

1. Write a procedure whose input is a list of numbers $X = (x_1, x_2, \dots, x_n)$, and whose output is the list in reverse order.

Procedure Reverse(X)

```

begin
   $Y := X$  .....  $Y = (y_1, \dots, y_n)$  is a copy of  $X = (x_1, \dots, x_n)$ 
  for  $i := 1$  to  $n$  do
    |  $y_i := x_{n-i+1}$  ..... fill in  $Y$  as the reverse of  $X$ 
  end
  return  $Y$ 
end

```

3. Write a procedure whose input is a list of numbers $X = (x_1, x_2, \dots, x_n)$, and whose output is “YES” if X is in numeric order (i.e., $x_1 \leq x_2 \leq \dots \leq x_n$), and “NO” otherwise.

Procedure Check(X)

```

begin
   $ordered := YES$  ..... list assumed ordered until found not to be ordered
   $i := 1$ 
  while  $(ordered = YES) \wedge (i < n)$  do
    | if  $x_i > x_{i+1}$  then
      | |  $ordered := NO$ 
    | end
    |  $i := i + 1$ 
  end
  return  $ordered$ 
end

```

5. Write a procedure whose input is a list $X = (0, 0, 1, 0, 1, \dots, 1)$ of 0's and 1's, of length n . The procedure returns the number of 1's in X .

Procedure Ones(X)

```

begin
   $total := 0$  ..... so far total number of 1's found is zero
  for  $i := 1$  to  $n$  do
    | if  $x_i = 1$  then
      | |  $total := total + 1$ 
    | end
  end
  return  $total$ 
end

```

7. Write a procedure whose input is a list of numbers $X = (x_1, x_2, \dots, x_n)$, and whose output is the product of $x_1 x_2 \dots x_n$ of all the entries.

Procedure Prod(X)

```

begin
  |  $product := 1$  for  $i := 1$  to  $n$  do
  | |  $product := product \cdot x_i$ 
  | end
  | return  $prod$ 
end

```

9. Write a procedure whose input is two lists of numbers $X = (x_1, x_2, \dots, x_n)$ and $Y = (y_1, y_2, \dots, y_n)$, and whose output is the list $Z = (x_1, x_2, x_3, \dots, x_n, y_n, \dots, y_3, y_2, y_1)$.

Procedure Glue(X, Y)

```

begin
  |  $Z := (0, 0, 0, \dots, 0)$  ..... a list of length  $2n$ 
  | for  $i := 1$  to  $n$  do
  | |  $z_i := x_i$ 
  | |  $z_{n+1-i} := y_i$ 
  | end
  | return  $Z$ 
end

```

11. Write a procedure whose input is two lists of numbers $X = (x_1, x_2, \dots, x_n)$ and $Y = (y_1, y_2, \dots, y_n)$, and whose output is the list $Z = (x_1 + y_1, x_2 + y_2, x_3 + y_3, \dots, x_n + y_n)$.

Procedure Add(X, Y)

```

begin
  |  $Z := X$  .....  $Z$  is a copy of  $X$ 
  | for  $i := 1$  to  $n$  do
  | |  $z_i := z_i + y_i$ 
  | end
  | return  $Z$ 
end

```

13. The **Fibonacci sequence** is the sequence 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, Write a *recursive* procedure whose input is an integer n and whose output is the n th Fibonacci number.

Procedure Fib(n)

```

begin
  | if  $(n = 1) \vee (n = 2)$  then
  | | return 1
  | else
  | | return  $Fib(n - 1) + Fib(n - 2)$ 
  | end
end

```

15. An **arithmetic sequence** with difference d is a sequence of numbers for which any term is d plus the previous term. For example, 5, 8, 11, 14, 17, 20, ... is a

arithmetic sequence with difference 3. Write an **recursive** procedure whose input is three numbers $a, d \in \mathbb{R}$, and $n \in \mathbb{N}$, and whose output is the n th term of the arithmetic sequence whose first term is a and whose difference is d .

Procedure Arithmetic(a, d, n)

```

begin
  if  $n = 1$  then
    | return  $a$ 
  else
    | return  $d + \text{Arithmetic}(n - 1)$ 
  end
end

```

Section 6.6

1. Count how many times Command is executed.

```

for  $i := 1$  to 60 do
  | for  $j := 1$  to  $i$  do
  | | Command
  | end
end

```

Solution Command is issued once for each pair (i, j) with $1 \leq j \leq i \leq 60$. Such a pair can be encoded as a star-and-bar list $***\dots*|***\dots*|***\dots*$ with 60 stars and two bars, where j is the number of stars before the first bar and i is the number of stars before the second bar.

Given that we have $1 \leq j$, the first list entry must be a star. The remaining entries form a list with 59 stars and two bars, of length 61. The number of such lists is $\binom{61}{2} = 1830$ so that is the number of times Command is executed.

3. Suppose n is a positive integer. In the following piece of code, how many times is Command executed? The answer will depend on the value of n .

```

for  $i := 0$  to  $n$  do
  | for  $j := 0$  to  $i$  do
  | | for  $j := 0$  to  $j$  do
  | | | for  $\ell = 0$  to  $k$  do
  | | | | Command
  | | | end
  | | end
  | end
end

```

Solution: Command is executed for each integer combination of i, j, k and ℓ for which $0 \leq \ell \leq k \leq j \leq i \leq n$. We can model such combinations with lists of n stars and 4 bars $***|**|*|**|*\dots***$ where ℓ is the number of stars to the left of the first bar, k is the number of stars to the left of the second bar, j is the number of stars to the left of the third bar, and i is the number of stars to the left of the fourth bar. Such a list has length $n + 4$, and we can make it by choosing 4 out of $n + 4$ spots for the bars and filling the rest with stars. Thus there are $\binom{n+4}{4}$ such lists so this is also the number of times Command is executed.

5. Count how many times Command is executed.

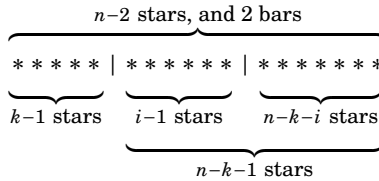
```

for  $i := 1$  to 2017 do
  if  $i$  is even then
    Command
  else
    Command
    Command
  end
end
    
```

Solution There are $2018/2 = 1009$ odd integers between 1 and 2017, and 1008 even integers between 1 and 2017. Because Command gets issued once for every even integer and twice for every odd integer, it gets executed a total of $1009 + 2 \cdot 1008 = 3025$ times.

7. How many steps does the bubble sort algorithm (Algorithm 5 on page 182) take if its input list $X = (x_1, x_2, \dots, x_n)$ is already sorted?

Solution: The if statement inside the nested for loops gets executed once for each pair (k, i) of integers with $1 \leq k \leq n - 1$, and $1 \leq i \leq n - k$. We can model such pairs as lists of length n , made of $n - 2$ stars and 2 bars. There are $k - 1$ stars before the first bar, and $i - 1$ stars between the two bars.



For example, suppose $n = 8$. Then $***|*|**$ corresponds to $(k, i) = (4, 2)$, whereas $***||***$ corresponds to $(k, i) = (4, 1)$. Also $|*****|$ means $(k, i) = (1, 7)$, and $||*****$ is $(k, i) = (1, 1)$. The number of such lists is $\binom{n}{2} = \frac{n(n-1)}{2} = \frac{1}{2}n^2 - \frac{1}{2}n$, the number of ways to choose 2 out of n spots for the bars. So the if-statement gets executed $\frac{1}{2}n^2 - \frac{1}{2}n$ times (but $x_i > x_{i+1}$ is always false, so the three statements in its body do not get executed). Thus the algorithm does $\frac{1}{2}n^2 - \frac{1}{2}n$ steps.

9. Find a formula for the number of steps that Algorithm 2 (page 178) executes for an input of n .

Solution: For each i between 1 and n , it executes 2 steps, to the total number of steps is $2n$.

11. Find a formula for the number of steps (in the worst case) that Algorithm 4 (page 180) executes when the input is a list of length n .

Solution: The algorithm starts by making one assignment ($biggest := x_1$) and then executes an if statement n times, so the answer is $1 + n$.

13. Find a formula for the number of steps that The division algorithm (Algorithm 6 on page 185) executes when the input is two positive integers a and b . (The answer will depend on a and b .)

Solution: There are 4 statements outside of the while loop. The while loop goes through $\lceil \frac{a}{b} \rceil$ iterations, and each iteration executes two statements. Thus the answer is $4 + 2 \lceil \frac{a}{b} \rceil$.

Part III

Conditional Proof

Quantified Statements

We have seen that the symbols \wedge , \vee , \sim , \Rightarrow and \Leftrightarrow can guide the logical flow of algorithms. We have learned how to use them to deconstruct many English sentences into a symbolic form. We have studied how this symbolic form can help us understand the logical structure of sentences and how different sentences may actually have the same meaning (as in logical equivalence). This will be particularly significant as we begin proving theorems in the next chapter.

But these logical symbols alone are not powerful enough to capture the full meaning of every statement. To see why, imagine that we are dealing with some set $S = \{x_1, x_2, x_3, \dots\}$ of integers. (For emphasis, say S is an infinite set.) Suppose we want to express the statement “*Every element of S is odd.*” We would have to write

$$P(x_1) \wedge P(x_2) \wedge P(x_3) \wedge P(x_4) \wedge \dots,$$

where $P(x)$ is the open sentence “ x is odd.” And if we wanted to express “*There is at least one element of S that is odd,*” we’d have to write

$$P(x_1) \vee P(x_2) \vee P(x_3) \vee P(x_4) \vee \dots.$$

The problem is that these expressions might never end.

To overcome this defect, we will introduce two new symbols \forall and \exists . The symbol \forall stands for the phrase “*for all*” and \exists stands for “*there exists.*” Thus the statement “*Every element of S is odd.*” is written symbolically as

$$\forall x \in S, P(x),$$

and “*There is at least one element of S that is odd,*” is written succinctly as

$$\exists x \in S, P(x),$$

These new symbols are called *quantifiers*. They are the subject of this chapter.

7.1 Quantifiers

To repeat, here are the main ideas of this chapter.

Definition 7.1 The symbols \forall and \exists are called **quantifiers**.

\forall stands for the phrase “For all” or “For every,” or “For each,”

\exists stands for the phrase “There exists a” or “There is a.”

Thus the statement

For every $n \in \mathbb{Z}$, $2n$ is even,

can be expressed in either of the following ways:

$\forall n \in \mathbb{Z}$, $2n$ is even,

$\forall n \in \mathbb{Z}$, $E(2n)$.

Likewise, a statement such as

There exists a subset X of \mathbb{N} for which $|X| = 5$.

can be translated as

$\exists X, (X \subseteq \mathbb{N}) \wedge (|X| = 5)$ or $\exists X \subseteq \mathbb{N}, |X| = 5$ or $\exists X \in \mathcal{P}(\mathbb{N}), |X| = 5$.

The symbols \forall and \exists are called quantifiers because they refer in some sense to the quantity (i.e., all or some) of the variable that follows them. Symbol \forall is called the **universal quantifier** and \exists is called the **existential quantifier**. Statements which contain them are called **quantified** statements. A statement beginning with \forall is called a **universally quantified** statement, and one beginning with \exists is called an **existentially quantified** statement.

Example 7.1 The following English statements are paired with their translations into symbolic form.

Every integer that is not odd is even.

$\forall n \in \mathbb{Z}, \sim (n \text{ is odd}) \Rightarrow (n \text{ is even}),$ or $\forall n \in \mathbb{Z}, \sim O(n) \Rightarrow E(n)$.

There is an integer that is not even.

$\exists n \in \mathbb{Z}, \sim E(n)$.

For every real number x , there is a real number y for which $y^3 = x$.

$\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, y^3 = x$.

Given any two rational numbers a and b , it follows that ab is rational.

$\forall a, b \in \mathbb{Q}, ab \in \mathbb{Q}$.



Given a set S (such as, but not limited to, \mathbb{N} , \mathbb{Z} , \mathbb{Q} etc.), a quantified statement of form $\forall x \in S, P(x)$ is understood to be true if $P(x)$ is true for every $x \in S$. If there is at least one $x \in S$ for which $P(x)$ is false, then $\forall x \in S, P(x)$ is a false statement. Similarly, $\exists x \in S, P(x)$ is true provided that $P(x)$ is true for at least one element $x \in S$; otherwise it is false. Thus each statement in Example 7.1 is true. Here are some that are false:

Example 7.2 The following false quantified statements are paired with their translations.

Every integer is even.

$$\forall n \in \mathbb{Z}, E(n).$$

There is an integer n for which $n^2 = 2$.

$$\exists n \in \mathbb{Z}, n^2 = 2.$$

For every real number x , there is a real number y for which $y^2 = x$.

$$\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, y^2 = x.$$

Given any two rational numbers a and b , it follows that \sqrt{ab} is rational.

$$\forall a, b \in \mathbb{Q}, \sqrt{ab} \in \mathbb{Q}. \quad \text{✎}$$

Example 7.3 When a statement contains two quantifiers you must be very alert to their order, for reversing the order can change the meaning. Consider the following statement from Example 7.1.

$$\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, y^3 = x.$$

This statement is true, for no matter what number x is there exists a number $y = \sqrt[3]{x}$ for which $y^3 = x$. Now reverse the order of the quantifiers to get the new statement

$$\exists y \in \mathbb{R}, \forall x \in \mathbb{R}, y^3 = x.$$

This new statement says that there exists a particular number y with the property that $y^3 = x$ for every real number x . Since no number y can have this property, the statement is false. The two statements above have entirely different meanings. ✎

Quantified statements are often misused in casual conversation. Maybe you've heard someone say "All students do not pay full tuition." when they mean "Not all students pay full tuition." While the mistake is perhaps marginally forgivable in casual conversation, it must never be made in a mathematical context. Do not say "All integers are not even." because that means there are no even integers. Instead, say "Not all integers are even."

Exercises for Section 7.1

Write the following as English sentences. Say whether they are true or false.

- | | |
|---|---|
| 1. $\forall x \in \mathbb{R}, x^2 > 0$ | 6. $\exists n \in \mathbb{N}, \forall X \in \mathcal{P}(\mathbb{N}), X < n$ |
| 2. $\forall x \in \mathbb{R}, \exists n \in \mathbb{N}, x^n \geq 0$ | 7. $\forall X \subseteq \mathbb{N}, \exists n \in \mathbb{Z}, X = n$ |
| 3. $\exists a \in \mathbb{R}, \forall x \in \mathbb{R}, ax = x$ | 8. $\forall n \in \mathbb{Z}, \exists X \subseteq \mathbb{N}, X = n$ |
| 4. $\forall X \in \mathcal{P}(\mathbb{N}), X \subseteq \mathbb{R}$ | 9. $\forall n \in \mathbb{Z}, \exists m \in \mathbb{Z}, m = n + 5$ |
| 5. $\forall n \in \mathbb{N}, \exists X \in \mathcal{P}(\mathbb{N}), X < n$ | 10. $\exists m \in \mathbb{Z}, \forall n \in \mathbb{Z}, m = n + 5$ |
-

7.2 More on Conditional Statements

It is time to address a very important point about conditional statements that contain variables. To motivate this, let's return to the following example concerning integers x :

$$(x \text{ is a multiple of } 6) \Rightarrow (x \text{ is even}).$$

As noted earlier, since every multiple of 6 is even, this is a true statement no matter what integer x is. We could even underscore this fact by writing this true statement as

$$\forall x \in \mathbb{Z}, (x \text{ is a multiple of } 6) \Rightarrow (x \text{ is even}).$$

But now switch things around to get the different statement

$$(x \text{ is even}) \Rightarrow (x \text{ is a multiple of } 6).$$

This is true for some values of x such as $-6, 12, 18$, etc., but false for others (such as $2, 4$, etc.). Thus we do not have a statement, but rather an open sentence. (Recall from Section 3.1 that an *open sentence* is a sentence whose truth value depends on the value of a certain variable or variables.) However, by putting a universal quantifier in front we get

$$\forall x \in \mathbb{Z}, (x \text{ is even}) \Rightarrow (x \text{ is a multiple of } 6),$$

which is definitely false, so this new expression is a statement, *not an open sentence*. In general, given any two open sentences $P(x)$ and $Q(x)$ about integers x , the expression $\forall x \in \mathbb{Z}, P(x) \Rightarrow Q(x)$ is either true or false, so it is a statement, not an open sentence.

Now we come to the very important point. In mathematics, whenever $P(x)$ and $Q(x)$ are open sentences concerning elements x in some set S (depending on context), an expression of form $P(x) \Rightarrow Q(x)$ is understood to be the *statement* $\forall x \in S, P(x) \Rightarrow Q(x)$. In other words, if a conditional statement is not explicitly quantified then there is an implied universal quantifier in front of it. This is done because statements of the form $\forall x \in S, P(x) \Rightarrow Q(x)$ are so common in mathematics that we would get tired of putting the $\forall x \in S$ in front of them.

Thus the following sentence is a true statement (as it is true for all x).

If x is a multiple of 6, then x is even.

Likewise, the next sentence is a false statement (as it is not true for all x).

If x is even, then x is a multiple of 6.

This leads to the following significant interpretation of a conditional statement, which is more general than (but consistent with) the interpretation from Section 3.3.

Definition 7.2 If P and Q are statements or open sentences, then

“If P , then Q ,”

is a statement. This statement is true if it’s impossible for P to be true while Q is false. It is false if there is at least one instance in which P is true but Q is false.

Thus the following are **true** statements:

If $x \in \mathbb{R}$, then $x^2 + 1 > 0$.

If a function f is differentiable on \mathbb{R} , then f is continuous on \mathbb{R} .

If a list has n entries, then it has $n!$ permutations.

Likewise, the following are **false** statements:

If p is a prime number, then p is odd. (2 is prime.)

If f is a rational function, then f has an asymptote. (x^2 is rational.)

If a set X has n elements, then $|\mathcal{P}(X)| = n^2$. (true only if $|X| = 2$.)

7.3 Translating English to Symbolic Logic

In writing (and reading) proofs of theorems, we must always be alert to the logical structure and meanings of the sentences. Sometimes it is necessary or helpful to parse them into expressions involving logic symbols. This may be done mentally or on scratch paper, or occasionally even explicitly within the body of a proof. The purpose of this section is to give you sufficient practice in translating English sentences into symbolic form so that you can better understand their logical structure. Here are some examples:

Example 7.4 Consider the Mean Value Theorem from Calculus:

If f is continuous on the interval $[a, b]$ and differentiable on (a, b) , then there is a number $c \in (a, b)$ for which $f'(c) = \frac{f(b)-f(a)}{b-a}$.

Here is a translation to symbolic form:

$$\left((f \text{ cont. on } [a, b]) \wedge (f \text{ is diff. on } (a, b)) \right) \Rightarrow \left(\exists c \in (a, b), f'(c) = \frac{f(b)-f(a)}{b-a} \right). \quad \Rightarrow$$

Example 7.5 Consider Goldbach's conjecture, from Section 3.1:

Every even integer greater than 2 is the sum of two primes.

This can be translated in the following ways, where P is the set of prime numbers and $S = \{4, 6, 8, 10, \dots\}$ is the set of even integers greater than 2.

$$(n \in S) \Rightarrow (\exists p, q \in P, n = p + q)$$

$$\forall n \in S, \exists p, q \in P, n = p + q \quad \Rightarrow$$

These translations of Goldbach's conjecture illustrate an important point. The first has the basic structure $(n \in S) \Rightarrow Q(n)$ and the second has structure $\forall n \in S, Q(n)$, yet they have exactly the same meaning. This is significant. Every universally quantified statement can be expressed as a conditional statement.

Fact 7.1 Suppose S is a set and $Q(x)$ is a statement about x for any $x \in S$. The following statements mean the same thing:

$$\forall x \in S, Q(x)$$

$$(x \in S) \Rightarrow Q(x).$$

This fact is significant because so many theorems have the form of a conditional statement. (The Mean Value Theorem is an example!) In proving a theorem we have to think carefully about what it says. Sometimes a theorem will be expressed as a universally quantified statement but it will

be more convenient to think of it as a conditional statement. Understanding the above fact allows us to switch between the two forms.

We close this section with some final points. In translating a statement, be attentive to its intended meaning. Don't jump into, for example, automatically replacing every "and" with \wedge and "or" with \vee . An example:

At least one of the integers x and y is even.

Don't be led astray by the presence of the word "and." The meaning of the statement is that one or both of the numbers is even, so it should be translated with "or," not "and":

$(x \text{ is even}) \vee (y \text{ is even})$.

Finally, the logical meaning of "but" can be captured by "and." The sentence "*The integer x is even, but the integer y is odd,*" is translated as

$(x \text{ is even}) \wedge (y \text{ is odd})$.

Exercises for Section 7.3

Translate each of the following sentences into symbolic logic.

1. If f is a polynomial and its degree is greater than 2, then f' is not constant.
2. The number x is positive, but the number y is not positive.
3. If x is prime then \sqrt{x} is not a rational number.
4. For every prime number p there is another prime number q with $q > p$.
5. For every positive number ε , there is a positive number δ for which $|x - a| < \delta$ implies $|f(x) - f(a)| < \varepsilon$.
6. For every positive number ε there is a positive number M for which $|f(x) - b| < \varepsilon$, whenever $x > M$.
7. There exists a real number a for which $a + x = x$ for every real number x .
8. I don't eat anything that has a face.
9. If x is a rational number and $x \neq 0$, then $\tan(x)$ is not a rational number.
10. If $\sin(x) < 0$, then it is not the case that $0 \leq x \leq \pi$.
11. There is a Providence that protects idiots, drunkards, children and the United States of America. (Otto von Bismarck)
12. You can fool some of the people all of the time, and you can fool all of the people some of the time, but you can't fool all of the people all of the time. (Abraham Lincoln)
13. Everything is funny as long as it is happening to somebody else. (Will Rogers)

7.4 Negating Statements

Given a statement R , the statement $\sim R$ is called the **negation** of R . If R is a complex statement, then it is often the case that its negation $\sim R$ can be written in a simpler or more useful form. The process of finding this form is called **negating** R . In proving theorems it is often necessary to negate certain statements. We now investigate how to do this.

We have already examined part of this topic. **DeMorgan's laws**

$$\sim(P \wedge Q) = (\sim P) \vee (\sim Q) \quad (7.1)$$

$$\sim(P \vee Q) = (\sim P) \wedge (\sim Q) \quad (7.2)$$

(from Section 3.6) can be viewed as rules that tell us how to negate the statements $P \wedge Q$ and $P \vee Q$. Here are some examples that illustrate how DeMorgan's laws are used to negate statements involving "and" or "or."

Example 7.6 Consider negating the following statement.


R : You can solve it by factoring or with the quadratic formula.

Now, R means (You can solve it by factoring) \vee (You can solve it with Q.F.), which we will denote as $P \vee Q$. The negation of this is

$$\sim(P \vee Q) = (\sim P) \wedge (\sim Q).$$

Therefore, in words, the negation of R is

$\sim R$: You can't solve it by factoring and you can't solve it with the quadratic formula.

Maybe you can find $\sim R$ without invoking DeMorgan's laws. That is good; you have internalized the laws and are using them unconsciously. 

Example 7.7 We will negate the following sentence.


R : The numbers x and y are both odd.

This statement means $(x \text{ is odd}) \wedge (y \text{ is odd})$, so its negation is

$$\begin{aligned} \sim((x \text{ is odd}) \wedge (y \text{ is odd})) &= \sim(x \text{ is odd}) \vee \sim(y \text{ is odd}) \\ &= (x \text{ is even}) \vee (y \text{ is even}). \end{aligned}$$

Therefore the negation of R can be expressed in the following ways:

$\sim R$: The number x is even or the number y is even.

$\sim R$: At least one of x and y is even. 

Now let's move on to a slightly different kind of problem. It's often necessary to find the negations of quantified statements. For example, consider $\sim(\forall x \in \mathbb{N}, P(x))$. Reading this in words, we have the following:

It is not the case that $P(x)$ is true for all natural numbers x .

This means $P(x)$ is false for at least one x . In symbols, this is $\exists x \in \mathbb{N}, \sim P(x)$. Thus $\sim(\forall x \in \mathbb{N}, P(x)) = \exists x \in \mathbb{N}, \sim P(x)$. Similarly, you can reason out that $\sim(\exists x \in \mathbb{N}, P(x)) = \forall x \in \mathbb{N}, \sim P(x)$. In general:

$$\sim(\forall x \in S, P(x)) = \exists x \in S, \sim P(x), \quad (7.3)$$


$$\sim(\exists x \in S, P(x)) = \forall x \in S, \sim P(x). \quad (7.4)$$

Example 7.8 Consider negating the following statement.

R : The square of every real number is non-negative.

Symbolically, R can be expressed as $\forall x \in \mathbb{R}, x^2 \geq 0$, and thus its negation is $\sim(\forall x \in \mathbb{R}, x^2 \geq 0) = \exists x \in \mathbb{R}, \sim(x^2 \geq 0) = \exists x \in \mathbb{R}, x^2 < 0$. In words, this is

$\sim R$: There exists a real number whose square is negative.

Observe that R is true and $\sim R$ is false. You may be able to get $\sim R$ immediately, without using Equation (7.3) as we did above. If so, that is good; if not, you will probably be there soon. 

If a statement has multiple quantifiers, negating it will involve several iterations of Equations (7.3) and (7.4). Consider the following:

S : For every real number x there is a real number y for which $y^3 = x$.

This statement asserts any real number x has a cube root y , so it's true. Symbolically S can be expressed as

$$\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, y^3 = x.$$

Let's work out the negation of this statement.

$$\begin{aligned} \sim(\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, y^3 = x) &= \exists x \in \mathbb{R}, \sim(\exists y \in \mathbb{R}, y^3 = x) \\ &= \exists x \in \mathbb{R}, \forall y \in \mathbb{R}, \sim(y^3 = x) \\ &= \exists x \in \mathbb{R}, \forall y \in \mathbb{R}, y^3 \neq x. \end{aligned}$$

Therefore the negation is the following (false) statement.

$\sim S$: There is a real number x for which $y^3 \neq x$ for all real numbers y .

In writing proofs you will sometimes have to negate a conditional statement $P \Rightarrow Q$. The remainder of this section describes how to do this. To begin, look at the expression $\sim(P \Rightarrow Q)$, which literally says “ $P \Rightarrow Q$ is false.” You know from the truth table for \Rightarrow that the only way that $P \Rightarrow Q$ can be false is if P is true and Q is false. Therefore $\sim(P \Rightarrow Q) = P \wedge \sim Q$.

$$\sim(P \Rightarrow Q) = P \wedge \sim Q \quad (7.5)$$

(In fact, in Exercise 12 of Section 3.6, you used a truth table to verify that these two statements are indeed logically equivalent.)

Example 7.9 Negate the following statement about a particular (i.e., constant) number a .

R : If a is odd then a^2 is odd.

Using Equation (7.5), we get the following negation.

$\sim R$: a is odd and a^2 is not odd.

Notice that R is true. Also $\sim R$ is false, no matter the value of a . 

Example 7.10 This example is like the previous one, but the constant a is replaced by a variable x . We will negate the following statement.

R : If x is odd then x^2 is odd.

As discussed in Section 7.2, we interpret this as the universally quantified statement


R : $\forall x \in \mathbb{Z}, (x \text{ odd}) \Rightarrow (x^2 \text{ odd})$.

By Equations (7.3) and (7.5), we get the following negation for R .

$$\begin{aligned} \sim(\forall x \in \mathbb{Z}, (x \text{ odd}) \Rightarrow (x^2 \text{ odd})) &= \exists x \in \mathbb{Z}, \sim((x \text{ odd}) \Rightarrow (x^2 \text{ odd})) \\ &= \exists x \in \mathbb{Z}, (x \text{ odd}) \wedge \sim(x^2 \text{ odd}). \end{aligned}$$

Translating back into words, we have

$\sim R$: There is an odd integer x whose square is not odd.

Notice that R is true and $\sim R$ is false. 

The above Example 7.10 showed how to negate a conditional statement $P(x) \Rightarrow Q(x)$. This type of problem can sometimes be embedded in more complex negation. See Exercise 5 below (and its solution).

Exercises for Section 7.4

Negate the following sentences.

1. The number x is positive, but the number y is not positive.
2. If x is prime, then \sqrt{x} is not a rational number.
3. For every prime number p , there is another prime number q with $q > p$.
4. For every positive number ε , there is a positive number δ such that $|x - a| < \delta$ implies $|f(x) - f(a)| < \varepsilon$.
5. For every positive number ε , there is a positive number M for which $|f(x) - b| < \varepsilon$ whenever $x > M$.
6. There exists a real number a for which $a + x = x$ for every real number x .
7. I don't eat anything that has a face.
8. If x is a rational number and $x \neq 0$, then $\tan(x)$ is not a rational number.
9. If $\sin(x) < 0$, then it is not the case that $0 \leq x \leq \pi$.
10. If f is a polynomial and its degree is greater than 2, then f' is not constant.
11. You can fool all of the people all of the time.
12. Whenever I have to choose between two evils, I choose the one I haven't tried yet. (Mae West)

7.5 Logical Inference

There are four very significant reasons that we study logic. First, truth tables tell us the exact meanings of the words such as “and,” “or,” “not” and so on. So, whenever we encounter the “*If... then*” construction in a mathematical context, logic tells us exactly what is meant. Second, logical rules such as DeMorgan's laws help us correctly change certain statements into (potentially more useful) statements with the same meaning. Third, logic is an essential ingredient in the design and flow of algorithms.

This section covers the fourth reason that logic is important. It provides a means of combining facts and information to produce new facts.

To begin, suppose we know that a statement of form $P \Rightarrow Q$ is true. This tells us that whenever P is true, Q will also be true. By itself, $P \Rightarrow Q$ being true does not tell us that either P or Q is true (they could both be false, or P could be false and Q true). However if in addition we happen to know that P is true then it must be that Q is true. This is called a **logical inference**: Given two true statements we can infer that a third statement is true. In this instance true statements $P \Rightarrow Q$ and P are “added together” to get Q . This is described below with $P \Rightarrow Q$ and P stacked one atop the other with a

line separating them from Q . The intended meaning is that $P \Rightarrow Q$ combined with P produces Q .

$$\frac{P \Rightarrow Q}{P} \quad \frac{}{Q}$$

This is a very frequently-used pattern of thought. (In fact, it is exactly the pattern we used in the example on page 51.) This rule even has a name. It is called the **modus ponens** rule.

Two other logical inferences, called **modus tollens** and **elimination** are listed below. In each case you should convince yourself (based on your knowledge of the relevant truth tables) that the truth of the statements above the line forces the statement below the line to be true.

MODUS PONENS

$$\frac{P \Rightarrow Q}{P} \quad \frac{}{Q}$$

MODUS TOLLENS

$$\frac{P \Rightarrow Q}{\sim Q} \quad \frac{}{\sim P}$$

ELIMINATION

$$\frac{P \vee Q}{\sim P} \quad \frac{}{Q}$$

It is important to internalize these rules. (You surely already use at least modus ponens and elimination in daily life anyway.) But don't bother remembering their names; very few working mathematicians and computer scientists can recall the names of these rules, though they use the rules constantly. The names are not important, but the rules are.

Three additional logical inferences are listed below. The first states the obvious fact that if P and Q are both true, then so is the statement $P \wedge Q$. On the other hand, $P \wedge Q$ being true forces P (also Q) to be true. Finally, if P is true, then $P \vee Q$ must be true, no matter what statement Q is.

$$\frac{P}{Q} \quad \frac{}{P \wedge Q}$$

$$\frac{P \wedge Q}{P}$$

$$\frac{P}{P \vee Q}$$

These inferences are so intuitively obvious that they scarcely need to be mentioned. However, they represent certain patterns of reasoning that we will frequently apply to sentences in proofs, so we should be cognizant of the fact that we are using them.

7.6 Solutions for Chapter 7

Section 7.1

Write the following as English sentences. Say whether the statements are true or false.

1. $\forall x \in \mathbb{R}, x^2 > 0$

Answer: For every real number x , $x^2 > 0$.

Also: For every real number x , it follows that $x^2 > 0$.

Also: The square of any real number is positive. (etc.)

This statement is FALSE. Reason: 0 is a real number, but it's not true that $0^2 > 0$.

3. $\exists a \in \mathbb{R}, \forall x \in \mathbb{R}, ax = x$.

Answer: There exists a real number a for which $ax = x$ for every real number x .

This statement is TRUE. Reason: Consider $a = 1$.

5. $\forall n \in \mathbb{N}, \exists X \in \mathcal{P}(\mathbb{N}), |X| < n$

Answer: For every natural number n , there is a subset X of \mathbb{N} with $|X| < n$.

This statement is TRUE. Reason: Suppose $n \in \mathbb{N}$. Let $X = \emptyset$. Then $|X| = 0 < n$.

7. $\forall X \subseteq \mathbb{N}, \exists n \in \mathbb{Z}, |X| = n$

Answer: For any subset X of \mathbb{N} , there exists an integer n for which $|X| = n$.

This statement is FALSE. For example, the set $X = \{2, 4, 6, 8, \dots\}$ of all even natural numbers is infinite, so there does not exist any integer n for which $|X| = n$.

9. $\forall n \in \mathbb{Z}, \exists m \in \mathbb{Z}, m = n + 5$

Answer: For every integer n there is another integer m such that $m = n + 5$.

This statement is TRUE.

Section 7.3

Translate each of the following sentences into symbolic logic.

1. If f is a polynomial and its degree is greater than 2, then f' is not constant.

Translation: $(P \wedge Q) \Rightarrow R$, where

P : f is a polynomial,

Q : f has degree greater than 2,

R : f' is not constant.

3. If x is prime then \sqrt{x} is not a rational number.

Translation: $P \Rightarrow \sim Q$, where

P : x is prime,

Q : \sqrt{x} is a rational number.

5. For every positive number ε , there is a positive number δ for which $|x - a| < \delta$ implies $|f(x) - f(a)| < \varepsilon$.

Translation: $\forall \varepsilon \in \mathbb{R}, \varepsilon > 0, \exists \delta \in \mathbb{R}, \delta > 0, (|x - a| < \delta) \Rightarrow (|f(x) - f(a)| < \varepsilon)$

7. There exists a real number a for which $a + x = x$ for every real number x .

Translation: $\exists a \in \mathbb{R}, \forall x \in \mathbb{R}, a + x = x$

9. If x is a rational number and $x \neq 0$, then $\tan(x)$ is not a rational number.

Translation: $((x \in \mathbb{Q}) \wedge (x \neq 0)) \Rightarrow (\tan(x) \notin \mathbb{Q})$

11. There is a Providence that protects idiots, drunkards, children and the United States of America.

One translation is as follows. Let R be union of the set of idiots, the set of drunkards, the set of children, and the set consisting of the USA. Let P be the open sentence $P(x)$: x is a Providence. Let S be the open sentence $S(x, y)$: x protects y . Then the translation is $\exists x, \forall y \in R, P(x) \wedge S(x, y)$.

(Notice that, although this is mathematically correct, some humor has been lost in the translation.)

13. Everything is funny as long as it is happening to somebody else.

Translation: $\forall x, (\sim M(x) \wedge S(x)) \Rightarrow F(x)$,

where $M(x)$: x is happening to me, $S(x)$: x is happening to someone, and $F(x)$: x is funny.

Section 7.4

Negate the following sentences.

1. The number x is positive, but the number y is not positive.

The “but” can be interpreted as “and.” Using DeMorgan’s law, the negation is: *The number x is not positive or the number y is positive.*

3. For every prime number p , there is another prime number q with $q > p$.

Negation: *There is a prime number p such that for every prime number q , $q \leq p$.*

Also: *There exists a prime number p for which $q \leq p$ for every prime number q .* (etc.)

5. For every positive number ε there is a positive number M for which $|f(x) - b| < \varepsilon$ whenever $x > M$.

To negate this, it may be helpful to first write it in symbolic form. The statement is $\forall \varepsilon \in (0, \infty), \exists M \in (0, \infty), (x > M) \Rightarrow (|f(x) - b| < \varepsilon)$.

Working out the negation, we have

$$\begin{aligned} \sim (\forall \varepsilon \in (0, \infty), \exists M \in (0, \infty), (x > M) \Rightarrow (|f(x) - b| < \varepsilon)) &= \\ \exists \varepsilon \in (0, \infty), \sim (\exists M \in (0, \infty), (x > M) \Rightarrow (|f(x) - b| < \varepsilon)) &= \\ \exists \varepsilon \in (0, \infty), \forall M \in (0, \infty), \sim ((x > M) \Rightarrow (|f(x) - b| < \varepsilon)). & \end{aligned}$$

Finally, using the idea from Example 7.10, we can negate the conditional statement that appears here to get

$$\exists \varepsilon \in (0, \infty), \forall M \in (0, \infty), \exists x, (x > M) \wedge \sim (|f(x) - b| < \varepsilon).$$

Negation: *There exists a positive number ε with the property that for every positive number M , there is a number x for which $x > M$ and $|f(x) - b| \geq \varepsilon$.*

7. I don't eat anything that has a face.

Negation: *I will eat some things that have a face.*

(Note. If your answer was "*I will eat anything that has a face.*" then that is wrong, both morally and mathematically.)

9. If $\sin(x) < 0$, then it is not the case that $0 \leq x \leq \pi$.

Negation: *There exists a number x for which $\sin(x) < 0$ and $0 \leq x \leq \pi$.*

11. You can fool all of the people all of the time.

There are several ways to negate this, including:

There is a person that you can't fool all the time. or

There is a person x and a time y for which x is not fooled at time y .

(But Abraham Lincoln said it better.)

Direct Proof

Using mathematics creatively and productively requires the ability to read, write and understand proofs. As designers of algorithms, we may need to *prove* that a certain algorithm performs correctly, or that a pivotal mathematical statement is true. Many significant and relevant mathematical theories (such as the theory of NP-completeness) are best understood in the context of mathematical proofs. Real progress in mathematics and applied mathematics requires skill with proofs, so studying this topic is essential.

There are various strategies for proving theorems. We now examine the most straightforward approach, a technique called *direct proof*. As we begin, it is important to keep in mind the meanings of three key terms: *Theorem*, *proof* and *definition*.

A **theorem** is a mathematical statement that is true and can be (and has been) verified as true. A **proof** of a theorem is a written verification that shows that the theorem is definitely and unequivocally true. A proof should be understandable and convincing to anyone who has the requisite background and knowledge. This knowledge includes an understanding of the meanings of the mathematical words, phrases and symbols that occur in the theorem and its proof. It is crucial that both the writer of the proof and the readers of the proof agree on the exact meanings of all the words, for otherwise there is an intolerable level of ambiguity. A **definition** is an exact, unambiguous explanation of the meaning of a mathematical word or phrase. We will elaborate on the terms *theorem* and *definition* in the next two sections, and then finally we will be ready to begin writing proofs.

8.1 Theorems

A **theorem** is a statement that is true and has been proved to be true. You have encountered many theorems in your mathematical education. Here are some theorems taken from an undergraduate calculus text. They will be familiar to you, though you may not have read all the proofs.

Theorem: Let f be differentiable on an open interval I and let $c \in I$. If $f(c)$ is the maximum or minimum value of f on I , then $f'(c) = 0$.

Theorem: If $\sum_{k=1}^{\infty} a_k$ converges, then $\lim_{k \rightarrow \infty} a_k = 0$.

Theorem: Suppose f is continuous on the interval $[a, b]$. Then f is integrable on $[a, b]$.

Theorem: Every absolutely convergent series converges.

Observe that each of these theorems either has the conditional form “*If P , then Q ,*” or can be put into that form. The first theorem has an initial sentence “*Let f be differentiable on an open interval I , and let $c \in I$,*” which sets up some notation, but a conditional statement follows it. The third theorem has form “*Suppose P . Then Q ,*” but this means the same thing as “*If P , then Q .*” The last theorem can be re-expressed as “*If a series is absolutely convergent, then it is convergent.*”

A theorem of form “*If P , then Q ,*” can be regarded as a device that produces new information from P . Whenever we are dealing with a situation in which P is true, then the theorem guarantees that, in addition, Q is true. Since this kind of expansion of information is useful, theorems of form “*If P , then Q ,*” are very common.

But not every theorem is a conditional statement. Some have the form of the biconditional $P \Leftrightarrow Q$, but, as we know, that can be expressed as two conditional statements. Other theorems simply state facts about specific things. For example, here is another theorem from your study of calculus.

Theorem: The series $1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \dots$ diverges.

It would be difficult (or at least awkward) to restate this as a conditional statement. Still, it is true that most theorems are conditional statements, so much of this book will concentrate on that type of theorem.

It is important to be aware that there are a number of words that mean essentially the same thing as the word “theorem,” but are used in slightly different ways. In general the word “theorem” is reserved for a statement that is considered important or significant (the Pythagorean theorem, for example). A statement that is true but not as significant is sometimes called a **proposition**. A **lemma** is a theorem whose main purpose is to help prove another theorem. A **corollary** is a result that is an immediate consequence of a theorem or proposition. It is not important that you remember all these words now, for their meanings will become clear with usage.

Our main task is to learn how to prove theorems. As the above examples suggest, proving theorems requires a clear understanding of the conditional statement, and that is the primary reason we studied it so extensively in Chapters 3 and 7. It is also crucial to understand the role of definitions.

8.2 Definitions

A proof of a theorem should be absolutely convincing. Ambiguity must be avoided. Everyone must agree on the exact meaning of each mathematical term. In Chapter 2 we defined the meanings of the sets \mathbb{N} , \mathbb{Z} , \mathbb{R} , \mathbb{Q} and \emptyset , as well as the meanings of the symbols \in and \subseteq , and we shall make frequent use of these things. Here is another definition that we use often.

Definition 8.1 An integer n is **even** if $n = 2a$ for some integer $a \in \mathbb{Z}$.

Thus, for example, 10 is even because $10 = 2 \cdot 5$. Also, according to the definition, 7 is not even because there is no integer a for which $7 = 2a$. While there would be nothing wrong with defining an integer to be odd if it's not even, the following definition is more concrete.

Definition 8.2 An integer n is **odd** if $n = 2a + 1$ for some integer $a \in \mathbb{Z}$.

Thus 7 is odd because $7 = 2 \cdot 3 + 1$. We will use these definitions whenever the concept of even or odd numbers arises. If in a proof a certain number turns out to be even, the definition allows us to write it as $2a$ for an appropriate integer a . If some quantity has form $2b + 1$ where b is an integer, then the definition tells us the quantity is odd.

Definition 8.3 Two integers have the **same parity** if they are both even or they are both odd. Otherwise they have **opposite parity**.

Thus 5 and 4 have the same parity, but 3 and 4 have opposite parity.

Two points about definitions are in order. First, in this book the word or term being defined appears in boldface type. Second, it is common to express definitions as conditional statements even though the biconditional would more appropriately convey the meaning. Consider the definition of an even integer. You understand full well that if n is even then $n = 2a$ (for $a \in \mathbb{Z}$), and if $n = 2a$, then n is even. Thus, technically the definition should read "An integer n is even if and only if $n = 2a$ for some $a \in \mathbb{Z}$." However, it is an almost-universal convention that definitions are phrased in the conditional form, even though they are interpreted as being in the biconditional form.

There is really no good reason for this, other than economy of words. It is the standard way of writing definitions, and we have to get used to it.

Here is another definition that we will use often.

Definition 8.4 Suppose a and b are integers. We say that a **divides** b , written $a \mid b$, if $b = ac$ for some $c \in \mathbb{Z}$. In this case we also say that a is a **divisor** of b , and that b is a **multiple** of a .

For example, 5 divides 15 because $15 = 5 \cdot 3$. We write this as $5 \mid 15$. Similarly $8 \mid 32$ because $32 = 8 \cdot 4$, and $-6 \mid 6$ because $6 = -6 \cdot -1$. However, 6 does not divide 9 because there is no integer c for which $9 = 6 \cdot c$. We express this as $6 \nmid 9$, which we read as “6 does not divide 9.”

Be careful of your interpretation of the symbols. There is a big difference between the expressions $a \mid b$ and a/b . The expression $a \mid b$ is a *statement*, while a/b is a fraction. For example, $8 \mid 16$ is true and $8 \mid 20$ is false. By contrast, $8/16 = 0.5$ and $8/20 = 0.4$ are numbers, not statements. Be careful not to write one when you mean the other.

Every integer has a set of integers that divide it. The set of divisors of 6 is $\{a \in \mathbb{Z} : a \mid 6\} = \{-6, -3, -2, -1, 1, 2, 3, 6\}$. The set of divisors of 5 is $\{-5, -1, 1, 5\}$. The set of divisors of 0 is \mathbb{Z} . This brings us to the following definition, with which you are already familiar.

Definition 8.5 A natural number n is **prime** if it has exactly two positive divisors, 1 and n .

For example, 2 is prime, as are 5 and 17. The definition implies that 1 is not prime, as it only has one (not two) positive divisor, namely 1. An integer n is **composite** if it factors as $n = ab$ where $a, b > 1$.

Definition 8.6 The **greatest common divisor** of integers a and b , denoted $\gcd(a, b)$, is the largest integer that divides both a and b .

The **least common multiple** of non-zero integers a and b , denoted $\text{lcm}(a, b)$, is smallest positive integer that is a multiple of both a and b .

So $\gcd(18, 24) = 6$, $\gcd(5, 5) = 5$ and $\gcd(32, -8) = 8$. Also $\gcd(50, 18) = 2$, but $\gcd(50, 9) = 1$. Note that $\gcd(0, 6) = 6$, because, although every integer divides 0, the largest divisor of 6 is 6.

The expression $\gcd(0, 0)$ is problematic. Every integer divides 0, so the only conclusion is that $\gcd(0, 0) = \infty$. We circumvent this irregularity by simply agreeing to consider $\gcd(a, b)$ only when a and b are not both zero.

Continuing our examples, $\text{lcm}(4,6) = 12$, and $\text{lcm}(7,7) = 7$.

Of course not all terms can be defined. If every word in a definition were defined, there would be separate definitions for the words that appeared in those definitions, and so on, until the chain of defined terms became circular. Thus we accept some ideas as being so intuitively clear that they require no definitions or verifications. For example, we will not find it necessary to define what an integer (or a real number) is. Nor will we define addition, multiplication, subtraction and division, though we will use these operations freely. We accept and use such things as the distributive and commutative properties of addition and multiplication, as well as other standard properties of arithmetic and algebra.

As mentioned in Section 2.9, we accept as fact the natural ordering of the elements of $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ and \mathbb{R} , so that (for example) statements such as “ $5 < 7$,” and “ $x < y$ implies $-x > -y$,” do not need to be justified.

In addition, we accept the following fact without justification or proof.

Fact 8.1 Suppose a and b are integers. Then:

- $a + b \in \mathbb{Z}$
- $a - b \in \mathbb{Z}$
- $ab \in \mathbb{Z}$

These three statements can be combined. For example, we see that if a, b and c are integers, then $a^2b - ca + b$ is also an integer.

We will also accept as obvious the fact that any integer a can be divided by a non-zero integer b , resulting in a unique quotient q and remainder r . For example, $b = 3$ goes into $a = 17$ $q = 5$ times with remainder $r = 2$. In symbols, $17 = 5 \cdot 3 + 2$, or $a = qb + r$. This fact, called the *division algorithm*, was mentioned on page 186 (Fact 6.1).

(The Division Algorithm) Given integers a and b with $b > 0$, there exist unique integers q and r for which $a = qb + r$ and $0 \leq r < b$.

Another fact that we will accept without proof (at least for now) is that every natural number greater than 1 has a unique factorization into primes. For example, the number 1176 can be factored into primes as $1176 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 7 \cdot 7 = 2^3 \cdot 3 \cdot 7^2$. By *unique* we mean that *any* factorization of 1176 into primes will have exactly the same factors (i.e., three 2's, one 3 and two 7's). Thus, for example, there is no valid factorization of 1176 that has a factor of 5. You may be so used to factoring numbers into primes that it seems obvious that there cannot be different prime factorizations of the

same number, but in fact this is a fundamental result whose proof is not transparent. Nonetheless, we will be content to assume that every natural number greater than 1 has a unique factorization into primes. (We will revisit the issue of a proof in Section 14.4.)

We will introduce other accepted facts, as well as definitions, as needed.

8.3 Direct Proof

This section explains a simple way to prove theorems or propositions that have the form of conditional statements. The technique is called **direct proof**. To simplify the discussion, our first examples will involve proving statements that are almost obviously true. Thus we will call the statements *propositions* rather than theorems. (Remember, a proposition is a statement that, although true, is not as significant as a theorem.)

To understand how the technique of direct proof works, suppose we have some proposition of the following form.

Proposition If P , then Q .

This proposition is a conditional statement of the form $P \Rightarrow Q$. Our goal is to show that this conditional statement is true. To see how to proceed, look at the truth table.

| P | Q | $P \Rightarrow Q$ |
|-----|-----|-------------------|
| T | T | T |
| T | F | F |
| F | T | T |
| F | F | T |

The table shows that if P is false, the statement $P \Rightarrow Q$ is automatically true. This means that if we are concerned with showing $P \Rightarrow Q$ is true, we don't have to worry about the situations where P is false (as in the last two lines of the table) because the statement $P \Rightarrow Q$ will be automatically true in those cases. But we must be very careful about the situations where P is true (as in the first two lines of the table). We must show that the condition of P being true forces Q to be true also, for that means the second line of the table cannot happen.

This gives a fundamental outline for proving statements of the form $P \Rightarrow Q$. Begin by assuming that P is true (remember, we don't need to worry about P being false) and show this forces Q to be true. We summarize this as follows.

Outline for Direct Proof

Proposition If P , then Q .

Proof. Suppose P .

⋮

Therefore Q . ■

So the setup for direct proof is remarkably simple. The first line of the proof is the sentence “*Suppose P .*” The last line is the sentence “*Therefore Q .*” Between the first and last line we use logic, definitions and standard math facts to transform the statement P to the statement Q . It is common to use the word “*Proof*” to indicate the beginning of a proof, and the symbol ■ to indicate the end.

As our first example, let’s prove that if x is odd then x^2 is also odd. (Granted, this is not a terribly impressive result, but we will move on to more significant things in due time.) The first step in the proof is to fill in the outline for direct proof. This is a lot like painting a picture, where the basic structure is sketched in first. We leave some space between the first and last line of the proof. The following series of frames indicates the steps you might take to fill in this space with a logical chain of reasoning.

Proposition If x is odd, then x^2 is odd.

Proof. Suppose x is odd.

Therefore x^2 is odd. ■

Now that we have written the first and last lines, we need to fill in the space with a chain of reasoning that shows that x being odd forces x^2 to be odd.

In doing this it’s always advisable to use any definitions that apply. The first line says x is odd, and by Definition 8.2 it must be that $x = 2a + 1$ for some $a \in \mathbb{Z}$, so we write this in as our second line.

Proposition If x is odd, then x^2 is odd.

Proof. Suppose x is odd.

Then $x = 2a + 1$ for some $a \in \mathbb{Z}$, by definition of an odd number.

Therefore x^2 is odd. ■

Now jump down to the last line, which says x^2 is odd. Think about what the line immediately above it would have to be in order for us to conclude that x^2 is odd. By the definition of an odd number, we would have to have $x^2 = 2a + 1$ for some $a \in \mathbb{Z}$. However, the symbol a now appears earlier in the proof in a different context, so we should use a different symbol, say b .

Proposition If x is odd, then x^2 is odd.

Proof. Suppose x is odd.

Then $x = 2a + 1$ for some $a \in \mathbb{Z}$, by definition of an odd number.

Thus $x^2 = 2b + 1$ for an integer b .

Therefore x^2 is odd, by definition of an odd number. ■

We are almost there. We can bridge the gap as follows.

Proposition If x is odd, then x^2 is odd.

Proof. Suppose x is odd.

Then $x = 2a + 1$ for some $a \in \mathbb{Z}$, by definition of an odd number.

Thus $x^2 = (2a + 1)^2 = 4a^2 + 4a + 1 = 2(2a^2 + 2a) + 1$.

So $x^2 = 2b + 1$ where b is the integer $b = 2a^2 + 2a$.

Thus $x^2 = 2b + 1$ for an integer b .

Therefore x^2 is odd, by definition of an odd number. ■

Finally, we may wish to clean up our work and write the proof in paragraph form. Here is our final version.

Proposition If x is odd, then x^2 is odd.

Proof. Suppose x is odd. Then $x = 2a + 1$ for some $a \in \mathbb{Z}$, by definition of an odd number. Thus $x^2 = (2a + 1)^2 = 4a^2 + 4a + 1 = 2(2a^2 + 2a) + 1$, so $x^2 = 2b + 1$ where $b = 2a^2 + 2a \in \mathbb{Z}$. Therefore x^2 is odd, by definition of an odd number. ■

At least initially, it's a good idea to write the first and last line of your proof first, and then fill the gap, jumping alternately between top and bottom until you meet in the middle, as we did above. This way you are constantly reminded that you are aiming for the statement at the bottom. Sometimes you will leave too much space, sometimes not enough. Sometimes you will get stuck before figuring out what to do. This is normal. Mathematicians do scratch work just as artists do sketches for paintings.

Here is another example. Consider proving the following proposition.

Proposition Let a, b and c be integers. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Let's apply the basic outline for direct proof. To clarify the procedure we will write the proof in stages again.

Proposition Let a, b and c be integers. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof. Suppose $a \mid b$ and $b \mid c$.

Therefore $a \mid c$. ■

Our first step is to apply Definition 8.4 to the first line. The definition says $a \mid b$ means $b = ac$ for some integer c , but since c already appears in a different context on the first line, we must use a different letter, say d . Similarly let's use a new letter e in the definition of $b \mid c$.

Proposition Let a, b and c be integers. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof. Suppose $a \mid b$ and $b \mid c$.

By Definition 8.4, we know $a \mid b$ means there is an integer d with $b = ad$.

Likewise, $b \mid c$ means there is an integer e for which $c = be$.

Therefore $a \mid c$. ■

We have almost bridged the gap. The line immediately above the last line should show that $a \mid c$. According to Definition 8.4, this line should say that $c = ax$ for some integer x . We can get this equation from the lines at the top, as follows.

Proposition Let a, b and c be integers. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof. Suppose $a \mid b$ and $b \mid c$.

By Definition 8.4, we know $a \mid b$ means there is an integer d with $b = ad$.

Likewise, $b \mid c$ means there is an integer e for which $c = be$.

Thus $c = be = (ad)e = a(de)$, so $c = ax$ for the integer $x = de$.

Therefore $a \mid c$. ■

The next example is presented all at once rather than in stages.

Proposition If x is an even integer, then $x^2 - 6x + 5$ is odd.

Proof. Suppose x is an even integer.

Then $x = 2a$ for some $a \in \mathbb{Z}$, by definition of an even integer.

So $x^2 - 6x + 5 = (2a)^2 - 6(2a) + 5 = 4a^2 - 12a + 5 = 4a^2 - 12a + 4 + 1 = 2(2a^2 - 6a + 2) + 1$.

Therefore we have $x^2 - 6x + 5 = 2b + 1$, where $b = 2a^2 - 6a + 2 \in \mathbb{Z}$.

Consequently $x^2 - 6x + 5$ is odd, by definition of an odd number. ■

One doesn't normally use a separate line for each sentence in a proof, but for clarity we will often do this for the next few chapters.

Our next example illustrates a standard technique for showing two quantities are equal. If we can show $m \leq n$ and $n \leq m$ then it follows that $m = n$. In general, the reasoning involved in showing $m \leq n$ can be quite different from that of showing $n \leq m$.

Recall Definition 8.6 of a least common multiple on page 227.

Proposition If $a, b, c \in \mathbb{N}$, then $\text{lcm}(ca, cb) = c \cdot \text{lcm}(a, b)$.

Proof. Assume $a, b, c \in \mathbb{N}$. Let $m = \text{lcm}(ca, cb)$ and $n = c \cdot \text{lcm}(a, b)$. We will show $m = n$. By definition, $\text{lcm}(a, b)$ is a multiple of both a and b , so $\text{lcm}(a, b) = ax = by$ for some $x, y \in \mathbb{Z}$. From this we see that $n = c \cdot \text{lcm}(a, b) = cax = cby$ is a multiple of both ca and cb . But $m = \text{lcm}(ca, cb)$ is the *smallest* multiple of both ca and cb . Thus $m \leq n$.

On the other hand, as $m = \text{lcm}(ca, cb)$ is a multiple of both ca and cb , we have $m = cax = cby$ for some $x, y \in \mathbb{Z}$. Then $\frac{1}{c}m = ax = by$ is a multiple of both a and b . Therefore $\text{lcm}(a, b) \leq \frac{1}{c}m$, so $c \cdot \text{lcm}(a, b) \leq m$, that is, $n \leq m$.

We've shown $m \leq n$ and $n \leq m$, so $m = n$. The proof is complete. ■

The examples we've looked at so far have all been proofs of statements about integers. In our next example, we are going to prove that if x and y are positive real numbers for which $x \leq y$, then $\sqrt{x} \leq \sqrt{y}$. You may feel that the proof is not as "automatic" as the proofs we have done so far. Finding the right steps in a proof can be challenging, and that is part of the fun.

Proposition Let x and y be positive numbers. If $x \leq y$, then $\sqrt{x} \leq \sqrt{y}$.

Proof. Suppose $x \leq y$. Subtracting y from both sides gives $x - y \leq 0$.

This can be written as $\sqrt{x}^2 - \sqrt{y}^2 \leq 0$.

Factor this to get $(\sqrt{x} - \sqrt{y})(\sqrt{x} + \sqrt{y}) \leq 0$.

Dividing both sides by the positive number $\sqrt{x} + \sqrt{y}$ produces $\sqrt{x} - \sqrt{y} \leq 0$.

Adding \sqrt{y} to both sides gives $\sqrt{x} \leq \sqrt{y}$. ■

This proposition tells us that whenever $x \leq y$, we can take the square root of both sides and be assured that $\sqrt{x} \leq \sqrt{y}$. This can be useful, as we will see in our next proposition.

That proposition will concern the expression $2\sqrt{xy} \leq x + y$. Notice when you substitute random positive values for the variables, the expression is true. For example, for $x = 6$ and $y = 4$, the left side is $2\sqrt{6 \cdot 4} = 4\sqrt{6} \approx 9.79$, which is less than the right side $6 + 4 = 10$. Is it true that $2\sqrt{xy} \leq x + y$ for any positive x and y ? How could we prove it?

To see how, let's first cast this into the form of a conditional statement: If x and y are positive real numbers, then $2\sqrt{xy} \leq x + y$. The proof begins with the assumption that x and y are positive, and ends with $2\sqrt{xy} \leq x + y$. In mapping out a strategy, it can be helpful to work backwards, working from $2\sqrt{xy} \leq x + y$ to something that is obviously true. Then the steps can be reversed in the proof. In this case, squaring both sides of $2\sqrt{xy} \leq x + y$ gives us

$$4xy \leq x^2 + 2xy + y^2.$$

Now subtract $4xy$ from both sides and factor.

$$\begin{aligned} 0 &\leq x^2 - 2xy + y^2 \\ 0 &\leq (x - y)^2 \end{aligned}$$

But this last line is clearly true, since the square of $x - y$ cannot be negative! This gives us a strategy for the proof, which follows.

Proposition If x and y are positive real numbers, then $2\sqrt{xy} \leq x + y$.

Proof. Suppose x and y are positive real numbers.

Then $0 \leq (x - y)^2$, that is, $0 \leq x^2 - 2xy + y^2$.

Adding $4xy$ to both sides gives $4xy \leq x^2 + 2xy + y^2$.

Factoring yields $4xy \leq (x + y)^2$.

Previously we proved that such an inequality still holds after taking the square root of both sides; doing so produces $2\sqrt{xy} \leq x + y$. ■

Notice that in the last step of the proof we took the square root of both sides of $4xy \leq (x + y)^2$ and got $\sqrt{4xy} \leq \sqrt{(x + y)^2}$, and the fact that this did not reverse the symbol \leq followed from our previous proposition. This is an important point. Often the proof of a proposition or theorem uses another proposition or theorem (that has already been proved).

8.4 Using Cases

In proving a statement is true, we sometimes have to examine multiple cases before showing the statement is true in all possible scenarios. This section illustrates a few examples.

Our examples will concern the expression $1 + (-1)^n(2n - 1)$. Here is a table showing its value for various integers for n . Notice that $1 + (-1)^n(2n - 1)$ is a multiple of 4 in every line.

| n | $1 + (-1)^n(2n - 1)$ |
|-----|----------------------|
| 1 | 0 |
| 2 | 4 |
| 3 | -4 |
| 4 | 8 |
| 5 | -8 |
| 6 | 12 |

Is $1 + (-1)^n(2n - 1)$ always a multiple of 4? We prove the answer is “yes” in our next example. Notice, however, that the expression $1 + (-1)^n(2n - 1)$ behaves differently depending on whether n is even or odd, for in the first case $(-1)^n = 1$, and in the second $(-1)^n = -1$. Thus the proof must examine these two possibilities separately.

Proposition If $n \in \mathbb{N}$, then $1 + (-1)^n(2n - 1)$ is a multiple of 4.

Proof. Suppose $n \in \mathbb{N}$.

Then n is either even or odd. Let’s consider these two cases separately.

Case 1. Suppose n is even. Then $n = 2k$ for some $k \in \mathbb{Z}$, and $(-1)^n = 1$.

Thus $1 + (-1)^n(2n - 1) = 1 + (1)(2 \cdot 2k - 1) = 4k$, which is a multiple of 4.

Case 2. Suppose n is odd. Then $n = 2k + 1$ for some $k \in \mathbb{Z}$, and $(-1)^n = -1$.

Thus $1 + (-1)^n(2n - 1) = 1 - (2(2k + 1) - 1) = -4k$, which is a multiple of 4.

These cases show that $1 + (-1)^n(2n - 1)$ is always a multiple of 4. ■

Now let’s examine the flip side of the question. We just proved that $1 + (-1)^n(2n - 1)$ is always a multiple of 4, but can we get *every* multiple of 4 this way? The following proposition and proof give an affirmative answer.

Proposition Every multiple of 4 equals $1 + (-1)^n(2n - 1)$ for some $n \in \mathbb{N}$.

Proof. In conditional form, the proposition is as follows:

If k is a multiple of 4, then there is an $n \in \mathbb{N}$ for which $1 + (-1)^n(2n - 1) = k$.

What follows is a proof of this conditional statement.

Suppose k is a multiple of 4.

This means $k = 4a$ for some integer a .

We must produce an $n \in \mathbb{N}$ for which $1 + (-1)^n(2n - 1) = k$.

This is done by cases, depending on whether a is zero, positive or negative.

Case 1. Suppose $a = 0$. Let $n = 1$. Then $1 + (-1)^n(2n - 1) = 1 + (-1)^1(2 - 1) = 0 = 4 \cdot 0 = 4a = k$.

Case 2. Suppose $a > 0$. Let $n = 2a$, which is in \mathbb{N} because a is positive. Also n is even, so $(-1)^n = 1$. Thus $1 + (-1)^n(2n - 1) = 1 + (2n - 1) = 2n = 2(2a) = 4a = k$.

Case 3. Suppose $a < 0$. Let $n = 1 - 2a$, which is an element of \mathbb{N} because a is negative, making $1 - 2a$ positive. Also n is odd, so $(-1)^n = -1$. Thus $1 + (-1)^n(2n - 1) = 1 - (2n - 1) = 1 - (2(1 - 2a) - 1) = 4a = k$.

The above cases show that no matter whether a multiple $k = 4a$ of 4 is zero, positive or negative, $k = 1 + (-1)^n(2n - 1)$ for some $n \in \mathbb{N}$. ■

8.5 Treating Similar Cases

Occasionally two or more cases in a proof will be so similar that writing them separately seems tedious or unnecessary. Here is an example.

Proposition If two integers have opposite parity, then their sum is odd.

Proof. Suppose m and n are two integers with opposite parity.

We need to show that $m + n$ is odd. This is done in two cases, as follows.

Case 1. Suppose m is even and n is odd. Thus $m = 2a$ and $n = 2b + 1$ for some integers a and b . Therefore $m + n = 2a + 2b + 1 = 2(a + b) + 1$, which is odd (by Definition 8.2).

Case 2. Suppose m is odd and n is even. Thus $m = 2a + 1$ and $n = 2b$ for some integers a and b . Therefore $m + n = 2a + 1 + 2b = 2(a + b) + 1$, which is odd (by Definition 8.2).

In either case, $m + n$ is odd. ■

The two cases in this proof are entirely alike except for the order in which the even and odd terms occur. It is entirely appropriate to just do one case and indicate that the other case is nearly identical. The phrase “*Without loss of generality...*” is a common way of signaling that the proof is treating just one of several nearly identical cases. Here is a second version of the above example.

Proposition If two integers have opposite parity, then their sum is odd.

Proof. Suppose m and n are two integers with opposite parity.

We need to show that $m + n$ is odd.

Without loss of generality, suppose m is even and n is odd.

Thus $m = 2a$ and $n = 2b + 1$ for some integers a and b .

Therefore $m + n = 2a + 2b + 1 = 2(a + b) + 1$, which is odd (by Definition 8.2). ■

In reading proofs in other texts, you may sometimes see the phrase “Without loss of generality” abbreviated as “WLOG.” However, in the interest of transparency we will avoid writing it this way. In a similar spirit, it is advisable—at least until you become more experienced in proof writing—that you write out all cases, no matter how similar they appear to be.

Please check your understanding by doing the following exercises. The odd numbered problems have complete proofs in the Solutions section in the back of the text.

Exercises for Chapter 8

Use the method of direct proof to prove the following statements.

1. If x is an even integer, then x^2 is even.
2. If x is an odd integer, then x^3 is odd.
3. If a is an odd integer, then $a^2 + 3a + 5$ is odd.
4. Suppose $x, y \in \mathbb{Z}$. If x and y are odd, then xy is odd.
5. Suppose $x, y \in \mathbb{Z}$. If x is even, then xy is even.
6. Suppose $a, b, c \in \mathbb{Z}$. If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.
7. Suppose $a, b \in \mathbb{Z}$. If $a \mid b$, then $a^2 \mid b^2$.
8. Suppose a is an integer. If $5 \mid 2a$, then $5 \mid a$.
9. Suppose a is an integer. If $7 \mid 4a$, then $7 \mid a$.
10. Suppose a and b are integers. If $a \mid b$, then $a \mid (3b^3 - b^2 + 5b)$.
11. Suppose $a, b, c, d \in \mathbb{Z}$. If $a \mid b$ and $c \mid d$, then $ac \mid bd$.
12. If $x \in \mathbb{R}$ and $0 < x < 4$, then $\frac{4}{x(4-x)} \geq 1$.
13. Suppose $x, y \in \mathbb{R}$. If $x^2 + 5y = y^2 + 5x$, then $x = y$ or $x + y = 5$.
14. If $n \in \mathbb{Z}$, then $5n^2 + 3n + 7$ is odd. (Try cases.)
15. If $n \in \mathbb{Z}$, then $n^2 + 3n + 4$ is even. (Try cases.)
16. If two integers have the same parity, then their sum is even. (Try cases.)
17. If two integers have opposite parity, then their product is even.
18. Suppose x and y are positive real numbers. If $x < y$, then $x^2 < y^2$.

19. Suppose a, b and c are integers. If $a^2 \mid b$ and $b^3 \mid c$, then $a^6 \mid c$.
20. If a is an integer and $a^2 \mid a$, then $a \in \{-1, 0, 1\}$.
21. If p is prime and k is an integer for which $0 < k < p$, then p divides $\binom{p}{k}$.
22. If $n \in \mathbb{N}$, then $n^2 = 2\binom{n}{2} + \binom{n}{1}$. (You may need a separate case for $n = 1$.)
23. If $n \in \mathbb{N}$, then $\binom{2n}{n}$ is even.
24. If $n \in \mathbb{N}$ and $n \geq 2$, then the numbers $n! + 2, n! + 3, n! + 4, n! + 5, \dots, n! + n$ are all composite. (Thus for any $n \geq 2$, one can find n consecutive composite numbers. This means there are arbitrarily large “gaps” between prime numbers.)
25. If $a, b, c \in \mathbb{N}$ and $c \leq b \leq a$, then $\binom{a}{b}\binom{b}{c} = \binom{a}{b-c}\binom{a-b+c}{c}$.
26. Every odd integer is a difference of two squares. (Example $7 = 4^2 - 3^2$, etc.)
27. Suppose $a, b \in \mathbb{N}$. If $\gcd(a, b) > 1$, then $b \mid a$ or b is not prime.
28. If $a, b, c \in \mathbb{Z}$, then $c \cdot \gcd(a, b) \leq \gcd(ca, cb)$.

8.6 Solutions for Chapter 8

1. If x is an even integer, then x^2 is even.

Proof. Suppose x is even. Thus $x = 2a$ for some $a \in \mathbb{Z}$.

Consequently $x^2 = (2a)^2 = 4a^2 = 2(2a^2)$.

Therefore $x^2 = 2b$, where b is the integer $2a^2$.

Thus x^2 is even by definition of an even number. ■

3. If a is an odd integer, then $a^2 + 3a + 5$ is odd.

Proof. Suppose a is odd.

Thus $a = 2c + 1$ for some integer c , by definition of an odd number.

Then $a^2 + 3a + 5 = (2c + 1)^2 + 3(2c + 1) + 5 = 4c^2 + 4c + 1 + 6c + 3 + 5 = 4c^2 + 10c + 9$
 $= 4c^2 + 10c + 8 + 1 = 2(2c^2 + 5c + 4) + 1$.

This shows $a^2 + 3a + 5 = 2b + 1$, where $b = 2c^2 + 5c + 4 \in \mathbb{Z}$.

Therefore $a^2 + 3a + 5$ is odd. ■

5. Suppose $x, y \in \mathbb{Z}$. If x is even, then xy is even.

Proof. Suppose $x, y \in \mathbb{Z}$ and x is even.

Then $x = 2a$ for some integer a , by definition of an even number.

Thus $xy = (2a)(y) = 2(ay)$.

Therefore $xy = 2b$ where b is the integer ay , so xy is even. ■

7. Suppose $a, b \in \mathbb{Z}$. If $a \mid b$, then $a^2 \mid b^2$.

Proof. Suppose $a \mid b$.

By definition of divisibility, this means $b = ac$ for some integer c .

Squaring both sides of this equation produces $b^2 = a^2c^2$.

Then $b^2 = a^2d$, where $d = c^2 \in \mathbb{Z}$.

By definition of divisibility, this means $a^2 \mid b^2$. ■

9. Suppose a is an integer. If $7 \mid 4a$, then $7 \mid a$.

Proof. Suppose $7 \mid 4a$.

By definition of divisibility, this means $4a = 7c$ for some integer c .

Since $4a = 2(2a)$ it follows that $4a$ is even, and since $4a = 7c$, we know $7c$ is even.

But then c can't be odd, because that would make $7c$ odd, not even.

Thus c is even, so $c = 2d$ for some integer d .

Now go back to the equation $4a = 7c$ and plug in $c = 2d$. We get $4a = 14d$.

Dividing both sides by 2 gives $2a = 7d$.

Now, since $2a = 7d$, it follows that $7d$ is even, and thus d cannot be odd.

Then d is even, so $d = 2e$ for some integer e .

Plugging $d = 2e$ back into $2a = 7d$ gives $2a = 14e$.

Dividing both sides of $2a = 14e$ by 2 produces $a = 7e$.

Finally, the equation $a = 7e$ means that $7 \mid a$, by definition of divisibility. ■

11. Suppose $a, b, c, d \in \mathbb{Z}$. If $a \mid b$ and $c \mid d$, then $ac \mid bd$.

Proof. Suppose $a \mid b$ and $c \mid d$.

As $a \mid b$, the definition of divisibility means there is an integer x for which $b = ax$.

As $c \mid d$, the definition of divisibility means there is an integer y for which $d = cy$.

Since $b = ax$, we can multiply one side of $d = cy$ by b and the other by ax .

This gives $bd = axcy$, or $bd = (ac)(xy)$.

Since $xy \in \mathbb{Z}$, the definition of divisibility applied to $bd = (ac)(xy)$ gives $ac \mid bd$. ■

13. Suppose $x, y \in \mathbb{R}$. If $x^2 + 5y = y^2 + 5x$, then $x = y$ or $x + y = 5$.

Proof. Suppose $x^2 + 5y = y^2 + 5x$.

Then $x^2 - y^2 = 5x - 5y$, and factoring gives $(x - y)(x + y) = 5(x - y)$.

Now consider two cases.

Case 1. If $x - y \neq 0$ we can divide both sides of $(x - y)(x + y) = 5(x - y)$ by the non-zero quantity $x - y$ to get $x + y = 5$.

Case 2. If $x - y = 0$, then $x = y$. (By adding y to both sides.)

Thus $x = y$ or $x + y = 5$. ■

15. If $n \in \mathbb{Z}$, then $n^2 + 3n + 4$ is even.

Proof. Suppose $n \in \mathbb{Z}$. We consider two cases.

Case 1. Suppose n is even. Then $n = 2a$ for some $a \in \mathbb{Z}$.

Therefore $n^2 + 3n + 4 = (2a)^2 + 3(2a) + 4 = 4a^2 + 6a + 4 = 2(2a^2 + 3a + 2)$.

So $n^2 + 3n + 4 = 2b$ where $b = 2a^2 + 3a + 2 \in \mathbb{Z}$, so $n^2 + 3n + 4$ is even.

Case 2. Suppose n is odd. Then $n = 2a + 1$ for some $a \in \mathbb{Z}$.

Therefore $n^2 + 3n + 4 = (2a + 1)^2 + 3(2a + 1) + 4 = 4a^2 + 4a + 1 + 6a + 3 + 4 = 4a^2 + 10a + 8 = 2(2a^2 + 5a + 4)$. So $n^2 + 3n + 4 = 2b$ where $b = 2a^2 + 5a + 4 \in \mathbb{Z}$, so $n^2 + 3n + 4$ is even.

In either case $n^2 + 3n + 4$ is even. ■

17. If two integers have opposite parity, then their product is even.

Proof. Suppose a and b are two integers with opposite parity. Thus one is even and the other is odd. Without loss of generality, suppose a is even and b is odd. Therefore there are integers c and d for which $a = 2c$ and $b = 2d + 1$. Then the product of a and b is $ab = 2c(2d + 1) = 2(2cd + c)$. Therefore $ab = 2k$ where $k = 2cd + c \in \mathbb{Z}$. Therefore the product ab is even. ■

19. Suppose $a, b, c \in \mathbb{Z}$. If $a^2 \mid b$ and $b^3 \mid c$ then $a^6 \mid c$.

Proof. Since $a^2 \mid b$ we have $b = ka^2$ for some $k \in \mathbb{Z}$. Since $b^3 \mid c$ we have $c = hb^3$ for some $h \in \mathbb{Z}$. Thus $c = h(ka^2)^3 = hk^3a^6$. Hence $a^6 \mid c$. ■

21. If p is prime and $0 < k < p$ then $p \mid \binom{p}{k}$.

Proof. From the formula $\binom{p}{k} = \frac{p!}{(p-k)!k!}$, we get $p! = \binom{p}{k}(p-k)!k!$. Now, since the prime number p is a factor of $p!$ on the left, it must also be a factor of $\binom{p}{k}(p-k)!k!$ on the right. Thus the prime number p appears in the prime factorization of $\binom{p}{k}(p-k)!k!$.

Now, $k!$ is a product of numbers smaller than p , so its prime factorization contains no p 's. Similarly the prime factorization of $(p-k)!$ contains no p 's. But we noted that the prime factorization of $\binom{p}{k}(p-k)!k!$ must contain a p , so it follows that the prime factorization of $\binom{p}{k}$ contains a p . Thus $\binom{p}{k}$ is a multiple of p , so p divides $\binom{p}{k}$. ■

23. If $n \in \mathbb{N}$ then $\binom{2n}{n}$ is even.

Proof. By definition, $\binom{2n}{n}$ is the number of n -element subsets of a set A with $2n$ elements. For each subset $X \subseteq A$ with $|X| = n$, the complement \overline{X} is a different set, but it also has $2n - n = n$ elements. Imagine listing out all the n -element subset of a set A . It could be done in such a way that the list has form

$$X_1, \overline{X_1}, X_2, \overline{X_2}, X_3, \overline{X_3}, X_4, \overline{X_4}, X_5, \overline{X_5} \dots$$

This list has an even number of items, for they are grouped in pairs. Thus $\binom{2n}{n}$ is even. ■

25. If $a, b, c \in \mathbb{N}$ and $c \leq b \leq a$ then $\binom{a}{b}\binom{b}{c} = \binom{a}{b-c}\binom{a-b+c}{c}$.

Proof. Assume $a, b, c \in \mathbb{N}$ with $c \leq b \leq a$. Then we have $\binom{a}{b}\binom{b}{c} = \frac{a!}{(a-b)!b!} \frac{b!}{(b-c)!c!} = \frac{a!}{(a-b+c)!(a-b)!} \frac{(a-b+c)!}{(b-c)!c!} = \frac{a!}{(b-c)!(a-b+c)!} \frac{(a-b+c)!}{(a-b)!c!} = \binom{a}{b-c}\binom{a-b+c}{c}$. ■

27. Suppose $a, b \in \mathbb{N}$. If $\gcd(a, b) > 1$, then $b \mid a$ or b is not prime.

Proof. Suppose $\gcd(a, b) > 1$. Let $c = \gcd(a, b) > 1$. Then since c is a divisor of both a and b , we have $a = cx$ and $b = cy$ for integers x and y . We divide into two cases according to whether or not b is prime.

Case I. Suppose b is prime. Then the above equation $b = cy$ with $c > 1$ forces $c = b$ and $y = 1$. Then $a = cx$ becomes $a = bx$, which means $b \mid a$. We conclude that the statement “ $b \mid a$ or b is not prime,” is true.

Case II. Suppose b is not prime. Then the statement “ $b \mid a$ or b is not prime,” is automatically true. ■

Contrapositive Proof

We now examine an alternative to direct proof called **contrapositive proof**. Like direct proof, the technique of contrapositive proof is used to prove conditional statements of the form “If P , then Q .” Although it is possible to use direct proof exclusively, there are occasions where contrapositive proof is much easier.

9.1 Contrapositive Proof

To understand how contrapositive proof works, imagine that you need to prove a proposition of the following form.

Proposition If P , then Q .

This is a conditional statement of form $P \Rightarrow Q$. Our goal is to show that this conditional statement is true. Recall that in Section 3.6 we observed that $P \Rightarrow Q$ is logically equivalent to $\sim Q \Rightarrow \sim P$. For convenience, we duplicate the truth table that verifies this fact.

| P | Q | $\sim Q$ | $\sim P$ | $P \Rightarrow Q$ | $\sim Q \Rightarrow \sim P$ |
|-----|-----|----------|----------|-------------------|-----------------------------|
| T | T | F | F | T | T |
| T | F | T | F | F | F |
| F | T | F | T | T | T |
| F | F | T | T | T | T |

According to the table, statements $P \Rightarrow Q$ and $\sim Q \Rightarrow \sim P$ are different ways of expressing exactly the same thing. The expression $\sim Q \Rightarrow \sim P$ is called the **contrapositive form** of $P \Rightarrow Q$.¹

Since $P \Rightarrow Q$ is logically equivalent to $\sim Q \Rightarrow \sim P$, it follows that to prove $P \Rightarrow Q$ is true, it suffices to instead prove that $\sim Q \Rightarrow \sim P$ is true. If we were

¹Do not confuse the words *contrapositive* and *converse*. Recall from Section 3.4 that the *converse* of $P \Rightarrow Q$ is the statement $Q \Rightarrow P$, which is not logically equivalent to $P \Rightarrow Q$.

to use direct proof to show $\sim Q \Rightarrow \sim P$ is true, we would assume $\sim Q$ is true use this to deduce that $\sim P$ is true. This in fact is the basic approach of contrapositive proof, summarized as follows.

Outline for Contrapositive Proof

Proposition If P , then Q .

Proof. Suppose $\sim Q$.

⋮

Therefore $\sim P$. ■

So the setup for contrapositive proof is very simple. The first line of the proof is the sentence “*Suppose Q is not true.*” (Or something to that effect.) The last line is the sentence “*Therefore P is not true.*” Between the first and last line we use logic and definitions to transform the statement $\sim Q$ to the statement $\sim P$.

To illustrate this new technique, and to contrast it with direct proof, we now prove a proposition in two ways: first with direct proof and then with contrapositive proof.

Proposition Suppose $x \in \mathbb{Z}$. If $7x + 9$ is even, then x is odd.

Proof. (Direct) Suppose $7x + 9$ is even.

Thus $7x + 9 = 2a$ for some integer a .

Subtracting $6x + 9$ from both sides, we get $x = 2a - 6x - 9$.

Thus $x = 2a - 6x - 9 = 2a - 6x - 10 + 1 = 2(a - 3x - 5) + 1$.

Consequently $x = 2b + 1$, where $b = a - 3x - 5 \in \mathbb{Z}$.

Therefore x is odd. ■

Here is a contrapositive proof of the same statement:

Proposition Suppose $x \in \mathbb{Z}$. If $7x + 9$ is even, then x is odd.

Proof. (Contrapositive) Suppose x is not odd.

Thus x is even, so $x = 2a$ for some integer a .

Then $7x + 9 = 7(2a) + 9 = 14a + 8 + 1 = 2(7a + 4) + 1$.

Therefore $7x + 9 = 2b + 1$, where b is the integer $7a + 4$.

Consequently $7x + 9$ is odd.

Therefore $7x + 9$ is not even. ■

Though the proofs are of equal length, you may feel that the contrapositive proof flowed more smoothly. This is because it is easier to transform information about x into information about $7x+9$ than the other way around. For our next example, consider the following proposition concerning an integer x :

Proposition If $x^2 - 6x + 5$ is even, then x is odd.

A direct proof would be problematic. We would begin by assuming that $x^2 - 6x + 5$ is even, so $x^2 - 6x + 5 = 2a$. Then we would need to transform this into $x = 2b + 1$ for $b \in \mathbb{Z}$. But it is not quite clear how that could be done, for it would involve isolating an x from the quadratic expression. However the proof becomes very simple if we use contrapositive proof.

Proposition Suppose $x \in \mathbb{Z}$. If $x^2 - 6x + 5$ is even, then x is odd.

Proof. (Contrapositive) Suppose x is not odd.

Thus x is even, so $x = 2a$ for some integer a .

So $x^2 - 6x + 5 = (2a)^2 - 6(2a) + 5 = 4a^2 - 12a + 5 = 4a^2 - 12a + 4 + 1 = 2(2a^2 - 6a + 2) + 1$.

Therefore $x^2 - 6x + 5 = 2b + 1$, where b is the integer $2a^2 - 6a + 2$.

Consequently $x^2 - 6x + 5$ is odd.

Therefore $x^2 - 6x + 5$ is not even. ■

In summary, since x being not odd ($\sim Q$) resulted in $x^2 - 6x + 5$ being not even ($\sim P$), then $x^2 - 6x + 5$ being even (P) means that x is odd (Q). Thus we have proved $P \Rightarrow Q$ by proving $\sim Q \Rightarrow \sim P$. Here is another example:

Proposition Suppose $x, y \in \mathbb{R}$. If $y^3 + yx^2 \leq x^3 + xy^2$, then $y \leq x$.

Proof. (Contrapositive) Suppose it is not true that $y \leq x$, so $y > x$.

Then $y - x > 0$. Multiply both sides of $y - x > 0$ by the positive value $x^2 + y^2$.

$$\begin{aligned} (y-x)(x^2+y^2) &> 0(x^2+y^2) \\ yx^2+y^3-x^3-xy^2 &> 0 \\ y^3+yx^2 &> x^3+xy^2 \end{aligned}$$

Therefore $y^3 + yx^2 > x^3 + xy^2$, so it is not true that $y^3 + yx^2 \leq x^3 + xy^2$. ■

Proving “If P , then Q ,” with the contrapositive approach necessarily involves the negated statements $\sim P$ and $\sim Q$. In working with these we may have to use the techniques for negating statements (e.g., DeMorgan’s laws) discussed in Section 7.4. We consider such an example next.

Proposition Suppose $x, y \in \mathbb{Z}$. If $5 \nmid xy$, then $5 \nmid x$ and $5 \nmid y$.

Proof. (Contrapositive) Suppose it is not true that $5 \nmid x$ **and** $5 \nmid y$. By DeMorgan's law, it is not true that $5 \nmid x$ **or** it is not true that $5 \nmid y$. Therefore $5 \mid x$ or $5 \mid y$. We consider these possibilities separately.

Case 1. Suppose $5 \mid x$. Then $x = 5a$ for some $a \in \mathbb{Z}$.

From this we get $xy = 5(ay)$, and that means $5 \mid xy$.

Case 2. Suppose $5 \mid y$. Then $y = 5a$ for some $a \in \mathbb{Z}$.

From this we get $xy = 5(ax)$, and that means $5 \mid xy$.


The above cases show that $5 \mid xy$, so it is not true that $5 \nmid xy$. ■

9.2 Congruence of Integers

This is a good time to introduce a new definition. It is not necessarily related to contrapositive proof, but introducing it now ensures that we have a sufficient variety of exercises to practice all our proof techniques on. This new definition occurs in many branches of mathematics, and it will surely play a role in some of your later courses. But our primary reason for introducing it is that it will give us more practice in writing proofs.

Definition 9.1 Given integers a and b and an $n \in \mathbb{N}$, we say a and b are **congruent modulo n** if $n \mid (a - b)$. We express this as $a \equiv b \pmod{n}$. If a and b are not congruent modulo n , we write this as $a \not\equiv b \pmod{n}$.

Example 9.1 Here are some examples:

1. $9 \equiv 1 \pmod{4}$ because $4 \mid (9 - 1)$.
2. $6 \equiv 10 \pmod{4}$ because $4 \mid (6 - 10)$.
3. $14 \not\equiv 8 \pmod{4}$ because $4 \nmid (14 - 8)$.
4. $20 \equiv 4 \pmod{8}$ because $8 \mid (20 - 4)$.
5. $17 \equiv -4 \pmod{3}$ because $3 \mid (17 - (-4))$. 

In practical terms, $a \equiv b \pmod{n}$ means that a and b have the same remainder when divided by n . For example, we saw above that $6 \equiv 10 \pmod{4}$ and indeed 6 and 10 both have remainder 2 when divided by 4. Also we saw $14 \not\equiv 8 \pmod{4}$, and sure enough 14 has remainder 2 when divided by 4, while 8 has remainder 0.

To see that this is true in general, note that if a and b both have the same remainder r when divided by n , then $a = kn + r$ and $b = \ell n + r$ for some $k, \ell \in \mathbb{Z}$. Then $a - b = (kn + r) - (\ell n + r) = n(k - \ell)$. But $a - b = n(k - \ell)$ means $n \mid (a - b)$, so $a \equiv b \pmod{n}$. Conversely, Exercise 9.32 asks you to show that if $a \equiv b \pmod{n}$, then a and b have the same remainder when divided by n .

We conclude this section with several proofs involving congruence of integers, but you will also test your skills with other proofs in the exercises.

Proposition Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. If $a \equiv b \pmod{n}$, then $a^2 \equiv b^2 \pmod{n}$.

Proof. We will use direct proof. Suppose $a \equiv b \pmod{n}$.

By definition of congruence of integers, this means $n \mid (a - b)$.

Then by definition of divisibility, there is an integer c for which $a - b = nc$.

Now multiply both sides of this equation by $a + b$.

$$\begin{aligned} a - b &= nc \\ (a - b)(a + b) &= nc(a + b) \\ a^2 - b^2 &= nc(a + b) \end{aligned}$$

Since $c(a + b) \in \mathbb{Z}$, the above equation tells us $n \mid (a^2 - b^2)$.

According to Definition 9.1, this gives $a^2 \equiv b^2 \pmod{n}$. ■

Let's pause to consider this proposition's meaning. It says $a \equiv b \pmod{n}$ implies $a^2 \equiv b^2 \pmod{n}$. In other words, it says that if integers a and b have the same remainder when divided by n , then a^2 and b^2 also have the same remainder when divided by n . As an example of this, 6 and 10 have the same remainder (2) when divided by $n = 4$, and their squares 36 and 100 also have the same remainder (0) when divided by $n = 4$. The proposition promises this will happen for all a, b and n . In our examples we tend to concentrate more on how to prove propositions than on what the propositions mean. This is reasonable since our main goal is to learn how to prove statements. But it is helpful to sometimes also think about the meaning of what we prove.

Proposition Let $a, b, c \in \mathbb{Z}$ and $n \in \mathbb{N}$. If $a \equiv b \pmod{n}$, then $ac \equiv bc \pmod{n}$.

Proof. We employ direct proof. Suppose $a \equiv b \pmod{n}$. By Definition 9.1, it follows that $n \mid (a - b)$. Therefore, by definition of divisibility, there exists an integer k for which $a - b = nk$. Multiply both sides of this equation by c to get $ac - bc = nkc$. Thus $ac - bc = n(kc)$ where $kc \in \mathbb{Z}$, which means $n \mid (ac - bc)$. By Definition 9.1, we have $ac \equiv bc \pmod{n}$. ■

Contrapositive proof seems to be the best approach in the next example, since it will eliminate the symbols \dagger and \neq .

Proposition Suppose $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. If $12a \not\equiv 12b \pmod{n}$, then $n \nmid 12$.

Proof. (Contrapositive) Suppose $n \mid 12$, so there is an integer c for which $12 = nc$. Now reason as follows.

$$\begin{aligned} 12 &= nc \\ 12(a - b) &= nc(a - b) \\ 12a - 12b &= n(ca - cb) \end{aligned}$$

Since $ca - cb \in \mathbb{Z}$, the equation $12a - 12b = n(ca - cb)$ implies $n \mid (12a - 12b)$. This in turn means $12a \equiv 12b \pmod{n}$. ■

9.3 Mathematical Writing

Now that we have begun writing proofs, it is a good time to contemplate the craft of writing. Unlike logic and mathematics, where there is a clear-cut distinction between what is right or wrong, the difference between good and bad writing is sometimes a matter of opinion. But there are some standard guidelines that will make your writing clearer. Some are listed below.

1. **Begin each sentence with a word, not a mathematical symbol.**

The reason is that sentences begin with capital letters, but mathematical symbols are case sensitive. Because x and X can have entirely different meanings, putting such symbols at the beginning of a sentence can lead to ambiguity. Here are some examples of bad usage (marked with \times) and good usage (marked with \checkmark).

A is a subset of B . \times

The set A is a subset of B . \checkmark

x is an integer, so $2x + 5$ is an integer. \times

Because x is an integer, $2x + 5$ is an integer. \checkmark

$x^2 - x + 2 = 0$ has two solutions. \times

$X^2 - x + 2 = 0$ has two solutions. \times (and silly too)

The equation $x^2 - x + 2 = 0$ has two solutions. \checkmark

2. **End each sentence with a period, even when the sentence ends with a mathematical symbol or expression.**

Euler proved that $\sum_{k=1}^{\infty} \frac{1}{k^s} = \prod_{p \in P} \frac{1}{1 - \frac{1}{p^s}}$ \times

Euler proved that $\sum_{k=1}^{\infty} \frac{1}{k^s} = \prod_{p \in P} \frac{1}{1 - \frac{1}{p^s}}$. \checkmark

Mathematical statements (equations, etc.) are like English phrases that happen to contain special symbols, so use normal punctuation.

3. **Separate mathematical symbols and expressions with words.** Not doing this can cause confusion by making distinct expressions appear to merge into one. Compare the clarity of the following examples.

Because $x^2 - 1 = 0$, $x = 1$ or $x = -1$. ×

Because $x^2 - 1 = 0$, it follows that $x = 1$ or $x = -1$. ✓

Unlike $A \cup B$, $A \cap B$ equals \emptyset . ×

Unlike $A \cup B$, the set $A \cap B$ equals \emptyset . ✓

4. **Avoid misuse of symbols.** Symbols such as $=$, \leq , \subseteq , \in , etc., are not words. While it is appropriate to use them in mathematical expressions, they are out of place in other contexts.

Since the two sets are $=$, one is a subset of the other. ×

Since the two sets are equal, one is a subset of the other. ✓

The empty set is a \subseteq of every set. ×

The empty set is a subset of every set. ✓

Since a is odd and x odd $\Rightarrow x^2$ odd, a^2 is odd. ×

Since a is odd and any odd number squared is odd, then a^2 is odd. ✓

5. **Avoid using unnecessary symbols.** Mathematics is confusing enough without them. Don't muddy the water even more.

No set X has negative cardinality. ×

No set has negative cardinality. ✓

6. **Use the first person plural.** In mathematical writing, it is common to use the words "we" and "us" rather than "I," "you" or "me." It is as if the reader and writer are having a conversation, with the writer guiding the reader through the details of the proof.

7. **Use the active voice.** This is just a suggestion, but the active voice makes your writing more lively.

The value $x = 3$ is obtained through the division of both sides by 5. ×

Dividing both sides by 5, we get the value $x = 3$. ✓

8. **Explain each new symbol.** In writing a proof, you must explain the meaning of every new symbol you introduce. Failure to do this can lead to ambiguity, misunderstanding and mistakes. For example, consider the following two possibilities for a sentence in a proof, where a and b have been introduced on a previous line.

- Since $a \mid b$, it follows that $b = ac$. ×
- Since $a \mid b$, it follows that $b = ac$ for some integer c . ✓

If you use the first form, then a reader who has been carefully following your proof may momentarily scan backwards looking for where the c entered into the picture, not realizing at first that it came from the definition of divides.

9. **Watch out for “it.”** The pronoun “it” can cause confusion when it is unclear what it refers to. If there is any possibility of confusion, you should avoid the word “it.” Here is an example:

Since $X \subseteq Y$, and $0 < |X|$, we see that it is not empty. ×

Is “it” X or Y ? Either one would make sense, but which do we mean?

Since $X \subseteq Y$, and $0 < |X|$, we see that Y is not empty. ✓

10. **Since, because, as, for, so.** In proofs, it is common to use these words as conjunctions joining two statements, and meaning that one statement is true and as a consequence the other true. The following statements all mean that P is true (or assumed to be true) and as a consequence Q is true also.

| | | | | |
|-----------------|-------------------|--------------|---------------|--------------|
| Q since P | Q because P | Q , as P | Q , for P | P , so Q |
| Since P , Q | Because P , Q | as P , Q | | |

Notice that the meaning of these constructions is different from that of “If P , then Q ,” for they are asserting not only that P implies Q , but **also** that P is true. Exercise care in using them. It must be the case that P and Q are both statements **and** that Q really does follow from P .

- $x \in \mathbb{N}$, so \mathbb{Z} ×
- $x \in \mathbb{N}$, so $x \in \mathbb{Z}$ ✓

11. **Thus, hence, therefore consequently.** These adverbs precede a statement that follows logically from previous sentences or clauses. Be sure that a statement follows them.

- Therefore $2k + 1$. ×
- Therefore $a = 2k + 1$. ✓

12. **Clarity is the gold standard of mathematical writing.** If you believe breaking a rule makes your writing clearer, then break the rule.

Your mathematical writing will evolve with practice usage. One of the best ways to develop a good mathematical writing style is to read other people’s proofs. Adopt what works and avoid what doesn’t.

9.4 The Euclidean Algorithm

Proofs and algorithms intersect in various ways. As we will see later in this book, one can *prove* that a given algorithm works correctly. In another direction, propositions and theorems that have been proved may be used in algorithms. This section explores an example of such an algorithm – the famous Euclidean algorithm for computing the greatest common divisor of two numbers.

This algorithm is named after Euclid, who recorded it more than 2000 years ago (although it is unlikely that he himself discovered it). It is based on the following proposition.

Proposition If a and b are integers, then $\gcd(a, b) = \gcd(a - b, b)$.

Proof. (Direct) Suppose $a, b \in \mathbb{Z}$. We will first prove $\gcd(a, b) \leq \gcd(a - b, b)$, then $\gcd(a, b) \geq \gcd(a - b, b)$. Together these will imply $\gcd(a, b) = \gcd(a - b, b)$.

So let's prove $\gcd(a, b) \leq \gcd(a - b, b)$. Put $d = \gcd(a, b)$. As d is a divisor of both a and b , we have $a = dx$ and $b = dy$ for some integers x and y . Then $a - b = dx - dy = d(x - y)$, which means d divides $a - b$. Thus d is divisor of both $a - b$ and b . But it can't be greater than the *greatest* common divisor of $a - b$ and b , which is to say $\gcd(a, b) = d \leq \gcd(a - b, b)$.

Next let $e = \gcd(a - b, b)$. Then e divides both $a - b$ and b , so $a - b = ex$ and $b = ey$ for integers x and y . Then $a = (a - b) + b = ex + ey = e(x + y)$, so now we see that e is a divisor of both a and b . But it is not more than their *greatest* common divisor, that is, $\gcd(a - b, b) = e \leq \gcd(a, b)$.

The previous two paragraphs show $\gcd(a, b) = \gcd(a - b, b)$. ■

This proposition means that if we need to compute $\gcd(a, b)$, then we will get the same answer by computing $\gcd(a - b, b)$, which might be easier, as it involves smaller numbers.

For a concrete example, suppose we wanted to compute $\gcd(30, 12)$. (Pretend for the moment that you don't see what the answer will be.) The proposition says $\gcd(30, 12) = \gcd(30 - 12, 12) = \gcd(18, 12)$, so we have reduced our problem to that of finding $\gcd(18, 12)$. For *this*, we can use the proposition *again* to get $\gcd(18, 12) = \gcd(18 - 12, 12) = \gcd(6, 12)$. Using it a third time would give the negative value $6 - 12$, but we *can* interchange the numbers to get $\gcd(6, 12) = \gcd(12, 6)$, and the proposition applied twice to this yields $\gcd(12, 6) = \gcd(12 - 6, 6) = \gcd(6, 6) = \gcd(6 - 6, 6) = \gcd(0, 6) = 6$. (Recall $\gcd(0, 6) = 6$, as *every* integer is a divisor of 0, but the greatest divisor of 6 is 6. Similarly, $\gcd(0, b) = b$ when $b \neq 0$.) Multiple applications of the proposition have given $\gcd(30, 12) = 6$.

For pedagogical honesty we point out that the Euclidean algorithm is not used in a substantial way for the remainder of the book, though it is a good case study in some important ideas. We consider one of those ideas now: the idea that we can *prove* that an algorithm terminates (i.e., it does not go into an infinite loop).

Proposition If its input numbers a, b are positive, then the Euclidean algorithm terminates.

Proof. (Direct) Suppose a and b are positive. As the algorithm starts, the main while loop begins its first iteration, because $a \neq 0$.

Let's trace the first iteration of this loop. As it begins, if $a < b$ then a and b are interchanged. Regardless, we have $a \geq b$ after the if command. Then, in the second (inner) while loop begins and continually decrements a by b as long as $a \geq b$. As $a \geq b$, the value $a := a - b$ that is assigned to a is never negative. Thus, at the end of the first iteration we have $0 \leq a < b$.

If $a = 0$ there are no further iterations, and the algorithm finishes. Otherwise in the second iteration a and b are swapped because $a < b$. This decreases the value of b , and makes $a \geq b$. Then the inner while loop decreases the value of a until $a < b$. But also $0 \leq a$ because the assignment $a := a - b$ is only performed if $a \geq b$. Thus after the second iteration both a and b have decreased and $0 \leq a < b$.

This pattern continues in all further iterations. The iteration begins with $0 < a < b$. Then a and b are swapped, decreasing the value of b . Then a is decreased until $0 \leq a < b$.

So each iteration after the first decreases both of the integers a and b , resulting in $0 \leq a < b$. Thus after a finite number of iterations we must reach $a = 0$, at which point the algorithm terminates. ■

Notice that Euclidean algorithm does its job with just one arithmetic operation – subtraction. Given that subtraction is an easy operation, the Euclidean algorithm is very straightforward, efficient and fast, especially compared to other methods of computing greatest common divisors.

For instance, you are probably familiar with the technique of finding $\gcd(a, b)$ by comparing the prime factorizations of a and b . Given, say, 310 and 90, we prime factor them as

$$310 = 2 \cdot 5 \cdot 31 \quad \text{and} \quad 90 = 2 \cdot 3^2 \cdot 5.$$

The common prime factors are 2 and 5, and so $\gcd(310, 90) = 2 \cdot 5 = 10$. If we were going to write a gcd algorithm that took this approach, it would have to

find the prime factors of each number, compare them to each other, collect the common ones and multiply. Such an algorithm would be nowhere as simple as the Euclidean algorithm.

We close with one final remark. Look at the inner while loop in the Euclidean algorithm. It shares a striking resemblance to part of the division algorithm on page 185.

```
while  $a \geq b$  do
  |  $a := a - b$ 
end
```

Before the while loop starts, we have $a = qb + r$ with $0 \leq r < b$, that is, b goes into a , q times with remainder r . When the while loop finishes, the q b 's have been subtracted from a , and a has been replaced with r . In some versions of the Euclidean algorithm (in other texts), this while loop is replaced with the command

$a := r$ where $a = qb + r$, by the division algorithm.

We have opted to code the computation of r directly into the Euclidean algorithm. See Exercise 9.31 below for a proposition leading to the alternate form of the Euclidean algorithm.

Exercises for Chapter 9

- A. Use the method of contrapositive proof to prove the following statements. (In each case you should also think about how a direct proof would work. You will find in most cases that contrapositive is easier.)
1. Suppose $n \in \mathbb{Z}$. If n^2 is even, then n is even.
 2. Suppose $n \in \mathbb{Z}$. If n^2 is odd, then n is odd.
 3. Suppose $a, b \in \mathbb{Z}$. If $a^2(b^2 - 2b)$ is odd, then a and b are odd.
 4. Suppose $a, b, c \in \mathbb{Z}$. If a does not divide bc , then a does not divide b .
 5. Suppose $x \in \mathbb{R}$. If $x^2 + 5x < 0$ then $x < 0$.
 6. Suppose $x \in \mathbb{R}$. If $x^3 - x > 0$ then $x > -1$.
 7. Suppose $a, b \in \mathbb{Z}$. If both ab and $a + b$ are even, then both a and b are even.
 8. Suppose $x \in \mathbb{R}$. If $x^5 - 4x^4 + 3x^3 - x^2 + 3x - 4 \geq 0$, then $x \geq 0$.
 9. Suppose $n \in \mathbb{Z}$. If $3 \nmid n^2$, then $3 \nmid n$.
 10. Suppose $x, y, z \in \mathbb{Z}$ and $x \neq 0$. If $x \nmid yz$, then $x \nmid y$ and $x \nmid z$.
 11. Suppose $x, y \in \mathbb{Z}$. If $x^2(y + 3)$ is even, then x is even or y is odd.
 12. Suppose $a \in \mathbb{Z}$. If a^2 is not divisible by 4, then a is odd.
 13. Suppose $x \in \mathbb{R}$. If $x^5 + 7x^3 + 5x \geq x^4 + x^2 + 8$, then $x \geq 0$.

- B.** Prove the following statements using either direct or contrapositive proof. Sometimes one approach will be much easier than the other.
14. If $a, b \in \mathbb{Z}$ and a and b have the same parity, then $3a + 7$ and $7b - 4$ do not.
 15. Suppose $x \in \mathbb{Z}$. If $x^3 - 1$ is even, then x is odd.
 16. Suppose $x \in \mathbb{Z}$. If $x + y$ is even, then x and y have the same parity.
 17. If n is odd, then $8 \mid (n^2 - 1)$.
 18. For any $a, b \in \mathbb{Z}$, it follows that $(a + b)^3 \equiv a^3 + b^3 \pmod{3}$.
 19. Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. If $a \equiv b \pmod{n}$ and $a \equiv c \pmod{n}$, then $c \equiv b \pmod{n}$.
 20. If $a \in \mathbb{Z}$ and $a \equiv 1 \pmod{5}$, then $a^2 \equiv 1 \pmod{5}$.
 21. Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. If $a \equiv b \pmod{n}$, then $a^3 \equiv b^3 \pmod{n}$.
 22. Let $a \in \mathbb{Z}$, $n \in \mathbb{N}$. If a has remainder r when divided by n , then $a \equiv r \pmod{n}$.
 23. Let $a, b, c \in \mathbb{Z}$ and $n \in \mathbb{N}$. If $a \equiv b \pmod{n}$, then $ca \equiv cb \pmod{n}$.
 24. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$.
 25. If $n \in \mathbb{N}$ and $2^n - 1$ is prime, then n is prime.
 26. If $n = 2^k - 1$ for $k \in \mathbb{N}$, then every entry in Row n of Pascal's Triangle is odd.
 27. If $a \equiv 0 \pmod{4}$ or $a \equiv 1 \pmod{4}$, then $\binom{a}{2}$ is even.
 28. If $n \in \mathbb{Z}$, then $4 \nmid (n^2 - 3)$.
 29. Write a recursive procedure to compute $\gcd(a, b)$. (This is the only exercise in this section that is not a proof.)
 30. If $a \equiv b \pmod{n}$, then $\gcd(a, n) = \gcd(b, n)$.
 31. Suppose the division algorithm applied to a and b yields $a = qb + r$. Then $\gcd(a, b) = \gcd(r, b)$.
 32. If $a \equiv b \pmod{n}$, then a and b have the same remainder when divided by n .

9.5 Solutions for Chapter 9

1. Proposition Suppose $n \in \mathbb{Z}$. If n^2 is even, then n is even.

Proof. (Contrapositive) Suppose n is not even. Then n is odd, so $n = 2a + 1$ for some integer a , by definition of an odd number. Thus $n^2 = (2a + 1)^2 = 4a^2 + 4a + 1 = 2(2a^2 + 2a) + 1$. Consequently $n^2 = 2b + 1$, where b is the integer $2a^2 + 2a$, so n^2 is odd. Therefore n^2 is not even. ■

3. Proposition Suppose $a, b \in \mathbb{Z}$. If $a^2(b^2 - 2b)$ is odd, then a and b are odd.

Proof. (Contrapositive) Suppose it is not the case that a and b are odd. Then, by DeMorgan's law, at least one of a and b is even. Let us look at these cases separately.

Case 1. Suppose a is even. Then $a = 2c$ for some integer c . Thus $a^2(b^2 - 2b) = (2c)^2(b^2 - 2b) = 2(2c^2(b^2 - 2b))$, which is even.

Case 2. Suppose b is even. Then $b = 2c$ for some integer c . Thus $a^2(b^2 - 2b) = a^2((2c)^2 - 2(2c)) = 2(a^2(2c^2 - 2c))$, which is even.

(A third case involving a and b both even is unnecessary, for either of the two cases above cover this case.) Thus in either case $a^2(b^2 - 2b)$ is even, so it is not odd. ■

5. Proposition Suppose $x \in \mathbb{R}$. If $x^2 + 5x < 0$ then $x < 0$.

Proof. (Contrapositive) Suppose it is not the case that $x < 0$, so $x \geq 0$. Then neither x^2 nor $5x$ is negative, so $x^2 + 5x \geq 0$. Thus it is not true that $x^2 + 5x < 0$. ■

7. Proposition Suppose $a, b \in \mathbb{Z}$. If both ab and $a + b$ are even, then both a and b are even.

Proof. (Contrapositive) Suppose it is not the case that both a and b are even. Then at least one of them is odd. There are three cases to consider.

Case 1. Suppose a is even and b is odd. Then there are integers c and d for which $a = 2c$ and $b = 2d + 1$. Then $ab = 2c(2d + 1)$, which is even; and $a + b = 2c + 2d + 1 = 2(c + d) + 1$, which is odd. Thus it is not the case that both ab and $a + b$ are even.

Case 2. Suppose a is odd and b is even. Then there are integers c and d for which $a = 2c + 1$ and $b = 2d$. Then $ab = (2c + 1)(2d) = 2(d(2c + 1))$, which is even; and $a + b = 2c + 1 + 2d = 2(c + d) + 1$, which is odd. Thus it is not the case that both ab and $a + b$ are even.

Case 3. Suppose a is odd and b is odd. Then there are integers c and d for which $a = 2c + 1$ and $b = 2d + 1$. Then $ab = (2c + 1)(2d + 1) = 4cd + 2c + 2d + 1 = 2(2cd + c + d) + 1$, which is odd; and $a + b = 2c + 1 + 2d + 1 = 2(c + d + 1)$, which is even. Thus it is not the case that both ab and $a + b$ are even.

These cases show that it is not the case that ab and $a + b$ are both even. (Note that unlike Exercise 3 above, we really did need all three cases here, for each case involved specific parities for **both** a and b .) ■

9. Proposition Suppose $n \in \mathbb{Z}$. If $3 \nmid n^2$, then $3 \nmid n$.

Proof. (Contrapositive) Suppose it is not the case that $3 \nmid n$, so $3 \mid n$. This means that $n = 3a$ for some integer a . Consequently $n^2 = 9a^2$, from which we get $n^2 = 3(3a^2)$. This shows that there is an integer $b = 3a^2$ for which $n^2 = 3b$, which means $3 \mid n^2$. Therefore it is not the case that $3 \nmid n^2$. ■

11. Proposition Suppose $x, y \in \mathbb{Z}$. If $x^2(y+3)$ is even, then x is even or y is odd.

Proof. (Contrapositive) Suppose it is not the case that x is even or y is odd. Using DeMorgan's law, this means x is not even and y is not odd, which is to say x is odd and y is even. Thus there are integers a and b for which $x = 2a + 1$ and $y = 2b$. Consequently $x^2(y+3) = (2a+1)^2(2b+3) = (4a^2+4a+1)(2b+3) = 8a^2b+8ab+2b+12a^2+12a+3 = 8a^2b+8ab+2b+12a^2+12a+2+1 = 2(4a^2b+4ab+b+6a^2+6a+1)+1$. This shows $x^2(y+3) = 2c+1$ for $c = 4a^2b+4ab+b+6a^2+6a+1 \in \mathbb{Z}$. Consequently, $x^2(y+3)$ is not even. ■

13. Proposition Suppose $x \in \mathbb{R}$. If $x^5 + 7x^3 + 5x \geq x^4 + x^2 + 8$, then $x \geq 0$.

Proof. (Contrapositive) Suppose it is not true that $x \geq 0$. Then $x < 0$, that is x is negative. Consequently, the expressions x^5 , $7x^3$ and $5x$ are all negative (note the odd powers) so $x^5 + 7x^3 + 5x < 0$. Similarly the terms x^4 , x^2 , and 8 are all positive (note the even powers), so $0 < x^4 + x^2 + 8$. From this we get $x^5 + 7x^3 + 5x < x^4 + x^2 + 8$, so it is not true that $x^5 + 7x^3 + 5x \geq x^4 + x^2 + 8$. ■

15. Proposition Suppose $x \in \mathbb{Z}$. If $x^3 - 1$ is even, then x is odd.

Proof. (Contrapositive) Suppose x is not odd. Thus x is even, so $x = 2a$ for some integer a . Then $x^3 - 1 = (2a)^3 - 1 = 8a^3 - 1 = 8a^3 - 2 + 1 = 2(4a^3 - 1) + 1$. Therefore $x^3 - 1 = 2b + 1$ where $b = 4a^3 - 1 \in \mathbb{Z}$, so $x^3 - 1$ is odd. Thus $x^3 - 1$ is not even. ■

17. Proposition If n is odd, then $8 \mid (n^2 - 1)$.

Proof. (Direct) Suppose n is odd, so $n = 2a + 1$ for some integer a . Then $n^2 - 1 = (2a+1)^2 - 1 = 4a^2 + 4a = 4(a^2 + a) = 4a(a+1)$. So far we have $n^2 - 1 = 4a(a+1)$, but we want a factor of 8, not 4. But notice that one of a or $a+1$ must be even, so $a(a+1)$ is even and hence $a(a+1) = 2c$ for some integer c . Now we have $n^2 - 1 = 4a(a+1) = 4(2c) = 8c$. But $n^2 - 1 = 8c$ means $8 \mid (n^2 - 1)$. ■

19. Proposition Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. If $a \equiv b \pmod{n}$ and $a \equiv c \pmod{n}$, then $c \equiv b \pmod{n}$.

Proof. (Direct) Suppose $a \equiv b \pmod{n}$ and $a \equiv c \pmod{n}$.

This means $n \mid (a - b)$ and $n \mid (a - c)$.

Thus there are integers d and e for which $a - b = nd$ and $a - c = ne$.

Subtracting the second equation from the first gives $c - b = nd - ne$.

Thus $c - b = n(d - e)$, so $n \mid (c - b)$ by definition of divisibility.

Therefore $c \equiv b \pmod{n}$ by definition of congruence modulo n . ■

21. Proposition Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. If $a \equiv b \pmod{n}$, then $a^3 \equiv b^3 \pmod{n}$.

Proof. (Direct) Suppose $a \equiv b \pmod{n}$. This means $n \mid (a - b)$, so there is an integer c for which $a - b = nc$. Then:

$$\begin{aligned} a - b &= nc \\ (a - b)(a^2 + ab + b^2) &= nc(a^2 + ab + b^2) \\ a^3 + a^2b + ab^2 - ba^2 - ab^2 - b^3 &= nc(a^2 + ab + b^2) \\ a^3 - b^3 &= nc(a^2 + ab + b^2). \end{aligned}$$

Since $a^2 + ab + b^2 \in \mathbb{Z}$, the equation $a^3 - b^3 = nc(a^2 + ab + b^2)$ implies $n \mid (a^3 - b^3)$, and therefore $a^3 \equiv b^3 \pmod{n}$. ■

23. Proposition Let $a, b, c \in \mathbb{Z}$ and $n \in \mathbb{N}$. If $a \equiv b \pmod{n}$, then $ca \equiv cb \pmod{n}$.

Proof. (Direct) Suppose $a \equiv b \pmod{n}$. This means $n \mid (a - b)$, so there is an integer d for which $a - b = nd$. Multiply both sides of this by c to get $ac - bc = ndc$. Consequently, there is an integer $e = dc$ for which $ac - bc = ne$, so $n \mid (ac - bc)$ and consequently $ac \equiv bc \pmod{n}$. ■

25. If $n \in \mathbb{N}$ and $2^n - 1$ is prime, then n is prime.

Proof. Assume n is not prime. Write $n = ab$ for some $a, b > 1$. Then $2^n - 1 = 2^{ab} - 1 = (2^b - 1)(2^{ab-b} + 2^{ab-2b} + 2^{ab-3b} + \dots + 2^{ab-ab})$. Hence $2^n - 1$ is composite. ■

27. If $a \equiv 0 \pmod{4}$ or $a \equiv 1 \pmod{4}$ then $\binom{a}{2}$ is even.

Proof. We prove this directly. Assume $a \equiv 0 \pmod{4}$. Then $\binom{a}{2} = \frac{a(a-1)}{2}$. Since $a = 4k$ for some $k \in \mathbb{N}$, we have $\binom{a}{2} = \frac{4k(4k-1)}{2} = 2k(4k-1)$. Hence $\binom{a}{2}$ is even.

Now assume $a \equiv 1 \pmod{4}$. Then $a = 4k + 1$ for some $k \in \mathbb{N}$. Hence $\binom{a}{2} = \frac{(4k+1)(4k)}{2} = 2k(4k+1)$. Hence, $\binom{a}{2}$ is even. This proves the result. ■

29. Write a recursive procedure to compute $\text{gcd}(a, b)$.

The following procedure is a recursive version of the Euclidean algorithm.

Procedure Euclidean(a, b)

```

begin
  if  $a < b$  then
     $c := a$ 
     $a := b$ 
     $b := c$ 
  end
  if  $a = 0$  then
    return  $b$ 
  else
    return Euclidean( $a - b, b$ )
  end
end

```

- 31.** Suppose the division algorithm applied to a and b yields $a = qb + r$. Then $\gcd(a, b) = \gcd(r, b)$.

Proof. Suppose $a = qb + r$. Let $d = \gcd(a, b)$, so d is a common divisor of a and b ; thus $a = dx$ and $b = dy$ for some integers x and y . Then $dx = a = qb + r = qdy + r$, hence $dx = qdy + r$, and so $r = dx - qdy = d(x - qy)$. Thus d is a divisor of r (and also of b), so $\gcd(a, b) = d \leq \gcd(r, b)$.

On the other hand, let $e = \gcd(r, b)$, so $r = ex$ and $b = ey$ for some integers x and y . Then $a = qb + r = qey + ex = e(qy + x)$. Hence e is a divisor of a (and of course also of b) so $\gcd(r, b) = e \leq \gcd(a, b)$.

We've now shown $\gcd(a, b) \leq \gcd(r, b)$ and $\gcd(r, b) \leq \gcd(a, b)$, so $\gcd(r, b) = \gcd(a, b)$. ■

Proof by Contradiction

We now explore a third method of proof: **proof by contradiction**. This method is not limited to proving just conditional statements—it can be used to prove any kind of statement whatsoever. The basic idea is to assume that the statement we want to prove is *false*, and then show that this assumption leads to nonsense. We are then led to conclude that we were wrong to assume the statement was false, so the statement must be true. As an example, consider the following proposition and its proof.

Proposition If $a, b \in \mathbb{Z}$, then $a^2 - 4b \neq 2$.

Proof. Suppose this proposition is *false*.

This conditional statement being false means there exist numbers a and b for which $a, b \in \mathbb{Z}$ is true, but $a^2 - 4b \neq 2$ is false.

In other words, there exist integers $a, b \in \mathbb{Z}$ for which $a^2 - 4b = 2$.

From this equation we get $a^2 = 4b + 2 = 2(2b + 1)$, so a^2 is even.

Because a^2 is even, it follows that a is even, so $a = 2c$ for some integer c .

Now plug $a = 2c$ back into the boxed equation to get $(2c)^2 - 4b = 2$, so $4c^2 - 4b = 2$. Dividing by 2, we get $2c^2 - 2b = 1$.

Therefore $1 = 2(c^2 - b)$, and because $c^2 - b \in \mathbb{Z}$, it follows that 1 is even.

We know 1 is **not** even, so something went wrong.

But all the logic after the first line of the proof is correct, so it must be that the first line was incorrect. In other words, we were wrong to assume the proposition was false. Thus the proposition is true. ■

You may be a bit suspicious of this line of reasoning, but in the next section we will see that it is logically sound. For now, notice that at the end of the proof we deduced that 1 is even, which conflicts with our knowledge that 1 is odd. In essence, we have obtained the statement $(1 \text{ is odd}) \wedge \sim(1 \text{ is odd})$, which has the form $C \wedge \sim C$. Notice that no matter what statement C is, and whether or not it is true, the statement $C \wedge \sim C$ is false. A statement—like this one—that cannot be true is called a **contradiction**. Contradictions play a key role in our new technique.

10.1 Proving Statements with Contradiction

Let's now see why the proof on the previous page is logically valid. In that proof we needed to show that a statement $P : (a, b \in \mathbb{Z}) \Rightarrow (a^2 - 4b \neq 2)$ was true. The proof began with the assumption that P was false, that is that $\sim P$ was true, and from this we deduced $C \wedge \sim C$. In other words we proved that $\sim P$ being true forces $C \wedge \sim C$ to be true, and this means that we proved that the *conditional* statement $(\sim P) \Rightarrow (C \wedge \sim C)$ is true. To see that this is the same as proving P is true, look at the following truth table for $(\sim P) \Rightarrow (C \wedge \sim C)$. Notice that the columns for P and $(\sim P) \Rightarrow (C \wedge \sim C)$ are exactly the same, so P is logically equivalent to $(\sim P) \Rightarrow (C \wedge \sim C)$.

| P | C | $\sim P$ | $C \wedge \sim C$ | $(\sim P) \Rightarrow (C \wedge \sim C)$ |
|----------|----------|----------|-------------------|--|
| T | T | F | F | T |
| T | F | F | F | T |
| F | T | T | F | F |
| F | F | T | F | F |

Therefore to prove a statement P , it suffices to instead prove the conditional statement $(\sim P) \Rightarrow (C \wedge \sim C)$. This can be done with direct proof: Assume $\sim P$ and deduce $C \wedge \sim C$. Here is the outline:

Outline for Proof by Contradiction

Proposition P .

Proof. Suppose $\sim P$.

⋮

Therefore $C \wedge \sim C$. ■

One slightly unsettling feature of this method is that we may not know at the beginning of the proof what the statement C is going to be. In doing the scratch work for the proof, you assume that $\sim P$ is true, then deduce new statements until you have deduced some statement C *and* its negation $\sim C$.

If this method seems confusing, look at it this way. In the first line of the proof we suppose $\sim P$ is true, that is we assume P is *false*. But if P is really true then this contradicts our assumption that P is false. But we haven't yet *proved* P to be true, so the contradiction is not obvious. We use logic and reasoning to transform the non-obvious contradiction $\sim P$ to an obvious contradiction $C \wedge \sim C$.

The idea of proof by contradiction is ancient, going back at least as far as the Pythagoreans, who used it to prove that certain numbers are irrational.

Our next example follows their logic to prove that $\sqrt{2}$ is irrational. Recall that a number is *rational* if it equals a fraction of two integers, and it is *irrational* if it cannot be expressed this way. Here is the exact definition.

Definition 10.1 A real number x is **rational** if $x = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$. Also, x is **irrational** if it is not rational, that is if $x \neq \frac{a}{b}$ for every $a, b \in \mathbb{Z}$.

We are now ready to use contradiction to prove that $\sqrt{2}$ is irrational. According to the outline, the first line of the proof should be “Suppose that it is not true that $\sqrt{2}$ is irrational.” But it is helpful (though not mandatory) to tip our reader off to the fact that we are using proof by contradiction. One standard way of doing this is to make the first line “*Suppose for the sake of contradiction that it is not true that $\sqrt{2}$ is irrational.*”

Proposition The number $\sqrt{2}$ is irrational.

Proof. Suppose for the sake of contradiction that it is not true that $\sqrt{2}$ is irrational. Then $\sqrt{2}$ is rational, so there are integers a and b for which

$$\sqrt{2} = \frac{a}{b}. \tag{10.1}$$

Let this fraction be fully reduced; in particular, this means that a and b are not both even. (If they were both even, the fraction could be further reduced by factoring 2's from the numerator and denominator and canceling.) Squaring both sides of Equation 10.1 gives $2 = \frac{a^2}{b^2}$, and therefore

$$a^2 = 2b^2. \tag{10.2}$$

From this it follows that a^2 is even. But we proved earlier (Exercise 1 on page 253) that a^2 being even implies a is even. Thus, as we know that a and b are not both even, it follows that b is **odd**. Now, since a is even there is an integer c for which $a = 2c$. Plugging this value for a into Equation (10.2), we get $(2c)^2 = 2b^2$, so $4c^2 = 2b^2$, and hence $b^2 = 2c^2$. This means b^2 is even, so b is even also. But previously we deduced that b is odd. Thus we have the contradiction b is even **and** b is odd. ■

To appreciate the power of proof by contradiction, imagine trying to prove $\sqrt{2}$ is irrational without it. Where would we begin? What would be our initial assumption? There are no clear answers. Proof by contradiction gives a starting point: Assume $\sqrt{2}$ is rational, and work from there.

In the above proof we got the contradiction $(b \text{ is even}) \wedge \sim(b \text{ is even})$ which has the form $C \wedge \sim C$. In general, your contradiction need not necessarily be

of this form. Any statement that is clearly false is sufficient. For example $2 \neq 2$ would be a fine contradiction, as would be $4 \mid 2$, provided that you could deduce them.

Here is another ancient example, dating back at least as far as Euclid:

Proposition There are infinitely many prime numbers.

Proof. For the sake of contradiction, suppose there are only finitely many prime numbers. Then we can list all the prime numbers as $p_1, p_2, p_3, \dots, p_n$, where $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7$ and so on. Thus p_n is the n th and largest prime number. Now consider the number $a = (p_1 p_2 p_3 \cdots p_n) + 1$, that is, a is the product of all prime numbers, plus 1. Now a , like any natural number greater than 1, has at least one prime divisor, and that means $p_k \mid a$ for at least one of our n prime numbers p_k . Thus there is an integer c for which $a = c p_k$, which is to say

$$(p_1 p_2 p_3 \cdots p_{k-1} p_{k+1} \cdots p_n) + 1 = c p_k.$$

Dividing both sides of this by p_k gives us

$$(p_1 p_2 p_3 \cdots p_{k-1} p_{k+1} \cdots p_n) + \frac{1}{p_k} = c,$$

so

$$\frac{1}{p_k} = c - (p_1 p_2 p_3 \cdots p_{k-1} p_{k+1} \cdots p_n).$$

The expression on the right is an integer, while the expression on the left is not an integer. This is a contradiction. ■

Proof by contradiction often works well in proving statements of the form $\forall x, P(x)$. The reason is that the proof set-up involves assuming $\sim \forall x, P(x)$, which as we know from Section 7.4 is equivalent to $\exists x, \sim P(x)$. This gives us a specific x for which $\sim P(x)$ is true, and often that is enough to produce a contradiction.

This happened in the proof that $\sqrt{2}$ is irrational on page 261. The statement “ $\sqrt{2}$ is irrational” is logically equivalent to $\forall a, b \in \mathbb{Z}, 2 \neq \left(\frac{a}{b}\right)^2$. Proof by contradiction involved assuming this was false, that is, we assumed $\sim \left(\forall a, b \in \mathbb{Z}, 2 \neq \left(\frac{a}{b}\right)^2\right)$, which became $\exists a, b \in \mathbb{Z}, 2 = \left(\frac{a}{b}\right)^2$. This gave a concrete equation $2 = \left(\frac{a}{b}\right)^2$ to work with, and that was what led to the contradiction.

Let's look at another example another example of form $\forall x, P(x)$.

Proposition For every real number $x \in [0, \pi/2]$, we have $\sin x + \cos x \geq 1$.

Proof. Suppose for the sake of contradiction that this is not true.

Then there exists an $x \in [0, \pi/2]$ for which $\sin x + \cos x < 1$.

Since $x \in [0, \pi/2]$, neither $\sin x$ nor $\cos x$ is negative, so $0 \leq \sin x + \cos x < 1$.

Thus $0^2 \leq (\sin x + \cos x)^2 < 1^2$, which gives $0^2 \leq \sin^2 x + 2 \sin x \cos x + \cos^2 x < 1^2$.

As $\sin^2 x + \cos^2 x = 1$, this becomes $0 \leq 1 + 2 \sin x \cos x < 1$, so $1 + 2 \sin x \cos x < 1$.

Subtracting 1 from both sides gives $2 \sin x \cos x < 0$.

But this contradicts the fact that neither $\sin x$ nor $\cos x$ is negative. ■

10.2 Proving Conditional Statements by Contradiction

As the previous two chapters dealt with proving conditional statements, we now formalize the method for proving conditional statements with contradiction. Suppose we want to prove a proposition of this form:

Proposition If P , then Q .

Thus we need to prove that $P \Rightarrow Q$ is a true statement. Proof by contradiction begins with the assumption that $\sim(P \Rightarrow Q)$ is true, that is, that $P \Rightarrow Q$ is false. But we know that $P \Rightarrow Q$ being false means that it is possible that P can be true while Q is false. Thus the first step in the proof is to assume P and $\sim Q$. Here is an outline:

Outline for Proving a Conditional Statement with Contradiction

Proposition If P , then Q .

Proof. Suppose P and $\sim Q$.

⋮

Therefore $C \wedge \sim C$. ■

To illustrate this new technique, we revisit a familiar result: If a^2 is even, then a is even. According to the outline, the first line of the proof should be “For the sake of contradiction, suppose a^2 is even and a is not even.”

Proposition Suppose $a \in \mathbb{Z}$. If a^2 is even, then a is even.

Proof. For the sake of contradiction, suppose a^2 is even and a is not even. Then a^2 is even, and a is odd.

Since a is odd, there is an integer c for which $a = 2c + 1$.

Then $a^2 = (2c + 1)^2 = 4c^2 + 4c + 1 = 2(2c^2 + 2c) + 1$, so a^2 is odd.

Thus a^2 is even and a^2 is not even, a contradiction. ■

Here is another example.

Proposition If $a, b \in \mathbb{Z}$ and $a \geq 2$, then $a \nmid b$ or $a \nmid (b + 1)$.

Proof. Suppose for the sake of contradiction there exist $a, b \in \mathbb{Z}$ with $a \geq 2$, and for which it is not true that $a \nmid b$ or $a \nmid (b + 1)$.

By DeMorgan's law, we have $a \mid b$ and $a \mid (b + 1)$.

The definition of divisibility says there are $c, d \in \mathbb{Z}$ with $b = ac$ and $b + 1 = ad$.

Subtracting one equation from the other gives $ad - ac = 1$, so $a(d - c) = 1$.

Since a is positive, $d - c$ is also positive (otherwise $a(d - c)$ would be negative).

Then $d - c$ is a positive integer and $a(d - c) = 1$, so $a = 1/(d - c) < 2$.

Thus we have $a \geq 2$ and $a < 2$, a contradiction. ■

10.3 Combining Techniques

Often, especially in more complex proofs, several proof techniques are combined within a single proof. For example, in proving a conditional statement $P \Rightarrow Q$, we might begin with direct proof and thus assume P to be true with the aim of ultimately showing Q is true. But the truth of Q might hinge on the truth of some other statement R which—together with P —would imply Q . We would then need to prove R , and we would use whichever proof technique seems most appropriate. This can lead to “proofs inside of proofs.” Consider the following example. The overall approach is direct, but inside the direct proof is a separate proof by contradiction.

Proposition Every non-zero rational number can be expressed as a product of two irrational numbers.

Proof. This proposition can be reworded as follows: If r is a non-zero rational number, then r is a product of two irrational numbers. In what follows, we prove this with direct proof.

Suppose r is a non-zero rational number. Then $r = \frac{a}{b}$ for integers a and b . Also, r can be written as a product of two numbers as follows:

$$r = \sqrt{2} \cdot \frac{r}{\sqrt{2}}.$$

We know $\sqrt{2}$ is irrational, so to complete the proof we must show $r/\sqrt{2}$ is also irrational. To show this, assume for the sake of contradiction that $r/\sqrt{2}$ is rational. This means

$$\frac{r}{\sqrt{2}} = \frac{c}{d}$$

for integers c and d , so

$$\sqrt{2} = r \frac{d}{c}.$$

But we know $r = a/b$, which combines with the above equation to give

$$\sqrt{2} = r \frac{d}{c} = \frac{a}{b} \frac{d}{c} = \frac{ad}{bc}.$$

This means $\sqrt{2}$ is rational, which is a contradiction because we know it is irrational. Therefore $r/\sqrt{2}$ is irrational.

Consequently $r = \sqrt{2} \cdot r/\sqrt{2}$ is a product of two irrational numbers. ■

For another example of a proof-within-a-proof, try Exercise 5 at the end of this chapter (or see its solution). Exercise 5 asks you to prove that $\sqrt{3}$ is irrational. This turns out to be slightly trickier than proving that $\sqrt{2}$ is irrational.

Despite the power of proof by contradiction, it's best to use it only when the direct and contrapositive approaches do not seem to work. The reason for this is that a proof by contradiction can often have hidden in it a simpler contrapositive proof, and if this is the case it's better to go with the simpler approach. Consider the following example.

Proposition Suppose $a \in \mathbb{Z}$. If $a^2 - 2a + 7$ is even, then a is odd.

Proof. To the contrary, suppose $a^2 - 2a + 7$ is even and a is not odd.

That is, suppose $a^2 - 2a + 7$ is even and a is even.

Since a is even, there is an integer c for which $a = 2c$.

Then $a^2 - 2a + 7 = (2c)^2 - 2(2c) + 7 = 2(2c^2 - 2c + 3) + 1$, so $a^2 - 2a + 7$ is odd.

Thus $a^2 - 2a + 7$ is both even and odd, a contradiction. ■

Though there is nothing really wrong with this proof, notice that part of it assumes a is not odd and deduces that $a^2 - 2a + 7$ is not even. That is the contrapositive approach! Thus it would be more efficient to proceed as follows, using contrapositive proof.

Proposition Suppose $a \in \mathbb{Z}$. If $a^2 - 2a + 7$ is even, then a is odd.

Proof. (Contrapositive) Suppose a is not odd.

Then a is even, so there is an integer c for which $a = 2c$.

Then $a^2 - 2a + 7 = (2c)^2 - 2(2c) + 7 = 2(2c^2 - 2c + 3) + 1$, so $a^2 - 2a + 7$ is odd.

Thus $a^2 - 2a + 7$ is not even. ■

10.4 Case Study: The Halting Problem

The ancient greeks used contradiction to prove that $\sqrt{2}$ is not a fraction of two whole numbers, or (as we would say today) it is irrational. This came as a shocking and unsettling truth. Prior to this they had no reason to even imagine that a number could be anything other than rational.

Millennia later, contradiction again rocked mathematics. Before 1930, mathematicians were of the mindset that any *true* mathematical statement could be *proved*. They also believed—roughly speaking—that any problem in discrete mathematics could be solved with an algorithm. Then Alan Turing proved that there are problems that no algorithm can solve. We now examine such a problem, and use contradiction to prove it is really insolvable.

Imagine a computer program (or algorithm) called `LoopCheck`. Its purpose is to decide whether any program would go into an infinite loop if run. Think of `LoopCheck` as being similar to a spell check program that reads in a document and finds the spelling errors. `LoopCheck` would read in a computer program and find “infinite loop” errors.

Turing discovered that it is absolutely impossible to write `LoopCheck`. No such algorithm can possibly exist. The problem of writing one is simply unsolvable. In computer science this is known as the **halting problem**, as a `LoopCheck` program would decide whether or not any program *halts*.

Before proving that `LoopCheck` is impossible, let’s pause to lay out its exact specifications, so we’ll know what we’re dealing with. Note that if we run a program on some input, one of two things will happen: either it gets hung up in an infinite loop, or it eventually halts. There may be several reasons for halting. Maybe it finishes its appointed task and returns some output. Or maybe it stops because of some internal error like division by zero, or some other meaningless operation. Maybe the input simply makes no sense for the program. When a program halts under such circumstances it may return garbage for output, but it *still halts*.

`LoopCheck` does not make any evaluation about whether or not a program’s output is garbage. Its purpose is only to decide whether or not a program goes into an infinite loop when run on certain input.

Think of it as a procedure `LoopCheck(prog, input)` that reads in a program `prog` and some input `input` for `prog`. Let `prog(input)` mean that `prog` is run with input `input`. Then `LoopCheck(prog, input)` simply returns the words “GOOD” or “BAD,” as follows.

$$\text{LoopCheck}(\text{prog}, \text{input}) = \begin{cases} \text{GOOD} & \text{if } \text{prog}(\text{input}) \text{ halts,} \\ \text{BAD} & \text{if } \text{prog}(\text{input}) \text{ loops infinitely.} \end{cases}$$

We're ready for Turing's famous proof that `LoopCheck` is impossible. In the proof you will see the expression `LoopCheck (prog, prog)`, which means `LoopCheck` is asked to decide whether or not a program `prog` halts with itself as input. Keep in mind that lots of programs can use themselves as input. Consider a program that counts the number of characters in a file. You could certainly run it on itself (or at least a copy of itself) and the output would be the number of characters in the program. Granted, most programs would come to a crashing halt if they read in themselves as input. And if they didn't halt, they'd run forever (i.e., they'd be stuck in an infinite loop).

Theorem 10.1 The program `LoopCheck` is impossible to write. (That is, the halting problem cannot be solved.)

Proof. For sake of contradiction, suppose that `LoopCheck` *can* be written, and it has been implemented. Now make the following procedure called `Test` that reads in a program `prog` as input.

| | |
|--|----------------------------------|
| Procedure <code>Test(prog)</code> | <i>(input prog is a program)</i> |
|--|----------------------------------|

```

1 begin
2   if LoopCheck (prog, prog) = GOOD then
3     i := 1
4     while (i > 0) do
5       i := i + 1 ..... this is an infinite loop
6     end
7   else
8     if LoopCheck (prog, prog) = BAD then
9       return UGLY ..... i.e., return the word "UGLY" and halt
10    end
11  end
12 end

```

We will get a contradiction by running `Test (Test)`. In other words, we will run the above procedure `Test` with the input `prog` replaced by `Test`.

Let's run `Test (Test)`. If in line 2, `LoopCheck (Test, Test) = GOOD`, then the while loop runs forever. Thus `Test (Test)` does not halt. But `LoopCheck (Test, Test) = GOOD` means that `Test (Test)` halts.

On the other hand, if `LoopCheck (Test, Test) = BAD`, then we see that `Test (Test)` halts at line 9 (and returns the word "UGLY"). But the fact `LoopCheck (Test, Test) = BAD` means `Test (Test)` does not halt.

Either way, `Test (Test)` halts and does not halt, a contradiction. ■

The fact that `LoopCheck` is impossible has some significant theoretical implications. For one, it means that certain strategies for proving theorems are hopeless. For example, consider Fermat's last theorem, from page 54:

For all numbers $a, b, c, n \in \mathbb{N}$ with $n > 2$, it is the case that $a^n + b^n \neq c^n$.

It would be easy to write an algorithm with nested while loops that runs through all possible combinations of a, b, c and n , and stops only when and if $a^n + b^n = c^n$. This algorithm reads in no input (that is, its input is \emptyset), but it either halts or loops forever. Moreover, this algorithm (call it `Fermat`) halts if Fermat's last theorem is false, and it loops forever if Fermat's last theorem is true. If `LoopCheck` were possible, and if it were written, we could prove or disprove Fermat's last theorem by running

`LoopCheck(Fermat, \emptyset).`

If it returned "GOOD," then Fermat's last theorem would be false. If it returned "BAD," then Fermat's last theorem would be true. The fact that `LoopCheck` is impossible means that we can't hope to prove Fermat's last theorem (or any other theorem) this way.

Our discussion of the halting problem has been somewhat informal. Most careful treatments of it use mathematical constructions called *Turing machines*, which are theoretical versions of computers. If this kind of thing piques your interest, you should definitely consider taking a computer science class in the theory of computation. You will need a command of all proof techniques covered in this book, including contradiction.

Exercises for Chapter 10

- A.** Use the method of proof by contradiction to prove the following statements. (In each case, you should also think about how a direct or contrapositive proof would work. You will find in most cases that proof by contradiction is easier.)
1. Suppose $n \in \mathbb{Z}$. If n is odd, then n^2 is odd.
 2. Suppose $n \in \mathbb{Z}$. If n^2 is odd, then n is odd.
 3. Prove that $\sqrt[3]{2}$ is irrational.
 4. Prove that $\sqrt{6}$ is irrational.
 5. Prove that $\sqrt{3}$ is irrational.
 6. If $a, b \in \mathbb{Z}$, then $a^2 - 4b - 2 \neq 0$.
 7. If $a, b \in \mathbb{Z}$, then $a^2 - 4b - 3 \neq 0$.
 8. Suppose $a, b, c \in \mathbb{Z}$. If $a^2 + b^2 = c^2$, then a or b is even.
 9. Suppose $a, b \in \mathbb{R}$. If a is rational and ab is irrational, then b is irrational.

10. There exist no integers a and b for which $21a + 30b = 1$.
11. There exist no integers a and b for which $18a + 6b = 1$.
12. For every positive $x \in \mathbb{Q}$, there is a positive $y \in \mathbb{Q}$ for which $y < x$.
13. For every $x \in [\pi/2, \pi]$, $\sin x - \cos x \geq 1$.
14. If A and B are sets, then $A \cap (B - A) = \emptyset$.
15. If $b \in \mathbb{Z}$ and $b \nmid k$ for every $k \in \mathbb{N}$, then $b = 0$.
16. If a and b are positive real numbers, then $a + b \geq 2\sqrt{ab}$.
17. For every $n \in \mathbb{Z}$, $4 \nmid (n^2 + 2)$.
18. Suppose $a, b \in \mathbb{Z}$. If $4 \mid (a^2 + b^2)$, then a and b are not both odd.

B. Prove the following statements using any method from Chapters 8, 9 or 10.

19. The product of any five consecutive integers is divisible by 120. (For example, the product of 3,4,5,6 and 7 is 2520, and $2520 = 120 \cdot 21$.)
20. We say that a point $P = (x, y)$ in \mathbb{R}^2 is **rational** if both x and y are rational. More precisely, P is rational if $P = (x, y) \in \mathbb{Q}^2$. An equation $F(x, y) = 0$ is said to have a **rational point** if there exists $x_0, y_0 \in \mathbb{Q}$ such that $F(x_0, y_0) = 0$. For example, the curve $x^2 + y^2 - 1 = 0$ has rational point $(x_0, y_0) = (1, 0)$. Show that the curve $x^2 + y^2 - 3 = 0$ has no rational points.
21. Exercise 20 (above) involved showing that there are no rational points on the curve $x^2 + y^2 - 3 = 0$. Use this fact to show that $\sqrt{3}$ is irrational.
22. Explain why $x^2 + y^2 - 3 = 0$ not having any rational solutions (Exercise 20) implies $x^2 + y^2 - 3^k = 0$ has no rational solutions for k an odd, positive integer.
23. Use the above result to prove that $\sqrt{3^k}$ is irrational for all odd, positive k .
24. The number $\log_2 3$ is irrational.

10.5 Solutions for Chapter 10

1. Suppose n is an integer. If n is odd, then n^2 is odd.

Proof. Suppose for the sake of contradiction that n is odd and n^2 is not odd. Then n^2 is even. Now, since n is odd, we have $n = 2a + 1$ for some integer a . Thus $n^2 = (2a + 1)^2 = 4a^2 + 4a + 1 = 2(2a^2 + 2a) + 1$. This shows $n^2 = 2b + 1$, where b is the integer $b = 2a^2 + 2a$. Therefore we have n^2 is odd and n^2 is even, a contradiction. ■

3. Prove that $\sqrt[3]{2}$ is irrational.

Proof. Suppose for the sake of contradiction that $\sqrt[3]{2}$ is not irrational. Therefore it is rational, so there exist integers a and b for which $\sqrt[3]{2} = \frac{a}{b}$. Let us assume that this fraction is reduced, so a and b are not both even. Now we have $\sqrt[3]{2^3} = \left(\frac{a}{b}\right)^3$, which gives $2 = \frac{a^3}{b^3}$, or $2b^3 = a^3$. From this we see that a^3 is even, from which we deduce that a is even. (For if a were odd, then $a^3 = (2c + 1)^3 = 8c^3 + 12c^2 + 6c + 1 = 2(4c^3 + 6c^2 + 3c) + 1$ would be odd, not even.) Since a is even, it follows that $a = 2d$ for some integer d . The equation $2b^3 = a^3$ from above then becomes $2b^3 = (2d)^3$, or $2b^3 = 8d^3$. Dividing by 2, we get $b^3 = 4d^3$, and it follows that b^3 is even. Thus b is even also. (Using the same argument we used when a^3 was even.) At this point we have discovered that both a and b are even, contradicting the fact (observed above) that the a and b are not both even. ■

Here is an alternative proof.

Proof. Suppose for the sake of contradiction that $\sqrt[3]{2}$ is not irrational. Therefore there exist integers a and b for which $\sqrt[3]{2} = \frac{a}{b}$. Cubing both sides, we get $2 = \frac{a^3}{b^3}$. From this, $a^3 = b^3 + b^3$, which contradicts Fermat's last theorem. ■

5. Prove that $\sqrt{3}$ is irrational.

Proof. Suppose for the sake of contradiction that $\sqrt{3}$ is not irrational. Therefore it is rational, so there exist integers a and b for which $\sqrt{3} = \frac{a}{b}$. Let us assume that this fraction is reduced, so a and b have no common factor. Notice that $\sqrt{3^2} = \left(\frac{a}{b}\right)^2$, so $3 = \frac{a^2}{b^2}$, or $3b^2 = a^2$. This means $3 \mid a^2$.

Now we are going to show that if $a \in \mathbb{Z}$ and $3 \mid a^2$, then $3 \mid a$. (This is a proof-within-a-proof.) We will use contrapositive proof to prove this conditional statement. Suppose $3 \nmid a$. Then there is a remainder of either 1 or 2 when 3 is divided into a .

Case 1. There is a remainder of 1 when 3 is divided into a . Then $a = 3m + 1$ for some integer m . Consequently, $a^2 = 9m^2 + 6m + 1 = 3(3m^2 + 2m) + 1$, and this means 3 divides into a^2 with a remainder of 1. Thus $3 \nmid a^2$.

Case 2. There is a remainder of 2 when 3 is divided into a . Then $a = 3m + 2$ for some integer m . Consequently, $a^2 = 9m^2 + 12m + 4 = 9m^2 + 12m + 3 + 1 = 3(3m^2 + 4m + 1) + 1$, and this means 3 divides into a^2 with a remainder of 1. Thus $3 \nmid a^2$.

In either case we have $3 \nmid a^2$, so we've shown $3 \nmid a$ implies $3 \nmid a^2$. Therefore, if $3 \mid a^2$, then $3 \mid a$.

Now go back to $3 \mid a^2$ in the first paragraph. This combined with the result of the second paragraph implies $3 \mid a$, so $a = 3d$ for some integer d . Now also in the first paragraph we had $3b^2 = a^2$, which now becomes $3b^2 = (3d)^2$ or $3b^2 = 9d^2$, so $b^2 = 3d^2$. But this means $3 \mid b^2$, and the second paragraph implies $3 \mid b$. Thus we have concluded that $3 \mid a$ and $3 \mid b$, but this contradicts the fact that the fraction $\frac{a}{b}$ is reduced. ■

7. If $a, b \in \mathbb{Z}$, then $a^2 - 4b - 3 \neq 0$.

Proof. Suppose for the sake of contradiction that $a, b \in \mathbb{Z}$ but $a^2 - 4b - 3 = 0$. Then we have $a^2 = 4b + 3 = 2(2b + 1) + 1$, which means a^2 is odd. Therefore a is odd also, so $a = 2c + 1$ for some integer c . Plugging this back into $a^2 - 4b - 3 = 0$ gives us

$$\begin{aligned}(2c + 1)^2 - 4b - 3 &= 0 \\ 4c^2 + 4c + 1 - 4b - 3 &= 0 \\ 4c^2 + 4c - 4b &= 2 \\ 2c^2 + 2c - 2b &= 1 \\ 2(c^2 + c - b) &= 1.\end{aligned}$$

From this last equation, we see that 1 is an even number, a contradiction. ■

9. Suppose $a, b \in \mathbb{R}$ and $a \neq 0$. If a is rational and ab is irrational, then b is irrational.

Proof. Suppose for the sake of contradiction that a is rational and ab is irrational and b is **not** irrational. Thus we have a and b rational, and ab irrational. Since a and b are rational, we know there are integers c, d, e, f for which $a = \frac{c}{d}$ and $b = \frac{e}{f}$. Then $ab = \frac{ce}{df}$, and since both ce and df are integers, it follows that ab is rational. But this is a contradiction because we started out with ab irrational. ■

11. There exist no integers a and b for which $18a + 6b = 1$.

Proof. Suppose for the sake of contradiction that there do exist integers a and b for which $18a + 6b = 1$. Then $1 = 2(9a + 3b)$, which means 1 is even, a contradiction. ■

13. For every $x \in [\pi/2, \pi]$, $\sin x - \cos x \geq 1$.

Proof. Suppose for the sake of contradiction that $x \in [\pi/2, \pi]$, but $\sin x - \cos x < 1$. Since $x \in [\pi/2, \pi]$, we know $\sin x \geq 0$ and $\cos x \leq 0$, so $\sin x - \cos x \geq 0$. Therefore we have $0 \leq \sin x - \cos x < 1$. Now the square of any number between 0 and 1 is still a number between 0 and 1, so we have $0 \leq (\sin x - \cos x)^2 < 1$, or $0 \leq \sin^2 x - 2\sin x \cos x + \cos^2 x < 1$. Using the fact that $\sin^2 x + \cos^2 x = 1$, this becomes $0 \leq -2\sin x \cos x + 1 < 1$. Subtracting 1, we obtain $-2\sin x \cos x < 0$. But above we remarked that $\sin x \geq 0$ and $\cos x \leq 0$, and hence $-2\sin x \cos x \geq 0$. We now have the contradiction $-2\sin x \cos x < 0$ and $-2\sin x \cos x \geq 0$. ■

15. If $b \in \mathbb{Z}$ and $b \nmid k$ for every $k \in \mathbb{N}$, then $b = 0$.

Proof. Suppose for the sake of contradiction that $b \in \mathbb{Z}$ and $b \nmid k$ for every $k \in \mathbb{N}$, but $b \neq 0$.

Case 1. Suppose $b > 0$. Then $b \in \mathbb{N}$, so $b|b$, contradicting $b \nmid k$ for every $k \in \mathbb{N}$.

Case 2. Suppose $b < 0$. Then $-b \in \mathbb{N}$, so $b|(-b)$, again a contradiction ■

17. For every $n \in \mathbb{Z}$, $4 \nmid (n^2 + 2)$.

Proof. Assume there exists $n \in \mathbb{Z}$ with $4 \mid (n^2 + 2)$. Then for some $k \in \mathbb{Z}$, $4k = n^2 + 2$ or $2k = n^2 + 2(1 - k)$. If n is odd, this means $2k$ is odd, and we've reached a contradiction. If n is even then $n = 2j$ and we get $k = 2j^2 + 1 - k$ for some $j \in \mathbb{Z}$. Hence $2(k - j^2) = 1$, so 1 is even, a contradiction. ■

Remark. It is fairly easy to see that two more than a perfect square is always either $2 \pmod{4}$ or $3 \pmod{4}$. This would end the proof immediately.

19. The product of 5 consecutive integers is a multiple of 120.

Proof. Starting from 0, every fifth integer is a multiple of 5, every fourth integer is a multiple of 4, every third integer is a multiple of 3, and every other integer is a multiple of 2. It follows that any set of 5 consecutive integers must contain a multiple of 5, a multiple of 4, at least one multiple of 3, and at least two multiples of 2 (possibly one of which is a multiple of 4). It follows that the product of five consecutive integers is a multiple of $5 \cdot 4 \cdot 3 \cdot 2 = 120$. ■

21. Hints for Exercises 20–23. For Exercises 20, first show that the equation $a^2 + b^2 = 3c^2$ has no solutions (other than the trivial solution $(a, b, c) = (0, 0, 0)$) in the integers. To do this, investigate the remainders of a sum of squares $\pmod{4}$. After you've done this, prove that the only solution is indeed the trivial solution. Next assume that the equation $x^2 + y^2 - 3 = 0$ has a rational solution. Use the definition of rational numbers to yield a contradiction.

Proofs Involving Sets

Students in their first advanced mathematics or computer science courses are often surprised by the extensive role that sets play and by the fact that most of the proofs they encounter are proofs about sets. Perhaps you've already seen such proofs in your linear algebra course, where a **vector space** was defined to be a *set* of objects (called vectors) that obey certain properties. Your text proved many things about vector spaces, such as the fact that the intersection of two vector spaces is also a vector space, and the proofs used ideas from set theory. As you go deeper into mathematics, you will encounter more and more ideas, theorems and proofs that involve sets. The purpose of this chapter is to give you a foundation that will prepare you for this new outlook.

We will discuss how to show that an object is an element of a set, how to prove one set is a subset of another and how to prove two sets are equal. As you read this chapter, you may need to occasionally refer back to Chapter 2 to refresh your memory. For your convenience, the main definitions from Chapter 2 are summarized below. If A and B are sets, then:

$$\begin{aligned}A \times B &= \{(x, y) : x \in A, y \in B\}, \\A \cup B &= \{x : (x \in A) \vee (x \in B)\}, \\A \cap B &= \{x : (x \in A) \wedge (x \in B)\}, \\A - B &= \{x : (x \in A) \wedge (x \notin B)\}, \\\overline{A} &= U - A.\end{aligned}$$

Recall that $A \subseteq B$ means that every element of A is also an element of B . Also, the empty set $\emptyset = \{\}$ is the unique set with no elements, and $\emptyset \subseteq B$ for any set B .

11.1 How to Prove $a \in A$

We will begin with a review of set-builder notation, and then review how to show that a given object a is an element of some set A .

Generally, a set A will be expressed in set-builder notation $A = \{x : P(x)\}$, where $P(x)$ is some statement (or open sentence) about x . The set A is understood to have as elements all those things x for which $P(x)$ is true. For example,

$$\{x : x \text{ is an odd integer}\} = \{\dots, -5, -3, -1, 1, 3, 5, \dots\}.$$

A common variation of this notation is to express a set as $A = \{x \in S : P(x)\}$. Here it is understood that A consists of all elements x of the (predetermined) set S for which $P(x)$ is true. Keep in mind that, depending on context, x could be any kind of object (integer, ordered pair, set, function, etc.). There is also nothing special about the particular variable x ; any reasonable symbol x, y, k , etc., would do. Some examples follow.

$$\begin{aligned} \{n \in \mathbb{Z} : n \text{ is odd}\} &= \{\dots, -5, -3, -1, 1, 3, 5, \dots\} \\ \{x \in \mathbb{N} : 6 \mid x\} &= \{6, 12, 18, 24, 30, \dots\} \\ \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : b = a + 5\} &= \{\dots, (-2, 3), (-1, 4), (0, 5), (1, 6), \dots\} \\ \{X \in \mathcal{P}(\mathbb{Z}) : |X| = 1\} &= \{\dots, \{-1\}, \{0\}, \{1\}, \{2\}, \{3\}, \{4\}, \dots\} \end{aligned}$$


Now it should be clear how to prove that an object a belongs to a set $\{x : P(x)\}$. Since $\{x : P(x)\}$ consists of all things x for which $P(x)$ is true, to show that $a \in \{x : P(x)\}$ we just need to show that $P(a)$ is true. Likewise, to show $a \in \{x \in S : P(x)\}$, we need to confirm that $a \in S$ and that $P(a)$ is true. These ideas are summarized below. However, you should **not** memorize these methods, you should **understand** them. With contemplation and practice, using them becomes natural and intuitive.


How to show $a \in \{x : P(x)\}$

Show that $P(a)$ is true.


How to show $a \in \{x \in S : P(x)\}$


1. Verify that $a \in S$.
2. Show that $P(a)$ is true.

Example 11.1 Let's investigate elements of $A = \{x : x \in \mathbb{N} \text{ and } 7 \mid x\}$. This set has form $A = \{x : P(x)\}$ where $P(x)$ is the open sentence $(x \in \mathbb{N}) \wedge (7 \mid x)$. Thus $21 \in A$ because $P(21)$ is true. Similarly, 7, 14, 28, 35, etc., are all elements of A . But $8 \notin A$ (for example) because $P(8)$ is false. Likewise $-14 \notin A$ because $P(-14)$ is false. 

Example 11.2 Consider the set $A = \{X \in \mathcal{P}(\mathbb{N}) : |X| = 3\}$. We know that $\{4, 13, 45\} \in A$ because $\{4, 13, 45\} \in \mathcal{P}(\mathbb{N})$ and $|\{4, 13, 45\}| = 3$. Also $\{1, 2, 3\} \in A$, $\{10, 854, 3\} \in A$, etc. However $\{1, 2, 3, 4\} \notin A$ because $|\{1, 2, 3, 4\}| \neq 3$. Further, $\{-1, 2, 3\} \notin A$ because $\{-1, 2, 3\} \notin \mathcal{P}(\mathbb{N})$. 

Example 11.3 Consider the set $B = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x \equiv y \pmod{5}\}$. Notice $(8, 23) \in B$ because $(8, 23) \in \mathbb{Z} \times \mathbb{Z}$ and $8 \equiv 23 \pmod{5}$. Likewise, $(100, 75) \in B$, $(102, 77) \in B$, etc., but $(6, 10) \notin B$.

Now suppose $n \in \mathbb{Z}$ and consider the ordered pair $(4n + 3, 9n - 2)$. Does this ordered pair belong to B ? To answer this, we first observe that $(4n + 3, 9n - 2) \in \mathbb{Z} \times \mathbb{Z}$. Next, we observe that $(4n + 3) - (9n - 2) = -5n + 5 = 5(1 - n)$, so $5 \mid ((4n + 3) - (9n - 2))$, which means $(4n + 3) \equiv (9n - 2) \pmod{5}$. Therefore we have established that $(4n + 3, 9n - 2)$ meets the requirements for belonging to B , so $(4n + 3, 9n - 2) \in B$ for every $n \in \mathbb{Z}$. 

Example 11.4 This illustrates another common way of defining a set. Consider the set $C = \{3x^3 + 2 : x \in \mathbb{Z}\}$. Elements of this set consist of all the values $3x^3 + 2$ where x is an integer. Thus $-22 \in C$ because $-22 = 3(-2)^3 + 2$. You can confirm $-1 \in C$ and $5 \in C$, etc. Also $0 \notin C$ and $\frac{1}{2} \notin C$, etc. 

11.2 How to Prove $A \subseteq B$

In this course (and more importantly, beyond it) you will encounter many circumstances where it is necessary to prove that one set is a subset of another. This section explains how to do this. The methods we discuss should improve your skills in both writing your own proofs and in comprehending the proofs that you read.

Recall (Definition 2.3) that if A and B are sets, then $A \subseteq B$ means that every element of A is also an element of B . In other words, it means *if $a \in A$, then $a \in B$* . Therefore to prove that $A \subseteq B$, we just need to prove that the conditional statement

“If $a \in A$, then $a \in B$ ”

is true. This can be proved directly, by assuming $a \in A$ and deducing $a \in B$. The contrapositive approach is another option: Assume $a \notin B$ and deduce $a \notin A$. Each of these two approaches is outlined below.

How to Prove $A \subseteq B$ (Direct approach)

Proof. Suppose $a \in A$.
 \vdots
 Therefore $a \in B$.
 Thus $a \in A$ implies $a \in B$,
 so it follows that $A \subseteq B$. ■

How to Prove $A \subseteq B$ (Contrapositive approach)

Proof. Suppose $a \notin B$.
 \vdots
 Therefore $a \notin A$.
 Thus $a \notin B$ implies $a \notin A$,
 so it follows that $A \subseteq B$. ■

In practice, the direct approach usually results in the most straightforward and easy proof, though occasionally the contrapositive is the most expedient. (You can even prove $A \subseteq B$ by contradiction: Assume $(a \in A) \wedge (a \notin B)$, and deduce a contradiction.) The remainder of this section consists of examples with occasional commentary. Unless stated otherwise, we will use the direct approach in all proofs; pay special attention to how the above outline for the direct approach is used.

Example 11.5 Prove that $\{x \in \mathbb{Z} : 18|x\} \subseteq \{x \in \mathbb{Z} : 6|x\}$.

Proof. Suppose $a \in \{x \in \mathbb{Z} : 18|x\}$.

This means that $a \in \mathbb{Z}$ and $18|a$.

By definition of divisibility, there is an integer c for which $a = 18c$.

Consequently $a = 6(3c)$, and from this we deduce that $6|a$.

Therefore a is one of the integers that 6 divides, so $a \in \{x \in \mathbb{Z} : 6|x\}$.

We've shown $a \in \{x \in \mathbb{Z} : 18|x\}$ implies $a \in \{x \in \mathbb{Z} : 6|x\}$, so it follows that $\{x \in \mathbb{Z} : 18|x\} \subseteq \{x \in \mathbb{Z} : 6|x\}$. ■

Example 11.6 Prove that $\{x \in \mathbb{Z} : 2|x\} \cap \{x \in \mathbb{Z} : 9|x\} \subseteq \{x \in \mathbb{Z} : 6|x\}$.

Proof. Suppose $a \in \{x \in \mathbb{Z} : 2|x\} \cap \{x \in \mathbb{Z} : 9|x\}$.

By definition of intersection, this means $a \in \{x \in \mathbb{Z} : 2|x\}$ and $a \in \{x \in \mathbb{Z} : 9|x\}$.

Since $a \in \{x \in \mathbb{Z} : 2|x\}$ we know $2|a$, so $a = 2c$ for some $c \in \mathbb{Z}$. Thus a is even.

Since $a \in \{x \in \mathbb{Z} : 9|x\}$ we know $9|a$, so $a = 9d$ for some $d \in \mathbb{Z}$.

As a is even, $a = 9d$ implies d is even. (Otherwise $a = 9d$ would be odd.)

Then $d = 2e$ for some integer e , and we have $a = 9d = 9(2e) = 6(3e)$.

From $a = 6(3e)$, we conclude $6|a$, and this means $a \in \{x \in \mathbb{Z} : 6|x\}$.

We have shown that $a \in \{x \in \mathbb{Z} : 2|x\} \cap \{x \in \mathbb{Z} : 9|x\}$ implies $a \in \{x \in \mathbb{Z} : 6|x\}$, so it follows that $\{x \in \mathbb{Z} : 2|x\} \cap \{x \in \mathbb{Z} : 9|x\} \subseteq \{x \in \mathbb{Z} : 6|x\}$. ■

Example 11.7 Show $\{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x \equiv y \pmod{6}\} \subseteq \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x \equiv y \pmod{3}\}$.

Proof. Suppose $(a, b) \in \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x \equiv y \pmod{6}\}$.

This means $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ and $a \equiv b \pmod{6}$.

Consequently $6|(a - b)$, so $a - b = 6c$ for some integer c .

It follows that $a - b = 3(2c)$, and this means $3|(a - b)$, so $a \equiv b \pmod{3}$.

Thus $(a, b) \in \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x \equiv y \pmod{3}\}$.

We've now seen that $(a, b) \in \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x \equiv y \pmod{6}\}$ implies $(a, b) \in \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x \equiv y \pmod{3}\}$, so it follows that $\{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x \equiv y \pmod{6}\} \subseteq \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x \equiv y \pmod{3}\}$. ■

Some statements involving subsets are transparent enough that we often accept (and use) them without proof. For example, if A and B are any sets, then it's very easy to confirm $A \cap B \subseteq A$. (Reason: Suppose $x \in A \cap B$. Then $x \in A$ and $x \in B$ by definition of intersection, so in particular $x \in A$. Thus $x \in A \cap B$ implies $x \in A$, so $A \cap B \subseteq A$.) Other statements of this nature include $A \subseteq A \cup B$ and $A - B \subseteq A$, as well as conditional statements such as $((A \subseteq B) \wedge (B \subseteq C)) \Rightarrow (A \subseteq C)$ and $(X \subseteq A) \Rightarrow (X \subseteq A \cup B)$. Our point of view in this text is that we do not need to prove such obvious statements unless we are explicitly asked to do so in an exercise. (Still, you should do some quick mental proofs to convince yourself that the above statements are true. If you don't see that $A \cap B \subseteq A$ is true but that $A \subseteq A \cap B$ is not necessarily true, then you need to spend more time on this topic.)

The next example will show that if A and B are sets, then $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$. Before beginning our proof, let's look at an example to see if this statement really makes sense. Suppose $A = \{1, 2\}$ and $B = \{2, 3\}$. Then

$$\begin{aligned} \mathcal{P}(A) \cup \mathcal{P}(B) &= \{\emptyset, \{1\}, \{2\}, \{1, 2\}\} \cup \{\emptyset, \{2\}, \{3\}, \{2, 3\}\} \\ &= \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{2, 3\}\}. \end{aligned}$$

Also $\mathcal{P}(A \cup B) = \mathcal{P}(\{1, 2, 3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{2, 3\}, \{1, 3\}, \{1, 2, 3\}\}$. Thus, even though $\mathcal{P}(A) \cup \mathcal{P}(B) \neq \mathcal{P}(A \cup B)$, it is true that $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$ for this particular A and B . Now let's prove $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$ no matter what sets A and B are.

Example 11.8 Prove: If A and B are sets, then $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$.

Proof. Suppose $X \in \mathcal{P}(A) \cup \mathcal{P}(B)$.

By definition of union, this means $X \in \mathcal{P}(A)$ or $X \in \mathcal{P}(B)$.

Therefore $X \subseteq A$ or $X \subseteq B$ (by definition of power sets). We consider cases.

Case 1. Suppose $X \subseteq A$. Then $X \subseteq A \cup B$, and this means $X \in \mathcal{P}(A \cup B)$.

Case 2. Suppose $X \subseteq B$. Then $X \subseteq A \cup B$, and this means $X \in \mathcal{P}(A \cup B)$.

(We do not need to consider the case where $X \subseteq A$ and $X \subseteq B$ because that is taken care of by either of cases 1 or 2.) The above cases show that $X \in \mathcal{P}(A \cup B)$.

Thus we've shown that $X \in \mathcal{P}(A) \cup \mathcal{P}(B)$ implies $X \in \mathcal{P}(A \cup B)$, and this completes the proof that $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$. ■

In our next example, we prove a conditional statement. Direct proof is used, and in the process we use our new technique for showing $A \subseteq B$.

Example 11.9 Suppose A and B are sets. If $\mathcal{P}(A) \subseteq \mathcal{P}(B)$, then $A \subseteq B$.

Proof. We use direct proof. Assume $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Based on this assumption, we must now show that $A \subseteq B$.

To show $A \subseteq B$, suppose that $a \in A$.

Then the one-element set $\{a\}$ is a subset of A , so $\{a\} \in \mathcal{P}(A)$.

But then, since $\mathcal{P}(A) \subseteq \mathcal{P}(B)$, it follows that $\{a\} \in \mathcal{P}(B)$.

This means that $\{a\} \subseteq B$, hence $a \in B$.

We've shown that $a \in A$ implies $a \in B$, so therefore $A \subseteq B$. ■

11.3 How to Prove $A = B$

In proofs it is often necessary to show that two sets are equal. There is a standard way of doing this. Suppose we want to show $A = B$. If we show $A \subseteq B$, then every element of A is also in B , but there is still a possibility that B could have some elements that are not in A , so we can't conclude $A = B$. But if *in addition* we also show $B \subseteq A$, then B can't contain anything that is not in A , so $A = B$. This is the standard procedure for proving $A = B$: Prove both $A \subseteq B$ and $B \subseteq A$.

How to Prove $A = B$

Proof.

[Prove that $A \subseteq B$.]

[Prove that $B \subseteq A$.]

Therefore, since $A \subseteq B$ and $B \subseteq A$,
it follows that $A = B$. ■

Example 11.10 Prove that $\{n \in \mathbb{Z} : 35|n\} = \{n \in \mathbb{Z} : 5|n\} \cap \{n \in \mathbb{Z} : 7|n\}$.

Proof. First we show $\{n \in \mathbb{Z} : 35|n\} \subseteq \{n \in \mathbb{Z} : 5|n\} \cap \{n \in \mathbb{Z} : 7|n\}$. Suppose $a \in \{n \in \mathbb{Z} : 35|n\}$. This means $35|a$, so $a = 35c$ for some $c \in \mathbb{Z}$. Thus $a = 5(7c)$ and $a = 7(5c)$. From $a = 5(7c)$ it follows that $5|a$, so $a \in \{n \in \mathbb{Z} : 5|n\}$. From $a = 7(5c)$ it follows that $7|a$, which means $a \in \{n \in \mathbb{Z} : 7|n\}$. As a belongs to both $\{n \in \mathbb{Z} : 5|n\}$ and $\{n \in \mathbb{Z} : 7|n\}$, we get $a \in \{n \in \mathbb{Z} : 5|n\} \cap \{n \in \mathbb{Z} : 7|n\}$. Thus we've shown that $\{n \in \mathbb{Z} : 35|n\} \subseteq \{n \in \mathbb{Z} : 5|n\} \cap \{n \in \mathbb{Z} : 7|n\}$.

Next we show $\{n \in \mathbb{Z} : 5|n\} \cap \{n \in \mathbb{Z} : 7|n\} \subseteq \{n \in \mathbb{Z} : 35|n\}$. Suppose that $a \in \{n \in \mathbb{Z} : 5|n\} \cap \{n \in \mathbb{Z} : 7|n\}$. By definition of intersection, this means that $a \in \{n \in \mathbb{Z} : 5|n\}$ and $a \in \{n \in \mathbb{Z} : 7|n\}$. Therefore it follows that $5|a$ and $7|a$. By definition of divisibility, there are integers c and d with $a = 5c$ and $a = 7d$. Then a has both 5 and 7 as prime factors, so the prime factorization of a

must include factors of 5 and 7. Hence $5 \cdot 7 = 35$ divides a , so $a \in \{n \in \mathbb{Z} : 35|n\}$. We've now shown that $\{n \in \mathbb{Z} : 5|n\} \cap \{n \in \mathbb{Z} : 7|n\} \subseteq \{n \in \mathbb{Z} : 35|n\}$.

At this point we've shown that $\{n \in \mathbb{Z} : 35|n\} \subseteq \{n \in \mathbb{Z} : 5|n\} \cap \{n \in \mathbb{Z} : 7|n\}$ and $\{n \in \mathbb{Z} : 5|n\} \cap \{n \in \mathbb{Z} : 7|n\} \subseteq \{n \in \mathbb{Z} : 35|n\}$, so we've proved $\{n \in \mathbb{Z} : 35|n\} = \{n \in \mathbb{Z} : 5|n\} \cap \{n \in \mathbb{Z} : 7|n\}$. ■

You know from algebra that if $c \neq 0$ and $ac = bc$, then $a = b$. The next example shows that an analogous statement holds for sets A, B and C . The example asks us to prove a conditional statement. We will prove it with direct proof. In carrying out the process of direct proof, we will have to use the new techniques from this section.

Example 11.11 Suppose A, B , and C are sets, and $C \neq \emptyset$. Prove that if $A \times C = B \times C$, then $A = B$.

Proof. Suppose $A \times C = B \times C$. We must now show $A = B$.

First we will show $A \subseteq B$. Suppose $a \in A$. Since $C \neq \emptyset$, there exists an element $c \in C$. Thus, since $a \in A$ and $c \in C$, we have $(a, c) \in A \times C$, by definition of the Cartesian product. But then, since $A \times C = B \times C$, it follows that $(a, c) \in B \times C$. Again by definition of the Cartesian product, it follows that $a \in B$. We have shown $a \in A$ implies $a \in B$, so $A \subseteq B$.

Next we show $B \subseteq A$. We use the same argument as above, with the roles of A and B reversed. Suppose $a \in B$. Since $C \neq \emptyset$, there exists an element $c \in C$. Thus, since $a \in B$ and $c \in C$, we have $(a, c) \in B \times C$. But then, since $B \times C = A \times C$, we have $(a, c) \in A \times C$. It follows that $a \in A$. We have shown $a \in B$ implies $a \in A$, so $B \subseteq A$.

The previous two paragraphs have shown $A \subseteq B$ and $B \subseteq A$, so $A = B$. In summary, we have shown that if $A \times C = B \times C$, then $A = B$. This completes the proof. ■

Now we'll look at another way that set operations are similar to operations on numbers. From algebra you are familiar with the distributive property $a \cdot (b + c) = a \cdot b + a \cdot c$. Replace the numbers a, b, c with sets A, B, C , and replace \cdot with \times and $+$ with \cap . We get $A \times (B \cap C) = (A \times B) \cap (A \times C)$. This statement turns out to be true, as we now prove.

Example 11.12 Given sets A, B , and C , prove $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

Proof. First we will show that $A \times (B \cap C) \subseteq (A \times B) \cap (A \times C)$.

Suppose $(a, b) \in A \times (B \cap C)$.

By definition of the Cartesian product, this means $a \in A$ and $b \in B \cap C$.

By definition of intersection, it follows that $b \in B$ and $b \in C$.

Thus, since $a \in A$ and $b \in B$, it follows that $(a, b) \in A \times B$ (by definition of \times). Also, since $a \in A$ and $b \in C$, it follows that $(a, b) \in A \times C$ (by definition of \times). Now we have $(a, b) \in A \times B$ and $(a, b) \in A \times C$, so $(a, b) \in (A \times B) \cap (A \times C)$. We've shown that $(a, b) \in A \times (B \cap C)$ implies $(a, b) \in (A \times B) \cap (A \times C)$ so we have $A \times (B \cap C) \subseteq (A \times B) \cap (A \times C)$.

Next we will show that $(A \times B) \cap (A \times C) \subseteq A \times (B \cap C)$.

Suppose $(a, b) \in (A \times B) \cap (A \times C)$.

By definition of intersection, this means $(a, b) \in A \times B$ and $(a, b) \in A \times C$.

By definition of the Cartesian product, $(a, b) \in A \times B$ means $a \in A$ and $b \in B$.

By definition of the Cartesian product, $(a, b) \in A \times C$ means $a \in A$ and $b \in C$.

We now have $b \in B$ and $b \in C$, so $b \in B \cap C$, by definition of intersection.

Thus we've deduced that $a \in A$ and $b \in B \cap C$, so $(a, b) \in A \times (B \cap C)$.

In summary, we've shown that $(a, b) \in (A \times B) \cap (A \times C)$ implies $(a, b) \in A \times (B \cap C)$ so we have $(A \times B) \cap (A \times C) \subseteq A \times (B \cap C)$.

The previous two paragraphs show that $A \times (B \cap C) \subseteq (A \times B) \cap (A \times C)$ and $(A \times B) \cap (A \times C) \subseteq A \times (B \cap C)$, so it follows that $(A \times B) \cap (A \times C) = A \times (B \cap C)$. ■

Occasionally you can prove two sets are equal by working out a series of equalities leading from one set to the other. This is analogous to showing two algebraic expressions are equal by manipulating one until you obtain the other. We illustrate this in the following example, which gives an alternate solution to the previous example. You are cautioned that this approach is sometimes difficult to apply, but when it works it can shorten a proof dramatically.

Before beginning the example, a note is in order. Notice that any statement P is logically equivalent to $P \wedge P$. (Write out a truth table if you are in doubt.) At one point in the following example we will replace the expression $x \in A$ with the logically equivalent statement $(x \in A) \wedge (x \in A)$.

Example 11.13 Given sets A , B , and C , prove $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

Proof. Just observe the following sequence of equalities.

$$\begin{aligned}
 A \times (B \cap C) &= \{(x, y) : (x \in A) \wedge (y \in B \cap C)\} && \text{(def. of } \times \text{)} \\
 &= \{(x, y) : (x \in A) \wedge (y \in B) \wedge (y \in C)\} && \text{(def. of } \cap \text{)} \\
 &= \{(x, y) : (x \in A) \wedge (x \in A) \wedge (y \in B) \wedge (y \in C)\} && (P = P \wedge P) \\
 &= \{(x, y) : ((x \in A) \wedge (y \in B)) \wedge ((x \in A) \wedge (y \in C))\} && \text{(rearrange)} \\
 &= \{(x, y) : (x \in A) \wedge (y \in B)\} \cap \{(x, y) : (x \in A) \wedge (y \in C)\} && \text{(def. of } \cap \text{)} \\
 &= (A \times B) \cap (A \times C) && \text{(def. of } \times \text{)}
 \end{aligned}$$

The proof is complete. ■

The equation $A \times (B \cap C) = (A \times B) \cap (A \times C)$ just obtained is a fundamental law that you may actually use fairly often as you continue with mathematics. Some similar equations are listed below. Each of these can be proved with this section's techniques, and the exercises will ask that you do so.

$$\left. \begin{array}{l} \overline{A \cap B} = \overline{A} \cup \overline{B} \\ \overline{A \cup B} = \overline{A} \cap \overline{B} \end{array} \right\} \text{DeMorgan's laws for sets}$$

$$\left. \begin{array}{l} A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \\ A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \end{array} \right\} \text{Distributive laws for sets}$$

$$\left. \begin{array}{l} A \times (B \cup C) = (A \times B) \cup (A \times C) \\ A \times (B \cap C) = (A \times B) \cap (A \times C) \end{array} \right\} \text{Distributive laws for sets}$$

It is very good practice to prove these equations. Depending on your learning style, it is probably not necessary to commit them to memory. But don't forget them entirely. They may well be useful later in your mathematical education. If so, you can look them up or re-derive them on the spot. If you go on to study mathematics deeply, you will at some point realize that you've internalized them without even being cognizant of it.

11.4 Case Study: Perfect Numbers

Sometimes it takes a good bit of work and creativity to show that one set is a subset of another or that they are equal. We illustrate this now with examples from number theory involving what are called perfect numbers. Even though this topic is quite old, dating back more than 2000 years, it leads to some questions that are unanswered even today.

The problem involves adding up the positive divisors of a natural number. To begin the discussion, consider the number 12. If we add up the positive divisors of 12 that are less than 12, we obtain $1 + 2 + 3 + 4 + 6 = 16$, which is greater than 12. Doing the same thing for 15, we get $1 + 3 + 5 = 9$ which is less than 15. For the most part, given a natural number p , the sum of its positive divisors less than itself will either be greater than p or less than p . But occasionally the divisors add up to exactly p . If this happens, then p is said to be a *perfect number*.

Definition 11.1 A number $p \in \mathbb{N}$ is **perfect** if it equals the sum of its positive divisors less than itself. Some examples follow.

- The number 6 is perfect since $6 = 1 + 2 + 3$.
- The number 28 is perfect since $28 = 1 + 2 + 4 + 7 + 14$.
- The number 496 is perfect since $496 = 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248$.

Though it would take a while to find it by trial-and-error, the next perfect number after 496 is 8128. You can check that 8128 is perfect. Its divisors are 1, 2, 4, 8, 16, 32, 64, 127, 254, 508, 1016, 2032, 4064 and indeed

$$8128 = 1 + 2 + 4 + 8 + 16 + 32 + 64 + 127 + 254 + 508 + 1016 + 2032 + 4064.$$

Are there other perfect numbers? How can they be found? Do they obey any patterns? These questions fascinated the ancient Greek mathematicians. In what follows we will develop an idea—recorded by Euclid—that partially answers these questions. Although Euclid did not use sets, we will nonetheless phrase his idea using the language of sets.

Since our goal is to understand what numbers are perfect, let's define the following set:

$$P = \{p \in \mathbb{N} : p \text{ is perfect}\}.$$

Therefore $P = \{6, 28, 496, 8128, \dots\}$, but it is unclear what numbers are in P other than the ones listed. Our goal is to gain a better understanding of just which numbers the set P includes. To do this, we will examine the following set A . It looks more complicated than P , but it will be very helpful for understanding P , as we will soon see.

$$A = \{2^{n-1}(2^n - 1) : n \in \mathbb{N}, \text{ and } 2^n - 1 \text{ is prime}\}$$

In words, A consists of every natural number of form $2^{n-1}(2^n - 1)$, where $2^n - 1$ is prime. To get a feel for what numbers belong to A , look at the following table. For each natural number n , it tallies the corresponding numbers 2^{n-1} and $2^n - 1$. If $2^n - 1$ happens to be prime, then the product $2^{n-1}(2^n - 1)$ is given; otherwise that entry is labeled with an $*$.

| n | 2^{n-1} | $2^n - 1$ | $2^{n-1}(2^n - 1)$ |
|-----|-----------|-----------|--------------------|
| 1 | 1 | 1 | * |
| 2 | 2 | 3 | 6 |
| 3 | 4 | 7 | 28 |
| 4 | 8 | 15 | * |
| 5 | 16 | 31 | 496 |
| 6 | 32 | 63 | * |
| 7 | 64 | 127 | 8128 |
| 8 | 128 | 255 | * |
| 9 | 256 | 511 | * |
| 10 | 512 | 1023 | * |
| 11 | 1024 | 2047 | * |
| 12 | 2048 | 4095 | * |
| 13 | 4096 | 8191 | 33,550,336 |

Notice that the first four entries of A are the perfect numbers 6, 28, 496 and 8128. At this point you may want to jump to the conclusion that $A = P$. But it is a shocking fact that in over 2000 years no one has ever been able to determine whether or not $A = P$. But it is known that $A \subseteq P$, and we will now prove it. In other words, we are going to show that every element of A is perfect. (But by itself, that leaves open the possibility that there may be some perfect numbers in P that are not in A .)

The main ingredient for the proof will be the formula for the sum of a geometric series with common ratio r . You probably saw this most recently in Calculus II. The formula is

$$\sum_{k=0}^n r^k = \frac{r^{n+1} - 1}{r - 1}.$$

We will need this for the case $r = 2$, which is

$$\sum_{k=0}^n 2^k = 2^{n+1} - 1. \quad (11.1)$$

(See the solution for Exercise 19 in Section 12.4 for a proof of this formula.) Now we are ready to prove our result. Let's draw attention to its significance by calling it a theorem rather than a proposition.

Theorem 11.1 If $A = \{2^{n-1}(2^n - 1) : n \in \mathbb{N}, \text{ and } 2^n - 1 \text{ is prime}\}$ and $P = \{p \in \mathbb{N} : p \text{ is perfect}\}$, then $A \subseteq P$.

Proof. Assume A and P are as stated. To show $A \subseteq P$, we must show that $p \in A$ implies $p \in P$. Thus suppose $p \in A$. By definition of A , this means

$$p = 2^{n-1}(2^n - 1) \quad (11.2)$$

for some $n \in \mathbb{N}$ for which $2^n - 1$ is prime. We want to show that $p \in P$, that is, we want to show p is perfect. Thus, we need to show that the sum of the positive divisors of p that are less than p add up to p . Notice that since $2^n - 1$ is prime, any divisor of $p = 2^{n-1}(2^n - 1)$ must have the form 2^k or $2^k(2^n - 1)$ for $0 \leq k \leq n - 1$. Thus the positive divisors of p are as follows:

$$\begin{array}{cccccc} 2^0, & 2^1, & 2^2, & \dots & 2^{n-2}, & 2^{n-1}, \\ 2^0(2^n - 1), & 2^1(2^n - 1), & 2^2(2^n - 1), & \dots & 2^{n-2}(2^n - 1), & 2^{n-1}(2^n - 1). \end{array}$$

Notice that this list starts with $2^0 = 1$ and ends with $2^{n-1}(2^n - 1) = p$.

If we add up all these divisors except for the last one (which equals p) we get the following:

$$\begin{aligned}
 \sum_{k=0}^{n-1} 2^k + \sum_{k=0}^{n-2} 2^k (2^n - 1) &= \sum_{k=0}^{n-1} 2^k + (2^n - 1) \sum_{k=0}^{n-2} 2^k \\
 &= (2^n - 1) + (2^n - 1)(2^{n-1} - 1) \quad (\text{by Equation (11.1)}) \\
 &= [1 + (2^{n-1} - 1)](2^n - 1) \\
 &= 2^{n-1}(2^n - 1) \\
 &= p \quad (\text{by Equation (11.2)}).
 \end{aligned}$$

This shows that the positive divisors of p that are less than p add up to p . Therefore p is perfect, by definition of a perfect number. Thus $p \in P$, by definition of P .

We have shown that $p \in A$ implies $p \in P$, which means $A \subseteq P$. ■

Combined with the chart on the previous page, this theorem gives us a new perfect number! The element $p = 2^{13-1}(2^{13} - 1) = 33,550,336$ in A is perfect.

Observe also that every element of A is a multiple of a power of 2, and therefore even. But this does not necessarily mean every perfect number is even, because we've only shown $A \subseteq P$, not $A = P$. For all we know there may be odd perfect numbers in $P - A$ that are not in A .

Are there any odd perfect numbers? No one knows.

In over 2000 years, no one has ever found an odd perfect number, nor has anyone been able to prove that there are none. But it *is* known that the set A does contain every *even* perfect number. This fact was first proved by Euler, and we duplicate his reasoning in the next theorem, which proves that $A = E$, where E is the set of all *even* perfect numbers. It is a good example of how to prove two sets are equal.

For convenience, we are going to use a slightly different definition of a perfect number. A number $p \in \mathbb{N}$ is **perfect** if its positive divisors add up to $2p$. For example, the number 6 is perfect since the sum of its divisors is $1 + 2 + 3 + 6 = 2 \cdot 6$. This definition is simpler than the first one because we do not have to stipulate that we are adding up the divisors that are *less than* p . Instead we add in the last divisor p , and that has the effect of adding an additional p , thereby doubling the answer.

Theorem 11.2 If $A = \{2^{n-1}(2^n - 1) : n \in \mathbb{N}, \text{ and } 2^n - 1 \text{ is prime}\}$ and $E = \{p \in \mathbb{N} : p \text{ is perfect and even}\}$, then $A = E$.

Proof. To show that $A = E$, we need to show $A \subseteq E$ and $E \subseteq A$.

First we will show that $A \subseteq E$. Suppose $p \in A$. This means p is even, because the definition of A shows that every element of A is a multiple of a power of 2. Also, p is a perfect number because Theorem 11.1 states that every element of A is also an element of P , hence perfect. Thus p is an even perfect number, so $p \in E$. Therefore $A \subseteq E$.

Next we show that $E \subseteq A$. Suppose $p \in E$. This means p is an even perfect number. Write the prime factorization of p as $p = 2^k 3^{n_1} 5^{n_2} 7^{n_3} \dots$, where some of the powers $n_1, n_2, n_3 \dots$ may be zero. But, as p is even, the power k must be greater than zero. It follows $p = 2^k q$ for some positive integer k and an odd integer q . Now, our aim is to show that $p \in A$, which means we must show p has form $p = 2^{n-1}(2^n - 1)$. To get our current $p = 2^k q$ closer to this form, let $n = k + 1$, so we now have

$$p = 2^{n-1}q. \tag{11.3}$$

List the positive divisors of q as $d_1, d_2, d_3, \dots, d_m$. (Where $d_1 = 1$ and $d_m = q$.) Then the divisors of p are:

$$\begin{array}{cccccc} 2^0 d_1 & 2^0 d_2 & 2^0 d_3 & \dots & 2^0 d_m \\ 2^1 d_1 & 2^1 d_2 & 2^1 d_3 & \dots & 2^1 d_m \\ 2^2 d_1 & 2^2 d_2 & 2^2 d_3 & \dots & 2^2 d_m \\ 2^3 d_1 & 2^3 d_2 & 2^3 d_3 & \dots & 2^3 d_m \\ \vdots & \vdots & \vdots & & \vdots \\ 2^{n-1} d_1 & 2^{n-1} d_2 & 2^{n-1} d_3 & \dots & 2^{n-1} d_m \end{array}$$

Since p is perfect, these divisors add up to $2p$. By Equation (11.3), their sum is $2p = 2(2^{n-1}q) = 2^n q$. Adding the divisors column-by-column, we get

$$\sum_{k=0}^{n-1} 2^k d_1 + \sum_{k=0}^{n-1} 2^k d_2 + \sum_{k=0}^{n-1} 2^k d_3 + \dots + \sum_{k=0}^{n-1} 2^k d_m = 2^n q.$$

Applying Equation (11.1), this becomes

$$\begin{aligned} (2^n - 1)d_1 + (2^n - 1)d_2 + (2^n - 1)d_3 + \dots + (2^n - 1)d_m &= 2^n q \\ (2^n - 1)(d_1 + d_2 + d_3 + \dots + d_m) &= 2^n q \\ d_1 + d_2 + d_3 + \dots + d_m &= \frac{2^n q}{2^n - 1}, \end{aligned}$$

so that

$$d_1 + d_2 + d_3 + \cdots + d_m = \frac{(2^n - 1 + 1)q}{2^n - 1} = \frac{(2^n - 1)q + q}{2^n - 1} = q + \frac{q}{2^n - 1}.$$

From this we see that $\frac{q}{2^n - 1}$ is an integer. It follows that both q and $\frac{q}{2^n - 1}$ are positive divisors of q . Since their sum equals the sum of *all* positive divisors of q , it follows that q has only two positive divisors, q and $\frac{q}{2^n - 1}$. Since one of its divisors must be 1, it must be that $\frac{q}{2^n - 1} = 1$, which means $q = 2^n - 1$. Now a number with just two positive divisors is prime, so $q = 2^n - 1$ is prime. Plugging this into Equation (11.3) gives $p = 2^{n-1}(2^n - 1)$, where $2^n - 1$ is prime. This means $p \in A$, by definition of A . We have now shown that $p \in E$ implies $p \in A$, so $E \subseteq A$.

Since $A \subseteq E$ and $E \subseteq A$, it follows that $A = E$. ■

Do not be alarmed if you feel that you wouldn't have thought of this proof. It took the genius of Euler to discover this approach.

We'll conclude this chapter with some facts about perfect numbers.

- The sixth perfect number is $p = 2^{17-1}(2^{17} - 1) = 8589869056$.
- The seventh perfect number is $p = 2^{19-1}(2^{19} - 1) = 137438691328$.
- The eighth perfect number is $p = 2^{31-1}(2^{31} - 1) = 2305843008139952128$.
- The twentieth perfect number is $p = 2^{4423-1}(2^{4423} - 1)$. It has 2663 digits.
- The twenty-third perfect number $p = 2^{11213-1}(2^{11213} - 1)$ has 6957 digits.

As mentioned earlier, no one knows whether or not there are any odd perfect numbers. It is not even known whether there are finitely many or infinitely many perfect numbers. It **is** known that the last digit of every even perfect number is either a 6 or an 8. Perhaps this is something you'd enjoy proving.

We've seen that perfect numbers are closely related to prime numbers that have the form $2^n - 1$. Such prime numbers are called **Mersenne primes**, after the French scholar Marin Mersenne (1588–1648), who popularized them. The first several Mersenne primes are $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 31$, $2^7 - 1 = 127$ and $2^{13} - 1 = 8191$. To date, only 48 Mersenne primes are known, the largest of which is $2^{57,885,161} - 1$. There is a substantial cash prize for anyone who finds a 49th. (See <http://www.mersenne.org/prime.htm>.) You will probably have better luck with the exercises.

Exercises for Chapter 11

Use the methods introduced in this chapter to prove the following statements.

1. Prove that $\{12n : n \in \mathbb{Z}\} \subseteq \{2n : n \in \mathbb{Z}\} \cap \{3n : n \in \mathbb{Z}\}$.
2. Prove that $\{6n : n \in \mathbb{Z}\} = \{2n : n \in \mathbb{Z}\} \cap \{3n : n \in \mathbb{Z}\}$.
3. If $k \in \mathbb{Z}$, then $\{n \in \mathbb{Z} : n | k\} \subseteq \{n \in \mathbb{Z} : n | k^2\}$.
4. If $m, n \in \mathbb{Z}$, then $\{x \in \mathbb{Z} : mn | x\} \subseteq \{x \in \mathbb{Z} : m | x\} \cap \{x \in \mathbb{Z} : n | x\}$.
5. If p and q are positive integers, then $\{pn : n \in \mathbb{N}\} \cap \{qn : n \in \mathbb{N}\} \neq \emptyset$.
6. Suppose A, B and C are sets. Prove that if $A \subseteq B$, then $A - C \subseteq B - C$.
7. Suppose A, B and C are sets. If $B \subseteq C$, then $A \times B \subseteq A \times C$.
8. If A, B and C are sets, then $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.
9. If A, B and C are sets, then $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
10. If A and B are sets in a universal set U , then $\overline{A \cap B} = \overline{A} \cup \overline{B}$.
11. If A and B are sets in a universal set U , then $\overline{A \cup B} = \overline{A} \cap \overline{B}$.
12. If A, B and C are sets, then $A - (B \cap C) = (A - B) \cup (A - C)$.
13. If A, B and C are sets, then $A - (B \cup C) = (A - B) \cap (A - C)$.
14. If A, B and C are sets, then $(A \cup B) - C = (A - C) \cup (B - C)$.
15. If A, B and C are sets, then $(A \cap B) - C = (A - C) \cap (B - C)$.
16. If A, B and C are sets, then $A \times (B \cup C) = (A \times B) \cup (A \times C)$.
17. If A, B and C are sets, then $A \times (B \cap C) = (A \times B) \cap (A \times C)$.
18. If A, B and C are sets, then $A \times (B - C) = (A \times B) - (A \times C)$.
19. Prove that $\{9^n : n \in \mathbb{Z}\} \subseteq \{3^n : n \in \mathbb{Z}\}$, but $\{9^n : n \in \mathbb{Z}\} \neq \{3^n : n \in \mathbb{Z}\}$.
20. Prove that $\{9^n : n \in \mathbb{Q}\} = \{3^n : n \in \mathbb{Q}\}$.
21. For each $a \in \mathbb{R}$, let $A_a = \{(x, a(x^2 - 1)) \in \mathbb{R}^2 : x \in \mathbb{R}\}$. Prove that $\bigcap_{a \in \mathbb{R}} A_a = \{(-1, 0), (1, 0)\}$.
22. Prove that $\bigcap_{x \in \mathbb{R}} [3 - x^2, 5 + x^2] = [3, 5]$.
23. Suppose A, B, C and D are sets. Prove that $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$.
24. Prove $\{4k + 5 : k \in \mathbb{Z}\} = \{4k + 1 : k \in \mathbb{Z}\}$.
25. Prove $\{12a + 4b : a, b \in \mathbb{Z}\} = \{4c : c \in \mathbb{Z}\}$.
26. Prove $\{12a + 25b : a, b \in \mathbb{Z}\} = \mathbb{Z}$.
27. Suppose $B \neq \emptyset$ and $A \times B \subseteq B \times C$. Prove $A \subseteq C$.
28. Prove that $(\mathbb{Z} \times \mathbb{N}) \cap (\mathbb{N} \times \mathbb{Z}) = \mathbb{N} \times \mathbb{N}$.

11.5 Solutions for Chapter 11

1. Prove that $\{12n : n \in \mathbb{Z}\} \subseteq \{2n : n \in \mathbb{Z}\} \cap \{3n : n \in \mathbb{Z}\}$.

Proof. Suppose $a \in \{12n : n \in \mathbb{Z}\}$. This means $a = 12n$ for some $n \in \mathbb{Z}$. Therefore $a = 2(6n)$ and $a = 3(4n)$. From $a = 2(6n)$, it follows that a is multiple of 2, so $a \in \{2n : n \in \mathbb{Z}\}$. From $a = 3(4n)$, it follows that a is multiple of 3, so $a \in \{3n : n \in \mathbb{Z}\}$. Thus by definition of the intersection of two sets, we have $a \in \{2n : n \in \mathbb{Z}\} \cap \{3n : n \in \mathbb{Z}\}$. Thus $\{12n : n \in \mathbb{Z}\} \subseteq \{2n : n \in \mathbb{Z}\} \cap \{3n : n \in \mathbb{Z}\}$. ■

3. If $k \in \mathbb{Z}$, then $\{n \in \mathbb{Z} : n \mid k\} \subseteq \{n \in \mathbb{Z} : n \mid k^2\}$.

Proof. Suppose $k \in \mathbb{Z}$. We now need to show $\{n \in \mathbb{Z} : n \mid k\} \subseteq \{n \in \mathbb{Z} : n \mid k^2\}$. Suppose $a \in \{n \in \mathbb{Z} : n \mid k\}$. Then it follows that $a \mid k$, so there is an integer c for which $k = ac$. Then $k^2 = a^2c^2$. Therefore $k^2 = a(ac^2)$, and from this the definition of divisibility gives $a \mid k^2$. But $a \mid k^2$ means that $a \in \{n \in \mathbb{Z} : n \mid k^2\}$. We have now shown $\{n \in \mathbb{Z} : n \mid k\} \subseteq \{n \in \mathbb{Z} : n \mid k^2\}$. ■

5. If p and q are integers, then $\{pn : n \in \mathbb{N}\} \cap \{qn : n \in \mathbb{N}\} \neq \emptyset$.

Proof. Suppose p and q are integers. Consider the integer pq . Observe that $pq \in \{pn : n \in \mathbb{N}\}$ and $pq \in \{qn : n \in \mathbb{N}\}$, so $pq \in \{pn : n \in \mathbb{N}\} \cap \{qn : n \in \mathbb{N}\}$. Therefore $\{pn : n \in \mathbb{N}\} \cap \{qn : n \in \mathbb{N}\} \neq \emptyset$. ■

7. Suppose A, B and C are sets. If $B \subseteq C$, then $A \times B \subseteq A \times C$.

Proof. This is a conditional statement, and we'll prove it with direct proof. Suppose $B \subseteq C$. (Now we need to prove $A \times B \subseteq A \times C$.)

Suppose $(a, b) \in A \times B$. Then by definition of the Cartesian product we have $a \in A$ and $b \in B$. But since $b \in B$ and $B \subseteq C$, we have $b \in C$. Since $a \in A$ and $b \in C$, it follows that $(a, b) \in A \times C$. Now we've shown $(a, b) \in A \times B$ implies $(a, b) \in A \times C$, so $A \times B \subseteq A \times C$.

In summary, we've shown that if $B \subseteq C$, then $A \times B \subseteq A \times C$. This completes the proof. ■

9. If A, B and C are sets then $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Proof. We use the distributive law $P \wedge (Q \vee R) = (P \wedge Q) \vee (P \wedge R)$ from page 69.

$$\begin{aligned} A \cap (B \cup C) &= \{x : x \in A \wedge x \in B \cup C\} && \text{(def. of intersection)} \\ &= \{x : x \in A \wedge (x \in B \vee x \in C)\} && \text{(def. of union)} \\ &= \{x : (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C)\} && \text{(distributive law)} \\ &= \{x : (x \in A \cap B) \vee (x \in A \cap C)\} && \text{(def. of intersection)} \\ &= (A \cap B) \cup (A \cap C) && \text{(def. of union)} \end{aligned}$$

The proof is complete. ■

11. If A and B are sets in a universal set U , then $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

Proof. Just observe the following sequence of equalities.

$$\begin{aligned}
 \overline{A \cup B} &= U - (A \cup B) && \text{(def. of complement)} \\
 &= \{x : (x \in U) \wedge (x \notin A \cup B)\} && \text{(def. of } -) \\
 &= \{x : (x \in U) \wedge \sim(x \in A \cup B)\} \\
 &= \{x : (x \in U) \wedge \sim((x \in A) \vee (x \in B))\} && \text{(def. of } \cup) \\
 &= \{x : (x \in U) \wedge (\sim(x \in A) \wedge \sim(x \in B))\} && \text{(DeMorgan)} \\
 &= \{x : (x \in U) \wedge (x \notin A) \wedge (x \notin B)\} \\
 &= \{x : (x \in U) \wedge (x \in \overline{U}) \wedge (x \notin A) \wedge (x \notin B)\} && (x \in U) = (x \in U) \wedge (x \in U) \\
 &= \{x : ((x \in U) \wedge (x \notin A)) \wedge ((x \in U) \wedge (x \notin B))\} && \text{(regroup)} \\
 &= \{x : (x \in U) \wedge (x \notin A)\} \cap \{x : (x \in U) \wedge (x \notin B)\} && \text{(def. of } \cap) \\
 &= \overline{(U - A)} \cap \overline{(U - B)} && \text{(def. of } -) \\
 &= \overline{A} \cap \overline{B} && \text{(def. of complement)}
 \end{aligned}$$

The proof is complete. ■

13. If A, B and C are sets, then $A - (B \cup C) = (A - B) \cap (A - C)$.

Proof. Just observe the following sequence of equalities.

$$\begin{aligned}
 A - (B \cup C) &= \{x : (x \in A) \wedge (x \notin B \cup C)\} && \text{(def. of } -) \\
 &= \{x : (x \in A) \wedge \sim(x \in B \cup C)\} \\
 &= \{x : (x \in A) \wedge \sim((x \in B) \vee (x \in C))\} && \text{(def. of } \cup) \\
 &= \{x : (x \in A) \wedge (\sim(x \in B) \wedge \sim(x \in C))\} && \text{(DeMorgan)} \\
 &= \{x : (x \in A) \wedge (x \notin B) \wedge (x \notin C)\} \\
 &= \{x : (x \in A) \wedge (x \in A) \wedge (x \notin B) \wedge (x \notin C)\} && (x \in A) = (x \in A) \wedge (x \in A) \\
 &= \{x : ((x \in A) \wedge (x \notin B)) \wedge ((x \in A) \wedge (x \notin C))\} && \text{(regroup)} \\
 &= \{x : (x \in A) \wedge (x \notin B)\} \cap \{x : (x \in A) \wedge (x \notin C)\} && \text{(def. of } \cap) \\
 &= (A - B) \cap (A - C) && \text{(def. of } -)
 \end{aligned}$$

The proof is complete. ■

15. If A, B and C are sets, then $(A \cap B) - C = (A - C) \cap (B - C)$.

Proof. Just observe the following sequence of equalities.

$$\begin{aligned}
 (A \cap B) - C &= \{x : (x \in A \cap B) \wedge (x \notin C)\} && \text{(def. of } -) \\
 &= \{x : (x \in A) \wedge (x \in B) \wedge (x \notin C)\} && \text{(def. of } \cap) \\
 &= \{x : (x \in A) \wedge (x \notin C) \wedge (x \in B) \wedge (x \notin C)\} && \text{(regroup)} \\
 &= \{x : ((x \in A) \wedge (x \notin C)) \wedge ((x \in B) \wedge (x \notin C))\} && \text{(regroup)} \\
 &= \{x : (x \in A) \wedge (x \notin C)\} \cap \{x : (x \in B) \wedge (x \notin C)\} && \text{(def. of } \cap) \\
 &= (A - C) \cap (B - C) && \text{(def. of } \cap)
 \end{aligned}$$

The proof is complete. ■

17. If A, B and C are sets, then $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

Proof. See Example 11.12. ■

19. Prove that $\{9^n : n \in \mathbb{Z}\} \subseteq \{3^n : n \in \mathbb{Z}\}$, but $\{9^n : n \in \mathbb{Z}\} \neq \{3^n : n \in \mathbb{Z}\}$.

Proof. Suppose $a \in \{9^n : n \in \mathbb{Z}\}$. This means $a = 9^n$ for some integer $n \in \mathbb{Z}$. Thus $a = 9^n = (3^2)^n = 3^{2n}$. This shows a is an integer power of 3, so $a \in \{3^n : n \in \mathbb{Z}\}$. Therefore $a \in \{9^n : n \in \mathbb{Z}\}$ implies $a \in \{3^n : n \in \mathbb{Z}\}$, so $\{9^n : n \in \mathbb{Z}\} \subseteq \{3^n : n \in \mathbb{Z}\}$.

But notice $\{9^n : n \in \mathbb{Z}\} \neq \{3^n : n \in \mathbb{Z}\}$ as $3 \in \{3^n : n \in \mathbb{Z}\}$, but $3 \notin \{9^n : n \in \mathbb{Z}\}$. ■

21. For each $a \in \mathbb{R}$, let $A_a = \{(x, a(x^2 - 1)) \in \mathbb{R}^2 : x \in \mathbb{R}\}$. Prove that $\bigcap_{a \in \mathbb{R}} A_a = \{(-1, 0), (1, 0)\}$.

Proof. First we will show that $\{(-1,0), (1,0)\} \subseteq \bigcap_{a \in \mathbb{R}} A_a$. Notice that for any $a \in \mathbb{R}$, we have $(-1,0) \in A_a$ because A_a contains the ordered pair $(-1, a((-1)^2 - 1)) = (-1,0)$. Similarly $(1,0) \in A_a$. Thus each element of $\{(-1,0), (1,0)\}$ belongs to every set A_a , so every element of $\bigcap_{a \in \mathbb{R}} A_a$, so $\{(-1,0), (1,0)\} \subseteq \bigcap_{a \in \mathbb{R}} A_a$.

Now we will show $\bigcap_{a \in \mathbb{R}} A_a \subseteq \{(-1,0), (1,0)\}$. Suppose $(c,d) \in \bigcap_{a \in \mathbb{R}} A_a$. This means (c,d) is in every set A_a . In particular $(c,d) \in A_0 = \{(x, 0(x^2 - 1)) : x \in \mathbb{R}\} = \{(x, 0) : x \in \mathbb{R}\}$. It follows that $d = 0$. Then also we have $(c,d) = (c,0) \in A_1 = \{(x, 1(x^2 - 1)) : x \in \mathbb{R}\} = \{(x, x^2 - 1) : x \in \mathbb{R}\}$. Therefore $(c,0)$ has the form $(c, c^2 - 1)$, that is $(c,0) = (c, c^2 - 1)$. From this we get $c^2 - 1 = 0$, so $c = \pm 1$. Therefore $(c,d) = (1,0)$ or $(c,d) = (-1,0)$, so $(c,d) \in \{(-1,0), (1,0)\}$. This completes the demonstration that $(c,d) \in \bigcap_{a \in \mathbb{R}} A_a$ implies $(c,d) \in \{(-1,0), (1,0)\}$, so it follows that $\bigcap_{a \in \mathbb{R}} A_a \subseteq \{(-1,0), (1,0)\}$.

Now it's been shown that $\{(-1,0), (1,0)\} \subseteq \bigcap_{a \in \mathbb{R}} A_a$ and $\bigcap_{a \in \mathbb{R}} A_a \subseteq \{(-1,0), (1,0)\}$, so it follows that $\bigcap_{a \in \mathbb{R}} A_a = \{(-1,0), (1,0)\}$. ■

23. Suppose A, B, C and D are sets. Prove that $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$.

Proof. Suppose $(a,b) \in (A \times B) \cup (C \times D)$.

By definition of union, this means $(a,b) \in (A \times B)$ **or** $(a,b) \in (C \times D)$.

We examine these two cases individually.

Case 1. Suppose $(a,b) \in (A \times B)$. By definition of \times , it follows that $a \in A$ and $b \in B$. From this, it follows from the definition of \cup that $a \in A \cup C$ and $b \in B \cup D$.

Again from the definition of \times , we get $(a,b) \in (A \cup C) \times (B \cup D)$.

Case 2. Suppose $(a,b) \in (C \times D)$. By definition of \times , it follows that $a \in C$ and $b \in D$. From this, it follows from the definition of \cup that $a \in A \cup C$ and $b \in B \cup D$.

Again from the definition of \times , we get $(a,b) \in (A \cup C) \times (B \cup D)$.

In either case, we obtained $(a,b) \in (A \cup C) \times (B \cup D)$,

so we've proved that $(a,b) \in (A \times B) \cup (C \times D)$ implies $(a,b) \in (A \cup C) \times (B \cup D)$.

Therefore $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$. ■

25. Prove $\{12a + 4b : a, b \in \mathbb{Z}\} = \{4c : c \in \mathbb{Z}\}$.

Proof. First we show $\{12a + 4b : a, b \in \mathbb{Z}\} \subseteq \{4c : c \in \mathbb{Z}\}$. Suppose $x \in \{12a + 4b : a, b \in \mathbb{Z}\}$. Then $x = 12a + 4b$ for some integers a and b . From this we get $x = 4(3a + b)$, so $x = 4c$ where c is the integer $3a + b$. Consequently $x \in \{4c : c \in \mathbb{Z}\}$. This establishes that $\{12a + 4b : a, b \in \mathbb{Z}\} \subseteq \{4c : c \in \mathbb{Z}\}$.

Next we show $\{4c : c \in \mathbb{Z}\} \subseteq \{12a + 4b : a, b \in \mathbb{Z}\}$. Suppose $x \in \{4c : c \in \mathbb{Z}\}$. Then $x = 4c$ for some $c \in \mathbb{Z}$. Thus $x = (12 + 4(-2))c = 12c + 4(-2c)$, and since c and $-2c$ are integers we have $x \in \{12a + 4b : a, b \in \mathbb{Z}\}$.

This proves that $\{12a + 4b : a, b \in \mathbb{Z}\} = \{4c : c \in \mathbb{Z}\}$. ■

27. Suppose $B \neq \emptyset$ and $A \times B \subseteq B \times C$. Prove $A \subseteq C$.

Proof. Suppose $B \neq \emptyset$ and $A \times B \subseteq B \times C$. In what follows, we show that $A \subseteq C$. Let $x \in A$. Because B is not empty, it contains some element b . Observe that $(x, b) \in A \times B$. But as $A \times B \subseteq B \times C$, we also have $(x, b) \in B \times C$, so, in particular, $x \in B$. As $x \in A$ and $x \in B$, we have $(x, x) \in A \times B$. But as $A \times B \subseteq B \times C$, it follows that $(x, x) \in B \times C$. This implies $x \in C$.

Now we've shown $x \in A$ implies $x \in C$, so $A \subseteq C$. ■

Part IV

Other Types of Proof

Proving Non-Conditional Statements

The last three chapters introduced three major proof techniques: direct, contrapositive and contradiction. These three techniques are used to prove statements of the form “*If P, then Q.*” As we know, most theorems and propositions have this conditional form, or they can be reworded to have this form. Thus the three main techniques are quite important. But some theorems and propositions cannot be put into conditional form. For example, some theorems have form “*P if and only if Q.*” Such theorems are biconditional statements, not conditional statements. In this chapter we examine ways to prove them. In addition to learning how to prove if-and-only-if theorems, we will also look at two other types of theorems.

12.1 If-and-Only-If Proof

Some propositions have the form

P if and only if Q.

We know from Section 3.4 that this statement asserts that **both** of the following conditional statements are true:

If *P*, then *Q*.

If *Q*, then *P*.

So to prove “*P if and only if Q,*” we must prove **two** conditional statements. Recall from Section 3.4 that $Q \Rightarrow P$ is called the *converse* of $P \Rightarrow Q$. Thus we need to prove both $P \Rightarrow Q$ and its converse. Since these are both conditional statements we may prove them with either direct, contrapositive or contradiction proof. Here is an outline:

Outline for If-and-Only-If Proof

Proposition *P if and only if Q.*

Proof.

[Prove $P \Rightarrow Q$ using direct, contrapositive or contradiction proof.]

[Prove $Q \Rightarrow P$ using direct, contrapositive or contradiction proof.] ■

Let's start with a very simple example. You already know that an integer n is odd if and only if n^2 is odd, but let's prove it anyway, just to illustrate the outline. In this example we prove $(n \text{ is odd}) \Rightarrow (n^2 \text{ is odd})$ using direct proof and $(n^2 \text{ is odd}) \Rightarrow (n \text{ is odd})$ using contrapositive proof.

Proposition The integer n is odd if and only if n^2 is odd.

Proof. First we show that n being odd implies that n^2 is odd. Suppose n is odd. Then, by definition of an odd number, $n = 2a + 1$ for some integer a . Thus $n^2 = (2a + 1)^2 = 4a^2 + 4a + 1 = 2(2a^2 + 2a) + 1$. This expresses n^2 as twice an integer, plus 1, so n^2 is odd.

Conversely, we need to prove that n^2 being odd implies that n is odd. We use contrapositive proof. Suppose n is not odd. Then n is even, so $n = 2a$ for some integer a (by definition of an even number). Thus $n^2 = (2a)^2 = 2(2a^2)$, so n^2 is even because it's twice an integer. Thus n^2 is not odd. We've now proved that if n is not odd, then n^2 is not odd, and this is a contrapositive proof that if n^2 is odd then n is odd. ■

In proving " P if and only if Q ," you should begin a new paragraph when starting the proof of $Q \Rightarrow P$. Since this is the converse of $P \Rightarrow Q$, it's a good idea to begin the paragraph with the word "*Conversely*" (as we did above) to remind the reader that you've finished the first part of the proof and are moving on to the second. Likewise, it's a good idea to remind the reader of exactly what statement that paragraph is proving.

The next example uses direct proof in both parts of the proof.

Proposition Suppose a and b are integers. Then $a \equiv b \pmod{6}$ if and only if $a \equiv b \pmod{2}$ and $a \equiv b \pmod{3}$.

Proof. First we prove that if $a \equiv b \pmod{6}$, then $a \equiv b \pmod{2}$ and $a \equiv b \pmod{3}$. Suppose $a \equiv b \pmod{6}$. This means $6 \mid (a - b)$, so there is an integer n for which

$$a - b = 6n.$$

From this we get $a - b = 2(3n)$, which implies $2 \mid (a - b)$, so $a \equiv b \pmod{2}$. But we also get $a - b = 3(2n)$, which implies $3 \mid (a - b)$, so $a \equiv b \pmod{3}$. Therefore $a \equiv b \pmod{2}$ and $a \equiv b \pmod{3}$.

Conversely, suppose $a \equiv b \pmod{2}$ and $a \equiv b \pmod{3}$. Since $a \equiv b \pmod{2}$ we get $2 \mid (a - b)$, so there is an integer k for which $a - b = 2k$. Therefore $a - b$ is even. Also, from $a \equiv b \pmod{3}$ we get $3 \mid (a - b)$, so there is an integer ℓ for which

$$a - b = 3\ell.$$

But since we know $a - b$ is even, it follows that ℓ must be even also, for if it were odd then $a - b = 3\ell$ would be odd (because $a - b$ would be the product of two odd integers). Hence $\ell = 2m$ for some integer m . Thus $a - b = 3\ell = 3 \cdot 2m = 6m$. This means $6 \mid (a - b)$, so $a \equiv b \pmod{6}$. ■

Since if-and-only-if proofs simply combine methods with which we are already familiar, we will not do any further examples in this section. However, it is of utmost importance that you practice your skill on some of this chapter's exercises.

12.2 Equivalent Statements

In other courses you will sometimes encounter a certain kind of theorem that is neither a conditional nor a biconditional statement. Instead, it asserts that a list of statements is “*equivalent*.” You saw this (or will see it) in your linear algebra textbook, which featured the following theorem:

Theorem Suppose A is an $n \times n$ matrix. The following statements are equivalent:

- (a) The matrix A is invertible.
- (b) The equation $A\mathbf{x} = \mathbf{b}$ has a unique solution for every $\mathbf{b} \in \mathbb{R}^n$.
- (c) The equation $A\mathbf{x} = \mathbf{0}$ has only the trivial solution.
- (d) The reduced row echelon form of A is I_n .
- (e) $\det(A) \neq 0$.
- (f) The matrix A does not have 0 as an eigenvalue.

When a theorem asserts that a list of statements is “*equivalent*,” it is asserting that either the statements are all true, or they are all false. Thus the above theorem tells us that whenever we are dealing with a particular $n \times n$ matrix A , then either the statements (a) through (f) are all true for A , or statements (a) through (f) are all false for A . For example, if we happen to know that $\det(A) \neq 0$, the theorem assures us that in addition to statement (e) being true, **all** the statements (a) through (f) are true. On the other hand, if it happens that $\det(A) = 0$, the theorem tells us that all statements (a) through (f) are false. In this way, the theorem multiplies our knowledge of A by a factor of six. Obviously that can be very useful.

What method would we use to prove such a theorem? In a certain sense, the above theorem is like an if-and-only-if theorem. An if-and-only-if theorem of form $P \Leftrightarrow Q$ asserts that P and Q are either both true or both false, that is, that P and Q are equivalent. To prove $P \Leftrightarrow Q$ we prove $P \Rightarrow Q$ followed by $Q \Rightarrow P$, essentially making a “cycle” of implications from P to

Q and back to P . Similarly, one approach to proving the theorem about the $n \times n$ matrix would be to prove the conditional statement $(a) \Rightarrow (b)$, then $(b) \Rightarrow (c)$, then $(c) \Rightarrow (d)$, then $(d) \Rightarrow (e)$, then $(e) \Rightarrow (f)$ and finally $(f) \Rightarrow (a)$. This pattern is illustrated below.

$$\begin{array}{ccccc} (a) & \Rightarrow & (b) & \Rightarrow & (c) \\ \uparrow & & & & \downarrow \\ (f) & \Leftarrow & (e) & \Leftarrow & (d) \end{array}$$

Notice that if these six implications have been proved, then it really does follow that the statements (a) through (f) are either all true or all false. If one of them is true, then the circular chain of implications forces them all to be true. On the other hand, if one of them (say (c)) is false, the fact that $(b) \Rightarrow (c)$ is true forces (b) to be false. This combined with the truth of $(a) \Rightarrow (b)$ makes (a) false, and so on counterclockwise around the circle.

Thus to prove that n statements are equivalent, it suffices to prove n conditional statements showing each statement implies another, in circular pattern. But it is not necessary that the pattern be circular. The following schemes would also do the job:

$$\begin{array}{ccccc} (a) & \Rightarrow & (b) & \Leftarrow & (c) \\ \uparrow & & \downarrow & & \\ (f) & \Leftarrow & (e) & \Leftarrow & (d) \end{array}$$

$$\begin{array}{ccccc} (a) & \Leftarrow & (b) & \Leftarrow & (c) \\ & & \updownarrow & & \\ (f) & \Leftarrow & (e) & \Leftarrow & (d) \end{array}$$

But a circular pattern yields the fewest conditional statements that must be proved. Whatever the pattern, each conditional statement can be proved with either direct, contrapositive or contradiction proof.

Though we shall not do any of these proofs in this text, you are sure to encounter them in subsequent courses.

12.3 Existence Proofs; Existence and Uniqueness Proofs

Up until this point, we have dealt with proving conditional statements or with statements that can be expressed with two or more conditional statements. Generally, these conditional statements have form $P(x) \Rightarrow Q(x)$. (Possibly with more than one variable.) We saw in Section 7.2 that this can be interpreted as a universally quantified statement $\forall x, P(x) \Rightarrow Q(x)$.

Thus, conditional statements are universally quantified statements, so in proving a conditional statement—whether we use direct, contrapositive or contradiction proof—we are really proving a universally quantified statement.

But how would we prove an *existentially* quantified statement? What technique would we employ to prove a theorem of the following form?

$$\exists x, R(x)$$

This statement asserts that there exists some specific object x for which $R(x)$ is true. To prove $\exists x, R(x)$ is true, all we would have to do is find and display an *example* of a specific x that makes $R(x)$ true.

Though most theorems and propositions are conditional (or if-and-only-if) statements, a few have the form $\exists x, R(x)$. Such statements are called **existence statements**, and theorems that have this form are called **existence theorems**. To prove an existence theorem, all you have to do is provide a particular example that shows it is true. This is often quite simple. (But not always!) Here are some examples:

Proposition There exists an even prime number.

Proof. Observe that 2 is an even prime number. ■

Admittedly, this last proposition was a bit of an oversimplification. The next one is slightly more challenging.

Proposition There exists an integer that can be expressed as the sum of two perfect cubes in two different ways.

Proof. Consider the number 1729. Note that $1^3 + 12^3 = 1729$ and $9^3 + 10^3 = 1729$. Thus the number 1729 can be expressed as the sum of two perfect cubes in two different ways. ■

Sometimes in the proof of an existence statement, a little verification is needed to show that the example really does work. For example, the above proof would be incomplete if we just asserted that 1729 can be written as a sum of two cubes in two ways without showing *how* this is possible.

WARNING: Although an example suffices to prove an existence statement, a single example does not prove a conditional statement.

Often an existence statement will be embedded in a conditional statement. Consider the following. (Recall the definition of \gcd on page 227.)

If $a, b \in \mathbb{N}$, then there exist integers k and ℓ for which $\gcd(a, b) = ak + b\ell$.

This is a conditional statement that has the form

$$a, b \in \mathbb{N} \implies \exists k, \ell \in \mathbb{Z}, \gcd(a, b) = ak + b\ell.$$

To prove it with direct proof, we would first assume that $a, b \in \mathbb{N}$, then prove the existence statement $\exists k, \ell \in \mathbb{Z}, \gcd(a, b) = ak + b\ell$. That is, we would produce two integers k and ℓ (which depend on a and b) for which $\gcd(a, b) = ak + b\ell$. Let's carry out this plan. (We will use this fundamental proposition several times later, so it is given a number.)

Proposition 12.1 If $a, b \in \mathbb{N}$, then there exist integers k and ℓ for which $\gcd(a, b) = ak + b\ell$.

Proof. (Direct) Suppose $a, b \in \mathbb{N}$. Consider the set $A = \{ax + by : x, y \in \mathbb{Z}\}$. This set contains both positive and negative integers, as well as 0. (Reason: Let $y = 0$ and let x range over all integers. Then $ax + by = ax$ ranges over all multiples of a , both positive, negative and zero.) Let d be the smallest positive element of A . Then, because d is in A , it must have the form $d = ak + b\ell$ for some specific $k, \ell \in \mathbb{Z}$.

To finish, we will show $d = \gcd(a, b)$. We will first argue that d is a common divisor of a and b , and then that it is the *greatest* common divisor.

To see that $d \mid a$, use the division algorithm (page 186) to write $a = qd + r$ for integers q and r with $0 \leq r < d$. The equation $a = qd + r$ yields

$$\begin{aligned} r &= a - qd \\ &= a - q(ak + b\ell) \\ &= a(1 - qk) + b(-q\ell). \end{aligned}$$

Therefore r has form $r = ax + by$, so it belongs to A . But $0 \leq r < d$ and d is the smallest positive number in A , so r can't be positive; hence $r = 0$. Updating our equation $a = qd + r$, we get $a = qd$, so $d \mid a$. Repeating this argument with $b = qd + r$ shows $d \mid b$. Thus d is indeed a common divisor of a and b . It remains to show that it is the *greatest* common divisor.

As $\gcd(a, b)$ divides a and b , we have $a = \gcd(a, b) \cdot m$ and $b = \gcd(a, b) \cdot n$ for some $m, n \in \mathbb{Z}$. So $d = ak + b\ell = \gcd(a, b) \cdot mk + \gcd(a, b) \cdot n\ell = \gcd(a, b)(mk + n\ell)$, and thus d is a multiple of $\gcd(a, b)$. Therefore $d \geq \gcd(a, b)$. But d can't be a larger common divisor of a and b than $\gcd(a, b)$, so $d = \gcd(a, b)$. ■

We conclude this section with a discussion of so-called *uniqueness proofs*. Some existence statements have form “*There is a unique x for which $P(x)$.*” Such a statement asserts that there is *exactly one* example x for which $P(x)$ is true. To prove it, you must produce an example $x = d$ for which $P(d)$ is true, **and** you must show that d is the only such example. The next proposition illustrates this. In essence, it asserts that the set $\{ax + by : x, y \in \mathbb{Z}\}$ consists precisely of all the multiples of $\gcd(a, b)$.

Proposition Suppose $a, b \in \mathbb{N}$. Then there exists a unique $d \in \mathbb{N}$ for which: An integer m is a multiple of d if and only if $m = ax + by$ for some $x, y \in \mathbb{Z}$.

Proof. Suppose $a, b \in \mathbb{N}$. Let $d = \gcd(a, b)$. We now show that an integer m is a multiple of d if and only if $m = ax + by$ for some $x, y \in \mathbb{Z}$. Let $m = dn$ be a multiple of d . By Proposition 12.1 (on the previous page), there are integers k and ℓ for which $d = ak + b\ell$. Then $m = dn = (ak + b\ell)n = a(kn) + b(\ell n)$, so $m = ax + by$ for integers $x = kn$ and $y = \ell n$.

Conversely, suppose $m = ax + by$ for some $x, y \in \mathbb{Z}$. Since $d = \gcd(a, b)$ is a divisor of both a and b , we have $a = dc$ and $b = de$ for some $c, e \in \mathbb{Z}$. Then $m = ax + by = dcx + dey = d(cx + ey)$, and this is a multiple of d .

We have now shown that there is a natural number d with the property that m is a multiple of d if and only if $m = ax + by$ for some $x, y \in \mathbb{Z}$. It remains to show that d is the *unique* such natural number. To do this, suppose d' is *any* natural number with the property that d has:

$$m \text{ is a multiple of } d' \iff m = ax + by \text{ for some } x, y \in \mathbb{Z}. \quad (12.1)$$

We next argue that $d' = d$; that is, d is the *unique* natural number with the stated property. Because of (12.1), $m = a \cdot 1 + b \cdot 0 = a$ is a multiple of d' . Likewise $m = a \cdot 0 + b \cdot 1 = b$ is a multiple of d' . Hence a and b are both multiples of d' , so d' is a common divisor of a and b , and therefore

$$d' \leq \gcd(a, b) = d.$$

But also, by (12.1), the multiple $m = d' \cdot 1 = d'$ of d' can be expressed as $d' = ax + by$ for some $x, y \in \mathbb{Z}$. As noted in the second paragraph of the proof, $a = dc$ and $b = de$ for some $c, e \in \mathbb{Z}$. Thus $d' = ax + by = dcx + dey = d(cx + ey)$, so d' is a multiple of d . As d' and d are both positive, it follows that

$$d \leq d'.$$

We've now shown that $d' \leq d$ and $d \leq d'$, so $d = d'$. The proof is complete. ■

12.4 Constructive Versus Non-Constructive Proofs

Existence proofs fall into two categories: constructive and non-constructive. Constructive proofs display an explicit example that proves the theorem; non-constructive proofs prove an example exists without actually giving it. We illustrate the difference with two proofs of the same fact: There exist *irrational* numbers x and y (possibly equal) for which x^y is *rational*.

Proposition There exist irrational numbers x, y for which x^y is rational.

Proof. Let $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$. We know y is irrational, but it is not clear whether x is rational or irrational. On one hand, if x is irrational, then we have an irrational number to an irrational power that is rational:

$$x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\sqrt{2}} = \sqrt{2}^2 = 2.$$

On the other hand, if x is rational, then $y^y = \sqrt{2}^{\sqrt{2}} = x$ is rational. Either way, we have a irrational number to an irrational power that is rational. ■

The above is a classic example of a **non-constructive** proof. It shows that there exist irrational numbers x and y for which x^y is rational without actually producing (or constructing) an example. It convinces us that one of $(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}}$ or $\sqrt{2}^{\sqrt{2}}$ is an irrational number to an irrational power that is rational, but it does not say which one is the correct example. It thus proves that an example exists without explicitly stating one.

Next comes a **constructive proof** of this statement, one that produces (or constructs) two explicit irrational numbers x, y for which x^y is rational.

Proposition There exist irrational numbers x, y for which x^y is rational.

Proof. Let $x = \sqrt{2}$ and $y = \log_2 9$. Then

$$x^y = \sqrt{2}^{\log_2 9} = \sqrt{2}^{\log_2 3^2} = \sqrt{2}^{2\log_2 3} = \left(\sqrt{2}^2\right)^{\log_2 3} = 2^{\log_2 3} = 3.$$

As 3 is rational, we have shown that $x^y = 3$ is rational.

We know that $x = \sqrt{2}$ is irrational. The proof will be complete if we can show that $y = \log_2 9$ is irrational. Suppose for the sake of contradiction that $\log_2 9$ is rational, so there are integers a and b for which $\frac{a}{b} = \log_2 9$. This means $2^{a/b} = 9$, so $(2^{a/b})^b = 9^b$, which reduces to $2^a = 9^b$. But 2^a is even, while 9^b is odd (because it is the product of the odd number 9 with itself b times). This is a contradiction; the proof is complete. ■

This existence proof has inside of it a separate proof (by contradiction) that $\log_2 9$ is irrational. Such combinations of proof techniques are, of course, typical.

Be alert to constructive and non-constructive proofs as you read proofs in other books and articles, as well as to the possibility of crafting such proofs of your own.

Exercises for Chapter 12

Prove the following statements. These exercises are cumulative, covering all techniques addressed in Chapters 8–12.

1. Suppose $x \in \mathbb{Z}$. Then x is even if and only if $3x + 5$ is odd.
2. Suppose $x \in \mathbb{Z}$. Then x is odd if and only if $3x + 6$ is odd.
3. Given an integer a , then $a^3 + a^2 + a$ is even if and only if a is even.
4. Given an integer a , then $a^2 + 4a + 5$ is odd if and only if a is even.
5. An integer a is odd if and only if a^3 is odd.
6. Suppose $x, y \in \mathbb{R}$. Then $x^3 + x^2y = y^2 + xy$ if and only if $y = x^2$ or $y = -x$.
7. Suppose $x, y \in \mathbb{R}$. Then $(x + y)^2 = x^2 + y^2$ if and only if $x = 0$ or $y = 0$.
8. Suppose $a, b \in \mathbb{Z}$. Prove that $a \equiv b \pmod{10}$ if and only if $a \equiv b \pmod{2}$ and $a \equiv b \pmod{5}$.
9. Suppose $a \in \mathbb{Z}$. Prove that $14 \mid a$ if and only if $7 \mid a$ and $2 \mid a$.
10. If $a \in \mathbb{Z}$, then $a^3 \equiv a \pmod{3}$.
11. Suppose $a, b \in \mathbb{Z}$. Prove that $(a - 3)b^2$ is even if and only if a is odd or b is even.
12. There exist a positive real number x for which $x^2 < \sqrt{x}$.
13. Suppose $a, b \in \mathbb{Z}$. If $a + b$ is odd, then $a^2 + b^2$ is odd.
14. Suppose $a \in \mathbb{Z}$. Then $a^2 \mid a$ if and only if $a \in \{-1, 0, 1\}$.
15. Suppose $a, b \in \mathbb{Z}$. Prove that $a + b$ is even if and only if a and b have the same parity.
16. Suppose $a, b \in \mathbb{Z}$. If ab is odd, then $a^2 + b^2$ is even.
17. There is a prime number between 90 and 100.
18. There is a set X for which $\mathbb{N} \in X$ and $\mathbb{N} \subseteq X$.
19. If $n \in \mathbb{N}$, then $2^0 + 2^1 + 2^2 + 2^3 + 2^4 + \dots + 2^n = 2^{n+1} - 1$.
20. There exists an $n \in \mathbb{N}$ for which $11 \mid (2^n - 1)$.
21. Every real solution of $x^3 + x + 3 = 0$ is irrational.
22. If $n \in \mathbb{Z}$, then $4 \mid n^2$ or $4 \mid (n^2 - 1)$.
23. Suppose a, b and c are integers. If $a \mid b$ and $a \mid (b^2 - c)$, then $a \mid c$.
24. If $a \in \mathbb{Z}$, then $4 \nmid (a^2 - 3)$.

25. If $p > 1$ is an integer and $n \nmid p$ for each integer n for which $2 \leq n \leq \sqrt{p}$, then p is prime.
26. The product of any n consecutive positive integers is divisible by $n!$.
27. Suppose $a, b \in \mathbb{Z}$. If $a^2 + b^2$ is a perfect square, then a and b are not both odd.
28. Prove the division algorithm: If $a, b \in \mathbb{N}$, there exist *unique* integers q, r for which $a = bq + r$, and $0 \leq r < b$. (A proof of existence is given in Section 2.9, but uniqueness needs to be established too.)
29. If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.
(Suggestion: Use the proposition on page 300.)
30. Suppose $a, b, p \in \mathbb{Z}$ and p is prime. Prove that if $p \mid ab$ then $p \mid a$ or $p \mid b$. (Suggestion: Use the proposition on page 300.)
31. If $n \in \mathbb{Z}$, then $\gcd(n, n+1) = 1$.
32. If $n \in \mathbb{Z}$, then $\gcd(n, n+2) \in \{1, 2\}$.
33. If $n \in \mathbb{Z}$, then $\gcd(2n+1, 4n^2+1) = 1$.
34. If $\gcd(a, c) = \gcd(b, c) = 1$, then $\gcd(ab, c) = 1$.
(Suggestion: Use the proposition on page 300.)
35. Suppose $a, b \in \mathbb{N}$. Then $a = \gcd(a, b)$ if and only if $a \mid b$.
36. Suppose $a, b \in \mathbb{N}$. Then $a = \text{lcm}(a, b)$ if and only if $b \mid a$.
37. Suppose A and B are sets. Prove $A \subseteq B$ if and only if $A - B = \emptyset$.
38. Let A and B be sets. Prove that $A \subseteq B$ if and only if $A \cap B = A$.
39. Suppose $A \neq \emptyset$. Prove that $A \times B \subseteq A \times C$, if and only if $B \subseteq C$.

12.5 Solutions for Chapter 12

1. Suppose $x \in \mathbb{Z}$. Then x is even if and only if $3x + 5$ is odd.

Proof. We first use direct proof to show that if x is even, then $3x + 5$ is odd. If x is even, then $x = 2n$ for some integer n , so $3x + 5 = 3(2n) + 5 = 6n + 5 = 6n + 4 + 1 = 2(3n + 2) + 1$. Thus $3x + 5$ is odd because it has form $2k + 1$, where $k = 3n + 2 \in \mathbb{Z}$.

Conversely, we need to show that if $3x + 5$ is odd, then x is even. We will prove this using contrapositive proof. Suppose x is *not* even. Then x is odd, so $x = 2n + 1$ for some integer n . Thus $3x + 5 = 3(2n + 1) + 5 = 6n + 8 = 2(3n + 4)$. This means says $3x + 5$ is twice the integer $3n + 4$, so $3x + 5$ is even, not odd. ■

3. Given an integer a , then $a^3 + a^2 + a$ is even if and only if a is even.

Proof. First we will prove that if $a^3 + a^2 + a$ is even then a is even. This is done with contrapositive proof. Suppose a is not even. Then a is odd, so there is an integer n for which $a = 2n + 1$. Then

$$\begin{aligned} a^3 + a^2 + a &= (2n + 1)^3 + (2n + 1)^2 + (2n + 1) \\ &= 8n^3 + 12n^2 + 6n + 1 + 4n^2 + 4n + 1 + 2n + 1 \\ &= 8n^3 + 16n^2 + 12n + 2 + 1 \\ &= 2(4n^3 + 8n^2 + 6n + 1) + 1. \end{aligned}$$

This expresses $a^3 + a^2 + a$ as twice an integer plus 1, so $a^3 + a^2 + a$ is odd, not even. We have now shown that if $a^3 + a^2 + a$ is even then a is even.

Conversely, we need to show that if a is even, then $a^3 + a^2 + a$ is even. We will use direct proof. Suppose a is even, so $a = 2n$ for some integer n . Then $a^3 + a^2 + a = (2n)^3 + (2n)^2 + 2n = 8n^3 + 4n^2 + 2n = 2(4n^3 + 2n^2 + n)$. Therefore, $a^3 + a^2 + a$ is even because it's twice an integer. ■

5. An integer a is odd if and only if a^3 is odd.

Proof. Suppose that a is odd. Then $a = 2n + 1$ for some integer n , and $a^3 = (2n + 1)^3 = 8n^3 + 12n^2 + 6n + 1 = 2(4n^3 + 6n^2 + 3n) + 1$. This shows that a^3 is twice an integer, plus 1, so a^3 is odd. Thus we've proved that if a is odd then a^3 is odd.

Conversely we need to show that if a^3 is odd, then a is odd. For this we employ contrapositive proof. Suppose a is not odd. Thus a is even, so $a = 2n$ for some integer n . Then $a^3 = (2n)^3 = 8n^3 = 2(4n^3)$ is even (not odd). ■

7. Suppose $x, y \in \mathbb{R}$. Then $(x + y)^2 = x^2 + y^2$ if and only if $x = 0$ or $y = 0$.

Proof. First we prove with direct proof that if $(x + y)^2 = x^2 + y^2$, then $x = 0$ or $y = 0$. Suppose $(x + y)^2 = x^2 + y^2$. From this we get $x^2 + 2xy + y^2 = x^2 + y^2$, so $2xy = 0$, and hence $xy = 0$. Thus $x = 0$ or $y = 0$.

Conversely, we need to show that if $x = 0$ or $y = 0$, then $(x + y)^2 = x^2 + y^2$. This will be done with cases.

Case 1. If $x = 0$ then $(x + y)^2 = (0 + y)^2 = y^2 = 0^2 + y^2 = x^2 + y^2$.

Case 2. If $y = 0$ then $(x + y)^2 = (x + 0)^2 = x^2 = x^2 + 0^2 = x^2 + y^2$.

Either way, we have $(x + y)^2 = x^2 + y^2$. ■

9. Suppose $a \in \mathbb{Z}$. Prove that $14 \mid a$ if and only if $7 \mid a$ and $2 \mid a$.

Proof. First we prove that if $14 \mid a$, then $7 \mid a$ and $2 \mid a$. Direct proof is used. Suppose $14 \mid a$. This means $a = 14m$ for some integer m . Therefore $a = 7(2m)$, which means $7 \mid a$, and also $a = 2(7m)$, which means $2 \mid a$. Thus $7 \mid a$ and $2 \mid a$.

Conversely, we need to prove that if $7 \mid a$ and $2 \mid a$, then $14 \mid a$. Once again direct proof is used. Suppose $7 \mid a$ and $2 \mid a$. Since $2 \mid a$ it follows that $a = 2m$ for some integer m , and that in turn implies that a is even. Since $7 \mid a$ it follows that $a = 7n$ for some integer n . Now, since a is known to be even, and $a = 7n$, it follows that n is even (if it were odd, then $a = 7n$ would be odd). Thus $n = 2p$ for an appropriate integer p , and plugging $n = 2p$ back into $a = 7n$ gives $a = 7(2p)$, so $a = 14p$. Therefore $14 \mid a$. ■

11. Suppose $a, b \in \mathbb{Z}$. Prove that $(a - 3)b^2$ is even if and only if a is odd or b is even.

Proof. First we will prove that if $(a - 3)b^2$ is even, then a is odd or b is even. For this we use contrapositive proof. Suppose it is not the case that a is odd or b is even. Then by DeMorgan's law, a is even and b is odd. Thus there are integers m and n for which $a = 2m$ and $b = 2n + 1$. Now observe $(a - 3)b^2 = (2m - 3)(2n + 1)^2 = (2m - 3)(4n^2 + 4n + 1) = 8mn^2 + 8mn + 2m - 12n^2 - 12n - 3 = 8mn^2 + 8mn + 2m - 12n^2 - 12n - 4 + 1 = 2(4mn^2 + 4mn + m - 6n^2 - 6n - 2) + 1$. This shows $(a - 3)b^2$ is odd, so it's not even.

Conversely, we need to show that if a is odd or b is even, then $(a - 3)b^2$ is even. For this we use direct proof, with cases.

Case 1. Suppose a is odd. Then $a = 2m + 1$ for some integer m . Thus $(a - 3)b^2 = (2m + 1 - 3)b^2 = (2m - 2)b^2 = 2(m - 1)b^2$. Thus in this case $(a - 3)b^2$ is even.

Case 2. Suppose b is even. Then $b = 2n$ for some integer n . Thus $(a - 3)b^2 = (a - 3)(2n)^2 = (a - 3)4n^2 = 2(a - 3)2n^2$. Thus in this case $(a - 3)b^2$ is even.

Therefore, in any event, $(a - 3)b^2$ is even. ■

13. Suppose $a, b \in \mathbb{Z}$. If $a + b$ is odd, then $a^2 + b^2$ is odd.

Hint: Use direct proof. Suppose $a + b$ is odd. Argue that this means a and b have opposite parity. Then use cases.

15. Suppose $a, b \in \mathbb{Z}$. Prove that $a + b$ is even if and only if a and b have the same parity.

Proof. First we will show that if $a + b$ is even, then a and b have the same parity. For this we use contrapositive proof. Suppose it is not the case that a and b have the same parity. Then one of a and b is even and the other is odd. Without loss of generality, let's say that a is even and b is odd. Thus there are integers m and n for which $a = 2m$ and $b = 2n + 1$. Then $a + b = 2m + 2n + 1 = 2(m + n) + 1$, so $a + b$ is odd, not even.

Conversely, we need to show that if a and b have the same parity, then $a + b$ is even. For this, we use direct proof with cases. Suppose a and b have the same parity.

Case 1. Both a and b are even. Then there are integers m and n for which $a = 2m$ and $b = 2n$, so $a + b = 2m + 2n = 2(m + n)$ is clearly even.

Case 2. Both a and b are odd. Then there are integers m and n for which $a = 2m + 1$ and $b = 2n + 1$, so $a + b = 2m + 1 + 2n + 1 = 2(m + n + 1)$ is clearly even.

Either way, $a + b$ is even. This completes the proof. ■

17. There is a prime number between 90 and 100.

Proof. Simply observe that 97 is prime. ■

19. If $n \in \mathbb{N}$, then $2^0 + 2^1 + 2^2 + 2^3 + 2^4 + \dots + 2^n = 2^{n+1} - 1$.

Proof. We use direct proof. Suppose $n \in \mathbb{N}$. Let S be the number

$$S = 2^0 + 2^1 + 2^2 + 2^3 + 2^4 + \dots + 2^{n-1} + 2^n. \quad (1)$$

In what follows, we will solve for S and show $S = 2^{n+1} - 1$. Multiplying both sides of (1) by 2 gives

$$2S = 2^1 + 2^2 + 2^3 + 2^4 + 2^5 + \dots + 2^n + 2^{n+1}. \quad (2)$$

Now subtract Equation (1) from Equation (2) to obtain $2S - S = -2^0 + 2^{n+1}$, which simplifies to $S = 2^{n+1} - 1$. Combining this with Equation (1) produces $2^0 + 2^1 + 2^2 + 2^3 + 2^4 + \dots + 2^n = 2^{n+1} - 1$, so the proof is complete. ■

21. Every real solution of $x^3 + x + 3 = 0$ is irrational.

Proof. Suppose for the sake of contradiction that this polynomial has a rational solution $\frac{a}{b}$. We may assume that this fraction is fully reduced, so a and b are not both even. We have $(\frac{a}{b})^3 + \frac{a}{b} + 3 = 0$. Clearing the denominator gives

$$a^3 + ab^2 + 3b^3 = 0.$$

Consider two cases: First, if both a and b are odd, the left-hand side is a sum of three odds, which is odd, meaning 0 is odd, a contradiction. Second, if one of a and b is odd and the other is even, then the middle term of $a^3 + ab^2 + 3b^3$ is even, while a^3 and $3b^3$ have opposite parity. Then $a^3 + ab^2 + 3b^3$ is the sum of two evens and an odd, which is odd, again contradicting the fact that 0 is even. ■

23. Suppose a, b and c are integers. If $a \mid b$ and $a \mid (b^2 - c)$, then $a \mid c$.

Proof. (Direct) Suppose $a \mid b$ and $a \mid (b^2 - c)$. This means that $b = ad$ and $b^2 - c = ae$ for some integers d and e . Squaring the first equation produces $b^2 = a^2d^2$. Subtracting $b^2 - c = ae$ from $b^2 = a^2d^2$ gives $c = a^2d^2 - ae = a(ad^2 - e)$. As $ad^2 - e \in \mathbb{Z}$, it follows that $a \mid c$. ■

25. If $p > 1$ is an integer and $n \nmid p$ for each integer n for which $2 \leq n \leq \sqrt{p}$, then p is prime.

Proof. (Contrapositive) Suppose that p is not prime, so it factors as $p = mn$ for $1 < m, n < p$.

Observe that it is not the case that both $m > \sqrt{p}$ and $n > \sqrt{p}$, because if this were true the inequalities would multiply to give $mn > \sqrt{p}\sqrt{p} = p$, which contradicts $p = mn$.

Therefore $m \leq \sqrt{p}$ or $n \leq \sqrt{p}$. Without loss of generality, say $n \leq \sqrt{p}$. Then the equation $p = mn$ gives $n \mid p$, with $1 < n \leq \sqrt{p}$. Therefore it is not true that $n \nmid p$ for each integer n for which $2 \leq n \leq \sqrt{p}$. ■

27. Suppose $a, b \in \mathbb{Z}$. If $a^2 + b^2$ is a perfect square, then a and b are not both odd.

Proof. (Contradiction) Suppose $a^2 + b^2$ is a perfect square, and a and b are both odd. As $a^2 + b^2$ is a perfect square, say c is the integer for which $c^2 = a^2 + b^2$. As a and b are odd, we have $a = 2m + 1$ and $b = 2n + 1$ for integers m and n . Then

$$c^2 = a^2 + b^2 = (2m + 1)^2 + (2n + 1)^2 = 4(m^2 + n^2 + mn) + 2.$$

This is even, so c is even also; let $c = 2k$. Now the above equation results in $(2k)^2 = 4(m^2 + n^2 + mn) + 2$, which simplifies to $2k^2 = 2(m^2 + n^2 + mn) + 1$. Thus $2k^2$ is both even and odd, a contradiction. ■

29. If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.

Proof. (Direct) Suppose $a \mid bc$ and $\gcd(a, b) = 1$. The fact that $a \mid bc$ means $bc = az$ for some integer z . The fact that $\gcd(a, b) = 1$ means that $ax + by = 1$ for some integers x and y (by Proposition 12.1 on page 300). From this we get $acx + bcy = c$; substituting $bc = az$ yields $acx + azy = c$, that is, $a(cx + zy) = c$. Therefore $a \mid c$. ■

31. If $n \in \mathbb{Z}$, then $\gcd(n, n + 1) = 1$.

Proof. Suppose d is a positive integer that is a common divisor of n and $n + 1$. Then $n = dx$ and $n + 1 = dy$ for integers x and y . Then $1 = (n + 1) - n = dy - dx = d(y - x)$. Now, $1 = d(y - x)$ is only possible if $d = \pm 1$ and $y - x = \pm 1$. Thus the greatest common divisor of n and $n + 1$ can be no greater than 1. But 1 does divide both n and $n + 1$, so $\gcd(n, n + 1) = 1$. ■

33. If $n \in \mathbb{Z}$, then $\gcd(2n + 1, 4n^2 + 1) = 1$.

Proof. Note that $4n^2 + 1 = (2n + 1)(2n - 1) + 2$. Therefore, it suffices to show that $\gcd(2n + 1, (2n + 1)(2n - 1) + 2) = 1$. Let d be a common positive divisor of both $2n + 1$ and $(2n + 1)(2n - 1) + 2$, so $2n + 1 = dx$ and $(2n + 1)(2n - 1) + 2 = dy$ for integers x and y . Substituting the first equation into the second gives $dx(2n - 1) + 2 = dy$, so $2 = dy - dx(2n - 1) = d(y - 2nx - x)$. This means d divides 2, so d equals 1 or 2. But the equation $2n + 1 = dx$ means d must be odd. Therefore $d = 1$, that is, $\gcd(2n + 1, (2n + 1)(2n - 1) + 2) = 1$. ■

35. Suppose $a, b \in \mathbb{N}$. Then $a = \gcd(a, b)$ if and only if $a \mid b$.

Proof. Suppose $a = \gcd(a, b)$. This means a is a divisor of both a and b . In particular $a \mid b$.

Conversely, suppose $a \mid b$. Then a divides both a and b , so $a \leq \gcd(a, b)$. On the other hand, since $\gcd(a, b)$ divides a , we have $a = \gcd(a, b) \cdot x$ for some integer x . As all integers involved are positive, it follows that $a \geq \gcd(a, b)$.

It has been established that $a \leq \gcd(a, b)$ and $a \geq \gcd(a, b)$. Thus $a = \gcd(a, b)$. ■

37. Suppose A and B are sets. Prove $A \subseteq B$ if and only if $A - B = \emptyset$.

Proof. First we will prove that if $A \subseteq B$, then $A - B = \emptyset$. Contrapositive proof is used. Suppose that $A - B \neq \emptyset$. Thus there is an element $a \in A - B$, which means $a \in A$ but $a \notin B$. Since not every element of A is in B , we have $A \not\subseteq B$.

Conversely, we will prove that if $A - B = \emptyset$, then $A \subseteq B$. Again, contrapositive proof is used. Suppose $A \not\subseteq B$. This means that it is not the case that every element of A is an element of B , so there is an element $a \in A$ with $a \notin B$. Therefore we have $a \in A - B$, so $A - B \neq \emptyset$. ■

39. Suppose $A \neq \emptyset$. Prove that $A \times B \subseteq A \times C$, if and only if $B \subseteq C$.

Proof. First we will prove that if $A \times B \subseteq A \times C$, then $B \subseteq C$. Using contrapositive, suppose that $B \not\subseteq C$. This means there is an element $b \in B$ with $b \notin C$. Since $A \neq \emptyset$, there exists an element $a \in A$. Now consider the ordered pair (a, b) . Note that $(a, b) \in A \times B$, but $(a, b) \notin A \times C$. This means $A \times B \not\subseteq A \times C$.

Conversely, we will now show that if $B \subseteq C$, then $A \times B \subseteq A \times C$. We use direct proof. Suppose $B \subseteq C$. Assume that $(a, b) \in A \times B$. This means $a \in A$ and $b \in B$. But, as $B \subseteq C$, we also have $b \in C$. From $a \in A$ and $b \in C$, we get $(a, b) \in A \times C$. We've now shown $(a, b) \in A \times B$ implies $(a, b) \in A \times C$, so $A \times B \subseteq A \times C$. ■

Disproof

Ever since Chapter 8 we have dealt with one major theme: Given a statement, prove that it is true. In every example and exercise we were handed a true statement and charged with the task of proving it. Have you ever wondered what would happen if you were given a *false* statement to prove? The answer is that no (correct) proof would be possible, for if it were, the statement would be true, not false.

But how would you convince someone that a statement is false? The mere fact that you could not produce a proof does not automatically mean the statement is false, for you know (perhaps all too well) that proofs can be difficult to construct. It turns out that there is a very simple and utterly convincing procedure that proves a statement is false. The process of carrying out this procedure is called **disproof**. Thus, this chapter is concerned with **disproving** statements.

Before describing the new method, we will set the stage with some relevant background information. First, we point out that mathematical statements can be divided into three categories, described below.

One category consists of all those statements that have been proved to be true. For the most part we regard these statements as significant enough to be designated with special names such as “theorem,” “proposition,” “lemma” and “corollary.” Some examples of statements in this category are listed in the left-hand box in the diagram on the following page. There are also some wholly uninteresting statements (such as $2 = 2$) in this category, and although we acknowledge their existence we certainly do not dignify them with terms such as “theorem” or “proposition.”

At the other extreme is a category consisting of statements that are known to be false. Examples are listed in the box on the right. Since mathematicians are not very interested in them, these types of statements do not get any special names, other than the blanket term “false statement.”

But there is a third (and quite interesting) category between these two extremes. It consists of statements whose truth or falsity has not been determined. Examples include things like “*Every perfect number*

is even,” or “Every even integer greater than 2 is the sum of two primes.” (The latter statement is called the *Goldbach conjecture*. See Section 3.1.) Mathematicians have a special name for the statements in this category that they suspect (but haven’t yet proved) are true. Such statements are called **conjectures**.

THREE TYPES OF STATEMENTS:

| Known to be true (Theorems & propositions) | Truth unknown (Conjectures) | Known to be false |
|---|--|---|
| <p>Examples:</p> <ul style="list-style-type: none"> • Pythagorean theorem • Fermat’s last theorem (Section 3.1) • The square of an odd number is odd. • The series $\sum_{k=1}^{\infty} \frac{1}{k}$ diverges. | <p>Examples:</p> <ul style="list-style-type: none"> • All perfect numbers are even. • Any even number greater than 2 is the sum of two primes. (Goldbach’s conjecture, Section 3.1) • There are infinitely many prime numbers of form $2^n - 1$, with $n \in \mathbb{N}$. | <p>Examples:</p> <ul style="list-style-type: none"> • All prime numbers are odd. • Some quadratic equations have three solutions. • $0 = 1$ • There exist natural numbers a, b and c for which $a^3 + b^3 = c^3$. |

Mathematicians spend much of their time and energy attempting to prove or disprove conjectures. (They also expend considerable mental energy in creating new conjectures based on collected evidence or intuition.) When a conjecture is proved (or disproved) the proof or disproof will typically appear in a published paper, provided the conjecture is of sufficient interest. If it is proved, the conjecture attains the status of a theorem or proposition. If it is disproved, then no one is really very interested in it anymore—mathematicians do not care much for false statements.

Most conjectures that mathematicians are interested in are quite difficult to prove or disprove. We are not at that level yet. In this text, the “conjectures” that you will encounter are the kinds of statements that an experienced mathematician would immediately spot as true or false, but you may have to do some work before figuring out a proof or disproof. But in keeping with the cloud of uncertainty that surrounds conjectures at the advanced levels of mathematics, most exercises in this chapter (and many beyond it) will ask you to prove or disprove statements without giving any hint as to whether they are true or false. Your job will be to decide whether or not they are true and to either prove or disprove them. The examples in this chapter will illustrate the processes one typically goes through in deciding whether a statement is true or false, and then verifying that it’s true or false.

You know the three major methods of proving a statement: direct proof, contrapositive proof and proof by contradiction. Now we are ready to understand the method of disproving a statement. Suppose you want to disprove a statement P . In other words you want to prove that P is *false*. The way to do this is to prove that $\sim P$ is *true*, for if $\sim P$ is true, it follows immediately that P has to be false.

How to disprove P : Prove $\sim P$.

Our approach is incredibly simple. To disprove P , prove $\sim P$. In theory, this proof can be carried out by direct, contrapositive or contradiction approaches. However, in practice things can be even easier than that if we are disproving a universally quantified statement or a conditional statement. That is our next topic.

13.1 Disproving Universal Statements: Counterexamples

A conjecture may be described as a statement that we hope is a theorem. As we know, many theorems (hence many conjectures) are universally quantified statements. Thus it seems reasonable to begin our discussion by investigating how to disprove a universally quantified statement such as

$$\forall x \in S, P(x).$$

To disprove this statement, we must prove its negation. Its negation is

$$\sim (\forall x \in S, P(x)) = \exists x \in S, \sim P(x).$$

The negation is an existence statement. To prove the negation is true, we just need to produce an *example* of an $x \in S$ that makes $\sim P(x)$ true, that is, an x that makes $P(x)$ false. This leads to the following outline for disproving a universally quantified statement.

How to disprove $\forall x \in S, P(x)$.

Produce an example of an $x \in S$
that makes $P(x)$ false.

Things are even simpler if we want to disprove a conditional statement $P(x) \Rightarrow Q(x)$. This statement asserts that for every x that makes $P(x)$ true, $Q(x)$ will also be true. The statement can only be false if there is an x that makes $P(x)$ true and $Q(x)$ false. This leads to our next outline for disproof.

How to disprove $P(x) \Rightarrow Q(x)$.

Produce an example of an x that makes $P(x)$ true and $Q(x)$ false.

In both of the above outlines, the statement is disproved simply by exhibiting an example that shows the statement is not always true. (Think of it as an example that proves the statement is a promise that can be broken.) There is a special name for an example that disproves a statement: It is called a **counterexample**.

Example 13.1 As our first example, we will work through the process of deciding whether or not the following conjecture is true.

Conjecture: For every $n \in \mathbb{Z}$, the integer $f(n) = n^2 - n + 11$ is prime.

In resolving the truth or falsity of a conjecture, it's a good idea to gather as much information about the conjecture as possible. In this case let's start by making a table that tallies the values of $f(n)$ for some integers n .

| | | | | | | | | | | | | | | |
|--------|----|----|----|----|----|----|----|----|----|----|----|----|----|-----|
| n | -3 | -2 | -1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| $f(n)$ | 23 | 17 | 13 | 11 | 11 | 13 | 17 | 23 | 31 | 41 | 53 | 67 | 83 | 101 |

In every case, $f(n)$ is prime, so you may begin to suspect that the conjecture is true. Before attempting a proof, let's try one more n . Unfortunately, $f(11) = 11^2 - 11 + 11 = 11^2$ is not prime. The conjecture is false because $n = 11$ is a counterexample. We summarize our disproof as follows:

Disproof. The statement “For every $n \in \mathbb{Z}$, the integer $f(n) = n^2 - n + 11$ is prime,” is **false**. For a counterexample, note that for $n = 11$, the integer $f(11) = 121 = 11 \cdot 11$ is not prime. ■

In disproving a statement with a counterexample, it is important to explain exactly how the counterexample makes the statement false. Our work would not have been complete if we had just said “for a counterexample, consider $n = 11$,” and left it at that. We need to show that the answer $f(11)$ is not prime. Showing the factorization $f(11) = 11 \cdot 11$ suffices for this.

Example 13.2 Either prove or disprove the following conjecture.

Conjecture If A , B and C are sets, then $A - (B \cap C) = (A - B) \cap (A - C)$.

Disproof. This conjecture is false because of the following counterexample. Let $A = \{1, 2, 3\}$, $B = \{1, 2\}$ and $C = \{2, 3\}$. Notice that $A - (B \cap C) = \{1, 3\}$ and $(A - B) \cap (A - C) = \emptyset$, so $A - (B \cap C) \neq (A - B) \cap (A - C)$. ■

(To see where this counterexample came from, draw Venn diagrams for $A - (B \cap C)$ and $(A - B) \cap (A - C)$. You will see that the diagrams are different. The numbers 1, 2 and 3 can then be inserted into the regions of the diagrams in such a way as to create the above counterexample.)

13.2 Disproving Existence Statements

We have seen that we can disprove a universally quantified statement or a conditional statement simply by finding a counterexample. Now let's turn to the problem of disproving an existence statement such as

$$\exists x \in S, P(x).$$

Proving this would involve simply finding an example of an x that makes $P(x)$ true. To *disprove* it, we have to prove its negation $\sim(\exists x \in S, P(x)) = \forall x \in S, \sim P(x)$. But this negation is universally quantified. Proving *it* involves showing that $\sim P(x)$ is true for *all* $x \in S$, and for this an example does not suffice. Instead we must use direct, contrapositive or contradiction proof to prove the conditional statement “If $x \in S$, then $\sim P(x)$.” As an example, here is a conjecture to either prove or disprove.

Example 13.3 Either prove or disprove the following conjecture.

Conjecture: There is a real number x for which $x^4 < x < x^2$.

This may not seem like an unreasonable statement at first glance. After all, if the statement were asserting the existence of a real number for which $x^3 < x < x^2$, then it would be true: just take $x = -2$. But it asserts there is an x for which $x^4 < x < x^2$. When we apply some intelligent guessing to locate such an x we run into trouble. If $x = \frac{1}{2}$, then $x^4 < x$, but we don't have $x < x^2$; similarly if $x = 2$, we have $x < x^2$ but not $x^4 < x$. Since finding an x with $x^4 < x < x^2$ seems problematic, we may begin to suspect that the given statement is false.

Let's see if we can disprove it. According to our strategy for disproof, to *disprove* it we must *prove* its negation. Symbolically, the statement is

$\exists x \in \mathbb{R}, x^4 < x < x^2$, so its negation is

$$\sim (\exists x \in \mathbb{R}, x^4 < x < x^2) = \forall x \in \mathbb{R}, \sim (x^4 < x < x^2).$$

Thus, in words the negation is:

For every real number x , it is not the case that $x^4 < x < x^2$.

This can be proved with contradiction, as follows. Suppose for the sake of contradiction that there **is** an x for which $x^4 < x < x^2$. Then x must be positive since it's greater than the non-negative number x^4 . Dividing all parts of $x^4 < x < x^2$ by the positive number x produces $x^3 < 1 < x$. Now subtract 1 from all parts of $x^3 < 1 < x$ to obtain $x^3 - 1 < 0 < x - 1$ and reason as follows:

$$\begin{aligned} x^3 - 1 &< 0 < x - 1 \\ (x - 1)(x^2 + x + 1) &< 0 < (x - 1) \\ x^2 + x + 1 &< 0 < 1 \end{aligned}$$

(Division by $x - 1$ did not reverse the inequality $<$ because the second line above shows $0 < x - 1$, that is, $x - 1$ is positive.) Now we have $x^2 + x + 1 < 0$, which is a contradiction because x being positive forces $x^2 + x + 1 > 0$

We summarize our work as follows.

The statement “*There is a real number x for which $x^4 < x < x^2$* ” is **false** because we have proved its negation “*For every real number x , it is not the case that $x^4 < x < x^2$.*”

As you work the exercises, keep in mind that not every conjecture will be false. If one is true, then a disproof is impossible and you must produce a proof. Here is an example:

Example 13.4 Either prove or disprove the following conjecture.

Conjecture There exist three integers x, y, z , all greater than 1 and no two equal, for which $x^y = y^z$.

This conjecture is true. It is an existence statement, so to prove it we just need to give an example of three integers x, y, z , all greater than 1 and no two equal, so that $x^y = y^z$. A proof follows.

Proof. Note that if $x = 2$, $y = 16$ and $z = 4$, then $x^y = 2^{16} = (2^4)^4 = 16^4 = y^z$. ■

13.3 Disproof by Contradiction

Contradiction can be a very useful way to disprove a statement. To see how this works, suppose we wish to disprove a statement P . We know that to disprove P , we must *prove* $\sim P$. To prove $\sim P$ with contradiction, we assume $\sim\sim P$ is true and deduce a contradiction. But since $\sim\sim P = P$, this boils down to assuming P is true and deducing a contradiction. Here is an outline:

How to disprove P with contradiction:

Assume P is true, and deduce a contradiction.

To illustrate this, let's revisit Example 13.3 but do the disproof with contradiction. You will notice that the work duplicates much of what we did in Example 13.3, but is it much more streamlined because here we do not have to negate the conjecture.

Example 13.5 Disprove the following conjecture.

Conjecture: There is a real number x for which $x^4 < x < x^2$.

Disproof. Suppose for the sake of contradiction that this conjecture is true. Let x be a real number for which $x^4 < x < x^2$. Then x is positive, since it is greater than the non-negative number x^4 . Dividing all parts of $x^4 < x < x^2$ by the positive number x produces $x^3 < 1 < x$. Now subtract 1 from all parts of $x^3 < 1 < x$ to obtain $x^3 - 1 < 0 < x - 1$ and reason as follows:

$$\begin{aligned} x^3 - 1 &< 0 < x - 1 \\ (x - 1)(x^2 + x + 1) &< 0 < (x - 1) \\ x^2 + x + 1 &< 0 < 1 \end{aligned}$$

Now we have $x^2 + x + 1 < 0$, which is a contradiction because x is positive. Thus the conjecture must be false. ■

Exercises for Chapter 13

Each of the following statements is either true or false. If a statement is true, prove it. If a statement is false, disprove it. These exercises are cumulative, covering all topics addressed in Chapters 2–13.

1. If $x, y \in \mathbb{R}$, then $|x + y| = |x| + |y|$.
2. For every natural number n , the integer $2n^2 - 4n + 31$ is prime.

3. If $n \in \mathbb{Z}$ and $n^5 - n$ is even, then n is even.
4. For every natural number n , the integer $n^2 + 17n + 17$ is prime.
5. If A, B, C and D are sets, then $(A \times B) \cup (C \times D) = (A \cup C) \times (B \cup D)$.
6. If A, B, C and D are sets, then $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$.
7. If A, B and C are sets, and $A \times C = B \times C$, then $A = B$.
8. If A, B and C are sets, then $A - (B \cup C) = (A - B) \cap (A - C)$.
9. If A and B are sets, then $\mathcal{P}(A) - \mathcal{P}(B) \subseteq \mathcal{P}(A - B)$.
10. If A and B are sets and $A \cap B = \emptyset$, then $\mathcal{P}(A) - \mathcal{P}(B) \subseteq \mathcal{P}(A - B)$.
11. If $a, b \in \mathbb{N}$, then $a + b < ab$.
12. If $a, b, c \in \mathbb{N}$ and ab, bc and ac all have the same parity, then a, b and c all have the same parity.
13. There exists a set X for which $\mathbb{R} \subseteq X$ and $\emptyset \in X$.
14. If A and B are sets, then $\mathcal{P}(A) \cap \mathcal{P}(B) = \mathcal{P}(A \cap B)$.
15. Every odd integer is the sum of three odd integers.
16. If A and B are finite sets, then $|A \cup B| = |A| + |B|$.
17. For all sets A and B , if $A - B = \emptyset$, then $B \neq \emptyset$.
18. If $a, b, c \in \mathbb{N}$, then at least one of $a - b, a + c$ and $b - c$ is even.
19. For every $r, s \in \mathbb{Q}$ with $r < s$, there is an irrational number u for which $r < u < s$.
20. There exist prime numbers p and q for which $p - q = 1000$.
21. There exist prime numbers p and q for which $p - q = 97$.
22. If p and q are prime numbers for which $p < q$, then $2p + q^2$ is odd.
23. If $x, y \in \mathbb{R}$ and $x^3 < y^3$, then $x < y$.
24. The inequality $2^x \geq x + 1$ is true for all positive real numbers x .
25. For all $a, b, c \in \mathbb{Z}$, if $a | bc$, then $a | b$ or $a | c$.
26. Suppose A, B and C are sets. If $A = B - C$, then $B = A \cup C$.
27. The equation $x^2 = 2^x$ has three real solutions.
28. Suppose $a, b \in \mathbb{Z}$. If $a | b$ and $b | a$, then $a = b$.
29. If $x, y \in \mathbb{R}$ and $|x + y| = |x - y|$, then $y = 0$.
30. There exist integers a and b for which $42a + 7b = 1$.
31. No number (other than 1) appears in Pascal's triangle more than four times.
32. If $n, k \in \mathbb{N}$ and $\binom{n}{k}$ is a prime number, then $k = 1$ or $k = n - 1$.
33. Suppose $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ is a polynomial of degree 1 or greater, and for which each coefficient a_i is in \mathbb{N} . Then there is an $n \in \mathbb{N}$ for which the integer $f(n)$ is not prime.
34. If $X \subseteq A \cup B$, then $X \subseteq A$ or $X \subseteq B$.

13.4 Solutions for Chapter 13

1. If $x, y \in \mathbb{R}$, then $|x + y| = |x| + |y|$.
This is **false**.
Disproof: Here is a counterexample: Let $x = 1$ and $y = -1$. Then $|x + y| = 0$ and $|x| + |y| = 2$, so it's not true that $|x + y| = |x| + |y|$.
3. If $n \in \mathbb{Z}$ and $n^5 - n$ is even, then n is even.
This is **false**.
Disproof: Here is a counterexample: Let $n = 3$. Then $n^5 - n = 3^5 - 3 = 240$, but n is not even.
5. If A, B, C and D are sets, then $(A \times B) \cup (C \times D) = (A \cup C) \times (B \cup D)$.
This is **false**.
Disproof: Here is a counterexample: Let $A = \{1, 2\}$, $B = \{1, 2\}$, $C = \{2, 3\}$ and $D = \{2, 3\}$. Then $(A \times B) \cup (C \times D) = \{(1, 1), (1, 2), (2, 1), (2, 2)\} \cup \{(2, 2), (2, 3), (3, 2), (3, 3)\} = \{(1, 1), (1, 2), (2, 1), (2, 2), (2, 3), (3, 2), (3, 3)\}$. Also $(A \cup C) \times (B \cup D) = \{1, 2, 3\} \times \{1, 2, 3\} = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3)\}$, so you can see that $(A \times B) \cup (C \times D) \neq (A \cup C) \times (B \cup D)$.
7. If A, B and C are sets, and $A \times C = B \times C$, then $A = B$.
This is **false**.
Disproof: Here is a counterexample: Let $A = \{1\}$, $B = \{2\}$ and $C = \emptyset$. Then $A \times C = B \times C = \emptyset$, but $A \neq B$.
9. If A and B are sets, then $\mathcal{P}(A) - \mathcal{P}(B) \subseteq \mathcal{P}(A - B)$.
This is **false**.
Disproof: Here is a counterexample: Let $A = \{1, 2\}$ and $B = \{1\}$. Then $\mathcal{P}(A) - \mathcal{P}(B) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\} - \{\emptyset, \{1\}\} = \{\{2\}, \{1, 2\}\}$. Also $\mathcal{P}(A - B) = \mathcal{P}(\{2\}) = \{\emptyset, \{2\}\}$. In this example we have $\mathcal{P}(A) - \mathcal{P}(B) \not\subseteq \mathcal{P}(A - B)$.
11. If $a, b \in \mathbb{N}$, then $a + b < ab$.
This is **false**.
Disproof: Here is a counterexample: Let $a = 1$ and $b = 1$. Then $a + b = 2$ and $ab = 1$, so it's not true that $a + b < ab$.
13. There exists a set X for which $\mathbb{R} \subseteq X$ and $\emptyset \in X$. This is **true**.
Proof. Simply let $X = \mathbb{R} \cup \{\emptyset\}$. If $x \in \mathbb{R}$, then $x \in \mathbb{R} \cup \{\emptyset\} = X$, so $\mathbb{R} \subseteq X$. Likewise, $\emptyset \in \mathbb{R} \cup \{\emptyset\} = X$ because $\emptyset \in \{\emptyset\}$. ■
15. Every odd integer is the sum of three odd integers. This is **true**.
Proof. Suppose n is odd. Then $n = n + 1 + (-1)$, and therefore n is the sum of three odd integers. ■
17. For all sets A and B , if $A - B = \emptyset$, then $B \neq \emptyset$.
This is **false**.
Disproof: Here is a counterexample: Just let $A = \emptyset$ and $B = \emptyset$. Then $A - B = \emptyset$, but it's not true that $B \neq \emptyset$.

19. For every $r, s \in \mathbb{Q}$ with $r < s$, there is an irrational number u for which $r < u < s$. This is **true**.

Proof. (Direct) Suppose $r, s \in \mathbb{Q}$ with $r < s$. Consider the number $u = r + \sqrt{2}\frac{s-r}{2}$. In what follows we will show that u is irrational and $r < u < s$. Certainly since $s - r$ is positive, it follows that $r < r + \sqrt{2}\frac{s-r}{2} = u$. Also, since $\sqrt{2} < 2$ we have

$$u = r + \sqrt{2}\frac{s-r}{2} < r + 2\frac{s-r}{2} = s,$$

and therefore $u < s$. Thus we can conclude $r < u < s$.

Now we just need to show that u is irrational. Suppose for the sake of contradiction that u is rational. Then $u = \frac{a}{b}$ for some integers a and b . Since r and s are rational, we have $r = \frac{c}{d}$ and $s = \frac{e}{f}$ for some $c, d, e, f \in \mathbb{Z}$. Now we have

$$\begin{aligned} u &= r + \sqrt{2}\frac{s-r}{2} \\ \frac{a}{b} &= \frac{c}{d} + \sqrt{2}\frac{\frac{e}{f} - \frac{c}{d}}{2} \\ \frac{ad-bc}{bd} &= \sqrt{2}\frac{ed-cf}{2df} \\ \frac{(ad-bc)2df}{bd(ed-cf)} &= \sqrt{2} \end{aligned}$$

This expresses $\sqrt{2}$ as a quotient of two integers, so $\sqrt{2}$ is rational, a contradiction. Thus u is irrational.

In summary, we have produced an irrational number u with $r < u < s$, so the proof is complete. ■

21. There exist two prime numbers p and q for which $p - q = 97$. This statement is **false**.

Disproof: Suppose for the sake of contradiction that this is true. Let p and q be prime numbers for which $p - q = 97$. Now, since their difference is odd, p and q must have opposite parity, so one of p and q is even and the other is odd. But there exists only one even prime number (namely 2), so either $p = 2$ or $q = 2$. If $p = 2$, then $p - q = 97$ implies $q = 2 - 97 = -95$, which is not prime. On the other hand if $q = 2$, then $p - q = 97$ implies $p = 99$, but that's not prime either. Thus one of p or q is not prime, a contradiction.

23. If $x, y \in \mathbb{R}$ and $x^3 < y^3$, then $x < y$. This is **true**.

Proof. (Contrapositive) Suppose $x \geq y$. We need to show $x^3 \geq y^3$.

Case 1. Suppose x and y have opposite signs, that is one of x and y is positive and the other is negative. Then since $x \geq y$, x is positive and y is negative. Then, since the powers are odd, x^3 is positive and y^3 is negative, so $x^3 \geq y^3$.

Case 2. Suppose x and y do not have opposite signs. Then $x^2 + xy + y^2 \geq 0$ and

also $x - y \geq 0$ because $x \geq y$. Thus we have $x^3 - y^3 = (x - y)(x^2 + xy + y^2) \geq 0$. From this we get $x^3 - y^3 \geq 0$, so $x^3 \geq y^3$.

In either case we have $x^3 \geq y^3$. ■

- 25.** For all $a, b, c \in \mathbb{Z}$, if $a \mid bc$, then $a \mid b$ or $a \mid c$.

This is **false**.

Disproof: Let $a = 6$, $b = 3$ and $c = 4$. Note that $a \mid bc$, but $a \nmid b$ and $a \nmid c$.

- 27.** The equation $x^2 = 2^x$ has three real solutions.

Proof. By inspection, the numbers $x = 2$ and $x = 4$ are two solutions of this equation. But there is a third solution. Let m be the real number for which $m2^m = \frac{1}{2}$. Then negative number $x = -2m$ is a solution, as follows.

$$x^2 = (-2m)^2 = 4m^2 = 4 \left(\frac{m2^m}{2^m} \right)^2 = 4 \left(\frac{\frac{1}{2}}{2^m} \right)^2 = \frac{1}{2^{2m}} = 2^{-2m} = 2^x.$$

Therefore we have three solutions 2, 4 and m . ■

- 29.** If $x, y \in \mathbb{R}$ and $|x + y| = |x - y|$, then $y = 0$.

This is **false**.

Disproof: Let $x = 0$ and $y = 1$. Then $|x + y| = |x - y|$, but $y = 1$.

- 31.** No number appears in Pascal's triangle more than four times.

Disproof: The number 120 appears six times. Check that $\binom{10}{3} = \binom{10}{7} = \binom{16}{2} = \binom{16}{14} = \binom{120}{1} = \binom{120}{119} = 120$.

- 33.** Suppose $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ is a polynomial of degree 1 or greater, and for which each coefficient a_i is in \mathbb{N} . Then there is an $n \in \mathbb{N}$ for which the integer $f(n)$ is not prime.

Proof. (Outline) Note that, because the coefficients are all positive and the degree is greater than 1, we have $f(1) > 1$. Let $b = f(1) > 1$. Now, the polynomial $f(x) - b$ has a root 1, so $f(x) - b = (x - 1)g(x)$ for some polynomial g . Then $f(x) = (x - 1)g(x) + b$. Now note that $f(b + 1) = b g(b) + b = b(g(b) + 1)$. If we can now show that $g(b) + 1$ is an integer, then we have a nontrivial factoring $f(b + 1) = b(g(b) + 1)$, and $f(b + 1)$ is not prime. To complete the proof, use the fact that $f(x) - b = (x - 1)g(x)$ has integer coefficients, and deduce that $g(x)$ must also have integer coefficients. ■

Mathematical Induction

This chapter explains a powerful proof technique called **mathematical induction** (or just **induction** for short). To motivate the discussion, let's first examine the kinds of statements that induction is used to prove. Consider the following statement.

Conjecture. The sum of the first n odd natural numbers equals n^2 .

The following table illustrates what this conjecture says. Each row is headed by a natural number n , followed by the sum of the first n odd natural numbers, followed by n^2 .

| n | sum of the first n odd natural numbers | n^2 |
|-----|--|-------|
| 1 | $1 = \dots\dots\dots$ | 1 |
| 2 | $1 + 3 = \dots\dots\dots$ | 4 |
| 3 | $1 + 3 + 5 = \dots\dots\dots$ | 9 |
| 4 | $1 + 3 + 5 + 7 = \dots\dots\dots$ | 16 |
| 5 | $1 + 3 + 5 + 7 + 9 = \dots\dots\dots$ | 25 |
| ⋮ | ⋮ | ⋮ |
| n | $1 + 3 + 5 + 7 + 9 + 11 + \dots + (2n - 1) = \dots\dots$ | n^2 |
| ⋮ | ⋮ | ⋮ |

Note that in the first five lines of the table, the sum of the first n odd numbers really does add up to n^2 . Notice also that these first five lines indicate that the n th odd natural number (the last number in each sum) is $2n - 1$. (For instance, when $n = 2$, the second odd natural number is $2 \cdot 2 - 1 = 3$; when $n = 3$, the third odd natural number is $2 \cdot 3 - 1 = 5$, etc.)

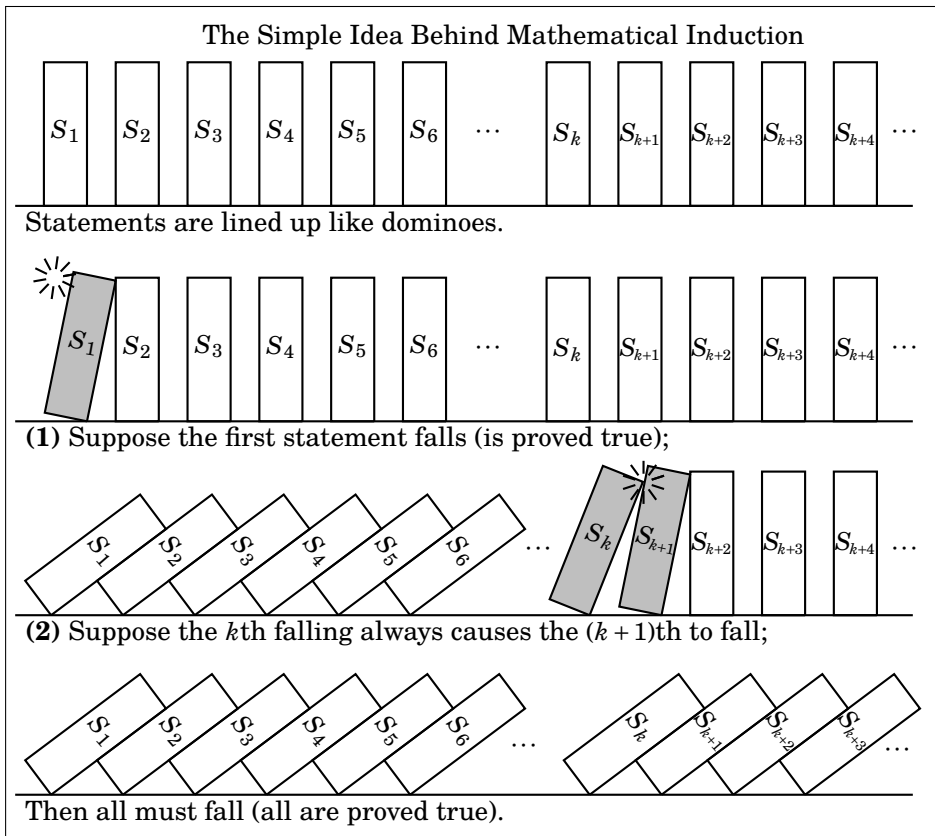
The table raises a question. Does the sum $1 + 3 + 5 + 7 + \dots + (2n - 1)$ really always equal n^2 ? In other words, is the conjecture true?

Let's rephrase this. For each natural number n (i.e., for each line of the table), we have a statement S_n , as follows:

$$\begin{aligned}
 S_1 &: 1 = 1^2 \\
 S_2 &: 1 + 3 = 2^2 \\
 S_3 &: 1 + 3 + 5 = 3^2 \\
 &\vdots \\
 S_n &: 1 + 3 + 5 + 7 + \cdots + (2n - 1) = n^2 \\
 &\vdots
 \end{aligned}$$

Our question is: Are all of these statements true?

Mathematical induction answers just this kind of question, where we have an infinite list of statements S_1, S_2, S_3, \dots that we want to prove true. The method is really quite simple. To visualize it, think of the statements as dominoes, lined up in a row. Suppose you can prove the first statement S_1 , and symbolize this as domino S_1 being knocked down. Also, say you can prove that any statement S_k being true (falling) forces the next statement S_{k+1} to be true (to fall). Then S_1 falls, knocking down S_2 . Next S_2 falls, knocking down S_3 , then S_3 knocks down S_4 , and so on. The inescapable conclusion is that all the statements are knocked down (proved true).



14.1 Proof by Induction

This domino analogy motivates an outline for our next major proof technique: *proof by mathematical induction*.

Outline for Proof by Induction

Proposition The statements $S_1, S_2, S_3, S_4, \dots$ are all true.

Proof. (Induction)

- (1) Prove that the first statement S_1 is true.
 - (2) Given any integer $k \geq 1$, prove that the statement $S_k \Rightarrow S_{k+1}$ is true.
- It follows by mathematical induction that every S_n is true. ■

In this setup, the first step (1) is called the **basis step**. Because S_1 is usually a very simple statement, the basis step is often quite easy to do. The second step (2) is called the **inductive step**. In the inductive step direct proof is most often used to prove $S_k \Rightarrow S_{k+1}$, so this step is usually carried out by assuming S_k is true and showing this forces S_{k+1} to be true. The assumption that S_k is true is called the **inductive hypothesis**.

Now let's apply this technique to our original conjecture that the sum of the first n odd natural numbers equals n^2 . Our goal is to show that for each $n \in \mathbb{N}$, the statement $S_n : 1 + 3 + 5 + 7 + \dots + (2n - 1) = n^2$ is true. Before getting started, observe that S_k is obtained from S_n by plugging k in for n . Thus S_k is the statement $S_k : 1 + 3 + 5 + 7 + \dots + (2k - 1) = k^2$. Also, we get S_{k+1} by plugging in $k + 1$ for n , so that $S_{k+1} : 1 + 3 + 5 + 7 + \dots + (2(k + 1) - 1) = (k + 1)^2$.

Proposition If $n \in \mathbb{N}$, then $1 + 3 + 5 + 7 + \dots + (2n - 1) = n^2$.

Proof. We will prove this with mathematical induction.

- (1) Observe that if $n = 1$, this statement is $1 = 1^2$, which is obviously true.
- (2) We must now prove $S_k \Rightarrow S_{k+1}$ for any $k \geq 1$. That is, we must show that if $1 + 3 + 5 + 7 + \dots + (2k - 1) = k^2$, then $1 + 3 + 5 + 7 + \dots + (2(k + 1) - 1) = (k + 1)^2$. We use direct proof. Suppose $1 + 3 + 5 + 7 + \dots + (2k - 1) = k^2$. Then

$$\begin{aligned}
 1 + 3 + 5 + 7 + \dots + (2(k + 1) - 1) &= \\
 1 + 3 + 5 + 7 + \dots + (2k - 1) + (2(k + 1) - 1) &= \\
 (1 + 3 + 5 + 7 + \dots + (2k - 1)) + (2(k + 1) - 1) &= \\
 k^2 + (2(k + 1) - 1) &= k^2 + 2k + 1 \\
 &= (k + 1)^2.
 \end{aligned}$$

Thus $1 + 3 + 5 + 7 + \dots + (2(k + 1) - 1) = (k + 1)^2$. This proves that $S_k \Rightarrow S_{k+1}$. It follows by induction that $1 + 3 + 5 + 7 + \dots + (2n - 1) = n^2$ for every $n \in \mathbb{N}$. ■

In induction proofs it is usually the case that the first statement S_1 is indexed by the natural number 1, but this need not always be so. Depending on the problem, the first statement could be S_0 , or S_m for any other integer m . In the next example the statements are $S_0, S_1, S_2, S_3, \dots$. The same outline is used, except that the basis step verifies S_0 , not S_1 .

Proposition If n is a non-negative integer, then $5 \mid (n^5 - n)$.

Proof. We will prove this with mathematical induction. Observe that the first non-negative integer is 0, so the basis step involves $n = 0$.

- (1) If $n = 0$, this statement is $5 \mid (0^5 - 0)$ or $5 \mid 0$, which is obviously true.
- (2) Let $k \geq 0$. We need to prove that if $5 \mid (k^5 - k)$, then $5 \mid ((k+1)^5 - (k+1))$. We use direct proof. Suppose $5 \mid (k^5 - k)$. Thus $k^5 - k = 5a$ for some $a \in \mathbb{Z}$. Observe that

$$\begin{aligned} (k+1)^5 - (k+1) &= k^5 + 5k^4 + 10k^3 + 10k^2 + 5k + 1 - k - 1 \\ &= (k^5 - k) + 5k^4 + 10k^3 + 10k^2 + 5k \\ &= 5a + 5k^4 + 10k^3 + 10k^2 + 5k \\ &= 5(a + k^4 + 2k^3 + 2k^2 + k). \end{aligned}$$

This shows $(k+1)^5 - (k+1)$ is an integer multiple of 5, so $5 \mid ((k+1)^5 - (k+1))$.

We have now shown that $5 \mid (k^5 - k)$ implies $5 \mid ((k+1)^5 - (k+1))$.

It follows by induction that $5 \mid (n^5 - n)$ for all non-negative integers n . ■

As noted, induction is used to prove statements of the form $\forall n \in \mathbb{N}, S_n$. But notice the outline does *not* work for statements of form $\forall n \in \mathbb{Z}, S_n$ (where n is in \mathbb{Z} , not \mathbb{N}). The reason is that if you are trying to prove $\forall n \in \mathbb{Z}, S_n$ by induction, and you've shown S_1 is true and $S_k \Rightarrow S_{k+1}$, then it only follows from this that S_n is true for $n \geq 1$. You haven't proved that any of the statements $S_0, S_{-1}, S_{-2}, \dots$ are true. If you ever want to prove $\forall n \in \mathbb{Z}, S_n$ by induction, you have to show that some S_a is true and $S_k \Rightarrow S_{k+1}$ **and** $S_k \Rightarrow S_{k-1}$.

Unfortunately, the term *mathematical induction* is sometimes confused with *inductive reasoning*, that is, the process of reaching the conclusion that something is likely to be true based on prior observations of similar circumstances. Please note that mathematical induction, as introduced here, is a rigorous method that proves statements with absolute certainty.

To round out this section, we present four additional induction proofs.

Proposition If $n \in \mathbb{Z}$ and $n \geq 0$, then $\sum_{i=0}^n i \cdot i! = (n+1)! - 1$.

Proof. We will prove this with mathematical induction.

(1) If $n = 0$, this statement is

$$\sum_{i=0}^0 i \cdot i! = (0+1)! - 1.$$

Since the left-hand side is $0 \cdot 0! = 0$, and the right-hand side is $1! - 1 = 0$, the equation $\sum_{i=0}^0 i \cdot i! = (0+1)! - 1$ holds, as both sides are zero.

(2) Consider any integer $k \geq 0$. We must show that S_k implies S_{k+1} . That is, we must show that

$$\sum_{i=0}^k i \cdot i! = (k+1)! - 1$$

implies

$$\sum_{i=0}^{k+1} i \cdot i! = ((k+1)+1)! - 1.$$

We use direct proof. Suppose $\sum_{i=0}^k i \cdot i! = (k+1)! - 1$. Observe that

$$\begin{aligned} \sum_{i=0}^{k+1} i \cdot i! &= \left(\sum_{i=0}^k i \cdot i! \right) + (k+1)(k+1)! \\ &= \left((k+1)! - 1 \right) + (k+1)(k+1)! \\ &= (k+1)! + (k+1)(k+1)! - 1 \\ &= (1 + (k+1))(k+1)! - 1 \\ &= (k+2)(k+1)! - 1 \\ &= (k+2)! - 1 \\ &= ((k+1)+1)! - 1. \end{aligned}$$

Therefore $\sum_{i=0}^{k+1} i \cdot i! = ((k+1)+1)! - 1$.

It follows by induction that $\sum_{i=0}^n i \cdot i! = (n+1)! - 1$ for every integer $n \geq 0$. ■

The next example illustrates a trick that is occasionally useful. You know that you can add equal quantities to both sides of an equation without violating equality. But don't forget that you can add *unequal* quantities to both sides of an *inequality*, as long as the quantity added to the bigger side is bigger than the quantity added to the smaller side. For example, if $x \leq y$ and $a \leq b$, then $x + a \leq y + b$. Similarly, if $x \leq y$ and b is positive, then $x \leq y + b$. This oft-forgotten fact is used in the next proof.

Proposition The inequality $2^n \leq 2^{n+1} - 2^{n-1} - 1$ holds for each $n \in \mathbb{N}$.

Proof. We will prove this with mathematical induction.

- (1) If $n = 1$, this statement is $2^1 \leq 2^{1+1} - 2^{1-1} - 1$, and this simplifies to $2 \leq 4 - 1 - 1$, which is obviously true.
- (2) Say $k \geq 1$. We use direct proof to show that $2^k \leq 2^{k+1} - 2^{k-1} - 1$ implies $2^{k+1} \leq 2^{(k+1)+1} - 2^{(k+1)-1} - 1$. Suppose $2^k \leq 2^{k+1} - 2^{k-1} - 1$. Then:

$$\begin{aligned} 2^k &\leq 2^{k+1} - 2^{k-1} - 1 \\ 2(2^k) &\leq 2(2^{k+1} - 2^{k-1} - 1) && \text{(multiply both sides by 2)} \\ 2^{k+1} &\leq 2^{k+2} - 2^k - 2 \\ 2^{k+1} &\leq 2^{k+2} - 2^k - 2 + 1 && \text{(add 1 to the bigger side)} \\ 2^{k+1} &\leq 2^{k+2} - 2^k - 1 \\ 2^{k+1} &\leq 2^{(k+1)+1} - 2^{(k+1)-1} - 1. \end{aligned}$$

It follows by induction that $2^n \leq 2^{n+1} - 2^{n-1} - 1$ for each $n \in \mathbb{N}$. ■

We next prove that if $n \in \mathbb{N}$, then the inequality $(1+x)^n \geq 1+nx$ holds for all $x \in \mathbb{R}$ with $x > -1$. Thus we will need to prove that the statement

$$S_n : (1+x)^n \geq 1+nx \text{ for every } x \in \mathbb{R} \text{ with } x > -1$$

is true for every natural number n . This is (only) slightly different from our other examples, which proved statements of the form $\forall n \in \mathbb{N}, P(n)$, where $P(n)$ is a statement about the number n . This time we are proving something of form

$$\forall n \in \mathbb{N}, P(n, x),$$

where the statement $P(n, x)$ involves not only n , but also a second variable x . (For the record, the inequality $(1+x)^n \geq 1+nx$ is known as *Bernoulli's inequality*.)

Proposition If $n \in \mathbb{N}$, then $(1+x)^n \geq 1+nx$ for all $x \in \mathbb{R}$ with $x > -1$.

Proof. We will prove this with mathematical induction.

- (1) For the basis step, notice that when $n = 1$ the statement is $(1+x)^1 \geq 1+1 \cdot x$, and this is true because both sides equal $1+x$.
- (2) Assume that for some $k \geq 1$, the statement $(1+x)^k \geq 1+kx$ is true for all $x \in \mathbb{R}$ with $x > -1$. From this we need to prove $(1+x)^{k+1} \geq 1+(k+1)x$. Now, $1+x$ is positive because $x > -1$, so we can multiply both sides of $(1+x)^k \geq 1+kx$ by $(1+x)$ without changing the direction of the \geq .

$$\begin{aligned} (1+x)^k(1+x) &\geq (1+kx)(1+x) \\ (1+x)^{k+1} &\geq 1+x+kx+kx^2 \\ (1+x)^{k+1} &\geq 1+(k+1)x+kx^2 \end{aligned}$$

The above term kx^2 is positive, so removing it from the right-hand side will only make that side smaller. Thus we get $(1+x)^{k+1} \geq 1+(k+1)x$. ■

Next, an example where the basis step involves more than routine checking. (It will be used later, so it is numbered for reference.)

Proposition 14.1 Suppose a_1, a_2, \dots, a_n are n integers, where $n \geq 2$. If p is prime and $p \mid (a_1 \cdot a_2 \cdot a_3 \cdots a_n)$, then $p \mid a_i$ for at least one of the a_i .

Proof. The proof is induction on n .

- (1) The basis step involves $n = 2$. Let p be prime and suppose $p \mid (a_1 a_2)$. We need to show that $p \mid a_1$ or $p \mid a_2$, or equivalently, if $p \nmid a_1$, then $p \mid a_2$. Thus suppose $p \nmid a_1$. Since p is prime, it follows that $\gcd(p, a_1) = 1$. By Proposition 12.1 (on page 300), there are integers k and ℓ for which $1 = pk + a_1 \ell$. Multiplying this by a_2 gives

$$a_2 = pka_2 + a_1 a_2 \ell.$$

As we are assuming that p divides $a_1 a_2$, it is clear that p divides the expression $pka_2 + a_1 a_2 \ell$ on the right; hence $p \mid a_2$. We've now proved that if $p \mid (a_1 a_2)$, then $p \mid a_1$ or $p \mid a_2$. This completes the basis step.

- (2) Suppose that $k \geq 2$, and $p \mid (a_1 \cdot a_2 \cdots a_k)$ implies then $p \mid a_i$ for some a_i . Now let $p \mid (a_1 \cdot a_2 \cdots a_k \cdot a_{k+1})$. Then $p \mid ((a_1 \cdot a_2 \cdots a_k) \cdot a_{k+1})$. By what we proved in the basis step, it follows that $p \mid (a_1 \cdot a_2 \cdots a_k)$ or $p \mid a_{k+1}$. This and the inductive hypothesis imply that p divides one of the a_i . ■

Please test your understanding now by working a few exercises.

14.2 Proving Recursive Procedures Work

In Section 6.5 (page 186), we devised the following procedure RFac for calculating the factorial of an integer n , that is, $\text{RFac}(n)$ supposedly returns the value $n!$. This procedure is *recursive*, meaning that within its body there is another call to RFac . Although this may seem circular, most high-level programming languages do allow for recursive procedures.

Procedure $\text{RFac}(n)$

```

1 begin
2   if  $n = 0$  then
3     | return 1 ..... because  $0! = 1$ 
4   else
5     | return  $n \cdot \text{RFac}(n - 1)$  ..... because  $n! = n \cdot (n - 1)!$ 
6   end
7 end
```

Induction can prove that properly-written recursive procedures are valid, and run correctly when implemented in programming languages that allow for recursion. As an example, we will prove that $\text{RFac}(n)$ really does return the correct value of $n!$.

Proposition 14.2 If n is a non-negative integer, then $\text{RFac}(n)$ returns the correct value of $n!$.

Proof. We will prove this with mathematical induction.

- (1) For the base case, suppose $n = 0$. Referring to lines 2 and 3 of RFac , we see that $\text{RFac}(0)$ returns 1, which is indeed $0!$.
- (2) Now take any integer $k \geq 0$. We need to show that if $\text{RFac}(k)$ returns $k!$, then $\text{RFac}(k + 1)$ returns $(k + 1)!$.

For this we use direct proof. Thus assume that $\text{RFac}(k)$ returns the correct value of $k!$. Now run $\text{RFac}(k + 1)$. Because $k + 1 > 0$, the procedure executes the else clause, and in line 5 it returns the value of

$$(k + 1) \cdot \text{RFac}((k + 1) - 1) = (k + 1) \cdot \text{RFac}(k).$$

By assumption, $\text{RFac}(k)$ in the above line returns the value $k!$, so the above line is $(k + 1) \cdot \text{RFac}(k) = (k + 1)k! = (k + 1)!$. Thus $\text{RFac}(k + 1)$ returns $(k + 1)!$.

It follows by induction that $\text{RFac}(n)$ returns $n!$ for any integer $n \geq 0$. ■

14.3 Proof by Strong Induction

Sometimes in an induction proof it is hard to show that S_k implies S_{k+1} . It may be easier to show some “lower” S_m (with $m < k$) implies S_{k+1} . For such situations there is a slight variant of induction called strong induction. Strong induction works just like regular induction, except that in Step (2) instead of assuming S_k is true and showing this forces S_{k+1} to be true, we assume that *all* the statements S_1, S_2, \dots, S_k are true and show this forces S_{k+1} to be true. The idea is that if the first k dominoes falling always make the $(k + 1)$ th domino to fall, then all the dominoes must fall.

Outline for Proof by Strong Induction

Proposition The statements $S_1, S_2, S_3, S_4, \dots$ are all true.

Proof. (Strong induction)

(1) Prove the first statement S_1 . (Or the first several S_n , if needed.)

(2) Given any integer $k \geq 1$, prove $(S_1 \wedge S_2 \wedge S_3 \wedge \dots \wedge S_k) \Rightarrow S_{k+1}$. ■

This is useful when S_k does not easily imply S_{k+1} . You might be better served by showing some earlier statement (S_{k-1} or S_{k-2} for instance) implies S_k . In strong induction you can use any (or all) of S_1, S_2, \dots, S_k to prove S_{k+1} .

Here is a classic “first” example of a strong induction proof. The problem is to prove that you can achieve any postage of 8 cents or more, exactly, using only 3¢ and 5¢ stamps. For example, for a postage of 47 cents, you could use nine 3¢ stamps and four 5¢ stamps. Let S_n be the statement S_n : *You can get a postage of exactly n ¢ using only 3¢ and 5¢ stamps.* Thus we need to prove all the statements $S_8, S_9, S_{10}, S_{11} \dots$ are true. In the proof, to show S_{k+1} is true we will need to “go back” two steps from S_k , so the basis step involves verifying the first **two** statements.

Proposition Any postage of 8¢ or more is possible using 3¢ and 5¢ stamps.

Proof. We will use strong induction.

- (1) The proposition is true for a postages of 8 and 9 cents: For 8 cents, use one 3¢ stamp and one 5¢ stamp. For 9 cents, use three 3¢ stamps.
- (2) Let $k \geq 9$, and for each $8 \leq m \leq k$, assume a postage of m cents can be obtained exactly with 3¢ and 5¢ stamps. (That is, assume statements S_8, S_9, \dots, S_k are all true.) We must show that S_{k+1} is true, that is, $(k + 1)$ -cents postage can be achieved with 3¢ and 5¢ stamps. By assumption, S_{k-2} is true. Thus we can get $(k - 2)$ -cents postage with 3¢ and 5¢ stamps. Now just add one more 3¢ stamp, and we have $(k - 2) + 3 = k + 1$ cents postage with 3¢ and 5¢ stamps. ■

Our next example proves that $12 \mid (n^4 - n^2)$ for any $n \in \mathbb{N}$. But first, let's see how regular induction is problematic. Regular induction starts by checking $12 \mid (n^4 - n^2)$ for $n = 1$. This reduces to $12 \mid 0$, which is true. Next we assume $12 \mid (k^4 - k^2)$ and try to show that this implies $12 \mid ((k+1)^4 - (k+1)^2)$. Now, $12 \mid (k^4 - k^2)$ means $k^4 - k^2 = 12a$ for some $a \in \mathbb{Z}$. We want to use this to get $(k+1)^4 - (k+1)^2 = 12b$ for some integer b . Working it out,

$$\begin{aligned} (k+1)^4 - (k+1)^2 &= (k^4 + 4k^3 + 6k^2 + 4k + 1) - (k^2 + 2k + 1) \\ &= (k^4 - k^2) + 4k^3 + 6k^2 + 6k \\ &= 12a + 4k^3 + 6k^2 + 6k. \end{aligned}$$

At this point we're stuck because we can't factor out a 12.

Let's try strong induction. Say S_n is the statement $S_n : 12 \mid (n^4 - n^2)$. In strong induction, we assume each of S_1, S_2, \dots, S_k is true, and show that this makes S_{k+1} true. In particular, if S_1 through S_k are true, then S_{k-5} is true, provided $1 \leq k-5 < k$. We will show $S_{k-5} \Rightarrow S_{k+1}$ instead of $S_k \Rightarrow S_{k+1}$. For this to make sense, our basis step must check that $S_1, S_2, S_3, S_4, S_5, S_6$ are all true. Once this is established, $S_{k-5} \Rightarrow S_{k+1}$ will imply that the other S_k are all true. For example, if $k = 6$, then $S_{k-5} \Rightarrow S_{k+1}$ is $S_1 \Rightarrow S_7$, so S_7 is true; for $k = 7$, then $S_{k-5} \Rightarrow S_{k+1}$ is $S_2 \Rightarrow S_8$, so S_8 is true, etc.

Proposition If $n \in \mathbb{N}$, then $12 \mid (n^4 - n^2)$.

Proof. We will prove this with strong induction.

(1) First note that the statement is true for the first six positive integers:

$$\begin{array}{ll} \text{If } n = 1, 12 \text{ divides } 1^4 - 1^2 = 0. & \text{If } n = 4, 12 \text{ divides } 4^4 - 4^2 = 240. \\ \text{If } n = 2, 12 \text{ divides } 2^4 - 2^2 = 12. & \text{If } n = 5, 12 \text{ divides } 5^4 - 5^2 = 600. \\ \text{If } n = 3, 12 \text{ divides } 3^4 - 3^2 = 72. & \text{If } n = 6, 12 \text{ divides } 6^4 - 6^2 = 1260. \end{array}$$

(2) For $k \geq 6$, assume $12 \mid (m^4 - m^2)$ for $1 \leq m \leq k$ (i.e., S_1, S_2, \dots, S_k are true).

We must show S_{k+1} is true, that is, $12 \mid ((k+1)^4 - (k+1)^2)$. Now, S_{k-5} being true means $12 \mid ((k-5)^4 - (k-5)^2)$. To simplify, put $\boxed{k-5 = \ell}$ so $12 \mid (\ell^4 - \ell^2)$, meaning $\boxed{\ell^4 - \ell^2 = 12a}$ for $a \in \mathbb{Z}$, and $\boxed{k+1 = \ell+6}$. Then:

$$\begin{aligned} (k+1)^4 - (k+1)^2 &= (\ell+6)^4 - (\ell+6)^2 \\ &= \ell^4 + 24\ell^3 + 216\ell^2 + 864\ell + 1296 - (\ell^2 + 12\ell + 36) \\ &= (\ell^4 - \ell^2) + 24\ell^3 + 216\ell^2 + 852\ell + 1260 \\ &= 12a + 24\ell^3 + 216\ell^2 + 852\ell + 1260 \\ &= 12(a + 2\ell^3 + 18\ell^2 + 71\ell + 105). \end{aligned}$$

Because $(a + 2\ell^3 + 18\ell^2 + 71\ell + 105) \in \mathbb{Z}$, we get $12 \mid ((k+1)^4 - (k+1)^2)$. ■

Our next example involves mathematical objects called *graphs*. In mathematics, the word *graph* is used in two contexts. One context involves the graphs of equations and functions from algebra and calculus. In the other context, a **graph** is a configuration consisting of points (called **vertices**) and **edges** which are lines connecting the vertices. Following are some pictures of graphs. Let's agree that all of our graphs will be in "one piece," that is, you can travel from any vertex of a graph to any other vertex by traversing a route of edges from one vertex to the other.

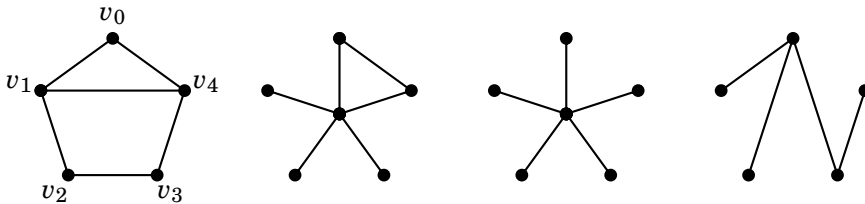


Figure 14.1. Examples of Graphs

A **cycle** in a graph is a sequence of distinct edges in the graph that form a route that ends where it began. For example, the graph on the far left of Figure 14.1 has a cycle that starts at vertex v_1 , then goes to v_2 , then to v_3 , then v_4 and finally back to its starting point v_1 . You can find cycles in both of the graphs on the left, but the two graphs on the right do not have cycles. There is a special name for a graph that has no cycles; it is called a **tree**. Thus the two graphs on the right of Figure 14.1 are trees, but the two graphs on the left are not trees.

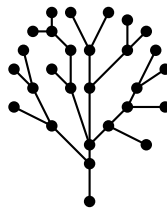


Figure 14.2. A tree

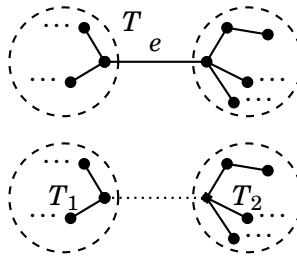
Note that the trees in Figure 14.1 both have one fewer edge than vertex. The tree on the far right has 5 vertices and 4 edges. The one next to it has 6 vertices and 5 edges. Draw any tree; you will find that if it has n vertices, then it has $n - 1$ edges. We now prove that this is always true.

Proposition If a tree has n vertices, then it has $n - 1$ edges.

Proof. Notice that this theorem asserts that for any $n \in \mathbb{N}$, the following statement is true: S_n : A tree with n vertices has $n - 1$ edges. We use strong induction to prove this.

- (1) Observe that if a tree has $n = 1$ vertex then it has no edges. Thus it has $n - 1 = 0$ edges, so the theorem is true when $n = 1$.
- (2) Now take an integer $k \geq 1$. We must show $(S_1 \wedge S_2 \wedge \cdots \wedge S_k) \Rightarrow S_{k+1}$. In words, we must show that if it is true that any tree with m vertices has $m - 1$ edges, where $1 \leq m \leq k$, then any tree with $k + 1$ vertices has $(k + 1) - 1 = k$ edges. We will use direct proof.

Suppose that for each integer m with $1 \leq m \leq k$, any tree with m vertices has $m - 1$ edges. Now let T be a tree with $k + 1$ vertices. Single out an edge of T and label it e , as illustrated below.



Now remove the edge e from T , but leave the two endpoints of e . This leaves two smaller trees that we call T_1 and T_2 . Let's say T_1 has x vertices and T_2 has y vertices. As each of these two smaller trees has fewer than $k + 1$ vertices, our inductive hypothesis guarantees that T_1 has $x - 1$ edges, and T_2 has $y - 1$ edges. Think about our original tree T . It has $x + y$ vertices. It has $x - 1$ edges that belong to T_1 and $y - 1$ edges that belong to T_2 , *plus* it has the additional edge e that belongs to neither T_1 nor T_2 . Thus, all together, the number of edges that T has is $(x - 1) + (y - 1) + 1 = (x + y) - 1$. In other words, T has one fewer edges than it has vertices. Thus it has $(k + 1) - 1 = k$ edges.

It follows by strong induction that a tree with n vertices has $n - 1$ edges. ■

Notice that it was absolutely essential that we used strong induction in the above proof because the two trees T_1 and T_2 will not both have k vertices. At least one will have fewer than k vertices. Thus the statement S_k is not enough to imply S_{k+1} . We need to use the assumption that S_m will be true whenever $m \leq k$, and strong induction allows us to do this.

14.4 Proof by Smallest Counterexample

This section introduces yet another proof technique, called **proof by smallest counterexample**. It is a hybrid of induction and proof by contradiction. It has the nice feature that it leads you straight to a contradiction. It is therefore more “automatic” than the proof by contradiction that was introduced in Chapter 10. Here is the outline:

Outline for Proof by Smallest Counterexample

Proposition The statements $S_1, S_2, S_3, S_4, \dots$ are all true.

Proof. (Smallest counterexample)

- (1) Check that the first statement S_1 is true.
- (2) For the sake of contradiction, suppose not every S_n is true.
- (3) Let $k > 1$ be the smallest integer for which S_k is **false**.
- (4) Then S_{k-1} is true and S_k is false. Use this to get a contradiction. ■

Notice that this setup leads you to a point where S_{k-1} is true and S_k is false. It is here, where true and false collide, that you will find a contradiction. Let's do an example.

Proposition If $n \in \mathbb{N}$, then $4 \mid (5^n - 1)$.

Proof. We use proof by smallest counterexample. (We will number the steps to match the outline, but that is not usually done in practice.)

- (1) If $n = 1$, then the statement is $4 \mid (5^1 - 1)$, or $4 \mid 4$, which is true.
- (2) For sake of contradiction, suppose it's not true that $4 \mid (5^n - 1)$ for all n .
- (3) Let $k > 1$ be the smallest integer for which $4 \nmid (5^k - 1)$.
- (4) Then $4 \mid (5^{k-1} - 1)$, so there is an integer a for which $5^{k-1} - 1 = 4a$. Then:

$$\begin{aligned} 5^{k-1} - 1 &= 4a \\ 5(5^{k-1} - 1) &= 5 \cdot 4a \\ 5^k - 5 &= 20a \\ 5^k - 1 &= 20a + 4 \\ 5^k - 1 &= 4(5a + 1) \end{aligned}$$

This means $4 \mid (5^k - 1)$, a contradiction, because $4 \nmid (5^k - 1)$ in Step 3. Thus, we were wrong in Step 2 to assume that it is untrue that $4 \mid (5^n - 1)$ for every n . Therefore $4 \mid (5^n - 1)$ is true for every n . ■

We next prove the **fundamental theorem of arithmetic**, which says any integer greater than 1 has a unique prime factorization. For example, 12 factors into primes as $12 = 2 \cdot 2 \cdot 3$, and moreover *any* factorization of 12 into primes uses exactly the primes 2, 2 and 3. Our proof combines the techniques of induction, cases, minimum counterexample and the idea of uniqueness of existence outlined at the end of Section 12.3. We dignify this fundamental result with the label of “Theorem.”

Theorem 14.1 (Fundamental Theorem of Arithmetic) Any integer $n > 1$ has a unique prime factorization. That is, if $n = p_1 \cdot p_2 \cdot p_3 \cdots p_k$ and $n = a_1 \cdot a_2 \cdot a_3 \cdots a_\ell$ are two prime factorizations of n , then $k = \ell$, and the primes p_i and a_i are the same, except that they may be in a different order.

Proof. Suppose $n > 1$. We first use strong induction to show that n has a prime factorization. For the basis step, if $n = 2$, it is prime, so it is already its own prime factorization. Let $n \geq 2$ and assume every integer between 2 and n (inclusive) has a prime factorization. Consider $n + 1$. If it is prime, then it is its own prime factorization. If it is not prime, then it factors as $n + 1 = ab$ with $a, b > 1$. Because a and b are both less than $n + 1$ they have prime factorizations $a = p_1 \cdot p_2 \cdot p_3 \cdots p_k$ and $b = p'_1 \cdot p'_2 \cdot p'_3 \cdots p'_\ell$. Then

$$n + 1 = ab = (p_1 \cdot p_2 \cdot p_3 \cdots p_k)(p'_1 \cdot p'_2 \cdot p'_3 \cdots p'_\ell)$$

is a prime factorization of $n + 1$. This completes the proof by strong induction that every integer greater than 1 has a prime factorization.

Next we use proof by smallest counterexample to prove that the prime factorization of any $n \geq 2$ is unique. If $n = 2$, then n clearly has only one prime factorization, namely itself. Assume for the sake of contradiction that there is an $n > 2$ that has different prime factorizations $n = p_1 \cdot p_2 \cdot p_3 \cdots p_k$ and $n = a_1 \cdot a_2 \cdot a_3 \cdots a_\ell$. Assume n is the smallest number with this property. From $n = p_1 \cdot p_2 \cdot p_3 \cdots p_k$, we see that $p_1 \mid n$, so $p_1 \mid (a_1 \cdot a_2 \cdot a_3 \cdots a_\ell)$. By Proposition 14.2 (page 328), p_1 divides one of the primes a_i . As a_i is prime, we have $p_1 = a_i$. Dividing $n = p_1 \cdot p_2 \cdot p_3 \cdots p_k = a_1 \cdot a_2 \cdot a_3 \cdots a_\ell$ by $p_1 = a_i$ yields

$$p_2 \cdot p_3 \cdots p_k = a_1 \cdot a_2 \cdot a_3 \cdots a_{i-1} \cdot a_{i+1} \cdots a_\ell.$$

These two factorizations are different, because the two prime factorizations of n were different. (Remember: the primes p_1 and a_i are equal, so the difference appears in the remaining factors, displayed above.) But also the above number $p_2 \cdot p_3 \cdots p_k$ is smaller than n , and this contradicts the fact that n was the smallest number with two different prime factorizations. ■

One word of warning about proof by smallest counterexample. In proofs in other textbooks or in mathematical papers, it often happens that the writer doesn't tell you up front that proof by smallest counterexample is being used. Instead, you will have to read through the proof to glean from context that this technique is being used. In fact, the same warning applies to *all* of our proof techniques. If you continue with mathematics, you will gradually gain through experience the ability to analyze a proof and understand exactly what approach is being used when it is not stated explicitly. Frustrations await you, but do not be discouraged by them. Frustration is a natural part of anything that's worth doing.

14.5 Fibonacci Numbers

Leonardo Pisano, now known as Fibonacci, was a mathematician born around 1175 in what is now Italy. His most significant work was a book *Liber Abaci*, which is recognized as a catalyst in medieval Europe's slow transition from Roman numbers to the Hindu-Arabic number system. But he is best known today for a number sequence that he described in his book and that bears his name. The **Fibonacci sequence** is

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, \dots$$

The numbers that appear in this sequence are called **Fibonacci numbers**. The first two numbers are 1 and 1, and thereafter any entry is the sum of the previous two entries. For example $3 + 5 = 8$, and $5 + 8 = 13$, etc. We denote the n th term of this sequence as F_n . Thus $F_1 = 1$, $F_2 = 1$, $F_3 = 2$, $F_4 = 3$, $F_7 = 13$ and so on. Notice that the Fibonacci Sequence is entirely determined by the rules $F_1 = 1$, $F_2 = 1$, and $F_n = F_{n-1} + F_{n-2}$.

We introduce Fibonacci's sequence here partly because it is something everyone should know about, but also because it is a great source of induction problems. This sequence, which appears with surprising frequency in nature, is filled with mysterious patterns and hidden structures. Some of these structures will be revealed to you in the examples and exercises.

We emphasize that the condition $F_n = F_{n-1} + F_{n-2}$ (or equivalently $F_{n+1} = F_n + F_{n-1}$) is the perfect setup for induction. It suggests that we can determine something about F_n by looking at earlier terms of the sequence. In using induction to prove something about the Fibonacci sequence, you should expect to use the equation $F_n = F_{n-1} + F_{n-2}$ somewhere.

For our first example we will prove that $F_{n+1}^2 - F_{n+1}F_n - F_n^2 = (-1)^n$ for any natural number n . For example, if $n = 5$ we have $F_6^2 - F_6F_5 - F_5^2 = 8^2 - 8 \cdot 5 - 5^2 = 64 - 40 - 25 = -1 = (-1)^5$.

Proposition The Fibonacci sequence obeys $F_{n+1}^2 - F_{n+1}F_n - F_n^2 = (-1)^n$.

Proof. We will prove this with mathematical induction.

- (1) If $n = 1$ we have $F_{n+1}^2 - F_{n+1}F_n - F_n^2 = F_2^2 - F_2F_1 - F_1^2 = 1^2 - 1 \cdot 1 - 1^2 = -1 = (-1)^1 = (-1)^n$, so indeed $F_{n+1}^2 - F_{n+1}F_n - F_n^2 = (-1)^n$ is true when $n = 1$.
- (2) Take any integer $k \geq 1$. We must show that if $F_{k+1}^2 - F_{k+1}F_k - F_k^2 = (-1)^k$, then $F_{k+2}^2 - F_{k+2}F_{k+1} - F_{k+1}^2 = (-1)^{k+1}$. We use direct proof. Suppose $F_{k+1}^2 - F_{k+1}F_k - F_k^2 = (-1)^k$. Now we are going to carefully work out the expression $F_{k+2}^2 - F_{k+2}F_{k+1} - F_{k+1}^2$ and show that it really does equal $(-1)^{k+1}$. In so doing, we will use the fact that $F_{k+2} = F_{k+1} + F_k$.

$$\begin{aligned}
 F_{k+2}^2 - F_{k+2}F_{k+1} - F_{k+1}^2 &= (F_{k+1} + F_k)^2 - (F_{k+1} + F_k)F_{k+1} - F_{k+1}^2 \\
 &= F_{k+1}^2 + 2F_{k+1}F_k + F_k^2 - F_{k+1}^2 - F_kF_{k+1} - F_{k+1}^2 \\
 &= -F_{k+1}^2 + F_{k+1}F_k + F_k^2 \\
 &= -(F_{k+1}^2 - F_{k+1}F_k - F_k^2) \\
 &= -(-1)^k && \text{(inductive hypothesis)} \\
 &= (-1)^1(-1)^k \\
 &= (-1)^{k+1}
 \end{aligned}$$

Therefore $F_{k+2}^2 - F_{k+2}F_{k+1} - F_{k+1}^2 = (-1)^{k+1}$.

It follows by induction that $F_{n+1}^2 - F_{n+1}F_n - F_n^2 = (-1)^n$ for every $n \in \mathbb{N}$. \blacksquare

Let's pause for a moment and think about what the result we just proved means. Dividing both sides of $F_{n+1}^2 - F_{n+1}F_n - F_n^2 = (-1)^n$ by F_n^2 gives

$$\left(\frac{F_{n+1}}{F_n} \right)^2 - \frac{F_{n+1}}{F_n} - 1 = \frac{(-1)^n}{F_n^2}.$$

For large values of n , the right-hand side is very close to zero, and the left-hand side is F_{n+1}/F_n plugged into the polynomial $x^2 - x - 1$. Thus, as n increases, the ratio F_{n+1}/F_n approaches a root of $x^2 - x - 1 = 0$. By the quadratic formula, the roots of $x^2 - x - 1$ are $\frac{1 \pm \sqrt{5}}{2}$. As $F_{n+1}/F_n > 1$, this ratio must be approaching the *positive* root $\frac{1 + \sqrt{5}}{2}$. Therefore

$$\lim_{n \rightarrow \infty} \frac{F_{n+1}}{F_n} = \frac{1 + \sqrt{5}}{2}. \tag{14.1}$$

For a quick spot check, note that $F_{13}/F_{12} \approx 1.618025$, while $\frac{1 + \sqrt{5}}{2} \approx 1.618033$. Even for the small value $n = 12$, the numbers match to four decimal places.

The number $\phi = \frac{1+\sqrt{5}}{2}$ is sometimes called the **golden ratio**, and there has been much speculation about its occurrence in nature as well as in classical art and architecture. One theory holds that the Parthenon and the Great Pyramids of Egypt were designed in accordance with this number.

But we are here concerned with things that can be proved. We close by observing how the Fibonacci sequence in many ways resembles a geometric sequence. Recall that a **geometric sequence** with first term a and common ratio r has the form

$$a, ar, ar^2, ar^3, ar^4, ar^5, ar^6, ar^7, ar^8, \dots$$

where any term is obtained by multiplying the previous term by r . In general its n th term is $G_n = ar^n$, and $G_{n+1}/G_n = r$. Equation (14.1) tells us that $F_{n+1}/F_n \approx \phi$. Thus even though it is not a geometric sequence, the Fibonacci sequence tends to behave like a geometric sequence with common ratio ϕ , and the further “out” you go, the higher the resemblance.

Exercises for Chapter 14

Prove the following statements with either induction, strong induction or proof by smallest counterexample.

1. Prove that $1 + 2 + 3 + 4 + \dots + n = \frac{n^2 + n}{2}$ for every positive integer n .
2. Prove that $1^2 + 2^2 + 3^2 + 4^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}$ for every positive integer n .
3. Prove that $1^3 + 2^3 + 3^3 + 4^3 + \dots + n^3 = \frac{n^2(n+1)^2}{4}$ for every positive integer n .
4. If $n \in \mathbb{N}$, then $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + 4 \cdot 5 + \dots + n(n+1) = \frac{n(n+1)(n+2)}{3}$.
5. If $n \in \mathbb{N}$, then $2^1 + 2^2 + 2^3 + \dots + 2^n = 2^{n+1} - 2$.
6. Prove that $\sum_{i=1}^n (8i - 5) = 4n^2 - n$ for every positive integer n .
7. If $n \in \mathbb{N}$, then $1 \cdot 3 + 2 \cdot 4 + 3 \cdot 5 + 4 \cdot 6 + \dots + n(n+2) = \frac{n(n+1)(2n+7)}{6}$.
8. If $n \in \mathbb{N}$, then $\frac{1}{2!} + \frac{2}{3!} + \frac{3}{4!} + \dots + \frac{n}{(n+1)!} = 1 - \frac{1}{(n+1)!}$.
9. Prove that $24 \mid (5^{2n} - 1)$ for every integer $n \geq 0$.
10. Prove that $3 \mid (5^{2n} - 1)$ for every integer $n \geq 0$.
11. Prove that $3 \mid (n^3 + 5n + 6)$ for every integer $n \geq 0$.
12. Prove that $9 \mid (4^{3n} + 8)$ for every integer $n \geq 0$.
13. Prove that $6 \mid (n^3 - n)$ for every integer $n \geq 0$.

14. Suppose $a \in \mathbb{Z}$. Prove that $5 \mid 2^n a$ implies $5 \mid a$ for any $n \in \mathbb{N}$.
15. If $n \in \mathbb{N}$, then $\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \frac{1}{4 \cdot 5} + \cdots + \frac{1}{n(n+1)} = 1 - \frac{1}{n+1}$.
16. Prove that $2^n + 1 \leq 3^n$ for every positive integer n .
17. Suppose A_1, A_2, \dots, A_n are sets in some universal set U , and $n \geq 2$. Prove that $\overline{A_1 \cap A_2 \cap \cdots \cap A_n} = \overline{A_1} \cup \overline{A_2} \cup \cdots \cup \overline{A_n}$.
18. Suppose A_1, A_2, \dots, A_n are sets in some universal set U , and $n \geq 2$. Prove that $\overline{A_1 \cup A_2 \cup \cdots \cup A_n} = \overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_n}$.
19. Prove that $\frac{1}{1} + \frac{1}{4} + \frac{1}{9} + \cdots + \frac{1}{n^2} \leq 2 - \frac{1}{n}$ for every $n \in \mathbb{N}$.
20. Prove that $(1+2+3+\cdots+n)^2 = 1^3 + 2^3 + 3^3 + \cdots + n^3$ for every $n \in \mathbb{N}$.
21. If $n \in \mathbb{N}$, then $\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \cdots + \frac{1}{2^n - 1} + \frac{1}{2^n} \geq 1 + \frac{n}{2}$.
(Note: This problem asserts that the sum of the first 2^n terms of the harmonic series is at least $1 + n/2$. It thus implies that the harmonic series diverges.)
22. If $n \in \mathbb{N}$, then $\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{4}\right)\left(1 - \frac{1}{8}\right)\left(1 - \frac{1}{16}\right) \cdots \left(1 - \frac{1}{2^n}\right) \geq \frac{1}{4} + \frac{1}{2^{n+1}}$.
23. Use mathematical induction to prove the binomial theorem (Theorem 4.1 on page 106). You may find that you need Equation (4.3) on page 104.
24. Prove that $\sum_{k=1}^n k \binom{n}{k} = n2^{n-1}$ for each natural number n .
25. Concerning the Fibonacci sequence, prove that $F_1 + F_2 + F_3 + F_4 + \cdots + F_n = F_{n+2} - 1$.
26. Concerning the Fibonacci sequence, prove that $\sum_{k=1}^n F_k^2 = F_n F_{n+1}$.
27. Concerning the Fibonacci sequence, prove that $F_1 + F_3 + F_5 + F_7 + \cdots + F_{2n-1} = F_{2n}$.
28. Concerning the Fibonacci sequence, prove that $F_2 + F_4 + F_6 + F_8 + \cdots + F_{2n} = F_{2n+1} - 1$.
29. In this problem $n \in \mathbb{N}$ and F_n is the n th Fibonacci number. Prove that

$$\binom{n}{0} + \binom{n-1}{1} + \binom{n-2}{2} + \binom{n-3}{3} + \cdots + \binom{0}{n} = F_{n+1}.$$

(For example, $\binom{6}{0} + \binom{5}{1} + \binom{4}{2} + \binom{3}{3} + \binom{2}{4} + \binom{1}{5} + \binom{0}{6} = 1 + 5 + 6 + 1 + 0 + 0 + 0 = 13 = F_{6+1}$.)

30. Here F_n is the n th Fibonacci number. Prove that

$$F_n = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}}.$$

31. Prove that $\sum_{k=0}^n \binom{k}{r} = \binom{n+1}{r+1}$, where $1 \leq r \leq n$.
32. Prove that the number of n -digit binary numbers that have no consecutive 1's is the Fibonacci number F_{n+2} . For example, for $n = 2$ there are three such numbers (00, 01, and 10), and $3 = F_{2+2} = F_4$. Also, for $n = 3$ there are five such numbers (000, 001, 010, 100, 101), and $5 = F_{3+2} = F_5$.

14.6 Solutions for Chapter 14

1. Prove that $1 + 2 + 3 + 4 + \cdots + n = \frac{n^2+n}{2}$ for every positive integer n .

Proof. We will prove this with mathematical induction.

- (1) Observe that if $n = 1$, this statement is $1 = \frac{1^2+1}{2}$, which is obviously true.
 (2) Consider any integer $k \geq 1$. We must show that S_k implies S_{k+1} . In other words, we must show that if $1 + 2 + 3 + 4 + \cdots + k = \frac{k^2+k}{2}$ is true, then

$$1 + 2 + 3 + 4 + \cdots + k + (k + 1) = \frac{(k + 1)^2 + (k + 1)}{2}$$

is also true. We use direct proof.

Suppose $k \geq 1$ and $1 + 2 + 3 + 4 + \cdots + k = \frac{k^2+k}{2}$. Observe that

$$\begin{aligned} 1 + 2 + 3 + 4 + \cdots + k + (k + 1) &= \\ (1 + 2 + 3 + 4 + \cdots + k) + (k + 1) &= \\ \frac{k^2 + k}{2} + (k + 1) &= \frac{k^2 + k + 2(k + 1)}{2} \\ &= \frac{k^2 + 2k + 1 + k + 1}{2} \\ &= \frac{(k + 1)^2 + (k + 1)}{2}. \end{aligned}$$

Therefore we have shown that $1 + 2 + 3 + 4 + \cdots + k + (k + 1) = \frac{(k+1)^2+(k+1)}{2}$. ■

3. Prove that $1^3 + 2^3 + 3^3 + 4^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}$ for every positive integer n .

Proof. We will prove this with mathematical induction.

- (1) When $n = 1$ the statement is $1^3 = \frac{1^2(1+1)^2}{4} = \frac{4}{4} = 1$, which is true.
 (2) Now assume the statement is true for some integer $n = k \geq 1$, that is assume $1^3 + 2^3 + 3^3 + 4^3 + \cdots + k^3 = \frac{k^2(k+1)^2}{4}$. Observe that this implies the statement is true for $n = k + 1$.

$$\begin{aligned} 1^3 + 2^3 + 3^3 + 4^3 + \cdots + k^3 + (k + 1)^3 &= \\ (1^3 + 2^3 + 3^3 + 4^3 + \cdots + k^3) + (k + 1)^3 &= \\ \frac{k^2(k + 1)^2}{4} + (k + 1)^3 &= \frac{k^2(k + 1)^2}{4} + \frac{4(k + 1)^3}{4} \\ &= \frac{k^2(k + 1)^2 + 4(k + 1)^3}{4} \\ &= \frac{(k + 1)^2(k^2 + 4(k + 1)^1)}{4} \\ &= \frac{(k + 1)^2(k^2 + 4k + 4)}{4} \\ &= \frac{(k + 1)^2(k + 2)^2}{4} \end{aligned}$$

$$= \frac{(k+1)^2((k+1)+1)^2}{4}$$

Therefore $1^3 + 2^3 + 3^3 + 4^3 + \dots + k^3 + (k+1)^3 = \frac{(k+1)^2((k+1)+1)^2}{4}$, which means the statement is true for $n = k+1$. ■

5. If $n \in \mathbb{N}$, then $2^1 + 2^2 + 2^3 + \dots + 2^n = 2^{n+1} - 2$.

Proof. The proof is by mathematical induction.

(1) When $n = 1$, this statement is $2^1 = 2^{1+1} - 2$, or $2 = 4 - 2$, which is true.

(2) Now assume the statement is true for some integer $n = k \geq 1$, that is assume $2^1 + 2^2 + 2^3 + \dots + 2^k = 2^{k+1} - 2$. Observe this implies that the statement is true for $n = k+1$, as follows:

$$\begin{aligned} 2^1 + 2^2 + 2^3 + \dots + 2^k + 2^{k+1} &= \\ (2^1 + 2^2 + 2^3 + \dots + 2^k) + 2^{k+1} &= \\ 2^{k+1} - 2 + 2^{k+1} &= 2 \cdot 2^{k+1} - 2 \\ &= 2^{k+2} - 2 \\ &= 2^{(k+1)+1} - 2 \end{aligned}$$

Thus we have $2^1 + 2^2 + 2^3 + \dots + 2^k + 2^{k+1} = 2^{(k+1)+1} - 2$, so the statement is true for $n = k+1$.

Thus the result follows by mathematical induction. ■

7. If $n \in \mathbb{N}$, then $1 \cdot 3 + 2 \cdot 4 + 3 \cdot 5 + 4 \cdot 6 + \dots + n(n+2) = \frac{n(n+1)(2n+7)}{6}$.

Proof. The proof is by mathematical induction.

(1) When $n = 1$, we have $1 \cdot 3 = \frac{1(1+1)(2+7)}{6}$, which is the true statement $3 = \frac{18}{6}$.

(2) Now assume the statement is true for some integer $n = k \geq 1$, that is assume $1 \cdot 3 + 2 \cdot 4 + 3 \cdot 5 + 4 \cdot 6 + \dots + k(k+2) = \frac{k(k+1)(2k+7)}{6}$. Now observe that

$$\begin{aligned} 1 \cdot 3 + 2 \cdot 4 + 3 \cdot 5 + 4 \cdot 6 + \dots + k(k+2) + (k+1)((k+1)+2) &= \\ (1 \cdot 3 + 2 \cdot 4 + 3 \cdot 5 + 4 \cdot 6 + \dots + k(k+2)) + (k+1)((k+1)+2) &= \\ \frac{k(k+1)(2k+7)}{6} + (k+1)((k+1)+2) &= \\ \frac{k(k+1)(2k+7)}{6} + \frac{6(k+1)(k+3)}{6} &= \\ \frac{k(k+1)(2k+7) + 6(k+1)(k+3)}{6} &= \\ \frac{(k+1)(k(2k+7) + 6(k+3))}{6} &= \\ \frac{(k+1)(2k^2 + 13k + 18)}{6} &= \\ \frac{(k+1)(k+2)(2k+9)}{6} &= \end{aligned}$$

$$\frac{(k+1)((k+1)+1)(2(k+1)+7)}{6}$$

Thus we have $1 \cdot 3 + 2 \cdot 4 + 3 \cdot 5 + 4 \cdot 6 + \cdots + k(k+2) + (k+1)((k+1)+2) = \frac{(k+1)((k+1)+1)(2(k+1)+7)}{6}$, and this means the statement is true for $n = k + 1$.

Thus the result follows by mathematical induction. ■

- 9.** Prove that $24 \mid (5^{2n} - 1)$ for every integer $n \geq 0$.

Proof. The proof is by mathematical induction.

- (1) For $n = 0$, the statement is $24 \mid (5^{2 \cdot 0} - 1)$. This is $24 \mid 0$, which is true.
 (2) Now assume the statement is true for some integer $n = k \geq 1$, that is assume $24 \mid (5^{2k} - 1)$. This means $5^{2k} - 1 = 24a$ for some integer a , and from this we get $5^{2k} = 24a + 1$. Now observe that

$$\begin{aligned} 5^{2(k+1)} - 1 &= \\ 5^{2k+2} - 1 &= \\ 5^2 5^{2k} - 1 &= \\ 5^2(24a + 1) - 1 &= \\ 25(24a + 1) - 1 &= \\ 25 \cdot 24a + 25 - 1 &= 24(25a + 1). \end{aligned}$$

This shows $5^{2(k+1)} - 1 = 24(25a + 1)$, which means $24 \mid 5^{2(k+1)} - 1$.

This completes the proof by mathematical induction. ■

- 11.** Prove that $3 \mid (n^3 + 5n + 6)$ for every integer $n \geq 0$.

Proof. The proof is by mathematical induction.

- (1) When $n = 0$, the statement is $3 \mid (0^3 + 5 \cdot 0 + 6)$, or $3 \mid 6$, which is true.
 (2) Now assume the statement is true for some integer $n = k \geq 0$, that is assume $3 \mid (k^3 + 5k + 6)$. This means $k^3 + 5k + 6 = 3a$ for some integer a . We need to show that $3 \mid ((k+1)^3 + 5(k+1) + 6)$. Observe that

$$\begin{aligned} (k+1)^3 + 5(k+1) + 6 &= k^3 + 3k^2 + 3k + 1 + 5k + 5 + 6 \\ &= (k^3 + 5k + 6) + 3k^2 + 3k + 6 \\ &= 3a + 3k^2 + 3k + 6 \\ &= 3(a + k^2 + k + 2). \end{aligned}$$

Thus we have deduced $(k+1)^3 + 5(k+1) + 6 = 3(a + k^2 + k + 2)$. Since $a + k^2 + k + 2$ is an integer, it follows that $3 \mid ((k+1)^3 + 5(k+1) + 6)$.

It follows by mathematical induction that $3 \mid (n^3 + 5n + 6)$ for every $n \geq 0$. ■

- 13.** Prove that $6 \mid (n^3 - n)$ for every integer $n \geq 0$.

Proof. The proof is by mathematical induction.

- (1) When $n = 0$, the statement is $6 \mid (0^3 - 0)$, or $6 \mid 0$, which is true.

- (2) Now assume the statement is true for some integer $n = k \geq 0$, that is, assume $6 \mid (k^3 - k)$. This means $k^3 - k = 6a$ for some integer a . We need to show that $6 \mid ((k+1)^3 - (k+1))$. Observe that

$$\begin{aligned}(k+1)^3 - (k+1) &= k^3 + 3k^2 + 3k + 1 - k - 1 \\ &= (k^3 - k) + 3k^2 + 3k \\ &= 6a + 3k^2 + 3k \\ &= 6a + 3k(k+1).\end{aligned}$$

Thus we have deduced $(k+1)^3 - (k+1) = 6a + 3k(k+1)$. Since one of k or $(k+1)$ must be even, it follows that $k(k+1)$ is even, so $k(k+1) = 2b$ for some integer b . Consequently $(k+1)^3 - (k+1) = 6a + 3k(k+1) = 6a + 3(2b) = 6(a+b)$. Since $(k+1)^3 - (k+1) = 6(a+b)$ it follows that $6 \mid ((k+1)^3 - (k+1))$.

Thus the result follows by mathematical induction. \blacksquare

15. If $n \in \mathbb{N}$, then $\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \frac{1}{4 \cdot 5} + \cdots + \frac{1}{n(n+1)} = 1 - \frac{1}{n+1}$.

Proof. The proof is by mathematical induction.

- (1) When $n = 1$, the statement is $\frac{1}{1(1+1)} = 1 - \frac{1}{1+1}$, which simplifies to $\frac{1}{2} = \frac{1}{2}$.
 (2) Now assume the statement is true for some integer $n = k \geq 1$, that is assume $\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \frac{1}{4 \cdot 5} + \cdots + \frac{1}{k(k+1)} = 1 - \frac{1}{k+1}$. Next we show that the statement for $n = k+1$ is true. Observe that

$$\begin{aligned}\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \frac{1}{4 \cdot 5} + \cdots + \frac{1}{k(k+1)} + \frac{1}{(k+1)((k+1)+1)} &= \\ \left(\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \frac{1}{4 \cdot 5} + \cdots + \frac{1}{k(k+1)} \right) + \frac{1}{(k+1)(k+2)} &= \\ \left(1 - \frac{1}{k+1} \right) + \frac{1}{(k+1)(k+2)} &= \\ 1 - \frac{1}{k+1} + \frac{1}{(k+1)(k+2)} &= \\ 1 - \frac{k+2}{(k+1)(k+2)} + \frac{1}{(k+1)(k+2)} &= \\ 1 - \frac{k+1}{(k+1)(k+2)} &= \\ 1 - \frac{1}{k+2} &= \\ 1 - \frac{1}{(k+1)+1}.\end{aligned}$$

This establishes $\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \frac{1}{4 \cdot 5} + \cdots + \frac{1}{(k+1)((k+1)+1)} = 1 - \frac{1}{(k+1)+1}$, which is to say that the statement is true for $n = k+1$.

This completes the proof by mathematical induction. \blacksquare

17. Suppose A_1, A_2, \dots, A_n are sets in some universal set U , and $n \geq 2$. Prove that $\overline{A_1 \cap A_2 \cap \cdots \cap A_n} = \overline{A_1} \cup \overline{A_2} \cup \cdots \cup \overline{A_n}$.

Proof. The proof is by strong induction.

- (1) When $n = 2$ the statement is $\overline{A_1 \cap A_2} = \overline{A_1} \cup \overline{A_2}$. This is not an entirely obvious statement, so we have to prove it. Observe that

$$\begin{aligned}
 \overline{A_1 \cap A_2} &= \{x : (x \in U) \wedge (x \notin A_1 \cap A_2)\} \quad (\text{definition of complement}) \\
 &= \{x : (x \in U) \wedge \sim(x \in A_1 \cap A_2)\} \\
 &= \{x : (x \in U) \wedge \sim((x \in A_1) \wedge (x \in A_2))\} \quad (\text{definition of } \cap) \\
 &= \{x : (x \in U) \wedge (\sim(x \in A_1) \vee \sim(x \in A_2))\} \quad (\text{DeMorgan}) \\
 &= \{x : (x \in U) \wedge ((x \notin A_1) \vee (x \notin A_2))\} \\
 &= \{x : (x \in U) \wedge (x \notin A_1) \vee (x \in U) \wedge (x \notin A_2)\} \quad (\text{distributive prop.}) \\
 &= \{x : ((x \in U) \wedge (x \notin A_1))\} \cup \{x : ((x \in U) \wedge (x \notin A_2))\} \quad (\text{def. of } \cup) \\
 &= \overline{A_1} \cup \overline{A_2} \quad (\text{definition of complement})
 \end{aligned}$$

- (2) Let $k \geq 2$. Assume the statement is true if it involves k or fewer sets. Then

$$\begin{aligned}
 \overline{A_1 \cap A_2 \cap \cdots \cap A_{k-1} \cap A_k \cap A_{k+1}} &= \\
 \overline{A_1 \cap A_2 \cap \cdots \cap A_{k-1} \cap (A_k \cap A_{k+1})} &= \overline{A_1} \cup \overline{A_2} \cup \cdots \cup \overline{A_{k-1}} \cup \overline{A_k \cap A_{k+1}} \\
 &= \overline{A_1} \cup \overline{A_2} \cup \cdots \cup \overline{A_{k-1}} \cup \overline{A_k} \cup \overline{A_{k+1}}
 \end{aligned}$$

Thus the statement is true when it involves $k + 1$ sets.

This completes the proof by strong induction. ■

- 19.** Prove $\sum_{k=1}^n 1/k^2 \leq 2 - 1/n$ for every n .

Proof. This clearly holds for $n = 1$. Assume it holds for some $n \geq 1$. Then $\sum_{k=1}^{n+1} 1/k^2 \leq 2 - 1/n + 1/(n+1)^2 = 2 - \frac{(n+1)^2 - n}{n(n+1)^2} \leq 2 - 1/(n+1)$. The proof is complete. ■

- 21.** If $n \in \mathbb{N}$, then $\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{2^n} \geq 1 + \frac{n}{2}$.

Proof. If $n = 1$, the result is obvious.

Assume the proposition holds for some $n > 1$. Then

$$\begin{aligned}
 \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{2^{n+1}} &= \left(\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{2^n} \right) + \left(\frac{1}{2^n + 1} + \frac{1}{2^n + 2} + \frac{1}{2^n + 3} + \cdots + \frac{1}{2^{n+1}} \right) \\
 &\geq \left(1 + \frac{n}{2} \right) + \left(\frac{1}{2^n + 1} + \frac{1}{2^n + 2} + \frac{1}{2^n + 3} + \cdots + \frac{1}{2^{n+1}} \right).
 \end{aligned}$$

Now, the sum $\left(\frac{1}{2^n + 1} + \frac{1}{2^n + 2} + \frac{1}{2^n + 3} + \cdots + \frac{1}{2^{n+1}} \right)$ on the right has $2^{n+1} - 2^n = 2^n$ terms, all greater than or equal to $\frac{1}{2^{n+1}}$, so the sum is greater than $2^n \frac{1}{2^{n+1}} = \frac{1}{2}$. Therefore we get $\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{2^{n+1}} \geq \left(1 + \frac{n}{2} \right) + \left(\frac{1}{2^n + 1} + \frac{1}{2^n + 2} + \frac{1}{2^n + 3} + \cdots + \frac{1}{2^{n+1}} \right) \geq \left(1 + \frac{n}{2} \right) + \frac{1}{2} = 1 + \frac{n+1}{2}$. This means the result is true for $n + 1$, so the theorem is proved. ■

- 23.** Use induction to prove the binomial theorem $(x + y)^n = \sum_{i=0}^n \binom{n}{i} x^{n-i} y^i$.

Proof. Notice that when $n = 1$, the formula is $(x + y)^1 = \binom{1}{0}x^1y^0 + \binom{1}{1}x^0y^1 = x + y$, which is true.

Now assume the theorem is true for some $n > 1$. We will show that this implies that it is true for the power $n + 1$. Just observe that

$$\begin{aligned}
 (x + y)^{n+1} &= (x + y)(x + y)^n \\
 &= (x + y) \sum_{i=0}^n \binom{n}{i} x^{n-i} y^i \\
 &= \sum_{i=0}^n \binom{n}{i} x^{(n+1)-i} y^i + \sum_{i=0}^n \binom{n}{i} x^{n-i} y^{i+1} \\
 &= \sum_{i=0}^n \left[\binom{n}{i} + \binom{n}{i-1} \right] x^{(n+1)-i} y^i + y^{n+1} \\
 &= \sum_{i=0}^n \binom{n+1}{i} x^{(n+1)-i} y^i + \binom{n+1}{n+1} y^{n+1} \\
 &= \sum_{i=0}^{n+1} \binom{n+1}{i} x^{(n+1)-i} y^i.
 \end{aligned}$$

This shows that the formula is true for $(x + y)^{n+1}$, so the theorem is proved. ■

25. Concerning the Fibonacci sequence, prove that $F_1 + F_2 + F_3 + F_4 + \dots + F_n = F_{n+2} - 1$.

Proof. The proof is by induction.

- (1) When $n = 1$ the statement is $F_1 = F_{1+2} - 1 = F_3 - 1 = 2 - 1 = 1$, which is true. Also when $n = 2$ the statement is $F_1 + F_2 = F_{2+2} - 1 = F_4 - 1 = 3 - 1 = 2$, which is true, as $F_1 + F_2 = 1 + 1 = 2$.
- (2) Now assume $k \geq 1$ and $F_1 + F_2 + F_3 + F_4 + \dots + F_k = F_{k+2} - 1$. We need to show $F_1 + F_2 + F_3 + F_4 + \dots + F_k + F_{k+1} = F_{k+3} - 1$. Observe that

$$\begin{aligned}
 F_1 + F_2 + F_3 + F_4 + \dots + F_k + F_{k+1} &= \\
 (F_1 + F_2 + F_3 + F_4 + \dots + F_k) + F_{k+1} &= \\
 F_{k+2} - 1 + F_{k+1} &= (F_{k+1} + F_{k+2}) - 1 \\
 &= F_{k+3} - 1.
 \end{aligned}$$

This completes the proof by induction. ■

27. Concerning the Fibonacci sequence, prove that $F_1 + F_3 + \dots + F_{2n-1} = F_{2n}$.

Proof. If $n = 1$, the result is immediate. Assume for some $n > 1$ we have $\sum_{i=1}^n F_{2i-1} = F_{2n}$. Then $\sum_{i=1}^{n+1} F_{2i-1} = F_{2n+1} + \sum_{i=1}^n F_{2i-1} = F_{2n+1} + F_{2n} = F_{2n+2} = F_{2(n+1)}$ as desired. ■

29. Prove that $\binom{n}{0} + \binom{n-1}{1} + \binom{n-2}{2} + \binom{n-3}{3} + \dots + \binom{1}{n-1} + \binom{0}{n} = F_{n+1}$.

Proof. (Strong Induction) For $n = 1$ this is $\binom{1}{0} + \binom{0}{1} = 1 + 0 = 1 = F_2 = F_{1+1}$. Thus the assertion is true when $n = 1$.

Now fix n and assume that $\binom{k}{0} + \binom{k-1}{1} + \binom{k-2}{2} + \binom{k-3}{3} + \dots + \binom{1}{k-1} + \binom{0}{k} = F_{k+1}$ whenever $k < n$. In what follows we use the identity $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$. We also often use $\binom{a}{b} = 0$ whenever it is untrue that $0 \leq b \leq a$.

$$\begin{aligned} & \binom{n}{0} + \binom{n-1}{1} + \binom{n-2}{2} + \dots + \binom{1}{n-1} + \binom{0}{n} \\ = & \binom{n}{0} + \binom{n-1}{1} + \binom{n-2}{2} + \dots + \binom{1}{n-1} \\ = & \binom{n-1}{-1} + \binom{n-1}{0} + \binom{n-2}{0} + \binom{n-2}{1} + \binom{n-3}{1} + \binom{n-3}{2} + \dots + \binom{0}{n-1} + \binom{0}{n} \\ = & \binom{n-1}{0} + \binom{n-2}{0} + \binom{n-2}{1} + \binom{n-3}{1} + \binom{n-3}{2} + \dots + \binom{0}{n-1} + \binom{0}{n} \\ = & \left[\binom{n-1}{0} + \binom{n-2}{1} + \dots + \binom{0}{n-1} \right] + \left[\binom{n-2}{0} + \binom{n-3}{1} + \dots + \binom{0}{n-2} \right] \\ = & F_n + F_{n-1} = F_n \end{aligned}$$

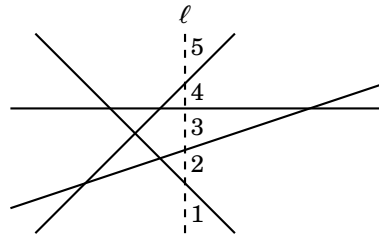
This completes the proof. ■

- 31. Prove that $\sum_{k=0}^n \binom{k}{r} = \binom{n+1}{r+1}$, where $r \in \mathbb{N}$.
Hint: Use induction on the integer n . After doing the basis step, break up the expression $\binom{k}{r}$ as $\binom{k}{r} = \binom{k-1}{r-1} + \binom{k-1}{r}$. Then regroup, use the induction hypothesis, and recombine using the above identity.
- 33. Suppose that n infinitely long straight lines lie on the plane in such a way that no two are parallel, and no three intersect at a single point. Show that this arrangement divides the plane into $\frac{n^2+n+2}{2}$ regions.

Proof. The proof is by induction. For the basis step, suppose $n = 1$. Then there is one line, and it clearly divides the plane into 2 regions, one on either side of the line. As $2 = \frac{1^2+1+2}{2} = \frac{n^2+n+2}{2}$, the formula is correct when $n = 1$.

Now suppose there are $n + 1$ lines on the plane, and that the formula is correct for when there are n lines on the plane. Single out one of the $n + 1$ lines on the plane, and call it ℓ . Remove line ℓ , so that there are now n lines on the plane.

By the induction hypothesis, these n lines divide the plane into $\frac{n^2+n+2}{2}$ regions. Now add line ℓ back. Doing this adds an additional $n + 1$ regions. (The diagram illustrates the case where $n + 1 = 5$. Without ℓ , there are $n = 4$ lines. Adding ℓ back produces $n + 1 = 5$ new regions.)



Thus, with $n + 1$ lines there are all together $(n + 1) + \frac{n^2+n+2}{2}$ regions. Observe

$$(n + 1) + \frac{n^2 + n + 2}{2} = \frac{2n + 2 + n^2 + n + 2}{2} = \frac{(n + 1)^2 + (n + 1) + 2}{2}.$$

Thus, with $n + 1$ lines, we have $\frac{(n+1)^2 + (n+1) + 2}{2}$ regions, which means that the formula is true for when there are $n + 1$ lines. We have shown that if the formula is true for n lines, it is also true for $n + 1$ lines. This completes the proof by induction. ■

35. If $n, k \in \mathbb{N}$, and n is even and k is odd, then $\binom{n}{k}$ is even.

Proof. Notice that if k is not a value between 0 and n , then $\binom{n}{k} = 0$ is even; thus from here on we can assume that $0 < k < n$. We will use strong induction.

For the basis case, notice that the assertion is true for the even values $n = 2$ and $n = 4$: $\binom{2}{1} = 2$; $\binom{4}{1} = 4$; $\binom{4}{3} = 4$ (even in each case).

Now fix an even n assume that $\binom{m}{k}$ is even whenever m is even, k is odd, and $m < n$. Using the identity $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$ three times, we get

$$\begin{aligned} \binom{n}{k} &= \binom{n-1}{k-1} + \binom{n-1}{k} \\ &= \binom{n-2}{k-2} + \binom{n-2}{k-1} + \binom{n-2}{k-1} + \binom{n-2}{k} \\ &= \binom{n-2}{k-2} + 2\binom{n-2}{k-1} + \binom{n-2}{k}. \end{aligned}$$

Now, $n - 2$ is even, and k and $k - 2$ are odd. By the inductive hypothesis, the outer terms of the above expression are even, and the middle is clearly even; thus we have expressed $\binom{n}{k}$ as the sum of three even integers, so it is even. ■

37. Prove that if $m, n \in \mathbb{N}$, then $\sum_{k=0}^n k \binom{m+k}{m} = n \binom{m+n+1}{m+1} - \binom{m+n+1}{m+2}$.

Proof. We will use induction on n . Let m be any integer.

(1) If $n = 1$, then the equation is $\sum_{k=0}^1 k \binom{m+k}{m} = 1 \binom{m+1+1}{m+1} - \binom{m+1+1}{m+2}$, and this is $0 \binom{m}{m} + 1 \binom{m+1}{m} = 1 \binom{m+2}{m+1} - \binom{m+2}{m+2}$, which yields the true statement $m+1 = m+2-1$.

(2) Now let $n > 1$ and assume the equation holds for n . (This is the inductive hypothesis.) Now we will confirm that it holds for $n + 1$. Observe that

$$\sum_{k=0}^{n+1} k \binom{m+k}{m} = \quad \text{(left-hand side for } n+1)$$

$$\sum_{k=0}^n k \binom{m+k}{m} + (n+1) \binom{m+(n+1)}{m} = \quad \text{(split off final term)}$$

$$n \binom{m+n+1}{m+1} - \binom{m+n+1}{m+2} + (n+1) \binom{m+n+1}{m} = \quad \text{(apply inductive hypothesis)}$$

$$n \binom{m+n+1}{m+1} + \binom{m+n+1}{m+1} - \binom{m+n+2}{m+2} + (n+1) \binom{m+n+1}{m} = \quad \text{(Pascal's formula)}$$

$$(n+1) \binom{m+n+1}{m+1} - \binom{m+n+2}{m+2} + (n+1) \binom{m+n+1}{m} = \quad \text{(factor)}$$

$$\begin{aligned}
(n+1) \left[\binom{m+n+1}{m+1} + \binom{m+n+1}{m} \right] - \binom{m+n+2}{m+2} &= && \text{(factor again)} \\
(n+1) \binom{m+n+2}{m+1} - \binom{m+n+2}{m+2} &= && \text{(Pascal's formula)} \\
(n+1) \binom{m+(n+1)+1}{m+1} - \binom{m+(n+1)+1}{m+2} &= && \text{(right-hand side for } n+1)
\end{aligned}$$

The proof is done. ■

39. If n and k are non-negative integers, then $\binom{n+0}{0} + \binom{n+1}{1} + \binom{n+2}{2} + \cdots + \binom{n+k}{k} = \binom{n+k+1}{k}$.

Proof. We will use induction on k . Let n be any non-negative integer.

- (1) If $k = 0$, then the equation is $\binom{n+0}{0} = \binom{n+0+1}{0}$, which reduces to $1 = 1$.
(2) Assume the equation holds for some $k \geq 1$. (This is the inductive hypothesis.)

Now we will show that it holds for $k+1$. Note that

$$\begin{aligned}
&\binom{n+0}{0} + \binom{n+1}{1} + \binom{n+2}{2} + \cdots + \binom{n+k}{k} + \binom{n+(k+1)}{k+1} && \text{(left side for } k+1) \\
&= \binom{n+k+1}{k} + \binom{n+k+1}{k+1} && \text{(apply inductive hypothesis)} \\
&= \binom{n+k+2}{k+1} && \text{(Pascal's formula)} \\
&= \binom{n+(k+1)+1}{k+1}. && \text{(right-hand side for } k+1)
\end{aligned}$$

The proof is complete. ■

41. Prove that $\sum_{k=0}^m \binom{m}{k} \binom{n}{p+k} = \binom{m+n}{m+p}$ for non-negative integers m, n and p .

Proof. We will use induction on n . Let m and p be any non-negative integers.

- (1) If $n = 0$, then the equation is $\sum_{k=0}^m \binom{m}{k} \binom{0}{p+k} = \binom{m+0}{m+p}$. This holds if $p > 0$, because then $\binom{0}{p+k} = 0 = \binom{m}{m+p}$, and both sides of the equation are zero. If $p = 0$, the equation is $\sum_{k=0}^m \binom{m}{k} \binom{0}{k} = \binom{m}{m}$, and both sides equal 1.
(2) Now take $n \geq 1$ and suppose the equation holds for n . (This is the inductive hypothesis.) Next we confirm that the equation holds for $n+1$.

$$\begin{aligned}
&\binom{m+(n+1)}{m+p} && \text{(right-hand side for } n+1) \\
&= \binom{m+n}{m+(p-1)} + \binom{m+n}{m+p} && \text{(Pascal's formula)} \\
&= \sum_{k=0}^m \binom{m}{k} \binom{n}{(p-1)+k} + \sum_{k=0}^m \binom{m}{k} \binom{n}{p+k} && \text{(apply inductive hypothesis)}
\end{aligned}$$

$$\begin{aligned} &= \sum_{k=0}^m \binom{m}{k} \left[\binom{n}{(p-1)+k} + \binom{n}{p+k} \right] && \text{(combine)} \\ &= \sum_{k=0}^m \binom{m}{k} \binom{n+1}{p+k} && \text{(Pascal's formula)} \end{aligned}$$

This final expression is left-hand side for $n + 1$, so the proof is finished. ■

Introduction to Graph Theory

In mathematical English the word *graph* has two meanings. In one context, a graph is a visual device that describes the relationship between two or more variables, as in the graph of a function; these are the kinds of graphs encountered in algebra and calculus. In its other meaning, a graph is a system of interconnecting nodes. In this second context, a graph can be visualized as set of nodes, and lines connecting pairs of nodes. Graphs are useful because they model relationships between entities in ways that cannot be expressed by arithmetic, algebra and calculus alone. A molecule is a graph: the nodes are atoms and the edges are bonds between atoms. A map of an airline's flights is a graph: the nodes are cities and the edges are routes between cities. Your family tree is a graph. In computer science, data structures of all types can be thought of and analyzed as graphs.

The mathematical study of properties of graphs is called *Graph Theory*. Graph theory is relatively new as a mathematical discipline. Although a few papers from the later half of the 1800's dealt with what we now call graphs, it wasn't until around 1950 that graph theory began to emerge as an independent field of study. Originally it had a somewhat recreational flavor, often dealing with mathematical questions motivated by games and puzzles. But it is a perfect language for expressing structures in computer science, and the field grew with the computer revolution.

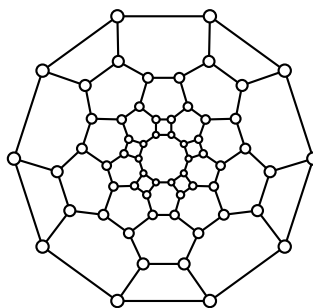


Figure 15.1. A graph.

Today graph theory is a vast and ever-expanding field of study. This chapter, then, can only be a brief introduction. We will lay out the main definitions, prove a few theorems, and examine some graph algorithms. You will build on this platform if you continue with discrete mathematics beyond this text.

This chapter also presents an opportunity to practice the various proof techniques that you learned in earlier chapters.

15.1 Graphs and Subgraphs

Technically, a node in a graph is called a **vertex**. The plural of vertex is **vertices**. Graphs are usually denoted by upper-case letters, like G or H . To specify a graph G , we need only to describe its vertices and edges. Here is the exact definition.

Definition 15.1 A **graph** G is a finite set $V(G)$ of objects, called **vertices**, together with a set $E(G)$ of two-element subsets of $V(G)$, called **edges**. An edge $\{x, y\} \in E(G)$ is abbreviated as xy or yx .

For example, consider the graph G with $V(G) = \{a, b, c, d, e\}$ and $E(G) = \{ab, bc, cd, de, ea, ad, eb\}$. We can make a picture of G by drawing a dot or small circle for each vertex in $V(G)$, and then drawing line segments joining any two vertices that appear as an edge in $E(G)$. Figure 15.2 shows three different pictures of this graph. In drawing a graph we do not mind if the edges cross each other, but we never allow an edge touch any vertex that is not one of its endpoints.

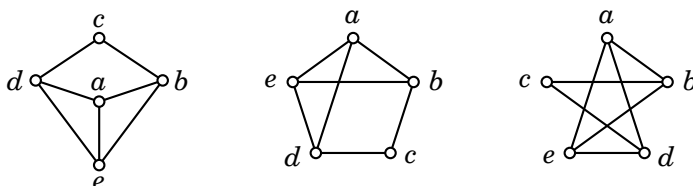
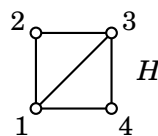


Figure 15.2. Three drawings of the same graph G .

We say two vertices $x, y \in V(G)$ are **adjacent** if $xy \in E(G)$. Thus for the graph G drawn in Figure 15.2, a and b are adjacent, but a and c are not. The **endpoints** an edge xy are the vertices x and y . Two edges are **incident** if they share an endpoint. So ab and bc are incident, but ab and cd are not. A vertex and an edge are **incident** if the vertex is an endpoint of the edge. Thus the edge ab is incident with both of the vertices a and b .

Please note that the sets $V(G)$ and $E(G)$ contain no information other than what the vertices are, and which pairs of them are adjacent. There are endless ways to draw the same graph.

Often we specify a graph simply by drawing it. The figure on the left conveys that H is a graph with vertex set $V(H) = \{1, 2, 3, 4\}$ and $E(G) = \{12, 23, 34, 41, 13\}$. Drawing the picture is easier than writing out $V(G)$ and $E(G)$.



Some graphs so common that we reserve special symbols for them. Given a positive integer n , the **path** P_n is the graph with n vertices v_1, v_2, \dots, v_n and edges $E(P_n) = \{v_1v_2, v_2v_3, v_3v_4, \dots, v_{n-1}v_n\}$. Thus P_n has n vertices and $n - 1$ edges. The **cycle** C_n is the graph with n vertices v_1, v_2, \dots, v_n and edges $E(C_n) = \{v_1v_2, v_2v_3, v_3v_4, \dots, v_{n-1}v_n, v_nv_1\}$. See Figure 15.3. We say a path or cycle is **even** if it has an even number of vertices; otherwise it is **odd**.

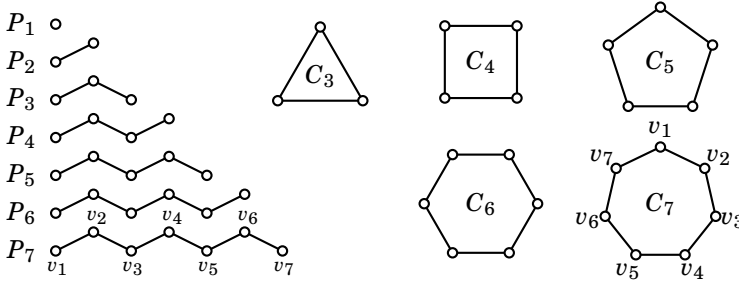


Figure 15.3. Paths and cycles

The **complete graph** K_n is the graph with n vertices and an edge joining every pair of vertices, as in Figure 15.4. The number of edges in K_n is $\binom{n}{2} = \frac{n(n-1)}{2}$, the number of ways to choose two endpoints from n vertices.

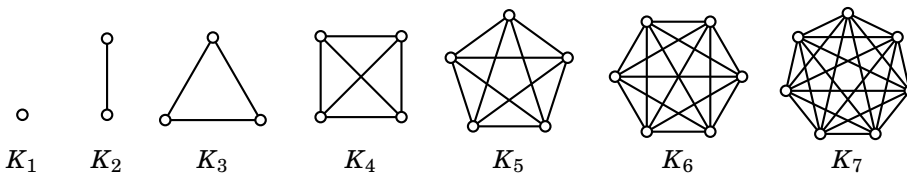


Figure 15.4. Complete graphs

For two positive integers m and n , the **complete bipartite graph** $K_{m,n}$ is the graph whose vertex set $V(K_{m,n}) = X \cup Y$ is the union of two disjoint sets X and Y of sizes m and n , respectively, and with $E(K_{m,n}) = \{xy : x \in X, y \in Y\}$.

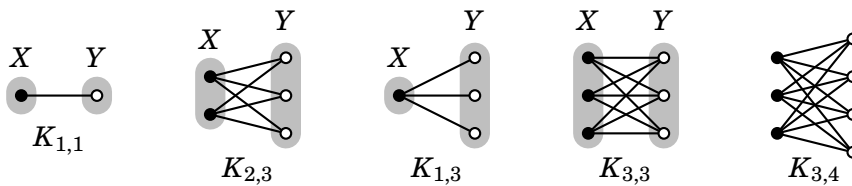
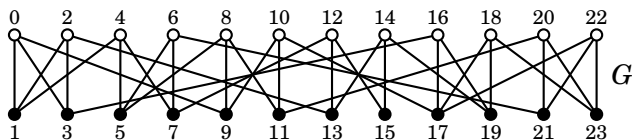


Figure 15.5. Complete bipartite graphs.

The complete bipartite graphs $K_{m,n}$ are special graphs in a larger class of graphs called *bipartite* graphs. A graph G is said to be **bipartite** if it is possible to find some partition $V(G) = X \cup Y$ of $V(G)$ into two disjoint sets, so that each edge of G has one endpoint in X and the other in Y . For example, here is a bipartite graph G , with $X = \{0, 2, 4, \dots, 22\}$ and $Y = \{1, 3, 5, \dots, 23\}$:



Think of a bipartite graph as one whose vertices can be colored black (X) and white (Y) so that each edge joins a black vertex to a white one. The graph by no means has to be drawn with the black and white vertices lined up on different sides. Here is a picture of the exact same graph G above.

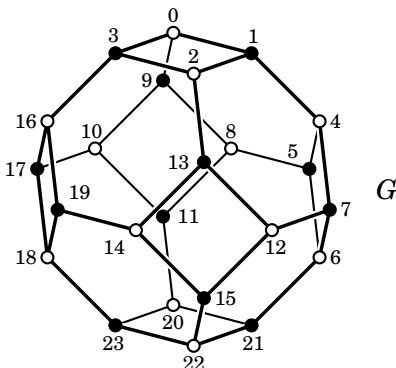


Figure 15.6 indicates that the even cycles C_4, C_6, C_8, \dots are bipartite. But the odd cycles C_3, C_5, C_7, \dots are *not* bipartite. Alternating black and white around the cycle forces two adjacent vertices of the same color at the end.

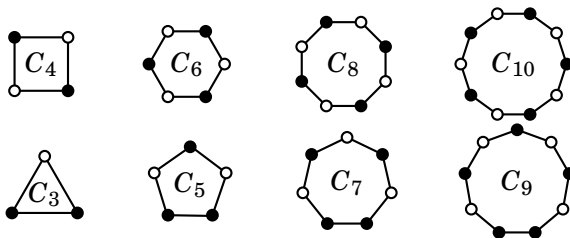
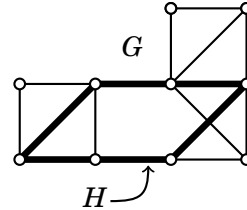


Figure 15.6. Even cycles are bipartite; odd cycles are not bipartite.

A graph inside a graph is called a *subgraph*.

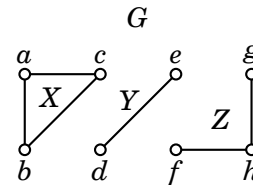
Definition 15.2 A graph H is said to be a **subgraph** of a graph G provided that $V(H) \subseteq V(G)$ and $E(H) \subseteq E(G)$.

For example, the bolded part of the graph G on the right is a graph H with $V(H) \subseteq V(G)$ and $E(H) \subseteq E(G)$, so H is a subgraph of G . When one graph H is a subgraph of another graph G , we say that G **contains** H , or H **is in** G . In this case, the graph H happens to be a cycle C_6 , so we say that G contains a C_6 . You can also find a P_{10} in G .



We say that a graph G is **connected** if for any two vertices $x, y \in V(G)$, there is a path in G that starts at x and ends at y . A graph that is not connected is said to be **disconnected**. For an example of a disconnected graph, let G be the roadmap of Hawaii, where roads are edges and intersections are vertices. This graph is not connected, because if x and y are vertices on different islands, then G has no subgraph that is a path from x to y .

For another example, see the graph G on the right. It has vertices $V(G) = \{a, b, c, d, e, f, g, h\}$, and edges $E(G) = \{ab, bc, ca, de, fh, gh\}$. This graph is not connected because it has no path joining (say) vertex a to vertex d . The connected “parts” of a disconnected graph are called its *components*. To be precise, a **component** of a graph is a connected



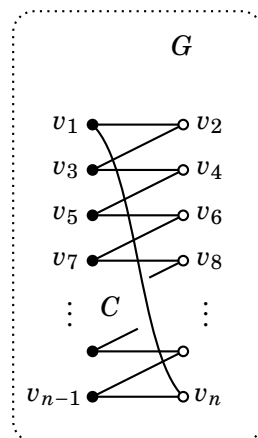
subgraph that is not a subgraph of a larger connected subgraph. Thus the above G has components X, Y and Z , as indicated. (Pay careful attention to the wording of the definition of a component. The single edge ab is a connected subgraph of G , but it is not a component because it is a subgraph of the larger connected subgraph X . But the subgraph X is a component because it is not a subgraph of any larger *connected* subgraph of G .) Note that a connected graph has just one component; a disconnected graph has more than one component.

There are many theorems in graph theory that explain how the structure of a graph is influenced by the structures of its subgraphs. Here is one.

Theorem 15.1 A graph is bipartite if and only if it contains no odd cycle.

Proof. This is an if and only if theorem, so proving it involves proving two implications.

First we prove that if a graph G is bipartite, then it has no cycle of odd length. We use direct proof. Let G be bipartite, say C be an arbitrary cycle in G . We must show that C has *even* length. Label the vertices of C as $V(C) = \{v_1, v_2, v_3, \dots, v_n\}$ with $E(C) = \{v_1v_2, v_2v_3, \dots, v_{n-1}v_n, v_nv_1\}$. As G is bipartite, its vertices can be colored black and white in such a way that the endpoints of each edge have different colors. Without loss of generality, say v_1 is black. Traversing C , its vertices alternate black, white, black, white, etc., until we get to v_n , which is white because it's adjacent to the black vertex v_1 . Thus C has as many white vertices as it does black vertices, so C is even.



Conversely, suppose G has no cycles of odd length. We prove G is bipartite using strong induction on $|E(G)|$.

For the basis step, suppose G has no odd cycles, and $|E(G)| = 0$. Then G has no edges, so it just a set of one or more vertices. Color the vertices of G black and white, in any arbitrary manner. Then G has no edge whose endpoints have the same color, so G is bipartite.

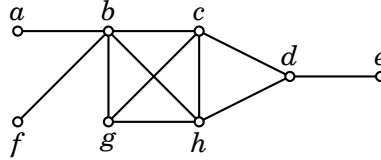
Now for the inductive step. Suppose that G has $|E(G)| > 0$ edges, and that any graph with no odd cycles and fewer than $|E(G)|$ edges is bipartite. Select an arbitrary edge $xy \in E(G)$. Let H be the graph with $V(H) = V(G)$ and $E(H) = E(G) - \{xy\}$. (That is, H is G with the edge xy removed.) Then H has no odd cycles, and fewer edges than does G , so H is bipartite. Thus the vertices of H can be colored black and white, in such a way that the two endpoints of any edge of H have different colors.

But because $V(H) = V(G)$, we have also colored the vertices of G black and white, and because $E(H) = E(G) - \{xy\}$, every edge of G except possibly xy has different-colored endpoints. If H has a path P from x to y , then P has odd length, for otherwise appending xy to P would result in an odd cycle in G . This means the endpoints x and y of P have different colors. Thus the vertices of G have now been colored black and white, so that every edge of G has different-colored endpoints. Therefore G is bipartite.

If H has no path from x to y , then x and y are in different components of H . Let K be the component of H that contains x . If x and y have the same color, swap the colors in the component K , so that black becomes white and white becomes black. Now the vertices of H are colored black and white, and each edge of H has different-colored endpoints, **and** x and y have different colors. Thus the vertices of G are colored black and white, and each edge of G has different-colored endpoints. Thus G is bipartite. ■

15.2 Vertex-degree and Trees

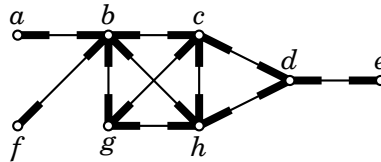
Given a vertex x of a graph G , the **degree** of x , denoted $\deg(x)$, is the number of edges of G that are incident with x . For example, for the graph below, we have $\deg(a) = 1$, $\deg(b) = 5$, $\deg(c) = 4$ and $\deg(d) = 3$.



Imagine adding up the degrees of all the vertices in a graph. In our example above, this would be

$$\deg(a) + \deg(b) + \deg(c) + \deg(d) + \deg(e) + \deg(f) + \deg(g) + \deg(h).$$

This adds up the total number of the bold “spokes” in the below diagram. Because each edge of the graph has exactly two spokes on it, the total number of spokes is twice the number of edges, or $2|E(G)|$.



From this reasoning, you can see that the sum of all the vertex degrees of a graph is twice the number of its edges. We use the notation $\sum_{x \in V(G)} \deg(x)$ to stand for the sum of the degrees of all the vertices of G , the idea being that we add in $\deg(x)$ once for each $x \in V(G)$. Let's summarize this as a fact.

Fact 15.1 For any graph G , the sum of the degrees its vertices is twice its number of its edges, that is,

$$\sum_{x \in V(G)} \deg(x) = 2|E(G)|.$$

In particular, this means that the sum of all the vertex degrees is *even*. Now, if the sum of integers is even, then the number of odd terms in the sum must be even. This yields an immediate proposition.

Proposition 15.1 A graph has an even number of vertices of odd degree.

For example, the graph on the previous page has 6 vertices of odd degree. Also, $K_{3,4}$ has 4 vertices of odd degree, and K_5 has 0 vertices of odd degree. Try to draw a graph with an odd number of odd-degree vertices. You can't.

Fact 15.1 yields a formula for the average degree of a vertex of a graph, which is the sum of all vertex degrees, divided by the number of vertices. The average vertex degree of a graph G is

$$\frac{\sum_{x \in V(G)} \deg(x)}{|V(G)|} = \frac{2|E(G)|}{|V(G)|}. \quad (15.1)$$

This equation is helpful for proving certain facts about trees. Recall that a **tree** is a connected graph that has no cycles. We first encountered trees in Chapter 14, where we used strong induction to prove that a tree always has one fewer edge than it has vertices (page 332). For easy reference, we record the definition of a tree again here, as well as the definition of a *forest*.

Definition 15.3 A **tree** is a connected graph that contains no subgraphs that are cycles. A **forest** is a graph that contains no cycles as subgraphs.

Thus a tree and a forest are graphs without cycles. The difference is that a tree must be connected, but a forest need not be. Thus every tree is a forest, but a forest is not a tree unless it is connected. Figure 15.7 shows an example of a forest. Note that every component of a forest is a tree.

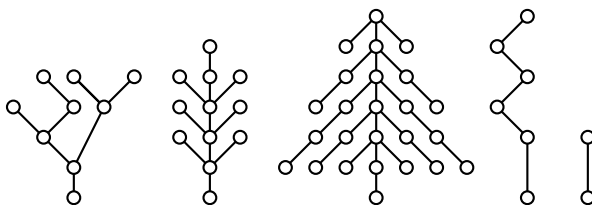


Figure 15.7. A forest. Every component of a forest is a tree.

For other examples, note that any path P_n is a tree. Also, any complete bipartite graph $K_{1,n}$ (where one partite set has size 1) is a tree.

Note that because a tree contains no cycles, it certainly has no odd cycles, so it is bipartite, by Theorem 15.1. (The same is true for forests.)

Proposition 15.2 If a tree has n vertices, then it has $n - 1$ edges. If a forest has n vertices and c components, then it has $n - c$ edges.

Proof. We have already proved part of this proposition. On page 332 we used induction to prove that a tree with n vertices has $n - 1$ edges.

Next suppose G is a forest with n vertices and c components. Call the components G_1, G_2, \dots, G_c . Because each component G_i is a tree, it has $|V(G_i)| - 1$ edges. Then the total number of edges of G is

$$\sum_{i=1}^c (|V(G_i)| - 1) = \left(\sum_{i=1}^c |V(G_i)| \right) - c = n - c. \quad \blacksquare$$

For example, the forest in Figure 15.7 has 54 vertices and 5 components, so it must have $54 - 5 = 49$ edges, which a count verifies.

One interesting thing about trees is that their average vertex degree is quite low. Equation (15.1) and Proposition 15.2 imply that a tree with n vertices has average degree $\frac{2|E(G)|}{|V(G)|} = \frac{2(n-1)}{n} = \frac{2n-2}{n} = 2 - \frac{2}{n}$. This is less than 2, that is, the average vertex degree of any tree is less than 2. Consequently every tree must have at least one vertex of degree 0 or 1. But if a tree has more than one vertex, it can't have any vertices of degree 0, because it is connected. This reasoning yields a lemma.

Lemma 15.1 A tree with more than one vertex has a vertex of degree 1.

Actually, you can prove a stronger result: Any tree with more than one vertex has at least *two* vertices of degree 1 (Exercise 15.??).

Lemma 15.1 can be useful when you are using induction to prove some proposition about trees. Your strategy might be as follows. First show the proposition is true for the tree with one vertex. Then let T be a larger tree, and assume the proposition is true for trees with fewer vertices than T . The lemma says T has a vertex x of degree 1. Remove x and the edge incident with x from T to form a smaller tree T' . By the induction hypothesis, the proposition holds for T' . Now use this to show the result is true for T .

15.3 Colorings and Chromatic Number

Many practical problems can be modeled and solved by assigning colors to the vertices of a graph. Given an integer k , a **k -coloring** of a graph is an assignment of k colors to the vertices of the graph, so that each vertex gets one of the k colors. Often we denote the k colors by the integers $1, 2, 3, \dots, k$. (For example, 1 means red, 2 means blue, 3 is yellow, etc.) Figure 15.8 shows two 3-colorings and a 5-coloring of a graph.

A coloring of a graph is said to be a **proper coloring** if no two adjacent vertices have the same color, that is, if the endpoints of each edge have different colors. The coloring on the left of Figure 15.8 is not proper because there are two edges whose endpoints have the same color. The other two colorings in the figure *are* proper colorings.

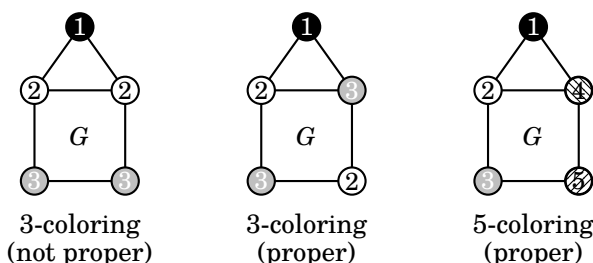


Figure 15.8. Three different colorings of a graph. The one on the left is not a proper coloring. The other two are proper colorings.

Figure 15.8 shows a proper 3-coloring and a proper 5-coloring of G . You will have no trouble finding a proper 4-coloring of G . But you can't draw a proper 2-coloring of this particular graph, because triangle in the graph can't be colored with 2 colors without the endpoints of one of its edges having the same color.

Definition 15.4 The **chromatic number** of a graph, denoted $\chi(G)$, is the smallest integer k for which the graph has a proper k -coloring.

For example, for the graph G in Figure 15.8, we have $\chi(G) = 3$ because the figure shows a proper 3-coloring, but we remarked that no proper 2-coloring (or 1-coloring) exists.

For another example, note that $\chi(K_n) = n$, because we can make a proper coloring by using n colors and giving each of the n vertices its own color. Further, if we colored the n vertices of K_n with fewer than n colors, then this would not be a proper coloring because two (adjacent) vertices would have to have the same color. Thus n is the smallest number of colors required for a proper coloring of K_n , which means $\chi(K_n) = n$.

But for complete bipartite graphs we have $\chi(K_{m,n}) = 2$, because $K_{m,n}$ is bipartite, which means its vertices can be colored with two colors, black and white, with no edge having endpoints of the same color. For the same reason, any bipartite graph that has at least one edge has chromatic number 2.

Concerning the chromatic number of cycles, C_n is bipartite when n is even, so $\chi(C_n) = 2$. For odd cycles, we can obtain a proper coloring with 3 colors as indicated in 15.9, by alternating black and white around the cycle until reaching a final (mismatched) vertex which must be assigned a third color gray. Therefore a formula for cycles is

$$\chi(C_n) = \begin{cases} 2 & \text{if } n \text{ is even} \\ 3 & \text{if } n \text{ is odd.} \end{cases}$$

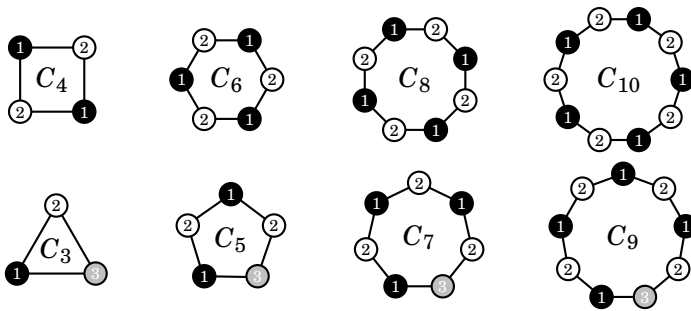


Figure 15.9. For even cycles, $\chi(C_n) = 2$. For odd cycles, $\chi(C_n) = 3$.

There are many practical optimization problems in fields as diverse as computer science and telecommunications that can be solved by finding the chromatic number of a graph. Here is a simple example involving scheduling.

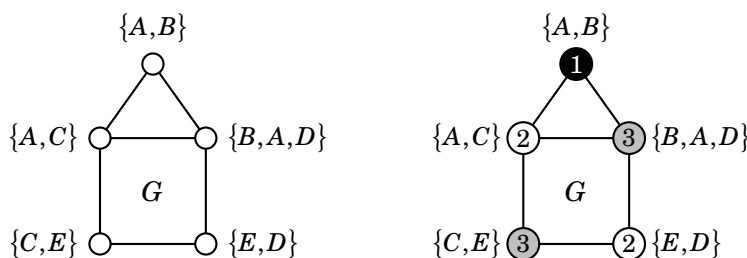
Example 15.1 An office has five employees, call them A, B, C, D and E . These five people belong to five committees, $\{A, B\}, \{A, C\}, \{B, A, D\}, \{C, E\}$ and $\{E, D\}$ (where the sets indicate who’s on each committee). One day, each committee has to meet for one hour. Obviously all five committees can’t meet during the same hour, because some people belong to several committees and can’t be two places at the same time. What is the fewest number of hours needed for all of the committees to meet?

The simple-minded solution is to block off hours of the day for each committee to meet, one after the other. This takes five hours.

| hour | time | committee meeting |
|------|-----------|-------------------|
| 1 | 1:00–2:00 | $\{A, B\}$ |
| 2 | 2:00–3:00 | $\{A, C\}$ |
| 3 | 3:00–4:00 | $\{B, A, D\}$ |
| 4 | 4:00–5:00 | $\{C, E\}$ |
| 5 | 5:00–6:00 | $\{E, D\}$ |

But the meetings can be done in fewer than five hours, because, for instance, committees $\{B, A, D\}$ and $\{C, E\}$ have no members in common, and can meet at the same time. We need to find the *fewest* number of hours required for all committees to meet.

This problem can be modeled with a graph. Let the vertices be the committees, and connect an edge between two committees whenever they have a person in common, and therefore can’t meet during the same hour. The resulting graph G is drawn below, left.



To find an optimal schedule, we can give G a proper coloring, using colors corresponding to hours 1,2,3,..., so that no two adjacent committees meet at the same hour (and using the fewest possible colors). This happens to be the same graph as in Figure 15.8, where $\chi(G) = 3$, and a proper 3-coloring is shown above on the right. Thus the optimal schedule uses only three hours:

| hour | time | committee meeting |
|------|-----------|-------------------|
| 1 | 1:00–2:00 | {A,B} |
| 2 | 2:00–3:00 | {A,C} and {E,D} |
| 3 | 3:00–4:00 | {C,E} and {B,A,D} |

Though this example is simple, you can imagine much more complicated situations in which the chromatic number would optimize efficiency.

Given that the chromatic number of a graph has the potential to solve real-life problems, we would hope for a formula or algorithm to compute it. Unfortunately, the general problem of finding the chromatic number turns out to be what is called an *NP-complete* problem, meaning—roughly—that the general consensus is that a simple formula or efficient algorithm for the chromatic number of an arbitrary graph is impossible. We will learn about NP-completeness in Chapter ???. What this means for us now is that computing chromatic numbers is somewhat of an art, and sometimes (for complex graphs) the best we can hope for is an estimate. Here is a proposition that, if cleverly used, gives a lower bound for $\chi(G)$.

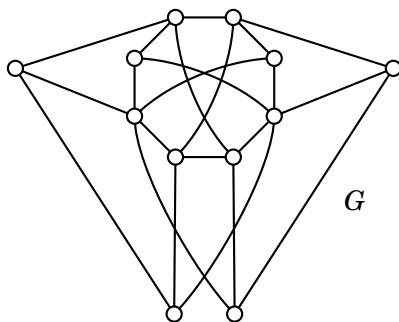
Proposition 15.3 If H is a subgraph of G , then $\chi(H) \leq \chi(G)$.

Proof. We use direct proof. Suppose that H is a subgraph of G . By definition of the chromatic number, G has a proper coloring with $\chi(G)$ colors. Because every vertex of H is also a vertex of G , the vertices of H are colored by the coloring of G . And because each edge of H is an edge of G , no two edges of H have the same color. Thus H is properly colored with no more than $\chi(G)$ colors. (Possibly some of the colors of G 's vertices do not appear in

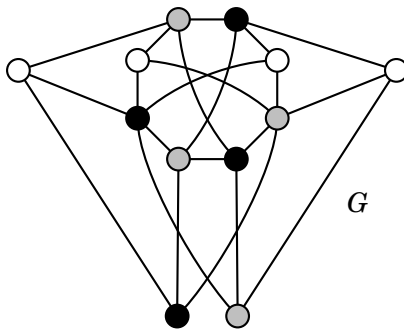
H 's.) It follows that the chromatic number of H is at most $\chi(G)$, that is, $\chi(H) \leq \chi(G)$. ■


We can use this proposition help find $\chi(G)$. If we can find a subgraph H of G that is a familiar graph with a known chromatic number (such as K_n or C_n), then we know the chromatic number of the unfamiliar graph G is not smaller than that of the familiar graph H . Thus we can rule out k -colorings of G that use fewer colors than $\chi(H)$. Sometimes this information is enough that a little informed experimentation can zero in on $\chi(G)$.

Example 15.2 Find the chromatic number of the graph drawn below.



Solution. This graph has a 5-cycle C_5 as a subgraph (find it), and $\chi(C_5) = 3$, so Proposition 15.3 says $3 = \chi(C_5) \leq \chi(G)$. Thus $\chi(G)$ cannot be smaller than 3. But trial-and-error gives the following coloring of G with exactly 3 colors.



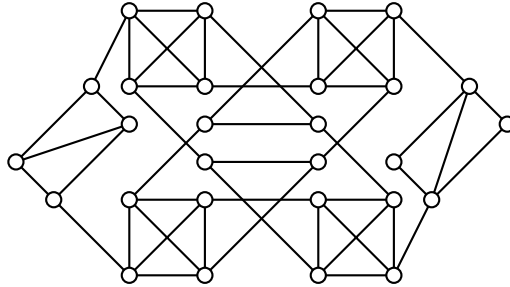
Thus in fact $\chi(G) = 3$. 


Proposition 15.3 gives a lower bound on $\chi(G)$, but it gives no information about how much bigger $\chi(G)$ is than $\chi(H)$. The previous example used an additional trial-and-error step to show $\chi(G)$ was exactly $\chi(H)$. For an upper bound, we have Brook's Theorem.

Theorem 15.2 (Brook's Theorem) Suppose G a connected graph that is neither a complete graph nor an odd cycle. If the largest vertex degree of G is Δ , then $\chi(G) \leq \Delta$.

The proof of Brook's theorem is too long to include here. (But if you have come this far it is within your grasp.) If you enjoy the subject, then perhaps you will encounter a proof of it later, in a first course in graph theory.

Example 15.3 Find the chromatic number of the graph drawn below.



Solution. The graph has a K_4 as a subgraph, and we know $\chi(K_4) = 4$. Thus Proposition 15.3 yields $4 = \chi(K_4) \leq \chi(G)$. But also the largest vertex degree is $\Delta = 4$, so Brook's theorem gives $\chi(G) \leq \Delta = 4$. Consequently $4 \leq \chi(G) \leq 4$, so $\chi(G) = 4$. 

Relations

In mathematics there are endless ways that two entities can be related to each other. Consider the following mathematical statements.

$$\begin{array}{ccccccccc}
 5 < 10 & 5 \leq 5 & 6 = \frac{30}{5} & 5 \mid 80 & 7 > 4 & x \neq y & 8 \nmid 3 \\
 a \equiv b \pmod{n} & 6 \in \mathbb{Z} & X \subseteq Y & \pi \approx 3.14 & 0 \geq -1 & \sqrt{2} \notin \mathbb{Z} & \mathbb{Z} \not\subseteq \mathbb{N}
 \end{array}$$

In each case two entities appear on either side of a symbol, and we interpret the symbol as expressing some relationship between the two entities. Symbols such as $<$, \leq , $=$, \mid , \nmid , \geq , $>$, \in and \subset , etc., are called *relations* because they convey relationships among things.

Relations are significant. In fact, you would have to admit that there would be precious little left of mathematics if we took away all the relations. Therefore it is important to have a firm understanding of them, and this chapter is intended to develop that understanding.

Rather than focusing on each relation individually (an impossible task anyway since there are infinitely many different relations), we will develop a general theory that encompasses *all* relations. Understanding this general theory will give us the conceptual framework and language needed to understand and discuss any specific relation.

16.1 Relations

Before stating the definition of a relation, let's look at a motivational example. This example will lead naturally to our definition.

Consider the set $A = \{1, 2, 3, 4, 5\}$. (There's nothing special about this particular set; any set of numbers would do for this example.) Elements of A can be compared to each other by the symbol " $<$." For example, $1 < 4$, $2 < 3$, $2 < 4$, and so on. You have no trouble understanding this because the notion of numeric order is so ingrained. But imagine you had to explain it to an idiot savant, one with an obsession for detail but absolutely no understanding of the meaning of (or relationships between) integers. You might consider writing down for your student the following set:

$$R = \{(1, 2), (1, 3), (1, 4), (1, 5), (2, 3), (2, 4), (2, 5), (3, 4), (3, 5), (4, 5)\}.$$

The set R encodes the meaning of the $<$ relation for elements in A . An ordered pair (a, b) appears in the set if and only if $a < b$. If asked whether or not it is true that $3 < 4$, your student could look through R until he found the ordered pair $(3, 4)$; then he would know $3 < 4$ is true. If asked about $5 < 2$, he would see that $(5, 2)$ *does not* appear in R , so $5 \not< 2$. The set R , which is a subset of $A \times A$, completely describes the relation $<$ for A .

Though it may seem simple-minded at first, this is exactly the idea we will use for our main definition. This definition is general enough to describe not just the relation $<$ for the set $A = \{1, 2, 3, 4, 5\}$, but *any* relation for *any* set A .


Definition 16.1 A **relation** on a set A is a subset $R \subseteq A \times A$. We often abbreviate the statement $(x, y) \in R$ as xRy . The statement $(x, y) \notin R$ is abbreviated as $x \not R y$.

Notice that a relation is a set, so we can use what we know about sets to understand and explore relations. But before getting deeper into the theory of relations, let's look at some examples of Definition 16.1.

Example 16.1 Let $A = \{1, 2, 3, 4\}$, and consider the following set:


$$R = \{(1, 1), (2, 1), (2, 2), (3, 3), (3, 2), (3, 1), (4, 4), (4, 3), (4, 2), (4, 1)\} \subseteq A \times A.$$


The set R is a relation on A , by Definition 16.1. Since $(1, 1) \in R$, we have $1R1$. Similarly $2R1$ and $2R2$, and so on. However, notice that (for example) $(3, 4) \notin R$, so $3 \not R 4$. Observe that R is the familiar relation \geq for the set A .

Chapter 1 proclaimed that all of mathematics can be described with sets. Just look at how successful this program has been! The greater-than-or-equal-to relation is now a set R . (We might even express this in the rather cryptic form $\geq = R$.) 

Example 16.2 Let $A = \{1, 2, 3, 4\}$, and consider the following set:


$$S = \{(1, 1), (1, 3), (3, 1), (3, 3), (2, 2), (2, 4), (4, 2), (4, 4)\} \subseteq A \times A.$$

Here we have $1S1$, $1S3$, $4S2$, etc., but $3 \not S 4$ and $2 \not S 1$. What does S mean? Think of it as meaning “*has the same parity as.*” Thus $1S1$ reads “*1 has the same parity as 1,*” and $4S2$ reads “*4 has the same parity as 2.*” 

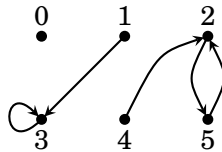
Example 16.3 Consider relations R and S of the previous two examples. Note that $R \cap S = \{(1, 1), (2, 2), (3, 3), (3, 1), (4, 4), (4, 2)\} \subseteq A \times A$ is a relation on A . The expression $x(R \cap S)y$ means “ *$x \geq y$, and x, y have the same parity.*” 

Example 16.4 Let $B = \{0, 1, 2, 3, 4, 5\}$, and consider the following set:

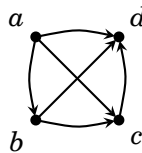
$$U = \{(1, 3), (3, 3), (5, 2), (2, 5), (4, 2)\} \subseteq B \times B.$$

Then U is a relation on B because $U \subseteq B \times B$. You may be hard-pressed to invent any “meaning” for this particular relation. A relation does not have to have any meaning. Any random subset of $B \times B$ is a relation on B , whether or not it describes anything familiar. 


Some relations can be described with pictures. For example, we can depict the above relation U on B by drawing points labeled by elements of B . The statement $(x, y) \in U$ is then represented by an arrow pointing from x to y , a graphic symbol meaning “ x relates to y .” Here’s a picture of U :




The next picture illustrates the relation R on the set $A = \{a, b, c, d\}$, where xRy means x comes before y in the alphabet. According to Definition 16.1, as a set this relation is $R = \{(a, b), (a, c), (a, d), (b, c), (b, d), (c, d)\}$. You may feel that the picture conveys the relation better than the set does. They are two different ways of expressing the same thing. In some instances pictures are more convenient than sets for discussing relations.



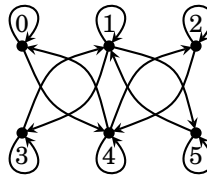
Although such diagrams can help us visualize relations, they do have their limitations. If A and R were infinite, then the diagram would be impossible to draw, but the set R might be easily expressed in set-builder notation. Here are some examples.

Example 16.5 Consider the set $R = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x - y \in \mathbb{N}\} \subseteq \mathbb{Z} \times \mathbb{Z}$. This is the $>$ relation on the set $A = \mathbb{Z}$. It is infinite because there are infinitely many ways to have $x > y$ where x and y are integers. 

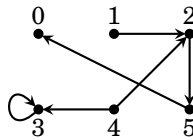
Example 16.6 The set $R = \{(x, x) : x \in \mathbb{R}\} \subseteq \mathbb{R} \times \mathbb{R}$ is the relation $=$ on the set \mathbb{R} , because xRy means the same thing as $x = y$. Thus R is a set that expresses the notion of equality of real numbers. 

Exercises for Section 16.1

1. Let $A = \{0, 1, 2, 3, 4, 5\}$. Write out the relation R that expresses $>$ on A . Then illustrate it with a diagram.
2. Let $A = \{1, 2, 3, 4, 5, 6\}$. Write out the relation R that expresses $|$ (divides) on A . Then illustrate it with a diagram.
3. Let $A = \{0, 1, 2, 3, 4, 5\}$. Write out the relation R that expresses \geq on A . Then illustrate it with a diagram.
4. Here is a diagram for a relation R on a set A . Write the sets A and R .

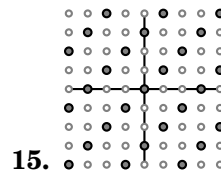
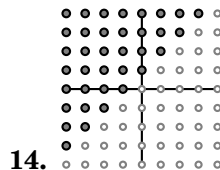
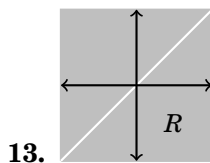
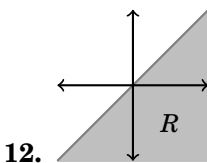


5. Here is a diagram for a relation R on a set A . Write the sets A and R .



6. Congruence modulo 5 is a relation on the set $A = \mathbb{Z}$. In this relation xRy means $x \equiv y \pmod{5}$. Write out the set R in set-builder notation.
7. Write the relation $<$ on the set $A = \mathbb{Z}$ as a subset R of $\mathbb{Z} \times \mathbb{Z}$. This is an infinite set, so you will have to use set-builder notation.
8. Let $A = \{1, 2, 3, 4, 5, 6\}$. Observe that $\emptyset \subseteq A \times A$, so $R = \emptyset$ is a relation on A . Draw a diagram for this relation.
9. Let $A = \{1, 2, 3, 4, 5, 6\}$. How many different relations are there on the set A ?
10. Consider the subset $R = (\mathbb{R} \times \mathbb{R}) - \{(x, x) : x \in \mathbb{R}\} \subseteq \mathbb{R} \times \mathbb{R}$. What familiar relation on \mathbb{R} is this? Explain.
11. Given a finite set A , how many different relations are there on A ?

In the following exercises, subsets R of $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ or $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$ are indicated by gray shading. In each case, R is a familiar relation on \mathbb{R} or \mathbb{Z} . State it.



16.2 Properties of Relations

A relational expression xRy is a *statement* (or an *open sentence*); it is either true or false. For example, $5 < 10$ is true, and $10 < 5$ is false. (Thus an operation like $+$ is not a relation, because, for instance, $5+10$ has a numeric value, not a T/F value.) Since relational expressions have T/F values, we can combine them with logical operators; for example, $xRy \Rightarrow yRx$ is a statement or open sentence whose truth or falsity may depend on x and y .

With this in mind, note that some relations have properties that others don't have. For example, the relation \leq on \mathbb{Z} satisfies $x \leq x$ for every $x \in \mathbb{Z}$. But this is not so for $<$ because $x < x$ is never true. The next definition lays out three particularly significant properties that relations may have.

Definition 16.2 Suppose R is a relation on a set A . Then:

- R is **reflexive** if xRx for every $x \in A$.
That is, R is reflexive if $\forall x \in A, xRx$.
- R is **symmetric** if xRy implies yRx for all $x, y \in A$.
That is, R is symmetric if $\forall x, y \in A, xRy \Rightarrow yRx$.
- R is **transitive** if whenever xRy and yRz , then also xRz .
That is, R is transitive if $\forall x, y, z \in A, ((xRy) \wedge (yRz)) \Rightarrow xRz$.

To illustrate this, let's consider the set $A = \mathbb{Z}$. Examples of reflexive relations on \mathbb{Z} include $\leq, =$, and $|$, because $x \leq x, x = x$ and $x|x$ are all true for any $x \in \mathbb{Z}$. On the other hand, $>, <, \neq$ and \nmid are not reflexive for none of the statements $x < x, x > x, x \neq x$ and $x \nmid x$ is ever true.

The relation \neq is symmetric, for if $x \neq y$, then surely $y \neq x$ also. Also, the relation $=$ is symmetric because $x = y$ always implies $y = x$.

The relation \leq is **not** symmetric, as $x \leq y$ does not necessarily imply $y \leq x$. For instance $5 \leq 6$ is true, but $6 \leq 5$ is false. Notice $(x \leq y) \Rightarrow (y \leq x)$ is true for some x and y (for example, it is true when $x = 2$ and $y = 2$), but still \leq is not symmetric because it is not the case that $(x \leq y) \Rightarrow (y \leq x)$ is true for *all* integers x and y .


The relation \leq is transitive because whenever $x \leq y$ and $y \leq z$, it also is true that $x \leq z$. Likewise $<, \geq, >$ and $=$ are all transitive. Examine the following table and be sure you understand why it is labeled as it is.

| Relations on \mathbb{Z} : | $<$ | \leq | $=$ | $ $ | \nmid | \neq |
|-----------------------------|-----|--------|-----|-----|---------|--------|
| Reflexive | no | yes | yes | yes | no | no |
| Symmetric | no | no | yes | no | no | yes |
| Transitive | yes | yes | yes | yes | no | no |

Example 16.7 Here $A = \{b, c, d, e\}$, and R is the following relation on A :
 $R = \{(b, b), (b, c), (c, b), (c, c), (d, d), (b, d), (d, b), (c, d), (d, c)\}$.

This relation is **not** reflexive, for although bRb , cRc and dRd , it is **not** true that eRe . For a relation to be reflexive, xRx must be true for *all* $x \in A$.

The relation R is symmetric, because whenever we have xRy , it follows that yRx too. Observe that bRc and cRb ; bRd and dRb ; dRc and cRd . Take away the ordered pair (c, b) from R , and R is no longer symmetric.

The relation R is transitive, but it takes some work to check it. We must check that the statement $(xRy \wedge yRz) \Rightarrow xRz$ is true for all $x, y, z \in A$. For example, taking $x = b$, $y = c$ and $z = d$, we have $(bRc \wedge cRd) \Rightarrow bRd$, which is the true statement $(T \wedge T) \Rightarrow T$. Likewise, $(bRd \wedge dRc) \Rightarrow bRc$ is the true statement $(T \wedge T) \Rightarrow T$. Take note that if $x = b$, $y = e$ and $z = c$, then $(bRe \wedge eRc) \Rightarrow bRc$ becomes $(F \wedge F) \Rightarrow T$, which is *still* true. It's not much fun, but going through all the combinations, you can verify that $(xRy \wedge yRz) \Rightarrow xRz$ is true for all choices $x, y, z \in A$. (Try at least a few of them.) 

The relation R from Example 16.7 has a meaning. You can think of xRy as meaning that x and y are both consonants. Thus bRc because b and c are both consonants; but bRe because it's not true that b and e are both consonants. Once we look at it this way, it's immediately clear that R has to be transitive. If x and y are both consonants and y and z are both consonants, then surely x and z are both consonants. This illustrates a point that we will see again later in this section: Knowing the meaning of a relation can help us understand it and prove things about it.

Here is a picture of R . Notice that we can immediately spot several properties of R that may not have been so clear from its set description. For instance, we see that R is not reflexive because it lacks a loop at e , hence eRe .

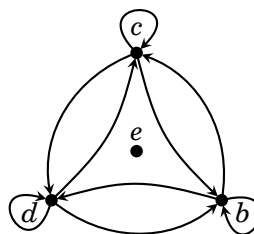




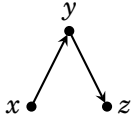
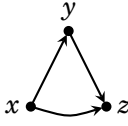




Figure 16.1. The relation R from Example 16.7

In what follows, we summarize how to spot the various properties of a relation from its diagram. Compare these with Figure 16.2.

| | | | | |
|----|--|---|--|--|
| 1. | A relation is reflexive if for each point x ... |  | ...there is a loop at x : |  |
| 2. | A relation is symmetric if whenever there is an arrow from x to y ... |  | ...there is also an arrow from y back to x : |  |
| 3. | A relation is transitive if whenever there are arrows from x to y and y to z ... (If $x = z$, this means that if there are arrows from x to y and from y to x ... |  | ...there is also an arrow from x to z : |  |
| | ...there is also a loop from x back to x .) |  | |  |

Consider the bottom diagram in Box 3, above. The transitive property demands $(xRy \wedge yRx) \Rightarrow xRx$. Thus, if xRy and yRx in a transitive relation, then also xRx , so there is a loop at x . In this case $(yRx \wedge xRy) \Rightarrow yRy$, so there will be a loop at y too.

Although these visual aids can be illuminating, their use is limited because many relations are too large and complex to be adequately described as diagrams. For example, it would be impossible to draw a diagram for the relation $\equiv \pmod{n}$, where $n \in \mathbb{N}$. Such a relation would best be explained in a more theoretical (and less visual) way.

We next prove that $\equiv \pmod{n}$ is reflexive, symmetric and transitive. Obviously we will not glean this from a drawing. Instead we will prove it from the properties of $\equiv \pmod{n}$ and Definition 16.2. Pay attention to this example. It illustrates how to **prove** things about relations.

Example 16.8 Prove the following proposition.

Proposition Let $n \in \mathbb{N}$. The relation $\equiv \pmod{n}$ on the set \mathbb{Z} is reflexive, symmetric and transitive.

Proof. First we will show that $\equiv \pmod{n}$ is reflexive. Take any integer $x \in \mathbb{Z}$, and observe that $n \mid 0$, so $n \mid (x - x)$. By definition of congruence modulo n , we have $x \equiv x \pmod{n}$. This shows $x \equiv x \pmod{n}$ for every $x \in \mathbb{Z}$, so $\equiv \pmod{n}$ is reflexive.

Next, we will show that $\equiv \pmod{n}$ is symmetric. For this, we must show that for all $x, y \in \mathbb{Z}$, the condition $x \equiv y \pmod{n}$ implies that $y \equiv x \pmod{n}$. We use direct proof. Suppose $x \equiv y \pmod{n}$. Thus $n \mid (x - y)$ by definition of congruence modulo n . Then $x - y = na$ for some $a \in \mathbb{Z}$ by definition of divisibility. Multiplying both sides by -1 gives $y - x = n(-a)$. Therefore $n \mid (y - x)$, and this means $y \equiv x \pmod{n}$. We've shown that $x \equiv y \pmod{n}$ implies that $y \equiv x \pmod{n}$, and this means $\equiv \pmod{n}$ is symmetric.

Finally we will show that $\equiv \pmod{n}$ is transitive. For this we must show that if $x \equiv y \pmod{n}$ and $y \equiv z \pmod{n}$, then $x \equiv z \pmod{n}$. Again we use direct proof. Suppose $x \equiv y \pmod{n}$ and $y \equiv z \pmod{n}$. This means $n \mid (x - y)$ and $n \mid (y - z)$. Therefore there are integers a and b for which $x - y = na$ and $y - z = nb$. Adding these two equations, we obtain $x - z = na + nb$. Consequently, $x - z = n(a + b)$, so $n \mid (x - z)$, hence $x \equiv z \pmod{n}$. This completes the proof that $\equiv \pmod{n}$ is transitive.

The past three paragraphs have shown that $\equiv \pmod{n}$ is reflexive, symmetric and transitive, so the proof is complete. ■

As you continue with mathematics you will find that the reflexive, symmetric and transitive properties take on special significance in a variety of settings. In preparation for this, the next section explores further consequences of these properties. But first work some of the following exercises.

Exercises for Section 16.2

1. Consider the relation $R = \{(a, a), (b, b), (c, c), (d, d), (a, b), (b, a)\}$ on set $A = \{a, b, c, d\}$. Is R reflexive? Symmetric? Transitive? If a property does not hold, say why.
2. Consider the relation $R = \{(a, b), (a, c), (c, c), (b, b), (c, b), (b, c)\}$ on the set $A = \{a, b, c\}$. Is R reflexive? Symmetric? Transitive? If a property does not hold, say why.
3. Consider the relation $R = \{(a, b), (a, c), (c, b), (b, c)\}$ on the set $A = \{a, b, c\}$. Is R reflexive? Symmetric? Transitive? If a property does not hold, say why.

4. Let $A = \{a, b, c, d\}$. Suppose R is the relation

$$R = \{(a, a), (b, b), (c, c), (d, d), (a, b), (b, a), (a, c), (c, a), \\ (a, d), (d, a), (b, c), (c, b), (b, d), (d, b), (c, d), (d, c)\}.$$

Is R reflexive? Symmetric? Transitive? If a property does not hold, say why.

5. Consider the relation $R = \{(0, 0), (\sqrt{2}, 0), (0, \sqrt{2}), (\sqrt{2}, \sqrt{2})\}$ on \mathbb{R} . Is R reflexive? Symmetric? Transitive? If a property does not hold, say why.
6. Consider the relation $R = \{(x, x) : x \in \mathbb{Z}\}$ on \mathbb{Z} . Is R reflexive? Symmetric? Transitive? If a property does not hold, say why. What familiar relation is this?
7. There are 16 possible different relations R on the set $A = \{a, b\}$. Describe all of them. (A picture for each one will suffice, but don't forget to label the nodes.) Which ones are reflexive? Symmetric? Transitive?
8. Define a relation on \mathbb{Z} as xRy if $|x - y| < 1$. Is R reflexive? Symmetric? Transitive? If a property does not hold, say why. What familiar relation is this?
9. Define a relation on \mathbb{Z} by declaring xRy if and only if x and y have the same parity. Is R reflexive? Symmetric? Transitive? If a property does not hold, say why. What familiar relation is this?
10. Suppose $A \neq \emptyset$. Since $\emptyset \subseteq A \times A$, the set $R = \emptyset$ is a relation on A . Is R reflexive? Symmetric? Transitive? If a property does not hold, say why.
11. Suppose $A = \{a, b, c, d\}$ and $R = \{(a, a), (b, b), (c, c), (d, d)\}$. Is R reflexive? Symmetric? Transitive? If a property does not hold, say why.
12. Prove that the relation $|$ (divides) on the set \mathbb{Z} is reflexive and transitive. (Use Example 16.8 as a guide if you are unsure of how to proceed.)
13. Consider the relation $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} : x - y \in \mathbb{Z}\}$ on \mathbb{R} . Prove that this relation is reflexive, symmetric and transitive.
14. Suppose R is a symmetric and transitive relation on a set A , and there is an element $a \in A$ for which aRx for every $x \in A$. Prove that R is reflexive.
15. Prove or disprove: If a relation is symmetric and transitive, then it is also reflexive.
16. Define a relation R on \mathbb{Z} by declaring that xRy if and only if $x^2 \equiv y^2 \pmod{4}$. Prove that R is reflexive, symmetric and transitive.
17. Modifying the above Exercise 8 (above) slightly, define a relation \sim on \mathbb{Z} as $x \sim y$ if and only if $|x - y| \leq 1$. Say whether \sim is reflexive. Is it symmetric? Transitive?
18. The table on page 368 shows that relations on \mathbb{Z} may obey various combinations of the reflexive, symmetric and transitive properties. In all, there are $2^3 = 8$ possible combinations, and the table shows 5 of them. (There is some redundancy, as \leq and $|$ have the same type.) Complete the table by finding examples of relations on \mathbb{Z} for the three missing combinations.
-

16.3 Equivalence Relations

The relation $=$ on the set \mathbb{Z} (or on any set A) is reflexive, symmetric and transitive. There are many other relations that are also reflexive, symmetric and transitive. Relations that have all three of these properties occur very frequently in mathematics and often play quite significant roles. (For instance, this is certainly true of the relation $=$.) Such relations are given a special name. They are called *equivalence relations*.

Definition 16.3 A relation R on a set A is an **equivalence relation** if it is reflexive, symmetric and transitive.

As an example, Figure 16.2 shows four different equivalence relations R_1, R_2, R_3 and R_4 on the set $A = \{-1, 1, 2, 3, 4\}$. Each one has its own meaning, as labeled. For example, in the second row the relation R_2 literally means “has the same parity as.” So $1R_23$ means “1 has the same parity as 3,” etc.

| Relation R | Diagram | Equivalence classes (see next page) |
|--|---------|---|
| <p>“is equal to” ($=$)</p> <p>$R_1 = \{(-1, -1), (1, 1), (2, 2), (3, 3), (4, 4)\}$</p> | | <p>$\{-1\}, \{1\}, \{2\},$ $\{3\}, \{4\}$</p> |
| <p>“has same parity as”</p> <p>$R_2 = \{(-1, -1), (1, 1), (2, 2), (3, 3), (4, 4),$ $(-1, 1), (1, -1), (-1, 3), (3, -1),$ $(1, 3), (3, 1), (2, 4), (4, 2)\}$</p> | | <p>$\{-1, 1, 3\}, \{2, 4\}$</p> |
| <p>“has same sign as”</p> <p>$R_3 = \{(-1, -1), (1, 1), (2, 2), (3, 3), (4, 4),$ $(1, 2), (2, 1), (1, 3), (3, 1), (1, 4), (4, 1), (3, 4),$ $(4, 3), (2, 3), (3, 2), (2, 4), (4, 2), (1, 3), (3, 1)\}$</p> | | <p>$\{-1\}, \{1, 2, 3, 4\}$</p> |
| <p>“has same parity and sign as”</p> <p>$R_4 = \{(-1, -1), (1, 1), (2, 2), (3, 3), (4, 4),$ $(1, 3), (3, 1), (2, 4), (4, 2)\}$</p> | | <p>$\{-1\}, \{1, 3\}, \{2, 4\}$</p> |


Figure 16.2. Examples of equivalence relations on the set $A = \{-1, 1, 2, 3, 4\}$


The above diagrams make it easy to check that each relation is reflexive, symmetric and transitive, i.e., that each is an equivalence relation. For example, R_1 is symmetric because $xR_1y \Rightarrow yR_1x$ is always true: When $x = y$ it becomes $T \Rightarrow T$ (true), and when $x \neq y$ it becomes $F \Rightarrow F$ (also true). In a similar fashion, R_1 is transitive because $(xR_1y \wedge yR_1z) \Rightarrow xR_1z$ is always true: It always works out to one of $T \Rightarrow T$, $F \Rightarrow T$ or $F \Rightarrow F$. (Check this.)


As you can see from the examples in Figure 16.2, equivalence relations on a set tend to express some measure of “sameness” among the elements of the set, whether it is true equality or something weaker (like having the same parity).

It’s time to introduce an important definition. Whenever you have an equivalence relation R on a set A , it divides A into subsets called *equivalence classes*. Here is the definition:

Definition 16.4 Suppose R is an equivalence relation on a set A . Given any element $a \in A$, the **equivalence class containing a** is the subset $\{x \in A : xRa\}$ of A consisting of all the elements of A that relate to a . This set is denoted as $[a]$. Thus the equivalence class containing a is the set $[a] = \{x \in A : xRa\}$.


Example 16.9 Consider the relation R_1 in Figure 16.2. The equivalence class containing 2 is the set $[2] = \{x \in A : xR_12\}$. Because in this relation the only element that relates to 2 is 2 itself, we have $[2] = \{2\}$. Other equivalence classes for R_1 are $[-1] = \{-1\}$, $[1] = \{1\}$, $[3] = \{3\}$ and $[4] = \{4\}$. Thus this relation has five separate equivalence classes. 

Example 16.10 Consider the relation R_2 in Figure 16.2. The equivalence class containing 2 is the set $[2] = \{x \in A : xR_22\}$. Because only 2 and 4 relate to 2, we have $[2] = \{2, 4\}$. Observe that we also have $[4] = \{x \in A : xR_24\} = \{2, 4\}$, so $[2] = [4]$. Another equivalence class for R_2 is $[1] = \{x \in A : xR_21\} = \{-1, 1, 3\}$. In addition, note that $[1] = [-1] = [3] = \{-1, 1, 3\}$. Thus this relation has just two equivalence classes, namely $\{2, 4\}$ and $\{-1, 1, 3\}$. 

Example 16.11 The relation R_4 in Figure 16.2 has three equivalence classes. They are $[-1] = \{-1\}$ and $[1] = [3] = \{1, 3\}$ and $[2] = [4] = \{2, 4\}$. 

Don’t be misled by Figure 16.2. It’s important to realize that not every equivalence relation can be drawn as a diagram involving nodes and arrows. Even the simple relation $R = \{(x, x) : x \in \mathbb{R}\}$, which expresses equality in the set \mathbb{R} , is too big to be drawn. Its picture would involve a point for every real number and a loop at each point. Clearly that’s too many points and loops to draw.

We close this section with several other examples of equivalence relations on infinite sets.

Example 16.12 Let P be the set of all polynomials with real coefficients. Define a relation R on P as follows. Given $f(x), g(x) \in P$, let $f(x)Rg(x)$ mean that $f(x)$ and $g(x)$ have the same degree. Thus $(x^2 + 3x - 4)R(3x^2 - 2)$ and $(x^3 + 3x^2 - 4)R(3x^2 - 2)$, for example. It takes just a quick mental check to see that R is an equivalence relation. (Do it.) It's easy to describe the equivalence classes of R . For example, $[3x^2 + 2]$ is the set of all polynomials that have the same degree as $3x^2 + 2$, that is, the set of all polynomials of degree 2. We can write this as $[3x^2 + 2] = \{ax^2 + bx + c : a, b, c \in \mathbb{R}, a \neq 0\}$. 

Example 16.8 proved that for a given $n \in \mathbb{N}$ the relation $\equiv \pmod{n}$ is reflexive, symmetric and transitive. Thus, in our new parlance, $\equiv \pmod{n}$ is an equivalence relation on \mathbb{Z} . Consider the case $n = 3$. Let's find the equivalence classes of the equivalence relation $\equiv \pmod{3}$. The equivalence class containing 0 seems like a reasonable place to start. Observe that

$$[0] = \{x \in \mathbb{Z} : x \equiv 0 \pmod{3}\} = \{x \in \mathbb{Z} : 3 \mid (x - 0)\} = \{x \in \mathbb{Z} : 3 \mid x\} = \{\dots, -3, 0, 3, 6, 9, \dots\}.$$

Thus the class $[0]$ consists of all the multiples of 3. (Or, said differently, $[0]$ consists of all integers that have a remainder of 0 when divided by 3). Note that $[0] = [3] = [6] = [9]$, etc. The number 1 does not show up in the set $[0]$ so let's next look at the equivalence class $[1]$:

$$[1] = \{x \in \mathbb{Z} : x \equiv 1 \pmod{3}\} = \{x \in \mathbb{Z} : 3 \mid (x - 1)\} = \{\dots, -5, -2, 1, 4, 7, 10, \dots\}.$$

The equivalence class $[1]$ consists of all integers that give a remainder of 1 when divided by 3. The number 2 is in neither of the sets $[0]$ or $[1]$, so we next look at the equivalence class $[2]$:

$$[2] = \{x \in \mathbb{Z} : x \equiv 2 \pmod{3}\} = \{x \in \mathbb{Z} : 3 \mid (x - 2)\} = \{\dots, -4, -1, 2, 5, 8, 11, \dots\}.$$

The equivalence class $[2]$ consists of all integers that give a remainder of 2 when divided by 3. Observe that any integer is in one of the sets $[0]$, $[1]$ or $[2]$, so we have listed all of the equivalence classes. Thus $\equiv \pmod{3}$ has exactly three equivalence classes, as described above.

Similarly, you can show that the equivalence relation $\equiv \pmod{n}$ has n equivalence classes $[0], [1], [2], \dots, [n - 1]$.

Exercises for Section 16.3

1. Let $A = \{1, 2, 3, 4, 5, 6\}$, and consider the following equivalence relation on A :
 $R = \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (6, 6), (2, 3), (3, 2), (4, 5), (5, 4), (4, 6), (6, 4), (5, 6), (6, 5)\}$
 List the equivalence classes of R .
 2. Let $A = \{a, b, c, d, e\}$. Suppose R is an equivalence relation on A . Suppose R has two equivalence classes. Also aRd , bRc and eRd . Write out R as a set.
 3. Let $A = \{a, b, c, d, e\}$. Suppose R is an equivalence relation on A . Suppose R has three equivalence classes. Also aRd and bRc . Write out R as a set.
 4. Let $A = \{a, b, c, d, e\}$. Suppose R is an equivalence relation on A . Suppose also that aRd and bRc , eRa and cRe . How many equivalence classes does R have?
 5. There are two different equivalence relations on the set $A = \{a, b\}$. Describe them. Diagrams will suffice.
 6. There are five different equivalence relations on the set $A = \{a, b, c\}$. Describe them all. Diagrams will suffice.
 7. Define a relation R on \mathbb{Z} as xRy if and only if $3x - 5y$ is even. Prove R is an equivalence relation. Describe its equivalence classes.
 8. Define a relation R on \mathbb{Z} as xRy if and only if $x^2 + y^2$ is even. Prove R is an equivalence relation. Describe its equivalence classes.
 9. Define a relation R on \mathbb{Z} as xRy if and only if $4|(x+3y)$. Prove R is an equivalence relation. Describe its equivalence classes.
 10. Suppose R and S are two equivalence relations on a set A . Prove that $R \cap S$ is also an equivalence relation. (For an example of this, look at Figure 16.2. Observe that for the equivalence relations R_2, R_3 and R_4 , we have $R_2 \cap R_3 = R_4$.)
 11. Prove or disprove: If R is an equivalence relation on an infinite set A , then R has infinitely many equivalence classes.
 12. Prove or disprove: If R and S are two equivalence relations on a set A , then $R \cup S$ is also an equivalence relation on A .
 13. Suppose R is an equivalence relation on a finite set A , and every equivalence class has the same cardinality m . Express $|R|$ in terms of m and $|A|$.
 14. Suppose R is a reflexive and symmetric relation on a finite set A . Define a relation S on A by declaring xSy if and only if for some $n \in \mathbb{N}$ there are elements $x_1, x_2, \dots, x_n \in A$ satisfying xRx_1 , x_1Rx_2 , x_2Rx_3 , $x_3Rx_4, \dots, x_{n-1}Rx_n$, and x_nRy . Show that S is an equivalence relation and $R \subseteq S$. Prove that S is the unique smallest equivalence relation on A containing R .
 15. Suppose R is an equivalence relation on a set A , with four equivalence classes. How many different equivalence relations S on A are there for which $R \subseteq S$?
-

16.4 Equivalence Classes and Partitions

This section collects several properties of equivalence classes.

Our first result proves that $[a] = [b]$ if and only if aRb . This is useful because it assures us that whenever we are in a situation where $[a] = [b]$, we also have aRb , and vice versa. Being able to switch back and forth between these two pieces of information can be helpful in a variety of situations, and you may find yourself using this result a lot. Be sure to notice that the proof uses all three properties (reflexive, symmetric and transitive) of equivalence relations. Notice also that we have to use some Chapter 11 techniques in dealing with the sets $[a]$ and $[b]$.

Theorem 16.1 Suppose R is an equivalence relation on a set A . Suppose also that $a, b \in A$. Then $[a] = [b]$ if and only if aRb .

Proof. Suppose $[a] = [b]$. Note that aRa by the reflexive property of R , so $a \in \{x \in A : xRa\} = [a] = [b] = \{x \in A : xRb\}$. But a belonging to $\{x \in A : xRb\}$ means aRb . This completes the first part of the if-and-only-if proof.

Conversely, suppose aRb . We need to show $[a] = [b]$. We will do this by showing $[a] \subseteq [b]$ and $[b] \subseteq [a]$.

First we show $[a] \subseteq [b]$. Suppose $c \in [a]$. As $c \in [a] = \{x \in A : xRa\}$, we get cRa . Now we have cRa and aRb , so cRb because R is transitive. But cRb implies $c \in \{x \in A : xRb\} = [b]$. This demonstrates that $c \in [a]$ implies $c \in [b]$, so $[a] \subseteq [b]$.

Next we show $[b] \subseteq [a]$. Suppose $c \in [b]$. As $c \in [b] = \{x \in A : xRb\}$, we get cRb . Remember that we are assuming aRb , so bRa because R is symmetric. Now we have cRb and bRa , so cRa because R is transitive. But cRa implies $c \in \{x \in A : xRa\} = [a]$. This demonstrates that $c \in [b]$ implies $c \in [a]$; hence $[b] \subseteq [a]$.

The previous two paragraphs imply that $[a] = [b]$. ■

To illustrate Theorem 16.1, recall how we worked out the equivalence classes of $\equiv \pmod{3}$ at the end of Section 16.3. We observed that

$$[-3] = [9] = \{\dots, -3, 0, 3, 6, 9, \dots\}.$$

Note that $[-3] = [9]$ and $-3 \equiv 9 \pmod{3}$, just as Theorem 16.1 predicts. The theorem assures us that this will work for any equivalence relation. In the future you may find yourself using the result of Theorem 16.1 often. Over time it may become natural and familiar; you will use it automatically, without even thinking of it as a theorem.


Our next topic addresses the fact that an equivalence relation on a set A divides A into various equivalence classes. There is a special word for this kind of situation. We address it now, as you are likely to encounter it in subsequent mathematics classes.


Definition 16.5 A **partition** of a set A is a set of non-empty subsets of A , such that the union of all the subsets equals A , and the intersection of any two different subsets is \emptyset .

Example 16.13 Let $A = \{a, b, c, d\}$. One partition of A is $\{\{a, b\}, \{c\}, \{d\}\}$. This is a set of three subsets $\{a, b\}$, $\{c\}$ and $\{d\}$ of A . The union of the three subsets equals A ; the intersection of any two subsets is \emptyset .

Other partitions of A are


$$\{\{a, b\}, \{c, d\}\}, \quad \{\{a, c\}, \{b\}, \{d\}\}, \quad \{\{a\}, \{b\}, \{c, d\}\}, \quad \{\{a, b, c, d\}\},$$

to name a few. Intuitively, a partition is just a dividing of A into parts. 

Example 16.14 Consider the equivalence relations in Figure 16.2. Each of these is a relation on the set $A = \{-1, 1, 2, 3, 4\}$. The equivalence classes of each relation are listed on the right side of the figure. Observe that, in each case, the set of equivalence classes forms a partition of A . For example, the relation R_1 yields the partition $\{\{-1\}, \{1\}, \{2\}, \{3\}, \{4\}\}$ of A . Also, the equivalence classes of R_2 form the partition $\{\{-1, 1, 3\}, \{2, 4\}\}$. 

Example 16.15 Recall that we worked out the equivalence classes of the equivalence relation $\equiv \pmod{3}$ on the set \mathbb{Z} . These equivalence classes give the following partition of \mathbb{Z} :

$$\{\{\dots, -3, 0, 3, 6, 9, \dots\}, \{\dots, -2, 1, 4, 7, 10, \dots\}, \{\dots, -1, 2, 5, 8, 11, \dots\}\}.$$

We can write it more compactly as $\{[0], [1], [2]\}$. 

Our examples and experience suggest that the equivalence classes of an equivalence relation on a set form a partition of that set. This is indeed the case, and we now prove it.

Theorem 16.2 Suppose R is an equivalence relation on a set A . Then the set $\{[a] : a \in A\}$ of equivalence classes of R forms a partition of A .

Proof. To show that $\{[a] : a \in A\}$ is a partition of A we need to show two things: We need to show that the union of all the sets $[a]$ equals A , and we need to show that if $[a] \neq [b]$, then $[a] \cap [b] = \emptyset$.

Notationally, the union of all the sets $[a]$ is $\bigcup_{a \in A} [a]$, so we need to prove $\bigcup_{a \in A} [a] = A$. Suppose $x \in \bigcup_{a \in A} [a]$. This means $x \in [a]$ for some $a \in A$. Since $[a] \subseteq A$, it then follows that $x \in A$. Thus $\bigcup_{a \in A} [a] \subseteq A$. On the other hand, suppose $x \in A$. As $x \in [x]$, we know $x \in [a]$ for some $a \in A$ (namely $a = x$). Therefore $x \in \bigcup_{a \in A} [a]$, and this shows $A \subseteq \bigcup_{a \in A} [a]$. Since $\bigcup_{a \in A} [a] \subseteq A$ and $A \subseteq \bigcup_{a \in A} [a]$, it follows that $\bigcup_{a \in A} [a] = A$.

Next we need to show that if $[a] \neq [b]$ then $[a] \cap [b] = \emptyset$. Let's use contrapositive proof. Suppose it's not the case that $[a] \cap [b] = \emptyset$, so there is some element c with $c \in [a] \cap [b]$. Thus $c \in [a]$ and $c \in [b]$. Now, $c \in [a]$ means cRa , and then aRc since R is symmetric. Also $c \in [b]$ means cRb . Now we have aRc and cRb , so aRb (because R is transitive). By Theorem 16.1, aRb implies $[a] = [b]$. Thus $[a] \neq [b]$ is not true.

We've now shown that the union of all the equivalence classes is A , and the intersection of two different equivalence classes is \emptyset . Therefore the set of equivalence classes is a partition of A . ■

Theorem 16.2 says the equivalence classes of any equivalence relation on a set A form a partition of A . Conversely, any partition of A describes an equivalence relation R where xRy if and only if x and y belong to the same set in the partition. (See Exercise 4 for this section, below.) Thus equivalence relations and partitions are really just two different ways of looking at the same thing. In your future mathematical studies, you may find yourself easily switching between these two points of view.

Exercises for Section 16.4

1. List all the partitions of the set $A = \{a, b\}$. Compare your answer to the answer to Exercise 5 of Section 16.3.
2. List all the partitions of the set $A = \{a, b, c\}$. Compare your answer to the answer to Exercise 6 of Section 16.3.
3. Describe the partition of \mathbb{Z} resulting from the equivalence relation $\equiv \pmod{4}$.
4. Suppose P is a partition of a set A . Define a relation R on A by declaring xRy if and only if $x, y \in X$ for some $X \in P$. Prove R is an equivalence relation on A . Then prove that P is the set of equivalence classes of R .
5. Consider the partition $P = \{\{\dots, -4, -2, 0, 2, 4, \dots\}, \{\dots, -5, -3, -1, 1, 3, 5, \dots\}\}$ of \mathbb{Z} . Let R be the equivalence relation whose equivalence classes are the two elements of P . What familiar equivalence relation is R ?

16.5 The Integers Modulo n

Example 16.8 proved that for a given $n \in \mathbb{N}$, the relation $\equiv (\text{mod } n)$ is reflexive, symmetric and transitive, so it is an equivalence relation. This is a particularly significant equivalence relation in mathematics, and in the present section we deduce some of its properties.

To make matters simpler, let's pick a concrete n , say $n = 5$. Let's begin by looking at the equivalence classes of the relation $\equiv (\text{mod } 5)$. There are five equivalence classes, as follows:

$$\begin{aligned} [0] &= \{x \in \mathbb{Z} : x \equiv 0 \pmod{5}\} = \{x \in \mathbb{Z} : 5 \mid (x-0)\} = \{\dots, -10, -5, 0, 5, 10, 15, \dots\}, \\ [1] &= \{x \in \mathbb{Z} : x \equiv 1 \pmod{5}\} = \{x \in \mathbb{Z} : 5 \mid (x-1)\} = \{\dots, -9, -4, 1, 6, 11, 16, \dots\}, \\ [2] &= \{x \in \mathbb{Z} : x \equiv 2 \pmod{5}\} = \{x \in \mathbb{Z} : 5 \mid (x-2)\} = \{\dots, -8, -3, 2, 7, 12, 17, \dots\}, \\ [3] &= \{x \in \mathbb{Z} : x \equiv 3 \pmod{5}\} = \{x \in \mathbb{Z} : 5 \mid (x-3)\} = \{\dots, -7, -2, 3, 8, 13, 18, \dots\}, \\ [4] &= \{x \in \mathbb{Z} : x \equiv 4 \pmod{5}\} = \{x \in \mathbb{Z} : 5 \mid (x-4)\} = \{\dots, -6, -1, 4, 9, 14, 19, \dots\}. \end{aligned}$$

Notice how these equivalence classes form a partition of the set \mathbb{Z} . We label the five equivalence classes as $[0], [1], [2], [3]$ and $[4]$, but you know of course that there are other ways to label them. For example, $[0] = [5] = [10] = [15]$, and so on; and $[1] = [6] = [-4]$, etc. Still, for this discussion we denote the five classes as $[0], [1], [2], [3]$ and $[4]$.

These five classes form a set, which we shall denote as \mathbb{Z}_5 . Thus

$$\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$$

is a set of five sets. The interesting thing about \mathbb{Z}_5 is that even though its elements are sets (and not numbers), it is possible to add and multiply them. In fact, we can define the following rules that tell how elements of \mathbb{Z}_5 can be added and multiplied.

$$\begin{aligned} [a] + [b] &= [a + b] \\ [a] \cdot [b] &= [a \cdot b] \end{aligned}$$

For example, $[2] + [1] = [2 + 1] = [3]$, and $[2] \cdot [2] = [2 \cdot 2] = [4]$. We stress that in doing this we are adding and multiplying *sets* (more precisely equivalence classes), not numbers. We added (or multiplied) two elements of \mathbb{Z}_5 and obtained another element of \mathbb{Z}_5 .

Here is a trickier example. Observe that $[2] + [3] = [5]$. This time we added elements $[2], [3] \in \mathbb{Z}_5$, and got the element $[5] \in \mathbb{Z}_5$. That was easy, except where is our answer $[5]$ in the set $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$? Since $[5] = [0]$, it is more appropriate to write $[2] + [3] = [0]$.

In a similar vein, $[2] \cdot [3] = [6]$ would be written as $[2] \cdot [3] = [1]$ because $[6] = [1]$. Test your skill with this by verifying the following addition and multiplication tables for \mathbb{Z}_5 .

| + | [0] | [1] | [2] | [3] | [4] |
|-----|-----|-----|-----|-----|-----|
| [0] | [0] | [1] | [2] | [3] | [4] |
| [1] | [1] | [2] | [3] | [4] | [0] |
| [2] | [2] | [3] | [4] | [0] | [1] |
| [3] | [3] | [4] | [0] | [1] | [2] |
| [4] | [4] | [0] | [1] | [2] | [3] |

| · | [0] | [1] | [2] | [3] | [4] |
|-----|-----|-----|-----|-----|-----|
| [0] | [0] | [0] | [0] | [0] | [0] |
| [1] | [0] | [1] | [2] | [3] | [4] |
| [2] | [0] | [2] | [4] | [1] | [3] |
| [3] | [0] | [3] | [1] | [4] | [2] |
| [4] | [0] | [4] | [3] | [2] | [1] |

We call the set $\mathbb{Z}_5 = \{[0],[1],[2],[3],[4]\}$ the **integers modulo 5**. As our tables suggest, \mathbb{Z}_5 is more than just a set: It is a little number system with its own addition and multiplication. In this way it is like the familiar set \mathbb{Z} which also comes equipped with an addition and a multiplication.

Of course, there is nothing special about the number 5. We can also define \mathbb{Z}_n for any natural number n . Here is the definition:

Definition 16.6 Let $n \in \mathbb{N}$. The equivalence classes of the equivalence relation $\equiv \pmod{n}$ are $[0],[1],[2],\dots,[n-1]$. The **integers modulo n** is the set $\mathbb{Z}_n = \{[0],[1],[2],\dots,[n-1]\}$. Elements of \mathbb{Z}_n can be added by the rule $[a] + [b] = [a + b]$ and multiplied by the rule $[a] \cdot [b] = [ab]$.

Given a natural number n , the set \mathbb{Z}_n is a number system containing n elements. It has many of the algebraic properties that \mathbb{Z}, \mathbb{R} and \mathbb{Q} possess. For example, it is probably obvious to you already that elements of \mathbb{Z}_n obey the commutative laws $[a] + [b] = [b] + [a]$ and $[a] \cdot [b] = [b] \cdot [a]$. You can also verify the distributive law $[a] \cdot ([b] + [c]) = [a] \cdot [b] + [a] \cdot [c]$, as follows:

$$\begin{aligned}
 [a] \cdot ([b] + [c]) &= [a] \cdot [b + c] \\
 &= [a(b + c)] \\
 &= [ab + ac] \\
 &= [ab] + [ac] \\
 &= [a] \cdot [b] + [a] \cdot [c].
 \end{aligned}$$

The integers modulo n are significant because they more closely fit certain applications than do other number systems such as \mathbb{Z} or \mathbb{R} . If you go on to

take a course in abstract algebra, then you will work extensively with \mathbb{Z}_n as well as other, more exotic, number systems. (In such a course you will also use all of the proof techniques that we have discussed, as well as the ideas of equivalence relations.)

To close this section we take up an issue that may have bothered you earlier. It has to do with our definitions of addition $[a] + [b] = [a + b]$ and multiplication $[a] \cdot [b] = [ab]$. These definitions define addition and multiplication of equivalence classes in terms of representatives a and b in the equivalence classes. Since there are many different ways to choose such representatives, we may well wonder if addition and multiplication are consistently defined. For example, suppose two people, Alice and Bob, want to multiply the elements $[2]$ and $[3]$ in \mathbb{Z}_5 . Alice does the calculation as $[2] \cdot [3] = [6] = [1]$, so her final answer is $[1]$. Bob does it differently. Since $[2] = [7]$ and $[3] = [8]$, he works out $[2] \cdot [3]$ as $[7] \cdot [8] = [56]$. Since $56 \equiv 1 \pmod{5}$, Bob's answer is $[56] = [1]$, and that agrees with Alice's answer. Will their answers always agree or did they just get lucky (with the arithmetic)?

The fact is that no matter how they do the multiplication in \mathbb{Z}_n , their answers will agree. To see why, suppose Alice and Bob want to multiply the elements $[a], [b] \in \mathbb{Z}_n$, and suppose $[a] = [a']$ and $[b] = [b']$. Alice and Bob do the multiplication as follows:

$$\begin{aligned} \text{Alice:} \quad & [a] \cdot [b] = [ab], \\ \text{Bob:} \quad & [a'] \cdot [b'] = [a'b']. \end{aligned}$$

We need to show that their answers agree, that is, we need to show $[ab] = [a'b']$. Since $[a] = [a']$, we know by Theorem 16.1 that $a \equiv a' \pmod{n}$. Thus $n \mid (a - a')$, so $a - a' = nk$ for some integer k . Likewise, as $[b] = [b']$, we know $b \equiv b' \pmod{n}$, or $n \mid (b - b')$, so $b - b' = n\ell$ for some integer ℓ . Thus we get $a = a' + nk$ and $b = b' + n\ell$. Therefore:

$$\begin{aligned} ab &= (a' + nk)(b' + n\ell) \\ &= a'b' + a'n\ell + nkb' + n^2k\ell, \\ \text{hence } ab - a'b' &= n(a'\ell + kb' + nk\ell). \end{aligned}$$

This shows $n \mid (ab - a'b')$, so $ab \equiv a'b' \pmod{n}$, and from that we conclude $[ab] = [a'b']$. Consequently Alice and Bob really do get the same answer, so we can be assured that the definition of multiplication in \mathbb{Z}_n is consistent.

Exercise 8 below asks you to show that addition in \mathbb{Z}_n is similarly consistent.

Exercises for Section 16.5

1. Write the addition and multiplication tables for \mathbb{Z}_2 .
 2. Write the addition and multiplication tables for \mathbb{Z}_3 .
 3. Write the addition and multiplication tables for \mathbb{Z}_4 .
 4. Write the addition and multiplication tables for \mathbb{Z}_6 .
 5. Suppose $[a], [b] \in \mathbb{Z}_5$ and $[a] \cdot [b] = [0]$. Is it necessarily true that either $[a] = [0]$ or $[b] = [0]$?
 6. Suppose $[a], [b] \in \mathbb{Z}_6$ and $[a] \cdot [b] = [0]$. Is it necessarily true that either $[a] = [0]$ or $[b] = [0]$?
 7. Do the following calculations in \mathbb{Z}_9 , in each case expressing your answer as $[a]$ with $0 \leq a \leq 8$.

| | | | |
|-----------------|-------------------|-----------------------|---------------------|
| (a) $[8] + [8]$ | (b) $[24] + [11]$ | (c) $[21] \cdot [15]$ | (d) $[8] \cdot [8]$ |
|-----------------|-------------------|-----------------------|---------------------|
 8. Suppose $[a], [b] \in \mathbb{Z}_n$, and $[a] = [a']$ and $[b] = [b']$. Alice adds $[a]$ and $[b]$ as $[a] + [b] = [a + b]$. Bob adds them as $[a'] + [b'] = [a' + b']$. Show that their answers $[a + b]$ and $[a' + b']$ are the same.
-

16.6 Relations Between Sets


In the beginning of this chapter, we defined a relation on a set A to be a subset $R \subseteq A \times A$. This created a framework that could model any situation in which elements of A are compared to themselves. In this setting, the statement xRy has elements x and y from A on either side of the R because R compares elements from A . But there are other relational symbols that don't work this way. Consider \in . The statement $5 \in \mathbb{Z}$ expresses a relationship between 5 and \mathbb{Z} (namely that the element 5 is in the set \mathbb{Z}) but 5 and \mathbb{Z} are not in any way naturally regarded as both elements of some set A . To overcome this difficulty, we generalize the idea of a relation on A to a *relation from A to B* .

Definition 16.7 A **relation** from a set A to a set B is a subset $R \subseteq A \times B$. We often abbreviate the statement $(x, y) \in R$ as xRy . The statement $(x, y) \notin R$ is abbreviated as $x \not R y$.

This definition will play a role in our treatment of *functions* in the next chapter. We close with one example.

Example 16.16 Suppose $A = \{1, 2\}$ and $B = \mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$. Here is a relation from A to B :

$$R = \{(1, \{1\}), (2, \{2\}), (1, \{1, 2\}), (2, \{1, 2\})\} \subseteq A \times B.$$

Note that we have $1R\{1\}$, $2R\{2\}$, $1R\{1, 2\}$ and $2R\{1, 2\}$. The relation R is the familiar relation \in for the set A , that is, $xR X$ means exactly the same thing as $x \in X$. 

Diagrams for relations from A to B differ from diagrams for relations on A . Since there are two sets A and B in a relation from A to B , we have to draw labeled nodes for each of the two sets. Then we draw arrows from x to y whenever xRy . The following figure illustrates this for Example 16.16.

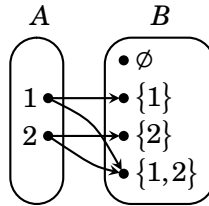


Figure 16.3. A relation from A to B

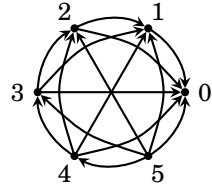
The ideas from this chapter show that any relation (whether it is a familiar one like \geq , \leq , $=$, $|$, \in or \subseteq , or a more exotic one) is really just a set. Therefore the theory of relations is a part of the theory of sets. In the next chapter, we will see that this idea touches on another important mathematical construction, namely functions. We will define a function to be a special kind of relation from one set to another, and in this context we will see that any function is really just a set.

16.7 Solutions for Chapter 16

Section 16.1 Exercises

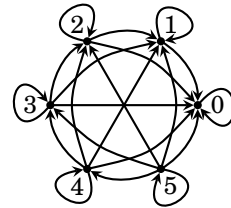
1. Let $A = \{0, 1, 2, 3, 4, 5\}$. Write out the relation R that expresses $>$ on A . Then illustrate it with a diagram.

$$R = \{(5, 4), (5, 3), (5, 2), (5, 1), (5, 0), (4, 3), (4, 2), (4, 1), (4, 0), (3, 2), (3, 1), (3, 0), (2, 1), (2, 0), (1, 0)\}$$



3. Let $A = \{0, 1, 2, 3, 4, 5\}$. Write out the relation R that expresses \geq on A . Then illustrate it with a diagram.

$$R = \{(5, 5), (5, 4), (5, 3), (5, 2), (5, 1), (5, 0), (4, 4), (4, 3), (4, 2), (4, 1), (4, 0), (3, 3), (3, 2), (3, 1), (3, 0), (2, 2), (2, 1), (2, 0), (1, 1), (1, 0), (0, 0)\}$$



5. The following diagram represents a relation R on a set A . Write the sets A and R . Answer: $A = \{0, 1, 2, 3, 4, 5\}$; $R = \{(3, 3), (4, 3), (4, 2), (1, 2), (2, 5), (5, 0)\}$

7. Write the relation $<$ on the set $A = \mathbb{Z}$ as a subset R of $\mathbb{Z} \times \mathbb{Z}$. This is an infinite set, so you will have to use set-builder notation.

Answer: $R = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : y - x \in \mathbb{N}\}$

9. How many different relations are there on the set $A = \{1, 2, 3, 4, 5, 6\}$? Consider forming a relation $R \subseteq A \times A$ on A . For each ordered pair $(x, y) \in A \times A$, we have two choices: we can either include (x, y) in R or not include it. There are $6 \cdot 6 = 36$ ordered pairs in $A \times A$. By the multiplication principle, there are thus 2^{36} different subsets R and hence also this many relations on A .

11. Answer: $2^{|A|^2}$

13. Answer: \neq

15. Answer: $\equiv \pmod{3}$

Section 16.2 Exercises

1. Consider the relation $R = \{(a, a), (b, b), (c, c), (d, d), (a, b), (b, a)\}$ on the set $A = \{a, b, c, d\}$. Which of the properties reflexive, symmetric and transitive does R possess and why? If a property does not hold, say why.

This is **reflexive** because $(x, x) \in R$ (i.e., xRx) for every $x \in A$.

It is **symmetric** because it is impossible to find an $(x, y) \in R$ for which $(y, x) \notin R$.

It is **transitive** because $(xRy \wedge yRz) \Rightarrow xRz$ always holds.

3. Consider the relation $R = \{(a, b), (a, c), (c, b), (b, c)\}$ on the set $A = \{a, b, c\}$. Which of the properties reflexive, symmetric and transitive does R possess and why? If a property does not hold, say why.

This is **not reflexive** because $(a, a) \notin R$ (for example).

It is **not symmetric** because $(a, b) \in R$ but $(b, a) \notin R$.

It is **not transitive** because cRb and bRc are true, but cRc is false.

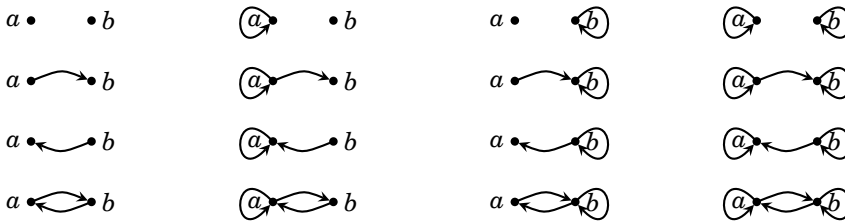
5. Consider the relation $R = \{(0, 0), (\sqrt{2}, 0), (0, \sqrt{2}), (\sqrt{2}, \sqrt{2})\}$ on \mathbb{R} . Say whether this relation is reflexive, symmetric and transitive. If a property does not hold, say why.

This is **not reflexive** because $(1, 1) \notin R$ (for example).

It is **symmetric** because it is impossible to find an $(x, y) \in R$ for which $(y, x) \notin R$.

It is **transitive** because $(xRy \wedge yRz) \Rightarrow xRz$ always holds.

7. There are 16 possible different relations R on the set $A = \{a, b\}$. Describe all of them. (A picture for each one will suffice, but don't forget to label the nodes.) Which ones are reflexive? Symmetric? Transitive?



Only the four in the right column are reflexive. Only the eight in the first and fourth rows are symmetric. All of them are transitive **except** the first three on the fourth row.

9. Define a relation on \mathbb{Z} by declaring xRy if and only if x and y have the same parity. Say whether this relation is reflexive, symmetric and transitive. If a property does not hold, say why. What familiar relation is this?

This is **reflexive** because xRx since x always has the same parity as x .

It is **symmetric** because if x and y have the same parity, then y and x must have the same parity (that is, $xRy \Rightarrow yRx$).

It is **transitive** because if x and y have the same parity and y and z have the same parity, then x and z must have the same parity. (That is $(xRy \wedge yRz) \Rightarrow xRz$ always holds.)

The relation is congruence modulo 2.

11. Suppose $A = \{a, b, c, d\}$ and $R = \{(a, a), (b, b), (c, c), (d, d)\}$. Say whether this relation is reflexive, symmetric and transitive. If a property does not hold, say why.

This is **reflexive** because $(x, x) \in R$ for every $x \in A$.

It is **symmetric** because it is impossible to find an $(x, y) \in R$ for which $(y, x) \notin R$.

It is **transitive** because $(xRy \wedge yRz) \Rightarrow xRz$ always holds.

(For example $(aRa \wedge aRa) \Rightarrow aRa$ is true, etc.)

13. Consider the relation $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} : x - y \in \mathbb{Z}\}$ on \mathbb{R} . Prove that this relation is reflexive and symmetric, and transitive.

Proof. In this relation, xRy means $x - y \in \mathbb{Z}$.

To see that R is reflexive, take any $x \in \mathbb{R}$ and observe that $x - x = 0 \in \mathbb{Z}$, so xRx . Therefore R is reflexive.

To see that R is symmetric, we need to prove $xRy \Rightarrow yRx$ for all $x, y \in \mathbb{R}$. We use direct proof. Suppose xRy . This means $x - y \in \mathbb{Z}$. Then it follows that $-(x - y) = y - x$ is also in \mathbb{Z} . But $y - x \in \mathbb{Z}$ means yRx . We've shown xRy implies yRx , so R is symmetric.

To see that R is transitive, we need to prove $(xRy \wedge yRz) \Rightarrow xRz$ is always true. We prove this conditional statement with direct proof. Suppose xRy and yRz . Since xRy , we know $x - y \in \mathbb{Z}$. Since yRz , we know $y - z \in \mathbb{Z}$. Thus $x - y$ and $y - z$ are both integers; by adding these integers we get another integer $(x - y) + (y - z) = x - z$. Thus $x - z \in \mathbb{Z}$, and this means xRz . We've now shown that if xRy and yRz , then xRz . Therefore R is transitive. ■

15. Prove or disprove: If a relation is symmetric and transitive, then it is also reflexive.

This is **false**. For a counterexample, consider the relation $R = \{(a, a), (a, b), (b, a), (b, b)\}$ on the set $A = \{a, b, c\}$. This is symmetric and transitive but it is not reflexive.

17. Define a relation \sim on \mathbb{Z} as $x \sim y$ if and only if $|x - y| \leq 1$. Say whether \sim is reflexive, symmetric and transitive.

This is reflexive because $|x - x| = 0 \leq 1$ for all integers x . It is symmetric because $x \sim y$ if and only if $|x - y| \leq 1$, if and only if $|y - x| \leq 1$, if and only if $y \sim x$. It is not transitive because, for example, $0 \sim 1$ and $1 \sim 2$, but is not the case that $0 \sim 2$.

Section 16.3 Exercises

1. Let $A = \{1, 2, 3, 4, 5, 6\}$, and consider the following equivalence relation on A : $R = \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (6, 6), (2, 3), (3, 2), (4, 5), (5, 4), (4, 6), (6, 4), (5, 6), (6, 5)\}$. List the equivalence classes of R .

The equivalence classes are: $[1] = \{1\}$; $[2] = [3] = \{2, 3\}$; $[4] = [5] = [6] = \{4, 5, 6\}$.

3. Let $A = \{a, b, c, d, e\}$. Suppose R is an equivalence relation on A . Suppose R has three equivalence classes. Also aRd and bRc . Write out R as a set.

Answer: $R = \{(a, a), (b, b), (c, c), (d, d), (e, e), (a, d), (d, a), (b, c), (c, b)\}$.

5. There are two different equivalence relations on the set $A = \{a, b\}$. Describe them all. Diagrams will suffice.

Answer: $R = \{(a, a), (b, b)\}$ and $R = \{(a, a), (b, b), (a, b), (b, a)\}$

7. Define a relation R on \mathbb{Z} as xRy if and only if $3x - 5y$ is even. Prove R is an equivalence relation. Describe its equivalence classes.

To prove that R is an equivalence relation, we must show it's reflexive, symmetric and transitive.

The relation R is reflexive for the following reason. If $x \in \mathbb{Z}$, then $3x - 5x = -2x$ is even. But then since $3x - 5x$ is even, we have xRx . Thus R is reflexive.

To see that R is symmetric, suppose xRy . We must show yRx . Since xRy , we know $3x - 5y$ is even, so $3x - 5y = 2a$ for some integer a . Now reason as follows:

$$\begin{aligned} 3x - 5y &= 2a \\ 3x - 5y + 8y - 8x &= 2a + 8y - 8x \\ 3y - 5x &= 2(a + 4y - 4x). \end{aligned}$$

From this it follows that $3y - 5x$ is even, so yRx . We've now shown xRy implies yRx , so R is symmetric.

To prove that R is transitive, assume that xRy and yRz . (We will show that this implies xRz .) Since xRy and yRz , it follows that $3x - 5y$ and $3y - 5z$ are both even, so $3x - 5y = 2a$ and $3y - 5z = 2b$ for some integers a and b . Adding these equations, we get $(3x - 5y) + (3y - 5z) = 2a + 2b$, and this simplifies to $3x - 5z = 2(a + b + y)$. Therefore $3x - 5z$ is even, so xRz . We've now shown that if xRy and yRz , then xRz , so R is transitive.

We've now shown that R is reflexive, symmetric and transitive, so it is an equivalence relation.

This completes the first part of the problem. Now we move on to the second part. To find the equivalence classes, first note that

$$[0] = \{x \in \mathbb{Z} : xR0\} = \{x \in \mathbb{Z} : 3x - 5 \cdot 0 \text{ is even}\} = \{x \in \mathbb{Z} : 3x \text{ is even}\} = \{x \in \mathbb{Z} : x \text{ is even}\}.$$

Thus the equivalence class $[0]$ consists of all even integers. Next, note that

$$[1] = \{x \in \mathbb{Z} : xR1\} = \{x \in \mathbb{Z} : 3x - 5 \cdot 1 \text{ is even}\} = \{x \in \mathbb{Z} : 3x - 5 \text{ is even}\} = \{x \in \mathbb{Z} : x \text{ is odd}\}.$$

Thus the equivalence class $[1]$ consists of all odd integers.

Consequently there are just two equivalence classes $\{\dots, -4, -2, 0, 2, 4, \dots\}$ and $\{\dots, -3, -1, 1, 3, 5, \dots\}$.

- 9.** Define a relation R on \mathbb{Z} as xRy if and only if $4 \mid (x+3y)$. Prove R is an equivalence relation. Describe its equivalence classes.

This is reflexive, because for any $x \in \mathbb{Z}$ we have $4 \mid (x+3x)$, so xRx .

To prove that R is symmetric, suppose xRy . Then $4 \mid (x+3y)$, so $x+3y = 4a$ for some integer a . Multiplying by 3, we get $3x+9y = 12a$, which becomes $y+3x = 12a - 8y$. Then $y+3x = 4(3a - 2y)$, so $4 \mid (y+3x)$, hence yRx . Thus we've shown xRy implies yRx , so R is symmetric.

To prove transitivity, suppose xRy and yRz . Then $4 \mid (x+3y)$ and $4 \mid (y+3z)$, so $x+3y = 4a$ and $y+3z = 4b$ for some integers a and b . Adding these two equations produces $x+4y+3z = 4a+4b$, or $x+3z = 4a+4b-4y = 4(a+b-y)$. Consequently $4 \mid (x+3z)$, so xRz , and R is transitive.

As R is reflexive, symmetric and transitive, it is an equivalence relation.

Now let's compute its equivalence classes.

$$[0] = \{x \in \mathbb{Z} : xR0\} = \{x \in \mathbb{Z} : 4 \mid (x+3 \cdot 0)\} = \{x \in \mathbb{Z} : 4 \mid x\} = \{\dots, -4, 0, 4, 8, 12, 16, \dots\}$$

$$\begin{aligned}
 [1] &= \{x \in \mathbb{Z} : xR1\} = \{x \in \mathbb{Z} : 4 \mid (x + 3 \cdot 1)\} = \{x \in \mathbb{Z} : 4 \mid (x + 3)\} = \{\dots - 3, 1, 5, 9, 13, 17, \dots\} \\
 [2] &= \{x \in \mathbb{Z} : xR2\} = \{x \in \mathbb{Z} : 4 \mid (x + 3 \cdot 2)\} = \{x \in \mathbb{Z} : 4 \mid (x + 6)\} = \{\dots - 2, 2, 6, 10, 14, 18, \dots\} \\
 [3] &= \{x \in \mathbb{Z} : xR3\} = \{x \in \mathbb{Z} : 4 \mid (x + 3 \cdot 3)\} = \{x \in \mathbb{Z} : 4 \mid (x + 9)\} = \{\dots - 1, 3, 7, 11, 15, 19, \dots\}
 \end{aligned}$$

11. Prove or disprove: If R is an equivalence relation on an infinite set A , then R has infinitely many equivalence classes.

This is **False**. Counterexample: consider the relation of congruence modulo 2. It is a relation on the infinite set \mathbb{Z} , but it has only two equivalence classes.

13. Answer: $m|A|$

15. Answer: 15

Section 16.4 Exercises

1. List all the partitions of the set $A = \{a, b\}$. Compare your answer to the answer to Exercise 5 of Section 16.3.

There are just two partitions $\{\{a\}, \{b\}\}$ and $\{\{a, b\}\}$. These correspond to the two equivalence relations $R_1 = \{(a, a), (b, b)\}$ and $R_2 = \{(a, a), (a, b), (b, a), (b, b)\}$, respectively, on A .

3. Describe the partition of \mathbb{Z} resulting from the equivalence relation $\equiv \pmod{4}$.

Answer: The partition is $\{[0], [1], [2], [3]\} = \{\{\dots, -4, 0, 4, 8, 12, \dots\}, \{\dots, -3, 1, 5, 9, 13, \dots\}, \{\dots, -2, 2, 4, 6, 10, 14, \dots\}, \{\dots, -1, 3, 7, 11, 15, \dots\}\}$

5. Answer: Congruence modulo 2, or “same parity.”

Section 16.5 Exercises

1. Write the addition and multiplication tables for \mathbb{Z}_2 .

| | | |
|-----|-----|-----|
| + | [0] | [1] |
| [0] | [0] | [1] |
| [1] | [1] | [0] |

| | | |
|-----|-----|-----|
| · | [0] | [1] |
| [0] | [0] | [0] |
| [1] | [0] | [1] |

3. Write the addition and multiplication tables for \mathbb{Z}_4 .

| | | | | |
|-----|-----|-----|-----|-----|
| + | [0] | [1] | [2] | [3] |
| [0] | [0] | [1] | [2] | [3] |
| [1] | [1] | [2] | [3] | [0] |
| [2] | [2] | [3] | [0] | [1] |
| [3] | [3] | [0] | [1] | [2] |

| | | | | |
|-----|-----|-----|-----|-----|
| · | [0] | [1] | [2] | [3] |
| [0] | [0] | [0] | [0] | [0] |
| [1] | [0] | [1] | [2] | [3] |
| [2] | [0] | [2] | [0] | [2] |
| [3] | [0] | [3] | [2] | [1] |

5. Suppose $[a], [b] \in \mathbb{Z}_5$ and $[a] \cdot [b] = [0]$. Is it necessarily true that either $[a] = [0]$ or $[b] = [0]$?

The multiplication table for \mathbb{Z}_5 is shown in Section 16.5. In the body of that table, the only place that $[0]$ occurs is in the first row or the first column. That row and column are both headed by $[0]$. It follows that if $[a] \cdot [b] = [0]$, then either $[a]$ or $[b]$ must be $[0]$.

7. Do the following calculations in \mathbb{Z}_9 , in each case expressing your answer as $[a]$ with $0 \leq a \leq 8$.
- (a) $[8] + [8] = [7]$ (b) $[24] + [11] = [8]$ (c) $[21] \cdot [15] = [0]$ (d) $[8] \cdot [8] = [1]$

Functions

You know from calculus that functions play a fundamental role in mathematics. You likely view a function as a kind of formula that describes a relationship between two (or more) quantities. You certainly understand and appreciate the fact that relationships between quantities are important in all scientific disciplines, so you do not need to be convinced that functions are important. Still, you may not be aware of the full significance of functions. Functions are more than merely descriptions of numeric relationships. In a more general sense, functions can compare and relate different kinds of mathematical structures. You will see this as your understanding of mathematics deepens. In preparation of this deepening, we will now explore a more general and versatile view of functions.

The concept of a relation between sets (Definition 16.7) plays a big role here, so you may want to quickly review it.

17.1 Functions

Let's start on familiar ground. Consider the function $f(x) = x^2$ from \mathbb{R} to \mathbb{R} . Its graph is the set of points $R = \{(x, x^2) : x \in \mathbb{R}\} \subseteq \mathbb{R} \times \mathbb{R}$.

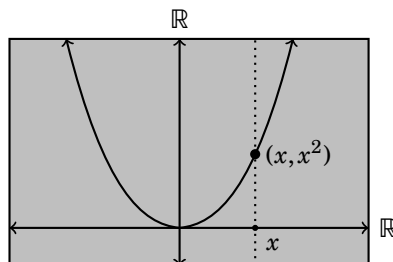


Figure 17.1. A familiar function

Having read Chapter 16, you may see f in a new light. Its graph $R \subseteq \mathbb{R} \times \mathbb{R}$ is a relation on the set \mathbb{R} . In fact, as we shall see, functions are just special kinds of relations. Before stating the exact definition, we look at another

example. Consider the function $f(n) = |n| + 2$ that converts integers n into natural numbers $|n| + 2$. Its graph is $R = \{(n, |n| + 2) : n \in \mathbb{Z}\} \subseteq \mathbb{Z} \times \mathbb{N}$.

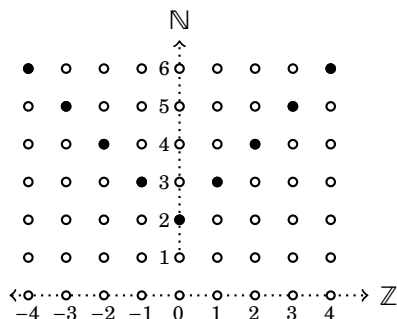



Figure 17.2. The function $f : \mathbb{Z} \rightarrow \mathbb{N}$, where $f(n) = |n| + 2$

Figure 17.2 shows the graph R as darkened dots in the grid of points $\mathbb{Z} \times \mathbb{N}$. Notice that in this example R is not a relation on a single set. The set of input values \mathbb{Z} is different from the set \mathbb{N} of output values, so the graph $R \subseteq \mathbb{Z} \times \mathbb{N}$ is a relation from \mathbb{Z} to \mathbb{N} .

This example illustrates three things. First, a function can be viewed as sending elements from one set A to another set B . (In the case of f , $A = \mathbb{Z}$ and $B = \mathbb{N}$.) Second, such a function can be regarded as a relation from A to B . Third, for every input value n , there is *exactly one* output value $f(n)$. In your high school algebra course, this was expressed by the *vertical line test*: Any vertical line intersects a function's graph at most once. It means that for any input value x , the graph contains exactly one point of form $(x, f(x))$. Our main definition, given below, incorporates all of these ideas.

Definition 17.1 Suppose A and B are sets. A **function** f from A to B (denoted as $f : A \rightarrow B$) is a relation $f \subseteq A \times B$ from A to B , satisfying the property that for each $a \in A$ the relation f contains exactly one ordered pair of form (a, b) . The statement $(a, b) \in f$ is abbreviated $f(a) = b$.

Example 17.1 Consider the function f graphed in Figure 17.2. According to Definition 17.1, we regard f as the set of points in its graph, that is, $f = \{(n, |n| + 2) : n \in \mathbb{Z}\} \subseteq \mathbb{Z} \times \mathbb{N}$. This is a relation from \mathbb{Z} to \mathbb{N} , and indeed given any $a \in \mathbb{Z}$ the set f contains exactly one ordered pair $(a, |a| + 2)$ whose first coordinate is a . Since $(1, 3) \in f$, we write $f(1) = 3$; and since $(-3, 5) \in f$ we write $f(-3) = 5$, etc. In general, $(a, b) \in f$ means that f sends the input value a to the output value b , and we express this as $f(a) = b$. This function can be

expressed by a formula: For each input value n , the output value is $|n| + 2$, so we may write $f(n) = |n| + 2$. All this agrees with the way we thought of functions in algebra and calculus; the only difference is that now we also think of a function as a relation. 


Definition 17.2 For a function $f : A \rightarrow B$, the set A is called the **domain** of f . (Think of the domain as the set of possible “input values” for f .) The set B is called the **codomain** of f . The **range** of f is the set $\{f(a) : a \in A\} = \{b : (a, b) \in f\}$. (Think of the range as the set of all possible “output values” for f . Think of the codomain as a sort of “target” for the outputs.)

Continuing Example 17.1, the domain of f is \mathbb{Z} and its codomain is \mathbb{N} . Its range is $\{f(a) : a \in \mathbb{Z}\} = \{|a| + 2 : a \in \mathbb{Z}\} = \{2, 3, 4, 5, \dots\}$. The range is a subset of the codomain, but it does not (in this case) equal the codomain.

In our examples so far, the domains and codomains are sets of numbers, but this needn't be the case in general, as the next example indicates.

Example 17.2 Let $A = \{p, q, r, s\}$ and $B = \{0, 1, 2\}$, and

$$f = \{(p, 0), (q, 1), (r, 2), (s, 2)\} \subseteq A \times B.$$

This is a function $f : A \rightarrow B$ because each element of A occurs exactly once as a first coordinate of an ordered pair in f . We have $f(p) = 0$, $f(q) = 1$, $f(r) = 2$ and $f(s) = 2$. The domain of f is $\{p, q, r, s\}$, and the codomain and range are both $\{0, 1, 2\}$. 

If A and B are not both sets of numbers it can be difficult to draw a graph of $f : A \rightarrow B$ in the traditional sense. Figure 17.3(a) shows an attempt at a graph of f from Example 17.2. The sets A and B are aligned roughly as x - and y -axes, and the Cartesian product $A \times B$ is filled in accordingly. The subset $f \subseteq A \times B$ is indicated with dashed lines, and this can be regarded as a “graph” of f . Figure 17.3(b) shows a more natural depiction of f . Sets A and B are drawn side-by-side, and arrows point from a to b when $f(a) = b$.

In general, if $f : A \rightarrow B$ is the kind of function you may have encountered in algebra or calculus, then conventional graphing techniques offer the best visual description of it. On the other hand, if A and B are finite or if we are thinking of them as generic sets, then describing f with arrows is often a more appropriate way of visualizing it.

We emphasize that, according to Definition 17.1, a function is really just a special kind of set. Any function $f : A \rightarrow B$ is a subset of $A \times B$. By contrast, your calculus text probably defined a function as a certain kind of “rule.” While that intuitive outlook is adequate for the first few semesters

of calculus, it does not hold up well to the rigorous mathematical standards necessary for further progress. The problem is that words like “rule” are too vague. Defining a function as a set removes the ambiguity and makes a function a concrete mathematical object. It allows us, for example, to talk about about a “set of functions” and know exactly what we are speaking of. A set of functions is just certain kind of set of sets. Such precision is necessary in proofs.

Still, in practice we tend to think of functions as rules. Given $f : \mathbb{Z} \rightarrow \mathbb{N}$ where $f(x) = |x| + 2$, we think of this as a rule that associates any number $n \in \mathbb{Z}$ to the number $|n| + 2$ in \mathbb{N} , rather than a set containing ordered pairs $(n, |n| + 2)$. It is only when we have to understand or interpret the theoretical nature of functions (as we do in this text) that Definition 17.1 comes to bear. The definition is a foundation that gives us license to think about functions in a more informal way.

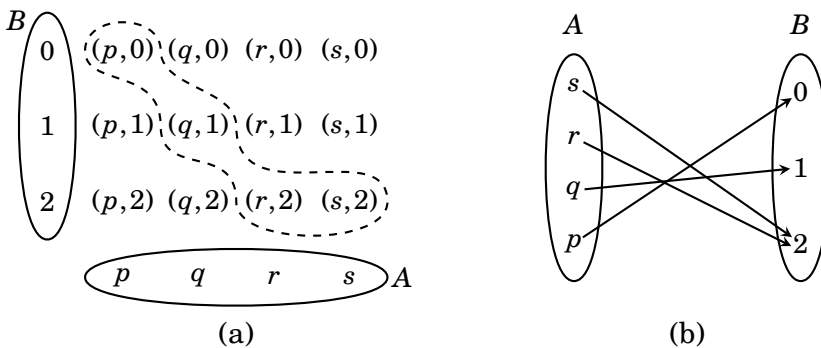



Figure 17.3. Two ways of drawing the function $f = \{(p, 0), (q, 1), (r, 2), (s, 2)\}$

The next example brings up a point about notation. Consider a function such as $f : \mathbb{Z}^2 \rightarrow \mathbb{Z}$, whose domain is a Cartesian product. This function takes as input an ordered pair $(m, n) \in \mathbb{Z}^2$ and sends it to a number $f((m, n)) \in \mathbb{Z}$. To simplify the notation, it is common to write $f(m, n)$ instead of $f((m, n))$, even though this is like writing fx instead of $f(x)$. We also remark that although we’ve been using the letters f, g and h for functions, any other reasonable symbol could be used. Greek letters such as φ and θ are common.

Example 17.3 Say a function $\varphi : \mathbb{Z}^2 \rightarrow \mathbb{Z}$ is defined as $\varphi(m, n) = 6m - 9n$. Note that as a set, this function is $\varphi = \{(m, n), 6m - 9n\} \subseteq \mathbb{Z}^2 \times \mathbb{Z}$. What is the range of φ ?

To answer this, first observe that for any $(m, n) \in \mathbb{Z}^2$, the value $f(m, n) = 6m - 9n = 3(2m - 3n)$ is a multiple of 3. Thus every number in the range is a multiple of 3, so the range is a *subset* of the set of all multiples of 3. On the other hand if $b = 3k$ is a multiple of 3 we have $\varphi(-k, -k) = 6(-k) - 9(-k) = 3k = b$, which means any multiple of 3 is in the range of φ . Therefore the range of φ is the set $\{3k : k \in \mathbb{Z}\}$ of all multiples of 3. 

To conclude this section, let's use Definition 17.1 to help us understand what it means for two functions $f : A \rightarrow B$ and $g : C \rightarrow D$ to be equal. According to our definition, functions f and g are subsets $f \subseteq A \times B$ and $g \subseteq C \times D$. It makes sense to say that f and g are equal if $f = g$, that is, if they are equal as sets.

Thus the two functions $f = \{(1, a), (2, a), (3, b)\}$ and $g = \{(3, b), (2, a), (1, a)\}$ are equal because the sets f and g are equal. Notice that the domain of both functions is $A = \{1, 2, 3\}$, the set of first elements x in the ordered pairs $(x, y) \in f = g$. In general, equal functions must have equal domains.

Observe also that the equality $f = g$ means $f(x) = g(x)$ for every $x \in A$. We repackage these ideas in the following definition.

Definition 17.3 Two functions $f : A \rightarrow B$ and $g : A \rightarrow D$ are **equal** if $f(x) = g(x)$ for every $x \in A$.

Observe that f and g can have different codomains and still be equal. Consider the functions $f : \mathbb{Z} \rightarrow \mathbb{N}$ and $g : \mathbb{Z} \rightarrow \mathbb{Z}$ defined as $f(x) = |x| + 2$ and $g(x) = |x| + 2$. Even though their codomains are different, the functions are equal because $f(x) = g(x)$ for every x in the domain.

Exercises for Section 17.1

1. Suppose $A = \{0, 1, 2, 3, 4\}$, $B = \{2, 3, 4, 5\}$ and $f = \{(0, 3), (1, 3), (2, 4), (3, 2), (4, 2)\}$. State the domain and range of f . Find $f(2)$ and $f(1)$.
2. Suppose $A = \{a, b, c, d\}$, $B = \{2, 3, 4, 5, 6\}$ and $f = \{(a, 2), (b, 3), (c, 4), (d, 5)\}$. State the domain and range of f . Find $f(b)$ and $f(d)$.
3. There are four different functions $f : \{a, b\} \rightarrow \{0, 1\}$. List them all. Diagrams will suffice.
4. There are eight different functions $f : \{a, b, c\} \rightarrow \{0, 1\}$. List them all. Diagrams will suffice.
5. Give an example of a relation from $\{a, b, c, d\}$ to $\{d, e\}$ that is not a function.
6. Suppose $f : \mathbb{Z} \rightarrow \mathbb{Z}$ is defined as $f = \{(x, 4x + 5) : x \in \mathbb{Z}\}$. State the domain, codomain and range of f . Find $f(10)$.

7. Consider the set $f = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : 3x + y = 4\}$. Is this a function from \mathbb{Z} to \mathbb{Z} ? Explain.
8. Consider the set $f = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x + 3y = 4\}$. Is this a function from \mathbb{Z} to \mathbb{Z} ? Explain.
9. Consider the set $f = \{(x^2, x) : x \in \mathbb{R}\}$. Is this a function from \mathbb{R} to \mathbb{R} ? Explain.
10. Consider the set $f = \{(x^3, x) : x \in \mathbb{R}\}$. Is this a function from \mathbb{R} to \mathbb{R} ? Explain.
11. Is the set $\theta = \{(X, |X|) : X \subseteq \mathbb{Z}_5\}$ a function? If so, what is its domain and range?
12. Is the set $\theta = \{(x, y), (3y, 2x, x + y) : x, y \in \mathbb{R}\}$ a function? If so, what is its domain, codomain and range?

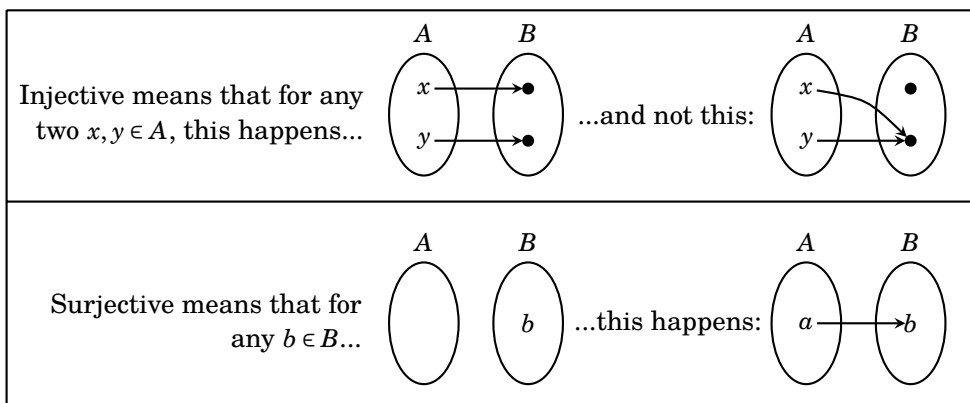
17.2 Injective and Surjective Functions

You may recall from algebra and calculus that a function may be *one-to-one* and *onto*, and these properties are related to whether or not the function is invertible. We now review these important ideas. In advanced mathematics, the word *injective* is often used instead of *one-to-one*, and *surjective* is used instead of *onto*. Here are the exact definitions:

Definition 17.4 A function $f : A \rightarrow B$ is:

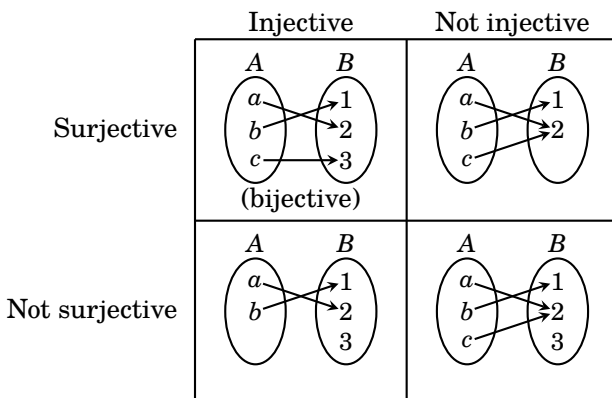
- **injective** (or one-to-one) if for every $x, y \in A$, $x \neq y$ implies $f(x) \neq f(y)$;
- **surjective** (or onto) if for every $b \in B$ there is an $a \in A$ with $f(a) = b$;
- **bijective** if f is both injective and surjective.

Below is a visual description of Definition 17.4. In essence, injective means that unequal elements in A always get sent to unequal elements in B . Surjective means that every element of B has an arrow pointing to it, that is, it equals $f(a)$ for some a in the domain of f .



For more concrete examples, consider the following functions from \mathbb{R} to \mathbb{R} . The function $f(x) = x^2$ is not injective because $-2 \neq 2$, but $f(-2) = f(2)$. Nor is it surjective, for if $b = -1$ (or if b is any negative number), then there is no $a \in \mathbb{R}$ with $f(a) = b$. On the other hand, $g(x) = x^3$ is both injective and surjective, so it is also bijective.

There are four possible injective/surjective combinations that a function may possess. This is illustrated in the following figure showing four functions from A to B . Functions in the first column are injective, those in the second column are not injective. Functions in the first row are surjective, those in the second row are not.



We note in passing that, according to the definitions, a function is surjective if and only if its codomain equals its range.

Often it is necessary to prove that a particular function $f : A \rightarrow B$ is injective. For this we must prove that for any two elements $x, y \in A$, the conditional statement $(x \neq y) \Rightarrow (f(x) \neq f(y))$ is true. The two main approaches for this are summarized below.

How to show a function $f : A \rightarrow B$ is injective:

Direct approach:
 Suppose $x, y \in A$ and $x \neq y$.
 \vdots
 Therefore $f(x) \neq f(y)$.

Contrapositive approach:
 Suppose $x, y \in A$ and $f(x) = f(y)$.
 \vdots
 Therefore $x = y$.

Of these two approaches, the contrapositive is often the easiest to use, especially if f is defined by an algebraic formula. This is because the contrapositive approach starts with the equation $f(x) = f(y)$ and proceeds to

the equation $x = y$. In algebra, as you know, it is usually easier to work with equalities than inequalities.

To prove that a function is *not* injective, you must *disprove* the statement $(x \neq y) \Rightarrow (f(x) \neq f(y))$. For this it suffices to find example of two elements $x, y \in A$ for which $x \neq y$ and $f(x) = f(y)$.

Next we examine how to prove that $f : A \rightarrow B$ is *surjective*. According to Definition 17.4, we must prove the statement $\forall b \in B, \exists a \in A, f(a) = b$. In words, we must show that for any $b \in B$, there is at least one $a \in A$ (which may depend on b) having the property that $f(a) = b$. Here is an outline.

How to show a function $f : A \rightarrow B$ is surjective:


Suppose $b \in B$.
 [Prove there exists $a \in A$ for which $f(a) = b$.]

In the second step, we have to prove the existence of an a for which $f(a) = b$. For this, just finding an example of such an a would suffice. (How to find such an example depends on how f is defined. If f is given as a formula, we may be able to find a by solving the equation $f(a) = b$ for a . Sometimes you can find a by just plain common sense.) To show f is *not* surjective, we must prove the negation of $\forall b \in B, \exists a \in A, f(a) = b$, that is, we must prove $\exists b \in B, \forall a \in A, f(a) \neq b$.

The following examples illustrate these ideas. (For the first example, note that the set $\mathbb{R} - \{0\}$ is \mathbb{R} with the number 0 removed.)

Example 17.4 Show that the function $f : \mathbb{R} - \{0\} \rightarrow \mathbb{R}$ defined as $f(x) = \frac{1}{x} + 1$ is injective but not surjective.

We will use the contrapositive approach to show that f is injective. Suppose $x, y \in \mathbb{R} - \{0\}$ and $f(x) = f(y)$. This means $\frac{1}{x} + 1 = \frac{1}{y} + 1$. Subtracting 1 from both sides and inverting produces $x = y$. Therefore f is injective.


Function f is not surjective because there exists an element $b = 1 \in \mathbb{R}$ for which $f(x) = \frac{1}{x} + 1 \neq 1$ for every $x \in \mathbb{R} - \{0\}$. 

Example 17.5 Show that the function $g : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z}$ defined by the formula $g(m, n) = (m + n, m + 2n)$, is both injective and surjective.

We will use the contrapositive approach to show that g is injective. Thus we need to show that $g(m, n) = g(k, \ell)$ implies $(m, n) = (k, \ell)$. Suppose $(m, n), (k, \ell) \in \mathbb{Z} \times \mathbb{Z}$ and $g(m, n) = g(k, \ell)$. Then $(m + n, m + 2n) = (k + \ell, k + 2\ell)$. It follows that $m + n = k + \ell$ and $m + 2n = k + 2\ell$. Subtracting the first equation from the second gives $n = \ell$. Next, subtract $n = \ell$ from $m + n = k + \ell$ to get $m = k$. Since $m = k$ and $n = \ell$, it follows that $(m, n) = (k, \ell)$. Therefore g is injective.

To see that g is surjective, consider an arbitrary element $(b, c) \in \mathbb{Z} \times \mathbb{Z}$. We need to show that there is some $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ for which $g(x, y) = (b, c)$. To find (x, y) , note that $g(x, y) = (b, c)$ means $(x + y, x + 2y) = (b, c)$. This leads to the following system of equations:

$$\begin{aligned}x + y &= b \\x + 2y &= c.\end{aligned}$$

Solving gives $x = 2b - c$ and $y = c - b$. Then $(x, y) = (2b - c, c - b)$. We now have $g(2b - c, c - b) = (b, c)$, and it follows that g is surjective. 

Example 17.6 Consider function $h : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Q}$ defined as $h(m, n) = \frac{m}{|n| + 1}$.

Determine whether this is injective and whether it is surjective.

This function is *not* injective because of the unequal elements $(1, 2)$ and $(1, -2)$ in $\mathbb{Z} \times \mathbb{Z}$ for which $h(1, 2) = h(1, -2) = \frac{1}{3}$. However, h is surjective: Take any element $b \in \mathbb{Q}$. Then $b = \frac{c}{d}$ for some $c, d \in \mathbb{Z}$. Notice we may assume d is positive by making c negative, if necessary. Then $h(c, d - 1) = \frac{c}{|d-1|+1} = \frac{c}{d} = b$.

Exercises for Section 17.2

- Let $A = \{1, 2, 3, 4\}$ and $B = \{a, b, c\}$. Give an example of a function $f : A \rightarrow B$ that is neither injective nor surjective.
- Consider the logarithm function $\ln : (0, \infty) \rightarrow \mathbb{R}$. Decide whether this function is injective and whether it is surjective.
- Consider the cosine function $\cos : \mathbb{R} \rightarrow \mathbb{R}$. Decide whether this function is injective and whether it is surjective. What if it had been defined as $\cos : \mathbb{R} \rightarrow [-1, 1]$?
- A function $f : \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z}$ is defined as $f(n) = (2n, n + 3)$. Verify whether this function is injective and whether it is surjective.
- A function $f : \mathbb{Z} \rightarrow \mathbb{Z}$ is defined as $f(n) = 2n + 1$. Verify whether this function is injective and whether it is surjective.
- A function $f : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ is defined as $f(m, n) = 3n - 4m$. Verify whether this function is injective and whether it is surjective.
- A function $f : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ is defined as $f(m, n) = 2n - 4m$. Verify whether this function is injective and whether it is surjective.
- A function $f : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z}$ is defined as $f(m, n) = (m + n, 2m + n)$. Verify whether this function is injective and whether it is surjective.
- Prove that the function $f : \mathbb{R} - \{2\} \rightarrow \mathbb{R} - \{5\}$ defined by $f(x) = \frac{5x + 1}{x - 2}$ is bijective.
- Prove the function $f : \mathbb{R} - \{1\} \rightarrow \mathbb{R} - \{1\}$ defined by $f(x) = \left(\frac{x + 1}{x - 1}\right)^3$ is bijective.
- Consider the function $\theta : \{0, 1\} \times \mathbb{N} \rightarrow \mathbb{Z}$ defined as $\theta(a, b) = (-1)^a b$. Is θ injective? Is it surjective? Bijective? Explain.

12. Consider the function $\theta : \{0,1\} \times \mathbb{N} \rightarrow \mathbb{Z}$ defined as $\theta(a,b) = a - 2ab + b$. Is θ injective? Is it surjective? Bijective? Explain.
13. Consider the function $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ defined by the formula $f(x,y) = (xy, x^3)$. Is f injective? Is it surjective? Bijective? Explain.
14. Consider the function $\theta : \mathcal{P}(\mathbb{Z}) \rightarrow \mathcal{P}(\mathbb{Z})$ defined as $\theta(X) = \overline{X}$. Is θ injective? Is it surjective? Bijective? Explain.
15. This question concerns functions $f : \{A,B,C,D,E,F,G\} \rightarrow \{1,2,3,4,5,6,7\}$. How many such functions are there? How many of these functions are injective? How many are surjective? How many are bijective?
16. This question concerns functions $f : \{A,B,C,D,E\} \rightarrow \{1,2,3,4,5,6,7\}$. How many such functions are there? How many of these functions are injective? How many are surjective? How many are bijective?
17. This question concerns functions $f : \{A,B,C,D,E,F,G\} \rightarrow \{1,2\}$. How many such functions are there? How many of these functions are injective? How many are surjective? How many are bijective?
18. Prove that the function $f : \mathbb{N} \rightarrow \mathbb{Z}$ defined as $f(n) = \frac{(-1)^n(2n-1)+1}{4}$ is bijective.

17.3 The Pigeonhole Principle Revisited

Here is a simple but useful idea. Imagine there is a set A of pigeons and a set B of pigeonholes, and all the pigeons fly into the pigeonholes. You can think of this as describing a function $f : A \rightarrow B$, where pigeon X flies into pigeonhole $f(X)$. Figure 17.4 illustrates this.

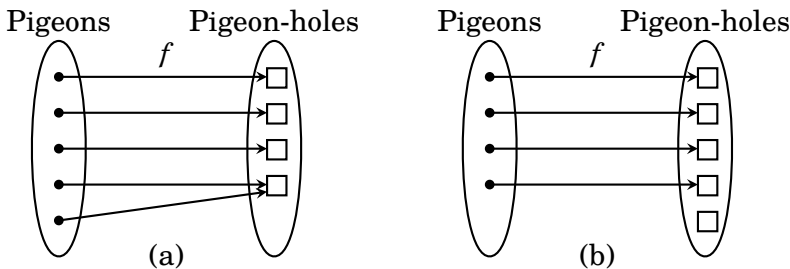


Figure 17.4. The pigeonhole principle

In Figure 17.4(a) there are more pigeons than pigeonholes, and it is obvious that in such a case at least two pigeons have to fly into the same pigeonhole, meaning that f is not injective. In Figure 17.4(b) there are fewer pigeons than pigeonholes, so clearly at least one pigeonhole remains empty, meaning that f is not surjective.

This simple idea is called the *pigeonhole principle*. We encountered it first in Section 4.9, but we restate it here in the language of functions.

Fact 17.1 The Pigeonhole Principle (function version)

Suppose A and B are finite sets and $f : A \rightarrow B$ is any function. Then:

- If $|A| > |B|$, then f is not injective.
- If $|A| < |B|$, then f is not surjective.

Here are two examples of proofs that use the pigeonhole principle.

Example 17.7 Prove the following proposition.

Proposition If A is any set of 10 integers between 1 and 100, then there exist two different subsets $X \subseteq A$ and $Y \subseteq A$ for which the sum of elements in X equals the sum of elements in Y .

To illustrate what this proposition is saying, consider the random set

$$A = \{5, 7, 12, 11, 17, 50, 51, 80, 90, 100\}$$

of 10 integers between 1 and 100. Notice that A has subsets $X = \{5, 80\}$ and $Y = \{7, 11, 17, 50\}$ for which the sum of the elements in X equals the sum of those in Y . If we tried to “mess up” A by changing the 5 to a 6, we get

$$A = \{6, 7, 12, 11, 17, 50, 51, 80, 90, 100\}$$

which has subsets $X = \{7, 12, 17, 50\}$ and $Y = \{6, 80\}$ both of whose elements add up to the same number (86). The proposition asserts that this is always possible, no matter what A is. Here is a proof:

Proof. Suppose $A \subseteq \{1, 2, 3, 4, \dots, 99, 100\}$ and $|A| = 10$, as stated. Notice that if $X \subseteq A$, then X has no more than 10 elements, each between 1 and 100, and therefore the sum of all the elements of X is less than $100 \cdot 10 = 1000$. Consider the function

$$f : \mathcal{P}(A) \rightarrow \{0, 1, 2, 3, 4, \dots, 1000\}$$

where $f(X)$ is the sum of the elements in X . (Examples: $f(\{3, 7, 50\}) = 60$; $f(\{1, 70, 80, 95\}) = 246$.) As $|\mathcal{P}(A)| = 2^{10} = 1024 > 1001 = |\{0, 1, 2, 3, \dots, 1000\}|$, it follows from the pigeonhole principle that f is not injective. Therefore there are two unequal sets $X, Y \in \mathcal{P}(A)$ for which $f(X) = f(Y)$. In other words, there are subsets $X \subseteq A$ and $Y \subseteq A$ for which the sum of elements in X equals the sum of elements in Y . ■

Example 17.8 Prove the following proposition.

Proposition There are at least two Texans with the same number of hairs on their heads.

Proof. We will use two facts. First, the population of Texas is more than twenty million. Second, it is a biological fact that every human head has fewer than one million hairs. Let A be the set of all Texans, and let $B = \{0, 1, 2, 3, 4, \dots, 1000000\}$. Let $f : A \rightarrow B$ be the function for which $f(x)$ equals the number of hairs on the head of x . Since $|A| > |B|$, the pigeonhole principle asserts that f is not injective. Thus there are two Texans x and y for whom $f(x) = f(y)$, meaning that they have the same number of hairs on their heads. ■

Proofs that use the pigeonhole principle tend to be inherently non-constructive, in the sense discussed in Section 12.4. For example, the above proof does not explicitly give us of two Texans with the same number of hairs on their heads; it only shows that two such people exist. If we were to make a constructive proof, we could find examples of two bald Texans. Then they have the same number of head hairs, namely zero.

Exercises for Section 17.3

1. Prove that if six numbers are chosen at random, then at least two of them will have the same remainder when divided by 5.
 2. Prove that if a is a natural number, then there exist two unequal natural numbers k and ℓ for which $a^k - a^\ell$ is divisible by 10.
 3. Prove that if six natural numbers are chosen at random, then the sum or difference of two of them is divisible by 9.
 4. Consider a square whose side-length is one unit. Select any five points from inside this square. Prove that at least two of these points are within $\frac{\sqrt{2}}{2}$ units of each other.
 5. Prove that any set of seven distinct natural numbers contains a pair of numbers whose sum or difference is divisible by 10.
 6. Given a sphere S , a *great circle* of S is the intersection of S with a plane through its center. Every great circle divides S into two parts. A *hemisphere* is the union of the great circle and one of these two parts. Prove that if five points are placed arbitrarily on S , then there is a hemisphere that contains four of them.
 7. Prove or disprove: Any subset $X \subseteq \{1, 2, 3, \dots, 2n\}$ with $|X| > n$ contains two (unequal) elements $a, b \in X$ for which $a \mid b$ or $b \mid a$.
-

17.4 Composition

You should be familiar with the notion of function composition from algebra and calculus. Still, it is worthwhile to revisit it now with our more sophisticated ideas about functions.

Definition 17.5 Suppose $f : A \rightarrow B$ and $g : B \rightarrow C$ are functions with the property that the codomain of f is the domain of g . The **composition** of f with g is another function, denoted as $g \circ f$ and defined as follows: If $x \in A$, then $g \circ f(x) = g(f(x))$. Therefore $g \circ f$ sends elements of A to elements of C , so $g \circ f : A \rightarrow C$.

Figure 17.4 illustrates this. Here $f : A \rightarrow B$, $g : B \rightarrow C$, and $g \circ f : A \rightarrow C$. We have, for example, $g \circ f(0) = g(f(0)) = g(2) = 4$. Be careful with the order of the symbols. Even though g comes first in the symbol $g \circ f$, we work out $g \circ f(x)$ as $g(f(x))$, with f acting on x first, followed by g acting on $f(x)$.

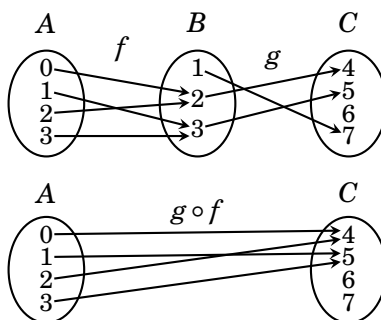




Figure 17.5. Composition of two functions

Notice that the composition $g \circ f$ also makes sense if the range of f is a *subset* of the domain of g . You should take note of this fact, but to keep matters simple we will continue to emphasize situations where the codomain of f equals the domain of g .


Example 17.9 Suppose $A = \{a, b, c\}$, $B = \{0, 1\}$, $C = \{1, 2, 3\}$. Let $f : A \rightarrow B$ be the function $f = \{(a, 0), (b, 1), (c, 0)\}$, and let $g : B \rightarrow C$ be the function $g = \{(0, 3), (1, 1)\}$. Then $g \circ f = \{(a, 3), (b, 1), (c, 3)\}$. 

Example 17.10 Suppose $A = \{a, b, c\}$, $B = \{0, 1\}$, $C = \{1, 2, 3\}$. Let $f : A \rightarrow B$ be the function $f = \{(a, 0), (b, 1), (c, 0)\}$, and let $g : C \rightarrow B$ be the function $g = \{(1, 0), (2, 1), (3, 1)\}$. In this situation the composition $g \circ f$ is not defined because the codomain B of f is not the same set as the domain C of g .

Remember: In order for $g \circ f$ to make sense, the codomain of f must equal the domain of g . (Or at least be a subset of it.) 

Example 17.11 Let $f : \mathbb{R} \rightarrow \mathbb{R}$ be defined as $f(x) = x^2 + x$, and $g : \mathbb{R} \rightarrow \mathbb{R}$ be defined as $g(x) = x + 1$. Then $g \circ f : \mathbb{R} \rightarrow \mathbb{R}$ is the function defined by the formula $g \circ f(x) = g(f(x)) = g(x^2 + x) = x^2 + x + 1$.

Since the domains and codomains of g and f are the same, we can in this case do a composition in the other order. Note that $f \circ g : \mathbb{R} \rightarrow \mathbb{R}$ is the function defined as $f \circ g(x) = f(g(x)) = f(x + 1) = (x + 1)^2 + (x + 1) = x^2 + 3x + 2$.

This example illustrates that even when $g \circ f$ and $f \circ g$ are both defined, they are not necessarily equal. We can express this fact by saying *function composition is not commutative*. 

We close this section by proving several facts about function composition that you are likely to encounter in your future study of mathematics. First, we note that, although it is not commutative, function composition *is* associative.

Theorem 17.1 Composition of functions is associative. That is if $f : A \rightarrow B$, $g : B \rightarrow C$ and $h : C \rightarrow D$, then $(h \circ g) \circ f = h \circ (g \circ f)$.

Proof. Suppose f, g, h are as stated. It follows from Definition 17.5 that both $(h \circ g) \circ f$ and $h \circ (g \circ f)$ are functions from A to D . To show that they are equal, we just need to show

$$\left((h \circ g) \circ f \right)(x) = \left(h \circ (g \circ f) \right)(x)$$

for every $x \in A$. Note that Definition 17.5 yields

$$\left((h \circ g) \circ f \right)(x) = (h \circ g)(f(x)) = h(g(f(x))).$$

Also

$$\left(h \circ (g \circ f) \right)(x) = h(g \circ f(x)) = h(g(f(x))).$$

Thus

$$\left((h \circ g) \circ f \right)(x) = \left(h \circ (g \circ f) \right)(x),$$

as both sides equal $h(g(f(x)))$. ■

Theorem 17.2 Suppose $f : A \rightarrow B$ and $g : B \rightarrow C$. If both f and g are injective, then $g \circ f$ is injective. If both f and g are surjective, then $g \circ f$ is surjective.

Proof. First suppose both f and g are injective. To see that $g \circ f$ is injective, we must show that $g \circ f(x) = g \circ f(y)$ implies $x = y$. Suppose $g \circ f(x) = g \circ f(y)$. This means $g(f(x)) = g(f(y))$. It follows that $f(x) = f(y)$. (For otherwise g wouldn't be injective.) But since $f(x) = f(y)$ and f is injective, it must be that $x = y$. Therefore $g \circ f$ is injective.

Next suppose both f and g are surjective. To see that $g \circ f$ is surjective, we must show that for any element $c \in C$, there is a corresponding element $a \in A$ for which $g \circ f(a) = c$. Thus consider an arbitrary $c \in C$. Because g is surjective, there is an element $b \in B$ for which $g(b) = c$. And because f is surjective, there is an element $a \in A$ for which $f(a) = b$. Therefore $g(f(a)) = g(b) = c$, which means $g \circ f(a) = c$. Thus $g \circ f$ is surjective. ■

Exercises for Section 17.4

1. Suppose $A = \{5, 6, 8\}$, $B = \{0, 1\}$, $C = \{1, 2, 3\}$. Let $f : A \rightarrow B$ be the function $f = \{(5, 1), (6, 0), (8, 1)\}$, and $g : B \rightarrow C$ be $g = \{(0, 1), (1, 1)\}$. Find $g \circ f$.
2. Suppose $A = \{1, 2, 3, 4\}$, $B = \{0, 1, 2\}$, $C = \{1, 2, 3\}$. Let $f : A \rightarrow B$ be

$$f = \{(1, 0), (2, 1), (3, 2), (4, 0)\},$$

and $g : B \rightarrow C$ be $g = \{(0, 1), (1, 1), (2, 3)\}$. Find $g \circ f$.

3. Suppose $A = \{1, 2, 3\}$. Let $f : A \rightarrow A$ be the function $f = \{(1, 2), (2, 2), (3, 1)\}$, and let $g : A \rightarrow A$ be the function $g = \{(1, 3), (2, 1), (3, 2)\}$. Find $g \circ f$ and $f \circ g$.
4. Suppose $A = \{a, b, c\}$. Let $f : A \rightarrow A$ be the function $f = \{(a, c), (b, c), (c, c)\}$, and let $g : A \rightarrow A$ be the function $g = \{(a, a), (b, b), (c, a)\}$. Find $g \circ f$ and $f \circ g$.
5. Consider the functions $f, g : \mathbb{R} \rightarrow \mathbb{R}$ defined as $f(x) = \sqrt[3]{x+1}$ and $g(x) = x^3$. Find the formulas for $g \circ f$ and $f \circ g$.
6. Consider the functions $f, g : \mathbb{R} \rightarrow \mathbb{R}$ defined as $f(x) = \frac{1}{x^2+1}$ and $g(x) = 3x+2$. Find the formulas for $g \circ f$ and $f \circ g$.
7. Consider the functions $f, g : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z}$ defined as $f(m, n) = (mn, m^2)$ and $g(m, n) = (m+1, m+n)$. Find the formulas for $g \circ f$ and $f \circ g$.
8. Consider the functions $f, g : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z}$ defined as $f(m, n) = (3m-4n, 2m+n)$ and $g(m, n) = (5m+n, m)$. Find the formulas for $g \circ f$ and $f \circ g$.
9. Consider the functions $f : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ defined as $f(m, n) = m+n$ and $g : \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z}$ defined as $g(m) = (m, m)$. Find the formulas for $g \circ f$ and $f \circ g$.
10. Consider the function $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ defined by the formula $f(x, y) = (xy, x^3)$. Find a formula for $f \circ f$.

17.5 Inverse Functions

You may recall from calculus that if a function f is injective and surjective, then it has an inverse function f^{-1} that “undoes” the effect of f in the sense that $f^{-1}(f(x)) = x$ for every x in the domain. (For example, if $f(x) = x^3$, then $f^{-1}(x) = \sqrt[3]{x}$.) We now review these ideas. Our approach uses two ingredients, outlined in the following definitions.

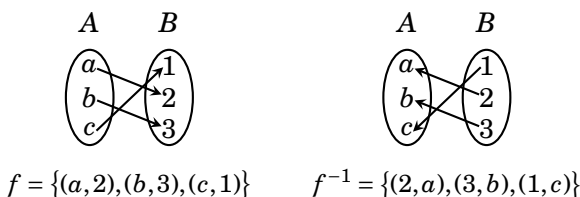
Definition 17.6 Given a set A , the **identity function** on A is the function $i_A : A \rightarrow A$ defined as $i_A(x) = x$ for every $x \in A$.

Example: If $A = \{1, 2, 3\}$, then $i_A = \{(1, 1), (2, 2), (3, 3)\}$. Also $i_{\mathbb{Z}} = \{(n, n) : n \in \mathbb{Z}\}$. The identity function on a set is the function that sends any element of the set to itself.

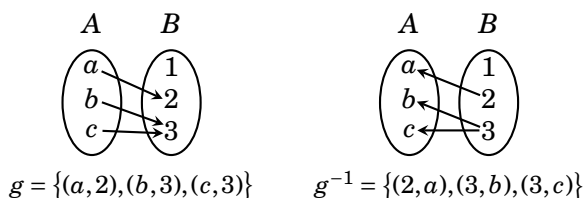
Notice that for any set A , the identity function i_A is bijective: It is injective because $i_A(x) = i_A(y)$ immediately reduces to $x = y$. It is surjective because if we take any element b in the codomain A , then b is also in the domain A , and $i_A(b) = b$.

Definition 17.7 Given a relation R from A to B , the **inverse relation of R** is the relation from B to A defined as $R^{-1} = \{(y, x) : (x, y) \in R\}$. In other words, the inverse of R is the relation R^{-1} obtained by interchanging the elements in every ordered pair in R .

For example, let $A = \{a, b, c\}$ and $B = \{1, 2, 3\}$, and suppose f is the relation $f = \{(a, 2), (b, 3), (c, 1)\}$ from A to B . Then $f^{-1} = \{(2, a), (3, b), (1, c)\}$, and this is a relation from B to A . Notice that f is actually a function from A to B , and f^{-1} is a function from B to A . These two relations are drawn below. Notice the drawing for relation f^{-1} is just the drawing for f with arrows reversed.



For another example, let A and B be the same sets as above, but consider the relation $g = \{(a, 2), (b, 3), (c, 3)\}$ from A to B . Then $g^{-1} = \{(2, a), (3, b), (3, c)\}$ is a relation from B to A . These two relations are sketched below.



This time, even though the relation g is a function, its inverse g^{-1} is not a function because the element 3 occurs twice as a first coordinate of an ordered pair in g^{-1} .

In the above examples, relations f and g are both functions, and f^{-1} is a function and g^{-1} is not. This raises a question: What properties does f have and g lack that makes f^{-1} a function and g^{-1} not a function? The answer is not hard to see. Function g is not injective because $g(b) = g(c) = 3$, and thus $(b, 3)$ and $(c, 3)$ are both in g . This causes a problem with g^{-1} because it means $(3, b)$ and $(3, c)$ are both in g^{-1} , so g^{-1} can't be a function. Thus, in order for g^{-1} to be a function, it would be necessary that g be injective.

But that is not enough. Function g also fails to be surjective because no element of A is sent to the element $1 \in B$. This means g^{-1} contains no ordered pair whose first coordinate is 1, so it can't be a function from B to A . If g^{-1} were to be a function it would be necessary that g be surjective.

The previous two paragraphs suggest that if g is a function, then it must be bijective in order for its inverse relation g^{-1} to be a function. Indeed, this is easy to verify. Conversely, if a function is bijective, then its inverse relation is easily seen to be a function. We summarize this in the following theorem.

Theorem 17.3 Let $f : A \rightarrow B$ be a function. Then f is bijective if and only if the inverse relation f^{-1} is a function from B to A .

Suppose $f : A \rightarrow B$ is bijective, so according to the theorem f^{-1} is a function. Observe that the relation f contains all the pairs $(x, f(x))$ for $x \in A$, so f^{-1} contains all the pairs $(f(x), x)$. But $(f(x), x) \in f^{-1}$ means $f^{-1}(f(x)) = x$. Therefore $f^{-1} \circ f(x) = x$ for every $x \in A$. From this we get $f^{-1} \circ f = i_A$. Similar reasoning produces $f \circ f^{-1} = i_B$. This leads to the following definitions.

Definition 17.8 If $f : A \rightarrow B$ is bijective then its **inverse** is the function $f^{-1} : B \rightarrow A$. The functions f and f^{-1} obey the equations $f^{-1} \circ f = i_A$ and $f \circ f^{-1} = i_B$.

You probably recall from algebra and calculus at least one technique for computing the inverse of a bijective function f : to find f^{-1} , start with the equation $y = f(x)$. Then interchange variables to get $x = f(y)$. Solving this equation for y (if possible) produces $y = f^{-1}(x)$. The next two examples illustrate this.


Example 17.12 The function $f: \mathbb{R} \rightarrow \mathbb{R}$ defined as $f(x) = x^3 + 1$ is bijective. Find its inverse.

We begin by writing $y = x^3 + 1$. Now interchange variables to obtain $x = y^3 + 1$. Solving for y produces $y = \sqrt[3]{x-1}$. Thus

$$f^{-1}(x) = \sqrt[3]{x-1}.$$

(You can check your answer by computing

$$f^{-1}(f(x)) = \sqrt[3]{f(x)-1} = \sqrt[3]{x^3+1-1} = x.$$

Therefore $f^{-1}(f(x)) = x$. Any answer other than x indicates a mistake.) 

We close with one final example. Example 17.5 showed that the function $g: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z}$ defined by the formula $g(m, n) = (m + n, m + 2n)$ is bijective. Let's find its inverse. The approach outlined above should work, but we need to be careful to keep track of coordinates in $\mathbb{Z} \times \mathbb{Z}$. We begin by writing $(x, y) = g(m, n)$, then interchanging the variables (x, y) and (m, n) to get $(m, n) = g(x, y)$. This gives

$$(m, n) = (x + y, x + 2y),$$

from which we get the following system of equations:

$$\begin{aligned} x + y &= m \\ x + 2y &= n. \end{aligned}$$

Solving this system using techniques from algebra with which you are familiar, we get

$$\begin{aligned} x &= 2m - n \\ y &= n - m. \end{aligned}$$

Then $(x, y) = (2m - n, n - m)$, so $\boxed{g^{-1}(m, n) = (2m - n, n - m)}$.

We can check our work by confirming that $g^{-1}(g(m, n)) = (m, n)$. Doing the math,

$$\begin{aligned} g^{-1}(g(m, n)) &= g^{-1}(m + n, m + 2n) \\ &= (2(m + n) - (m + 2n), (m + 2n) - (m + n)) \\ &= (m, n). \end{aligned}$$

Exercises for Section 17.5

1. Check that the function $f : \mathbb{Z} \rightarrow \mathbb{Z}$ defined by $f(n) = 6 - n$ is bijective. Then compute f^{-1} .
2. In Exercise 9 of Section 17.2 you proved that $f : \mathbb{R} - \{2\} \rightarrow \mathbb{R} - \{5\}$ defined by $f(x) = \frac{5x + 1}{x - 2}$ is bijective. Now find its inverse.
3. Let $B = \{2^n : n \in \mathbb{Z}\} = \{\dots, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, \dots\}$. Show that the function $f : \mathbb{Z} \rightarrow B$ defined as $f(n) = 2^n$ is bijective. Then find f^{-1} .
4. The function $f : \mathbb{R} \rightarrow (0, \infty)$ defined as $f(x) = e^{x^3 + 1}$ is bijective. Find its inverse.
5. The function $f : \mathbb{R} \rightarrow \mathbb{R}$ defined as $f(x) = \pi x - e$ is bijective. Find its inverse.
6. The function $f : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z}$ defined by the formula $f(m, n) = (5m + 4n, 4m + 3n)$ is bijective. Find its inverse.
7. Show that the function $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ defined by the formula $f(x, y) = ((x^2 + 1)y, x^3)$ is bijective. Then find its inverse.
8. Is the function $\theta : \mathcal{P}(\mathbb{Z}) \rightarrow \mathcal{P}(\mathbb{Z})$ defined as $\theta(X) = \overline{X}$ bijective? If so, what is its inverse?
9. Consider the function $f : \mathbb{R} \times \mathbb{N} \rightarrow \mathbb{N} \times \mathbb{R}$ defined as $f(x, y) = (y, 3xy)$. Check that this is bijective; find its inverse.
10. Consider $f : \mathbb{N} \rightarrow \mathbb{Z}$ defined as $f(n) = \frac{(-1)^n(2n - 1) + 1}{4}$. This function is bijective by Exercise 18 in Section 17.2. Find its inverse.

17.6 Solutions for Chapter 17

Section 17.1 Exercises

- Suppose $A = \{0, 1, 2, 3, 4\}$, $B = \{2, 3, 4, 5\}$ and $f = \{(0, 3), (1, 3), (2, 4), (3, 2), (4, 2)\}$. State the domain and range of f . Find $f(2)$ and $f(1)$.
Domain is A ; Range is $\{2, 3, 4\}$; $f(2) = 4$; $f(1) = 3$.
- There are four different functions $f : \{a, b\} \rightarrow \{0, 1\}$. List them all. Diagrams will suffice.
 $f_1 = \{(a, 0), (b, 0)\}$ $f_2 = \{(a, 1), (b, 0)\}$, $f_3 = \{(a, 0), (b, 1)\}$ $f_4 = \{(a, 1), (b, 1)\}$
- Give an example of a relation from $\{a, b, c, d\}$ to $\{d, e\}$ that is not a function. One example is $\{(a, d), (a, e), (b, d), (c, d), (d, d)\}$.
- Consider the set $f = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : 3x + y = 4\}$. Is this a function from \mathbb{Z} to \mathbb{Z} ? Explain.
Yes, since $3x + y = 4$ if and only if $y = 4 - 3x$, this is the function $f : \mathbb{Z} \rightarrow \mathbb{Z}$ defined as $f(x) = 4 - 3x$.
- Consider the set $f = \{(x^2, x) : x \in \mathbb{R}\}$. Is this a function from \mathbb{R} to \mathbb{R} ? Explain.
No. This is not a function. Observe that f contains the ordered pairs $(4, 2)$ and $(4, -2)$. Thus the real number 4 occurs as the first coordinate of more than one element of f .
- Is the set $\theta = \{(X, |X|) : X \subseteq \mathbb{Z}_5\}$ a function? If so, what is its domain and range?
Yes, this is a function. The domain is $\mathcal{P}(\mathbb{Z}_5)$. The range is $\{0, 1, 2, 3, 4, 5\}$.

Section 17.2 Exercises

- Let $A = \{1, 2, 3, 4\}$ and $B = \{a, b, c\}$. Give an example of a function $f : A \rightarrow B$ that is neither injective nor surjective.
Consider $f = \{(1, a), (2, a), (3, a), (4, a)\}$.
Then f is not injective because $f(1) = f(2)$.
Also f is not surjective because it sends no element of A to the element $c \in B$.
- Consider the cosine function $\cos : \mathbb{R} \rightarrow \mathbb{R}$. Decide whether this function is injective and whether it is surjective. What if it had been defined as $\cos : \mathbb{R} \rightarrow [-1, 1]$?
The function $\cos : \mathbb{R} \rightarrow \mathbb{R}$ is **not injective** because, for example, $\cos(0) = \cos(2\pi)$. It is **not surjective** because if $b = 5 \in \mathbb{R}$ (for example), there is no real number for which $\cos(x) = b$. The function $\cos : \mathbb{R} \rightarrow [-1, 1]$ is **surjective**, but not injective.
- A function $f : \mathbb{Z} \rightarrow \mathbb{Z}$ is defined as $f(n) = 2n + 1$. Verify whether this function is injective and whether it is surjective.
This function is injective. To see this, suppose $m, n \in \mathbb{Z}$ and $f(m) = f(n)$.
This means $2m + 1 = 2n + 1$, from which we get $2m = 2n$, and then $m = n$.
Thus f is injective.
This function is not surjective. To see this notice that $f(n)$ is odd for all $n \in \mathbb{Z}$.
So given the (even) number 2 in the codomain \mathbb{Z} , there is no n with $f(n) = 2$.
- A function $f : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ is defined as $f((m, n)) = 2n - 4m$. Verify whether this function is injective and whether it is surjective.

This is **not injective** because $(0, 2) \neq (-1, 0)$, yet $f((0, 2)) = f((-1, 0)) = 4$. This is **not surjective** because $f((m, n)) = 2n - 4m = 2(n - 2m)$ is always even. If $b \in \mathbb{Z}$ is odd, then $f((m, n)) \neq b$, for all $(m, n) \in \mathbb{Z} \times \mathbb{Z}$.

9. Prove that the function $f : \mathbb{R} - \{2\} \rightarrow \mathbb{R} - \{5\}$ defined by $f(x) = \frac{5x+1}{x-2}$ is bijective.

Proof. First, let's check that f is injective. Suppose $f(x) = f(y)$. Then

$$\begin{aligned} \frac{5x+1}{x-2} &= \frac{5y+1}{y-2} \\ (5x+1)(y-2) &= (5y+1)(x-2) \\ 5xy - 10x + y - 2 &= 5yx - 10y + x - 2 \\ -10x + y &= -10y + x \\ 11y &= 11x \\ y &= x. \end{aligned}$$

Since $f(x) = f(y)$ implies $x = y$, it follows that f is injective.

Next, let's check that f is surjective. For this, take an arbitrary element $b \in \mathbb{R} - \{5\}$. We want to see if there is an $x \in \mathbb{R} - \{2\}$ for which $f(x) = b$, or $\frac{5x+1}{x-2} = b$. Solving this for x , we get:

$$\begin{aligned} 5x+1 &= b(x-2) \\ 5x+1 &= bx-2b \\ 5x-xb &= -2b-1 \\ x(5-b) &= -2b-1. \end{aligned}$$

Since we have assumed $b \in \mathbb{R} - \{5\}$, the term $(5-b)$ is not zero, and we can divide with impunity to get $x = \frac{-2b-1}{5-b}$. This is an x for which $f(x) = b$, so f is surjective. Since f is both injective and surjective, it is bijective. ■

11. Consider the function $\theta : \{0, 1\} \times \mathbb{N} \rightarrow \mathbb{Z}$ defined as $\theta(a, b) = (-1)^a b$. Is θ injective? Is it surjective? Explain.

First we show that θ is injective. Suppose $\theta(a, b) = \theta(c, d)$. Then $(-1)^a b = (-1)^c d$. As b and d are both in \mathbb{N} , they are both positive. Then because $(-1)^a b = (-1)^c d$, it follows that $(-1)^a$ and $(-1)^c$ have the same sign. Since each of $(-1)^a$ and $(-1)^c$ equals ± 1 , we have $(-1)^a = (-1)^c$, so then $(-1)^a b = (-1)^c d$ implies $b = d$. But also $(-1)^a = (-1)^c$ means a and c have the same parity, and because $a, c \in \{0, 1\}$, it follows $a = c$. Thus $(a, b) = (c, d)$, so θ is injective.

Next note that θ is **not surjective** because $\theta(a, b) = (-1)^a b$ is either positive or negative, but never zero. Therefore there exist no element $(a, b) \in \{0, 1\} \times \mathbb{N}$ for which $\theta(a, b) = 0 \in \mathbb{Z}$.

13. Consider the function $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ defined by the formula $f(x, y) = (xy, x^3)$. Is f injective? Is it surjective?

Notice that $f(0,1) = (0,0)$ and $f(0,0) = (0,0)$, so f is **not injective**. To show that f is also **not surjective**, we will show that it's impossible to find an ordered pair (x,y) with $f(x,y) = (1,0)$. If there were such a pair, then $f(x,y) = (xy, x^3) = (1,0)$, which yields $xy = 1$ and $x^3 = 0$. From $x^3 = 0$ we get $x = 0$, so $xy = 0$, a contradiction.

15. This question concerns functions $f : \{A,B,C,D,E,F,G\} \rightarrow \{1,2,3,4,5,6,7\}$. How many such functions are there? How many of these functions are injective? How many are surjective? How many are bijective?

Function f can be described as a list $(f(A), f(B), f(C), f(D), f(E), f(F), f(G))$, where there are seven choices for each entry. By the multiplication principle, the total number of functions f is $7^7 = 823543$.

If f is injective, then this list can't have any repetition, so there are $7! = 5040$ injective functions. Since any injective function sends the seven elements of the domain to seven distinct elements of the codomain, all of the injective functions are surjective, and vice versa. Thus there are 5040 surjective functions and 5040 bijective functions.

17. This question concerns functions $f : \{A,B,C,D,E,F,G\} \rightarrow \{1,2\}$. How many such functions are there? How many of these functions are injective? How many are surjective? How many are bijective?

Function f can be described as a list $(f(A), f(B), f(C), f(D), f(E), f(F), f(G))$, where there are two choices for each entry. Therefore the total number of functions is $2^7 = 128$. It is impossible for any function to send all seven elements of $\{A,B,C,D,E,F,G\}$ to seven distinct elements of $\{1,2\}$, so none of these 128 functions is injective, hence none are bijective.

How many are surjective? Only two of the 128 functions are not surjective, and they are the "constant" functions $\{(A,1), (B,1), (C,1), (D,1), (E,1), (F,1), (G,1)\}$ and $\{(A,2), (B,2), (C,2), (D,2), (E,2), (F,2), (G,2)\}$. So there are 126 surjective functions.

Section 17.3 Exercises

1. If 6 integers are chosen at random, at least two will have the same remainder when divided by 5.

Proof. Write \mathbb{Z} as follows: $\mathbb{Z} = \bigcup_{j=0}^4 \{5k + j : k \in \mathbb{Z}\}$. This is a partition of \mathbb{Z} into 5 sets. If six integers are picked at random, by the pigeonhole principle, at least two will be in the same set. However, each set corresponds to the remainder of a number after being divided by 5 (for example, $\{5k + 1 : k \in \mathbb{Z}\}$ are all those integers that leave a remainder of 1 after being divided by 5). ■

3. Given any six positive integers, there are two for which their sum or difference is divisible by 9.

Proof. If for two of the integers n, m we had $n \equiv m \pmod{9}$, then $n - m \equiv 0 \pmod{9}$, and we would be done. Thus assume this is not the case. Observe that the only two element subsets of positive integers that sum to 9 are $\{1,8\}, \{2,7\}, \{3,6\}$, and $\{4,5\}$. However, since at least five of the six integers must have distinct remainders

from 1, 2, ..., 8 it follows from the pigeonhole principle that two integers n, m are in the same set. Hence $n + m \equiv 0 \pmod{9}$ as desired. ■

5. Prove that any set of 7 distinct natural numbers contains a pair of numbers whose sum or difference is divisible by 10.

Proof. Let $S = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7\}$ be any set of 7 natural numbers. Let's say that $a_1 < a_2 < a_3 < \dots < a_7$. Consider the set

$$A = \{a_1 - a_2, a_1 - a_3, a_1 - a_4, a_1 - a_5, a_1 - a_6, a_1 - a_7, \\ a_1 + a_2, a_1 + a_3, a_1 + a_4, a_1 + a_5, a_1 + a_6, a_1 + a_7\}$$

Thus $|A| = 12$. Now let $B = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, so $|B| = 10$. Let $f : A \rightarrow B$ be the function for which $f(n)$ equals the last digit of n . (That is $f(97) = 7$, $f(12) = 2$, $f(230) = 0$, etc.) Then, since $|A| > |B|$, the pigeonhole principle guarantees that f is not injective. Thus A contains elements $a_1 \pm a_i$ and $a_1 \pm a_j$ for which $f(a_1 \pm a_i) = f(a_1 \pm a_j)$. This means the last digit of $a_1 \pm a_i$ is the same as the last digit of $a_1 \pm a_j$. Thus the last digit of the difference $(a_1 \pm a_i) - (a_1 \pm a_j) = \pm a_i \pm a_j$ is 0. Hence $\pm a_i \pm a_j$ is a sum or difference of elements of S that is divisible by 10. ■

Section 17.4 Exercises

1. Suppose $A = \{5, 6, 8\}$, $B = \{0, 1\}$, $C = \{1, 2, 3\}$. Let $f : A \rightarrow B$ be the function $f = \{(5, 1), (6, 0), (8, 1)\}$, and $g : B \rightarrow C$ be $g = \{(0, 1), (1, 1)\}$. Find $g \circ f$.
 $g \circ f = \{(5, 1), (6, 1), (8, 1)\}$
3. Suppose $A = \{1, 2, 3\}$. Let $f : A \rightarrow A$ be the function $f = \{(1, 2), (2, 2), (3, 1)\}$, and let $g : A \rightarrow A$ be the function $g = \{(1, 3), (2, 1), (3, 2)\}$. Find $g \circ f$ and $f \circ g$.
 $g \circ f = \{(1, 1), (2, 1), (3, 3)\}$; $f \circ g = \{(1, 1), (2, 2), (3, 2)\}$.
5. Consider the functions $f, g : \mathbb{R} \rightarrow \mathbb{R}$ defined as $f(x) = \sqrt[3]{x+1}$ and $g(x) = x^3$. Find the formulas for $g \circ f$ and $f \circ g$.
 $g \circ f(x) = x + 1$; $f \circ g(x) = \sqrt[3]{x^3 + 1}$
7. Consider the functions $f, g : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z}$ defined as $f(m, n) = (mn, m^2)$ and $g(m, n) = (m + 1, m + n)$. Find the formulas for $g \circ f$ and $f \circ g$.
 Note $g \circ f(m, n) = g(f(m, n)) = g(mn, m^2) = (mn + 1, mn + m^2)$.
 Thus $g \circ f(m, n) = (mn + 1, mn + m^2)$.
 Note $f \circ g(m, n) = f(g(m, n)) = f(m + 1, m + n) = ((m + 1)(m + n), (m + 1)^2)$.
 Thus $f \circ g(m, n) = (m^2 + mn + m + n, m^2 + 2m + 1)$.
9. Consider the functions $f : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ defined as $f(m, n) = m + n$ and $g : \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z}$ defined as $g(m) = (m, m)$. Find the formulas for $g \circ f$ and $f \circ g$.
 $g \circ f(m, n) = (m + n, m + n)$
 $f \circ g(m) = 2m$

Section 17.5 Exercises

1. Check that the function $f : \mathbb{Z} \rightarrow \mathbb{Z}$ defined by $f(n) = 6 - n$ is bijective. Then compute f^{-1} .

It is injective as follows. Suppose $f(m) = f(n)$. Then $6 - m = 6 - n$, which reduces to $m = n$.

It is surjective as follows. If $b \in \mathbb{Z}$, then $f(6 - b) = 6 - (6 - b) = b$.

Inverse: $f^{-1}(n) = 6 - n$.

3. Let $B = \{2^n : n \in \mathbb{Z}\} = \{\dots, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, \dots\}$. Show that the function $f : \mathbb{Z} \rightarrow B$ defined as $f(n) = 2^n$ is bijective. Then find f^{-1} .

It is injective as follows. Suppose $f(m) = f(n)$, which means $2^m = 2^n$. Taking \log_2 of both sides gives $\log_2(2^m) = \log_2(2^n)$, which simplifies to $m = n$.

The function f is surjective as follows. Suppose $b \in B$. By definition of B this means $b = 2^n$ for some $n \in \mathbb{Z}$. Then $f(n) = 2^n = b$.

Inverse: $f^{-1}(n) = \log_2(n)$.

5. The function $f : \mathbb{R} \rightarrow \mathbb{R}$ defined as $f(x) = \pi x - e$ is bijective. Find its inverse.

Inverse: $f^{-1}(x) = \frac{x + e}{\pi}$.

7. Show that the function $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ defined by the formula $f((x, y)) = ((x^2 + 1)y, x^3)$ is bijective. Then find its inverse.

First we prove the function is injective. Assume $f(x_1, y_1) = f(x_2, y_2)$. Then $(x_1^2 + 1)y_1 = (x_2^2 + 1)y_2$ and $x_1^3 = x_2^3$. Since the real-valued function $f(x) = x^3$ is one-to-one, it follows that $x_1 = x_2$. Since $x_1 = x_2$, and $x_1^2 + 1 > 0$ we may divide both sides of $(x_1^2 + 1)y_1 = (x_1^2 + 1)y_2$ by $(x_1^2 + 1)$ to get $y_1 = y_2$. Hence $(x_1, y_1) = (x_2, y_2)$.

Now we prove the function is surjective. Let $(a, b) \in \mathbb{R}^2$. Set $x = b^{1/3}$ and $y = a/(b^{2/3} + 1)$. Then $f(x, y) = ((b^{2/3} + 1)\frac{a}{b^{2/3} + 1}, (b^{1/3})^3) = (a, b)$. It now follows that f is bijective.

Finally, we compute the inverse. Write $f(x, y) = (u, v)$. Interchange variables to get $(x, y) = f(u, v) = ((u^2 + 1)v, u^3)$. Thus $x = (u^2 + 1)v$ and $y = u^3$. Hence $u = y^{1/3}$ and $v = \frac{x}{y^{2/3} + 1}$. Therefore $f^{-1}(x, y) = (u, v) = \left(y^{1/3}, \frac{x}{y^{2/3} + 1}\right)$.

9. Consider the function $f : \mathbb{R} \times \mathbb{N} \rightarrow \mathbb{N} \times \mathbb{R}$ defined as $f(x, y) = (y, 3xy)$. Check that this is bijective; find its inverse.

To see that this is injective, suppose $f(a, b) = f(c, d)$. This means $(b, 3ab) = (d, 3cd)$. Since the first coordinates must be equal, we get $b = d$. As the second coordinates are equal, we get $3ab = 3dc$, which becomes $3ab = 3bc$. Note that, from the definition of f , $b \in \mathbb{N}$, so $b \neq 0$. Thus we can divide both sides of $3ab = 3bc$ by the non-zero quantity $3b$ to get $a = c$. Now we have $a = c$ and $b = d$, so $(a, b) = (c, d)$. It follows that f is injective.

Next we check that f is surjective. Given any (b, c) in the codomain $\mathbb{N} \times \mathbb{R}$, notice that $(\frac{c}{3b}, b)$ belongs to the domain $\mathbb{R} \times \mathbb{N}$, and $f(\frac{c}{3b}, b) = (b, c)$. Thus f is surjective. As it is both injective and surjective, it is bijective; thus the inverse exists.

To find the inverse, recall that we obtained $f(\frac{c}{3b}, b) = (b, c)$. Then $f^{-1}f(\frac{c}{3b}, b) = f^{-1}(b, c)$, which reduces to $(\frac{c}{3b}, b) = f^{-1}(b, c)$. Replacing b and c with x and y , respectively, we get $f^{-1}(x, y) = (\frac{y}{3x}, x)$.

Cardinality of Sets

This chapter is all about cardinality of sets. At first this looks like a very simple concept. To find the cardinality of a set, just count its elements. If $A = \{a, b, c, d\}$, then $|A| = 4$; if $B = \{n \in \mathbb{Z} : -5 \leq n \leq 5\}$, then $|B| = 11$. In this case $|A| < |B|$. What could be simpler than that?

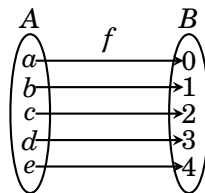
Actually, the idea of cardinality becomes quite subtle when the sets are infinite. The main point of this chapter is to explain how there are numerous different kinds of infinity, and some infinities are bigger than others. Two sets A and B can both have infinite cardinality, yet $|A| < |B|$.

18.1 Sets with Equal Cardinalities

We begin with a discussion of what it means for two sets to have the same cardinality. Up until this point we've said $|A| = |B|$ if A and B have the same number of elements: Count the elements of A , then count the elements of B . If you get the same number, then $|A| = |B|$.

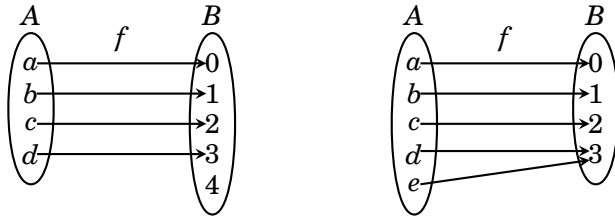
Although this is a fine strategy if the sets are finite (and not too big!), it doesn't apply to infinite sets because we'd never be done counting their elements. We need a new approach that applies to both finite and infinite sets. Here it is:

Definition 18.1 Two sets A and B have the **same cardinality**, written $|A| = |B|$, if there is a bijective function $f : A \rightarrow B$. If no such function exists, then the sets have **unequal cardinalities**, that is, $|A| \neq |B|$.



The above picture illustrates our definition. There is a bijective function $f : A \rightarrow B$, so $|A| = |B|$. The function f matches up A with B . Think of f as describing how to overlay A onto B so that they fit together perfectly.

On the other hand, if A and B are as indicated in either of the following figures, then there can be no bijection $f : A \rightarrow B$. (The best we can do is a function that is either injective or surjective, but not both). Therefore the definition says $|A| \neq |B|$ in these cases.



Example 18.1 The sets $A = \{n \in \mathbb{Z} : 0 \leq n \leq 5\}$ and $B = \{n \in \mathbb{Z} : -5 \leq n \leq 0\}$ have the same cardinality because there is a bijective function $f : A \rightarrow B$ given by the rule $f(n) = -n$.

Several comments are in order. First, if $|A| = |B|$, there can be *lots* of bijective functions from A to B . We only need to find one of them in order to conclude $|A| = |B|$. Second, as bijective functions play such a big role here, we use the word **bijection** to mean *bijective function*. Thus the function $f(n) = -n$ from Example 18.1 is a bijection. Also, an injective function is called an **injection** and a surjective function is called a **surjection**.

We emphasize and reiterate that Definition 18.1 applies to finite as well as infinite sets. If A and B are infinite, then $|A| = |B|$ provided there exists a bijection $f : A \rightarrow B$. If no such bijection exists, then $|A| \neq |B|$.

Example 18.2 This example shows that $|\mathbb{N}| = |\mathbb{Z}|$. To see why this is true, notice that the following table describes a bijection $f : \mathbb{N} \rightarrow \mathbb{Z}$.

| | | | | | | | | | | | | | | | | |
|--------|---|---|----|---|----|---|----|---|----|----|----|----|----|----|----|-----|
| n | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | ... |
| $f(n)$ | 0 | 1 | -1 | 2 | -2 | 3 | -3 | 4 | -4 | 5 | -5 | 6 | -6 | 7 | -7 | ... |

Notice that f is described in such a way that it is both injective and surjective. Every integer appears exactly once on the infinitely long second row. Thus, according to the table, given any $b \in \mathbb{Z}$ there is some natural number n with $f(n) = b$, so f is surjective. It is injective because the way the table is constructed forces $f(m) \neq f(n)$ whenever $m \neq n$. Because of this bijection $f : \mathbb{N} \rightarrow \mathbb{Z}$, we must conclude from Definition 18.1 that $|\mathbb{N}| = |\mathbb{Z}|$.

Example 18.2 may seem slightly unsettling. On one hand it makes sense that $|\mathbb{N}| = |\mathbb{Z}|$ because \mathbb{N} and \mathbb{Z} are both infinite, so their cardinalities are both “infinity.” On the other hand, \mathbb{Z} may seem twice as large as \mathbb{N} because

\mathbb{Z} has all the negative integers as well as the positive ones. Definition 18.1 settles the issue. Because the bijection $f : \mathbb{N} \rightarrow \mathbb{Z}$ matches up \mathbb{N} with \mathbb{Z} , it follows that $|\mathbb{N}| = |\mathbb{Z}|$. We summarize this with a theorem.

Theorem 18.1 There exists a bijection $f : \mathbb{N} \rightarrow \mathbb{Z}$. Therefore $|\mathbb{N}| = |\mathbb{Z}|$.

The fact that \mathbb{N} and \mathbb{Z} have the same cardinality might prompt us compare the cardinalities of other infinite sets. How, for example, do \mathbb{N} and \mathbb{R} compare? Let's turn our attention to this.

In fact, $|\mathbb{N}| \neq |\mathbb{R}|$. This was first recognized by Georg Cantor (1845–1918), who devised an ingenious argument to show that there are no surjective functions $f : \mathbb{N} \rightarrow \mathbb{R}$. (This in turn implies that there can be no bijections $f : \mathbb{N} \rightarrow \mathbb{R}$, so $|\mathbb{N}| \neq |\mathbb{R}|$ by Definition 18.1.)

We now describe Cantor's argument for why there are no surjections $f : \mathbb{N} \rightarrow \mathbb{R}$. We will reason informally, rather than writing out an exact proof. Take any arbitrary function $f : \mathbb{N} \rightarrow \mathbb{R}$. Here's why f can't be surjective:

Imagine making a table for f , where values of n in \mathbb{N} are in the left-hand column and the corresponding values $f(n)$ are on the right. The first few entries might look something as follows. In this table, the real numbers $f(n)$ are written with all their decimal places trailing off to the right. Thus, even though $f(1)$ happens to be the real number 0.4, we write it as 0.40000000...., etc.

| n | $f(n)$ |
|-----|-----------------------|
| 1 | 0.4000000000000000... |
| 2 | 8.50060708666900... |
| 3 | 7.50500940044101... |
| 4 | 5.50704008048050... |
| 5 | 6.90026000000506... |
| 6 | 6.82809582050020... |
| 7 | 6.50505550655808... |
| 8 | 8.72080640000448... |
| 9 | 0.55000088880077... |
| 10 | 0.50020722078051... |
| 11 | 2.90000880000900... |
| 12 | 6.50280008009671... |
| 13 | 8.89008024008050... |
| 14 | 8.50008742080226... |
| ⋮ | ⋮ |

There is a diagonal shaded band in the table. For each $n \in \mathbb{N}$, this band covers the n^{th} decimal place of $f(n)$:

- The 1st decimal place of $f(1)$ is the 1st entry on the diagonal.
- The 2nd decimal place of $f(2)$ is the 2nd entry on the diagonal.
- The 3rd decimal place of $f(3)$ is the 3rd entry on the diagonal.
- The 4th decimal place of $f(4)$ is the 4th entry on the diagonal, etc.

The diagonal helps us construct a number $b \in \mathbb{R}$ that is unequal to any $f(n)$. Just let the n th decimal place of b differ from the n th entry of the diagonal. Then the n th decimal place of b differs from the n th decimal place of $f(n)$. In order to be definite, define b to be the positive number less than 1 whose n th decimal place is 0 if the n th decimal place of $f(n)$ is not 0, and whose n th decimal place is 1 if the n th decimal place of $f(n)$ equals 0. Thus, for the function f illustrated in the above table, we have

$$b = 0.01010001001000\dots$$

and b has been defined so that, for any $n \in \mathbb{N}$, its n th decimal place is unequal to the n th decimal place of $f(n)$. Therefore $f(n) \neq b$ for every natural number n , meaning f is not surjective.

Since this argument applies to *any* function $f : \mathbb{N} \rightarrow \mathbb{R}$ (not just the one in the above example) we conclude that there exist no bijections $f : \mathbb{N} \rightarrow \mathbb{R}$, so $|\mathbb{N}| \neq |\mathbb{R}|$ by Definition 18.1. We summarize this as a theorem.

Theorem 18.2 There exists no bijection $f : \mathbb{N} \rightarrow \mathbb{R}$. Therefore $|\mathbb{N}| \neq |\mathbb{R}|$.

This is our first indication of how there are different kinds of infinities. Both \mathbb{N} and \mathbb{R} are infinite sets, yet $|\mathbb{N}| \neq |\mathbb{R}|$. We will continue to develop this theme throughout this chapter. The next example shows that the intervals $(0, \infty)$ and $(0, 1)$ on \mathbb{R} have the same cardinality.

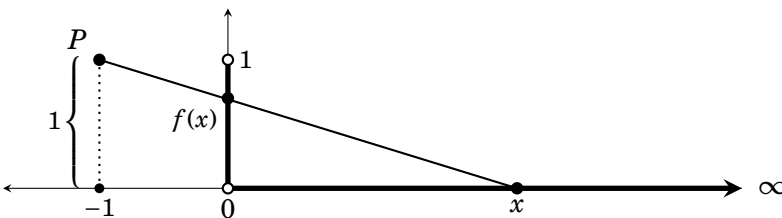


Figure 18.1. A bijection $f : (0, \infty) \rightarrow (0, 1)$

Example 18.3 Show that $|(0, \infty)| = |(0, 1)|$.


To accomplish this, we need to show that there is a bijection $f : (0, \infty) \rightarrow (0, 1)$. We describe this function geometrically. Consider the interval $(0, \infty)$ as the positive x -axis of \mathbb{R}^2 . Let the interval $(0, 1)$ be on the y -axis as illustrated in Figure 18.1, so that $(0, \infty)$ and $(0, 1)$ are perpendicular to each other.

The figure also shows a point $P = (-1, 1)$. Define $f(x)$ to be the point on $(0, 1)$ where the line from P to $x \in (0, \infty)$ intersects the y -axis. By similar triangles, we have

$$\frac{1}{x+1} = \frac{f(x)}{x},$$

and therefore


$$f(x) = \frac{x}{x+1}.$$

If it is not clear from the figure that $f : (0, \infty) \rightarrow (0, 1)$ is bijective, you can verify it using the techniques from Section 17.2. (Exercise 16, below.) 

It is important to note that equality of cardinalities is an equivalence relation on sets: it is reflexive, symmetric and transitive. Let us confirm this. Given a set A , the identity function $A \rightarrow A$ is a bijection, so $|A| = |A|$. (This is the reflexive property.) For the symmetric property, if $|A| = |B|$, then there is a bijection $f : A \rightarrow B$, and its inverse is a bijection $f^{-1} : B \rightarrow A$, so $|B| = |A|$. For transitivity, suppose $|A| = |B|$ and $|B| = |C|$. Then there are bijections $f : A \rightarrow B$ and $g : B \rightarrow C$. The composition $g \circ f : A \rightarrow C$ is a bijection (Theorem 17.2), so $|A| = |C|$.

The transitive property can be useful. If, in trying to show two sets A and C have the same cardinality, we can produce a third set B for which $|A| = |B|$ and $|B| = |C|$, then transitivity assures us that indeed $|A| = |C|$. The next example uses this idea.

Example 18.4 Show that $|\mathbb{R}| = |(0, 1)|$.

Because of the bijection $g : \mathbb{R} \rightarrow (0, \infty)$ where $g(x) = 2^x$, we have $|\mathbb{R}| = |(0, \infty)|$. Also, Example 18.3 shows that $|(0, \infty)| = |(0, 1)|$. Therefore $|\mathbb{R}| = |(0, 1)|$. 

So far in this chapter we have declared that two sets have “the same cardinality” if there is a bijection between them. They have “different cardinalities” if there exists no bijection between them. Using this idea, we showed that $|\mathbb{Z}| = |\mathbb{N}| \neq |\mathbb{R}| = |(0, \infty)| = |(0, 1)|$. So, we have a means of determining when two sets have the same or different cardinalities. But we have neatly avoided saying exactly what cardinality *is*. For example, we can say that $|\mathbb{Z}| = |\mathbb{N}|$, but what exactly *is* $|\mathbb{Z}|$, or $|\mathbb{N}|$? What exactly *are* these things that are equal? Certainly not numbers, for they are too big. And

saying they are “infinity” is not accurate, because we now know that there are different types of infinity. So just what kind of mathematical entity is $|\mathbb{Z}|$? In general, given a set X , exactly what *is* its cardinality $|X|$?

This is a lot like asking what a number is. A number, say 5, is an abstraction, not a physical thing. Early in life we instinctively grouped together certain sets of things (five apples, five oranges, etc.) and conceived of 5 as the thing common to all such sets. In a very real sense, the number 5 is an abstraction of the fact that any two of these sets can be matched up via a bijection. That is, it can be identified with a certain equivalence class of sets under the “*has the same cardinality as*” relation. (Recall that this is an equivalence relation.) This is easy to grasp because our sense of numeric quantity is so innate. But in exactly the same way we can say that the cardinality of a set X is what is common to all sets that can be matched to X via a bijection. This may be harder to grasp, but it is really no different from the idea of the magnitude of a (finite) number.

In fact, we could be concrete and define $|X|$ to be the equivalence class of all sets whose cardinality is the same as that of X . This has the advantage of giving an explicit meaning to $|X|$. But there is no harm in taking the intuitive approach and just interpreting the cardinality $|X|$ of a set X to be a measure the “size” of X . The point of this section is that we have a means of deciding whether two sets have the same size or different sizes.

Exercises for Section 18.1

- A.** Show that the two given sets have equal cardinality by describing a bijection from one to the other. Describe your bijection with a formula (not as a table).
1. \mathbb{R} and $(0, \infty)$
 2. \mathbb{R} and $(\sqrt{2}, \infty)$
 3. \mathbb{R} and $(0, 1)$
 4. The set of even integers and the set of odd integers
 5. $A = \{3k : k \in \mathbb{Z}\}$ and $B = \{7k : k \in \mathbb{Z}\}$
 6. \mathbb{N} and $S = \{\frac{\sqrt{2}}{n} : n \in \mathbb{N}\}$
 7. \mathbb{Z} and $S = \{\dots, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, 16, \dots\}$
 8. \mathbb{Z} and $S = \{x \in \mathbb{R} : \sin x = 1\}$
 9. $\{0, 1\} \times \mathbb{N}$ and \mathbb{N}
 10. $\{0, 1\} \times \mathbb{N}$ and \mathbb{Z}
 11. $[0, 1]$ and $(0, 1)$
 12. \mathbb{N} and \mathbb{Z} (Suggestion: use Exercise 18 of Section 17.2.)
 13. $\mathcal{P}(\mathbb{N})$ and $\mathcal{P}(\mathbb{Z})$ (Suggestion: use Exercise 12, above.)
 14. $\mathbb{N} \times \mathbb{N}$ and $\{(n, m) \in \mathbb{N} \times \mathbb{N} : n \leq m\}$
- B.** Answer the following questions concerning bijections from this section.
15. Find a formula for the bijection f in Example 18.2 (page 416).
 16. Verify that the function f in Example 18.3 is a bijection.

18.2 Countable and Uncountable Sets

Let's summarize the main points from the previous section.

1. $|A| = |B|$ if and only if there exists a bijection $A \rightarrow B$.
2. $|\mathbb{N}| = |\mathbb{Z}|$ because there exists a bijection $\mathbb{N} \rightarrow \mathbb{Z}$.
3. $|\mathbb{N}| \neq |\mathbb{R}|$ because there exists *no* bijection $\mathbb{N} \rightarrow \mathbb{R}$.

Thus, even though \mathbb{N} , \mathbb{Z} and \mathbb{R} are all infinite sets, their cardinalities are not all the same. The sets \mathbb{N} and \mathbb{Z} have the same cardinality, but \mathbb{R} 's cardinality is different from that of both the other sets. This means infinite sets can have different sizes. We now make some definitions to put words and symbols to this phenomenon.

In a certain sense you can count the elements of \mathbb{N} ; you can count its elements off as 1, 2, 3, 4, ..., but you'd have to continue this process forever to count the whole set. Thus we will call \mathbb{N} a *countably infinite set*, and the same term is used for any set whose cardinality equals that of \mathbb{N} .


Definition 18.2 Suppose A is a set. Then A is **countably infinite** if $|\mathbb{N}| = |A|$, that is, if there exists a bijection $\mathbb{N} \rightarrow A$. The set A is **uncountable** if A is infinite and $|\mathbb{N}| \neq |A|$, that is, if A is infinite and there exists *no* bijection $\mathbb{N} \rightarrow A$.

Thus \mathbb{Z} is countably infinite but \mathbb{R} is uncountable. This section deals mainly with countably infinite sets. Uncountable sets are treated later.

If A is countably infinite, then $|\mathbb{N}| = |A|$, so there is a bijection $f : \mathbb{N} \rightarrow A$. You can think of f as “counting” the elements of A . The first element of A is $f(1)$, followed by $f(2)$, then $f(3)$ and so on. It makes sense to think of a countably infinite set as the smallest type of infinite set, because if the counting process stopped, the set would be finite, not infinite; a countably infinite set has the fewest elements that a set can have and still be infinite. It is common to reserve the special symbol \aleph_0 to stand for the cardinality of countably infinite sets.

Definition 18.3 The cardinality of the natural numbers is denoted \aleph_0 . That is, $|\mathbb{N}| = \aleph_0$. Thus any countably infinite set has cardinality \aleph_0 .

(The symbol \aleph is the first letter in the Hebrew alphabet, and is pronounced “aleph.” The symbol \aleph_0 is pronounced “aleph naught.”) The summary of facts at the beginning of this section shows $|\mathbb{Z}| = \aleph_0$ and $|\mathbb{R}| \neq \aleph_0$.

Example 18.5 Let $E = \{2k : k \in \mathbb{Z}\}$ be the set of even integers. The function $f : \mathbb{Z} \rightarrow E$ defined as $f(n) = 2n$ is easily seen to be a bijection, so $|\mathbb{Z}| = |E|$. Thus, as $|\mathbb{N}| = |\mathbb{Z}| = |E|$, the set E is countably infinite and $|E| = \aleph_0$. 

Here is a significant fact: The elements of any countably infinite set A can be written in an infinitely long list $a_1, a_2, a_3, a_4, \dots$ that begins with some element $a_1 \in A$ and includes every element of A . For example, the set E in the above example can be written in list form as $0, 2, -2, 4, -4, 6, -6, 8, -8, \dots$. The reason that this can be done is as follows. Since A is countably infinite, Definition 18.2 says there is a bijection $f: \mathbb{N} \rightarrow A$. This allows us to list out the set A as an infinite list $f(1), f(2), f(3), f(4), \dots$. Conversely, if the elements of A can be written in list form as a_1, a_2, a_3, \dots , then the function $f: \mathbb{N} \rightarrow A$ defined as $f(n) = a_n$ is a bijection, so A is countably infinite. We summarize this as follows.

Theorem 18.3 A set A is countably infinite if and only if its elements can be arranged in an infinite list $a_1, a_2, a_3, a_4, \dots$

As an example of how this theorem might be used, let P denote the set of all prime numbers. Since we can list its elements as $2, 3, 5, 7, 11, 13, \dots$, it follows that the set P is countably infinite.

As another consequence of Theorem 18.3, note that we can interpret the fact that the set \mathbb{R} is not countably infinite as meaning that it is impossible to write out all the elements of \mathbb{R} in an infinite list. (After all, we tried to do that in the table on page 417, and failed!)

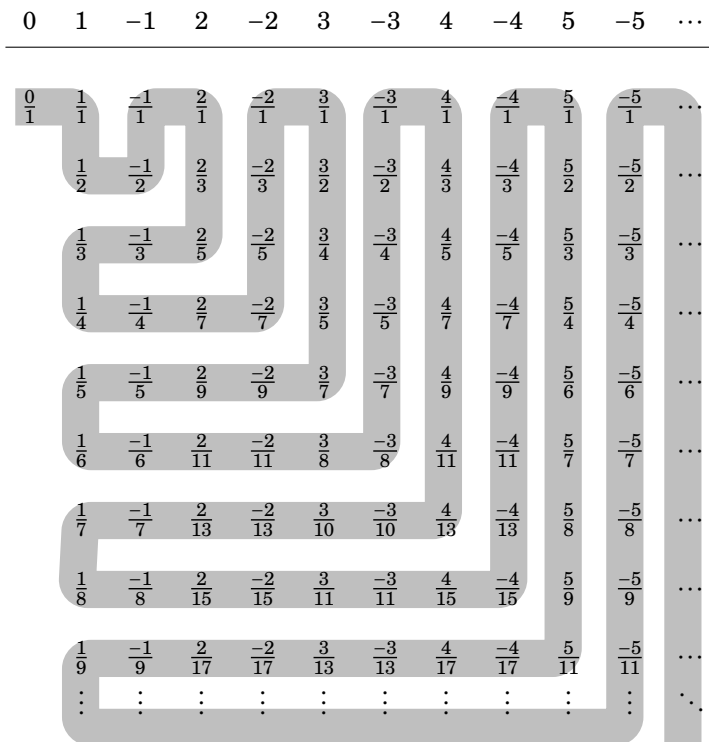
This raises a question. Is it also impossible to write out all the elements of \mathbb{Q} in an infinite list? In other words, is the set \mathbb{Q} of rational numbers countably infinite or uncountable? If you start plotting the rational numbers on the number line, they seem to mostly fill up \mathbb{R} . Sure, some numbers such as $\sqrt{2}$, π and e will not be plotted, but the dots representing rational numbers seem to predominate. We might thus expect \mathbb{Q} to be uncountable. However, it is a surprising fact that \mathbb{Q} is countable. The proof presented below arranges all the rational numbers in an infinitely long list.

Theorem 18.4 The set \mathbb{Q} of rational numbers is countably infinite.

Proof. To prove this, we just need to show how to write the set \mathbb{Q} in list form. Begin by arranging all rational numbers in an infinite array. This is done by making the following chart. The top row has a list of all integers, beginning with 0, then alternating signs as they increase. Each column headed by an integer k contains all the fractions (in reduced form) with numerator k . For example, the column headed by 2 contains the fractions $\frac{2}{1}, \frac{2}{3}, \frac{2}{5}, \frac{2}{7}, \dots$, and so on. It does not contain $\frac{2}{2}, \frac{2}{4}, \frac{2}{6}$, etc., because those are not reduced, and in fact their reduced forms appear in the column headed by 1. You should examine this table and convince yourself that it contains all rational numbers in \mathbb{Q} .

| | | | | | | | | | | | |
|---------------|---------------|----------------|----------------|-----------------|----------------|-----------------|----------------|-----------------|---------------|----------------|----------|
| 0 | 1 | -1 | 2 | -2 | 3 | -3 | 4 | -4 | 5 | -5 | ... |
| $\frac{0}{1}$ | $\frac{1}{1}$ | $\frac{-1}{1}$ | $\frac{2}{1}$ | $\frac{-2}{1}$ | $\frac{3}{1}$ | $\frac{-3}{1}$ | $\frac{4}{1}$ | $\frac{-4}{1}$ | $\frac{5}{1}$ | $\frac{-5}{1}$ | ... |
| | $\frac{1}{2}$ | $\frac{-1}{2}$ | $\frac{2}{3}$ | $\frac{-2}{3}$ | $\frac{3}{2}$ | $\frac{-3}{2}$ | $\frac{4}{3}$ | $\frac{-4}{3}$ | $\frac{5}{2}$ | $\frac{-5}{2}$ | ... |
| | $\frac{1}{3}$ | $\frac{-1}{3}$ | $\frac{2}{5}$ | $\frac{-2}{5}$ | $\frac{3}{4}$ | $\frac{-3}{4}$ | $\frac{4}{5}$ | $\frac{-4}{5}$ | $\frac{5}{3}$ | $\frac{-5}{3}$ | ... |
| | $\frac{1}{4}$ | $\frac{-1}{4}$ | $\frac{2}{7}$ | $\frac{-2}{7}$ | $\frac{3}{5}$ | $\frac{-3}{5}$ | $\frac{4}{7}$ | $\frac{-4}{7}$ | $\frac{5}{4}$ | $\frac{-5}{4}$ | ... |
| | $\frac{1}{5}$ | $\frac{-1}{5}$ | $\frac{2}{9}$ | $\frac{-2}{9}$ | $\frac{3}{7}$ | $\frac{-3}{7}$ | $\frac{4}{9}$ | $\frac{-4}{9}$ | $\frac{5}{6}$ | $\frac{-5}{6}$ | ... |
| | $\frac{1}{6}$ | $\frac{-1}{6}$ | $\frac{2}{11}$ | $\frac{-2}{11}$ | $\frac{3}{8}$ | $\frac{-3}{8}$ | $\frac{4}{11}$ | $\frac{-4}{11}$ | $\frac{5}{7}$ | $\frac{-5}{7}$ | ... |
| | $\frac{1}{7}$ | $\frac{-1}{7}$ | $\frac{2}{13}$ | $\frac{-2}{13}$ | $\frac{3}{10}$ | $\frac{-3}{10}$ | $\frac{4}{13}$ | $\frac{-4}{13}$ | $\frac{5}{8}$ | $\frac{-5}{8}$ | ... |
| | \vdots | \vdots | \vdots | \vdots | \vdots | \vdots | \vdots | \vdots | \vdots | \vdots | \ddots |

Next, draw an infinite path in this array, beginning at $\frac{0}{1}$ and snaking back and forth as indicated below. Every rational number is on this path.



Beginning at $\frac{0}{1}$ and following the path, we get an infinite list of all rational numbers:

$$0, 1, \frac{1}{2}, -\frac{1}{2}, -1, 2, \frac{2}{3}, \frac{2}{5}, -\frac{1}{3}, \frac{1}{3}, \frac{1}{4}, -\frac{1}{4}, \frac{2}{7}, -\frac{2}{7}, -\frac{2}{5}, -\frac{2}{3}, -\frac{2}{3}, -2, 3, \frac{3}{2}, \dots$$

By Theorem 18.3, it follows that \mathbb{Q} is countably infinite, that is, $|\mathbb{Q}| = |\mathbb{N}|$. ■

It is also true that the Cartesian product of two countably infinite sets is itself countably infinite, as our next theorem states.

Theorem 18.5 If A and B are both countably infinite, then so is $A \times B$.

Proof. Suppose A and B are both countably infinite. By Theorem 18.3, we know we can write A and B in list form as

$$\begin{aligned} A &= \{a_1, a_2, a_3, a_4, \dots\}, \\ B &= \{b_1, b_2, b_3, b_4, \dots\}. \end{aligned}$$

Figure 18.2 shows how to form an infinite path winding through all of $A \times B$. Therefore $A \times B$ can be written in list form, so it is countably infinite. ■

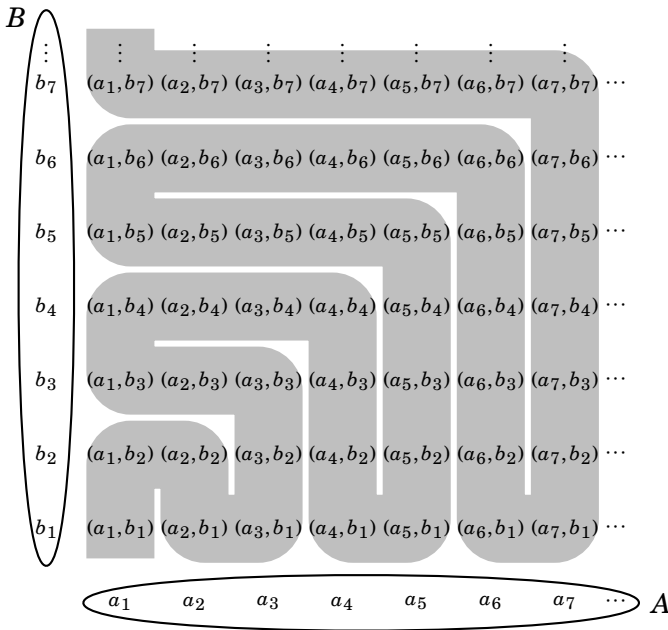


Figure 18.2. A product of two countably infinite sets is countably infinite

As an example of a consequence of this theorem, notice that since \mathbb{Q} is countably infinite, the set $\mathbb{Q} \times \mathbb{Q}$ is also countably infinite.

Recall that the word “corollary” means a result that follows easily from some other result. We have the following corollary of Theorem 18.5.

Corollary 18.1 Given n countably infinite sets $A_1, A_2, A_3, \dots, A_n$, with $n \geq 2$, the Cartesian product $A_1 \times A_2 \times A_3 \times \dots \times A_n$ is also countably infinite.

Proof. The proof is by induction on n . For the basis step, notice that when $n = 2$ the statement asserts that for countably infinite sets A_1 and A_2 , the product $A_1 \times A_2$ is countably infinite, and this is true by Theorem 18.5.

Assume that for $k \geq 2$, any product $A_1 \times A_2 \times A_3 \times \dots \times A_k$ of countably infinite sets is countably infinite. Consider a product $A_1 \times A_2 \times A_3 \times \dots \times A_{k+1}$ of $k + 1$ countably infinite sets. It is easily confirmed that the function

$$\begin{aligned} f : A_1 \times A_2 \times A_3 \times \dots \times A_k \times A_{k+1} &\longrightarrow (A_1 \times A_2 \times A_3 \times \dots \times A_k) \times A_{k+1} \\ f(x_1, x_2, \dots, x_k, x_{k+1}) &= ((x_1, x_2, \dots, x_k), x_{k+1}) \end{aligned}$$

is bijective, so $|A_1 \times A_2 \times A_3 \times \dots \times A_k \times A_{k+1}| = |(A_1 \times A_2 \times A_3 \times \dots \times A_k) \times A_{k+1}|$. By the induction hypothesis, $(A_1 \times A_2 \times A_3 \times \dots \times A_k) \times A_{k+1}$ is a product of two countably infinite sets, so it is countably infinite by Theorem 18.5. As noted above, $A_1 \times A_2 \times A_3 \times \dots \times A_k \times A_{k+1}$ has the same cardinality, so it too is countably infinite. ■

Theorem 18.6 If A and B are both countably infinite, then $A \cup B$ is countably infinite.

Proof. Suppose A and B are both countably infinite. By Theorem 18.3, we know we can write A and B in list form as

$$\begin{aligned} A &= \{a_1, a_2, a_3, a_4, \dots\}, \\ B &= \{b_1, b_2, b_3, b_4, \dots\}. \end{aligned}$$

We can “shuffle” A and B into one infinite list for $A \cup B$ as follows.

$$A \cup B = \{a_1, b_1, a_2, b_2, a_3, b_3, a_4, b_4, \dots\}.$$

(We agree not to list an element twice if it belongs to both A and B .) Therefore, by Theorem 18.3, it follows that $A \cup B$ is countably infinite. ■

Exercises for Section 18.2

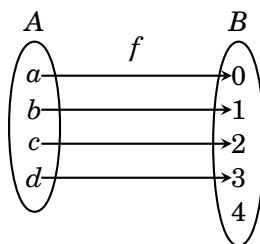
1. Prove that the set $A = \{\ln(n) : n \in \mathbb{N}\} \subseteq \mathbb{R}$ is countably infinite.
 2. Prove that the set $A = \{(m, n) \in \mathbb{N} \times \mathbb{N} : m \leq n\}$ is countably infinite.
 3. Prove that the set $A = \{(5n, -3n) : n \in \mathbb{Z}\}$ is countably infinite.
 4. Prove that the set of all irrational numbers is uncountable. (Suggestion: Consider proof by contradiction using Theorems 18.4 and 18.6.)
 5. Prove or disprove: There exists a countably infinite subset of the set of irrational numbers.
 6. Prove or disprove: There exists a bijective function $f : \mathbb{Q} \rightarrow \mathbb{R}$.
 7. Prove or disprove: The set \mathbb{Q}^{100} is countably infinite.
 8. Prove or disprove: The set $\mathbb{Z} \times \mathbb{Q}$ is countably infinite.
 9. Prove or disprove: The set $\{0, 1\} \times \mathbb{N}$ is countably infinite.
 10. Prove or disprove: The set $A = \{\frac{\sqrt{2}}{n} : n \in \mathbb{N}\}$ is countably infinite.
 11. Describe a partition of \mathbb{N} that divides \mathbb{N} into eight countably infinite subsets.
 12. Describe a partition of \mathbb{N} that divides \mathbb{N} into \aleph_0 countably infinite subsets.
 13. Prove or disprove: If $A = \{X \subseteq \mathbb{N} : X \text{ is finite}\}$, then $|A| = \aleph_0$.
 14. Suppose $A = \{(m, n) \in \mathbb{N} \times \mathbb{R} : n = \pi m\}$. Is it true that $|\mathbb{N}| = |A|$?
 15. Theorem 18.5 implies that $\mathbb{N} \times \mathbb{N}$ is countably infinite. Construct an alternate proof of this fact by showing that the function $\varphi : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ defined as $\varphi(m, n) = 2^{n-1}(2m - 1)$ is bijective.
-

18.3 Comparing Cardinalities

At this point we know that there are at least two different kinds of infinity. On one hand, there are countably infinite sets such as \mathbb{N} , of cardinality \aleph_0 . Then there is the uncountable set \mathbb{R} . Are there other kinds of infinity beyond these two kinds? The answer is “yes,” but to see why we first need to introduce some new definitions and theorems.

Our first task will be to formulate a definition for what we mean by $|A| < |B|$. Of course if A and B are finite we know exactly what this means: $|A| < |B|$ means that when the elements of A and B are counted, A is found to have fewer elements than B . But this process breaks down if A or B is infinite, for then the elements can't be counted.

The language of functions helps us overcome this difficulty. Notice that for finite sets A and B it is intuitively clear that $|A| < |B|$ if and only if there exists an injective function $f : A \rightarrow B$ but there are no surjective functions $f : A \rightarrow B$. The following diagram illustrates this:



We will use this idea to define what is meant by $|A| < |B|$ and $|A| \leq |B|$. For emphasis, the following definition also restates what is meant by $|A| = |B|$.

Definition 18.4 Suppose A and B are sets.

- $|A| = |B|$ means there is a bijection $A \rightarrow B$.
- $|A| < |B|$ means there is an injection $A \rightarrow B$, but no surjection $A \rightarrow B$.
- $|A| \leq |B|$ means $|A| < |B|$ or $|A| = |B|$.

For example, consider \mathbb{N} and \mathbb{R} . The function $f : \mathbb{N} \rightarrow \mathbb{R}$ defined as $f(n) = n$ is clearly injective, but it is not surjective because given the element $\frac{1}{2} \in \mathbb{R}$, we have $f(n) \neq \frac{1}{2}$ for every $n \in \mathbb{N}$. In fact, Theorem 18.2 of Section 18.1 asserts that there is no surjection $\mathbb{N} \rightarrow \mathbb{R}$. Definition 18.4 yields

$$|\mathbb{N}| < |\mathbb{R}|. \tag{18.1}$$

Said differently, $\aleph_0 < |\mathbb{R}|$.

Is there a set X for which $|\mathbb{R}| < |X|$? The answer is “yes,” and the next theorem explains why. It implies $|\mathbb{R}| < |\mathcal{P}(\mathbb{R})|$. (Recall that $\mathcal{P}(A)$ denotes the power set of A .)

Theorem 18.7 If A is any set, then $|A| < |\mathcal{P}(A)|$.

Proof. Before beginning the proof, we remark that this statement is obvious if A is finite, for then $|A| < 2^{|A|} = |\mathcal{P}(A)|$. But our proof must apply to *all* sets A , both finite and infinite, so it must use Definition 18.4.

We prove the theorem with direct proof. Let A be an arbitrary set. According to Definition 18.4, to prove $|A| < |\mathcal{P}(A)|$ we must show that there is an injection $f : A \rightarrow \mathcal{P}(A)$, but no surjection $f : A \rightarrow \mathcal{P}(A)$.

To see that there is an injection $f : A \rightarrow \mathcal{P}(A)$, define f by the rule $f(x) = \{x\}$. In words, f sends any element x of A to the one-element set $\{x\} \in \mathcal{P}(A)$. Then $f : A \rightarrow \mathcal{P}(A)$ is injective, as follows. Suppose $f(x) = f(y)$. Then $\{x\} = \{y\}$. Now, the only way that $\{x\}$ and $\{y\}$ can be equal is if $x = y$, so it follows that $x = y$. Thus f is injective.

Next we need to show that there exists no surjection $f : A \rightarrow \mathcal{P}(A)$. Suppose for the sake of contradiction that there does exist a surjection $f : A \rightarrow \mathcal{P}(A)$. Notice that for any element $x \in A$, we have $f(x) \in \mathcal{P}(A)$, so $f(x)$ is a subset of A . Thus f is a function that sends elements of A to subsets of A . It follows that for any $x \in A$, either x is an element of the subset $f(x)$ or it is not. Using this idea, define the following subset B of A :

$$B = \{x \in A : x \notin f(x)\} \subseteq A.$$

Now since $B \subseteq A$ we have $B \in \mathcal{P}(A)$, and since f is surjective there is an $a \in A$ for which $f(a) = B$. Now, either $a \in B$ or $a \notin B$. We will consider these two cases separately, and show that each leads to a contradiction.

Case 1. If $a \in B$, then the definition of B implies $a \notin f(a)$, and since $f(a) = B$ we have $a \notin B$, which is a contradiction.

Case 2. If $a \notin B$, then the definition of B implies $a \in f(a)$, and since $f(a) = B$ we have $a \in B$, again a contradiction.

Since the assumption that there is a surjection $f : A \rightarrow \mathcal{P}(A)$ leads to a contradiction, we conclude that there are no such surjective functions.

In conclusion, we have seen that there exists an injection $A \rightarrow \mathcal{P}(A)$ but no surjection $A \rightarrow \mathcal{P}(A)$, so Definition 18.4 implies that $|A| < |\mathcal{P}(A)|$. ■

Beginning with the set $A = \mathbb{N}$ and applying Theorem 18.7 over and over again, we get the following chain of infinite cardinalities.

$$\aleph_0 = |\mathbb{N}| < |\mathcal{P}(\mathbb{N})| < |\mathcal{P}(\mathcal{P}(\mathbb{N}))| < |\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N})))| < \dots \quad (18.2)$$

So we have an infinite sequence of different types of infinity, starting with \aleph_0 and becoming ever larger. The set \mathbb{N} is countable, and all the sets $\mathcal{P}(\mathbb{N})$, $\mathcal{P}(\mathcal{P}(\mathbb{N}))$, etc., are uncountable. It can be proved that $|\mathcal{P}(\mathbb{N})| = |\mathbb{R}|$. Thus $|\mathbb{N}|$ and $|\mathbb{R}|$ are the first two entries in the chain (18.2) above. They are just two relatively tame infinities in a long list of other wild and exotic infinities.

Unless you plan on studying advanced set theory or the foundations of mathematics, you are unlikely to ever encounter any types of infinity beyond \aleph_0 and $|\mathbb{R}|$. Still you may need to distinguish between countably infinite and uncountable sets, so we close with two final theorems for this.

Theorem 18.8 An infinite subset of a countably infinite set is countably infinite.

Proof. Suppose A is an infinite subset of the countably infinite set B . Because B is countably infinite, its elements can be written in a list $b_1, b_2, b_3, b_4, \dots$

Then we can also write A 's elements in list form by proceeding through the elements of B , in order, and selecting those that belong to A . Thus A can be written in list form, and since A is infinite, its list will be infinite. Consequently A is countably infinite. ■

Theorem 18.9 If $U \subseteq A$, and U is uncountable, then A is uncountable.

Proof. Suppose for the sake of contradiction that $U \subseteq A$, and U is uncountable but A is not uncountable. Then since $U \subseteq A$ and U is infinite, then A must be infinite too. Since A is infinite, and not uncountable, it must be countably infinite. Then U is an infinite subset of a countably infinite set A , so U is countably infinite by Theorem 18.8. Thus U is both uncountable and countably infinite, a contradiction. ■

Theorems 18.8 and 18.9 can be useful when we need to decide whether a set is countably infinite or uncountable. They sometimes allow us to decide its cardinality by comparing it to a set whose cardinality is known.

For example, suppose we want to decide whether or not the set $A = \mathbb{R}^2$ is uncountable. Since the x -axis $U = \{(x, 0) : x \in \mathbb{R}\} \subseteq \mathbb{R}^2$ has the same cardinality as \mathbb{R} , it is uncountable. Theorem 18.9 implies that \mathbb{R}^2 is uncountable. Other examples can be found in the exercises.

Exercises for Section 18.3

1. Suppose B is an uncountable set and A is a set. Given that there is a surjective function $f : A \rightarrow B$, what can be said about the cardinality of A ?
 2. Prove that the set \mathbb{C} of complex numbers is uncountable.
 3. Prove or disprove: If A is uncountable, then $|A| = |\mathbb{R}|$.
 4. Prove or disprove: If $A \subseteq B \subseteq C$ and A and C are countably infinite, then B is countably infinite.
 5. Prove or disprove: The set $\{0, 1\} \times \mathbb{R}$ is uncountable.
 6. Prove or disprove: Every infinite set is a subset of a countably infinite set.
 7. Prove or disprove: If $A \subseteq B$ and A is countably infinite and B is uncountable, then $B - A$ is uncountable.
 8. Prove or disprove: The set $\{(a_1, a_2, a_3, \dots) : a_i \in \mathbb{Z}\}$ of infinite sequences of integers is countably infinite.
 9. Prove that if A and B are finite sets with $|A| = |B|$, then any injection $f : A \rightarrow B$ is also a surjection. Show this is not necessarily true if A and B are not finite.
 10. Prove that if A and B are finite sets with $|A| = |B|$, then any surjection $f : A \rightarrow B$ is also an injection. Show this is not necessarily true if A and B are not finite.
-

18.4 Case Study: Computable Functions

This section uses some of our recent results on cardinality to explore certain theoretical limitations on the problems that computers can solve. Roughly, we will prove that there are more problems than there are algorithms to solve them, and therefore some problems cannot be solved with algorithms.

We will investigate this in the somewhat controlled environment of functions from \mathbb{N} to \mathbb{N} . Define a function $f : \mathbb{N} \rightarrow \mathbb{N}$ to be **computable** if there exists a procedure that accepts any $n \in \mathbb{N}$ as input, and outputs $f(n)$.

For example, the factorial function $f(n) = n!$ is computable because in Chapter 6 we wrote a procedure `Fac` for which `Fac(n) = n!` (see page 187). Also, the function f for which $f(n)$ is the n th Fibonacci number is a computable function because the procedure `Fib(n)` in the solution of Exercise 6.13 computes it. You can imagine writing a procedure for any function $f(n)$ that applies familiar algebraic operations to n , so such functions are computable. Even an arbitrary piecewise function like

$$g(n) = \begin{cases} 20 - n^2 & \text{if } n \leq 4 \\ 2^n & \text{if } 4 < n < 10 \\ 3 & \text{if } 10 \leq n \end{cases}$$

is computable because below is a procedure for which $g(n) = \text{Piece}(n)$.

Procedure `Piece(n)`

```

begin
  | if  $n \leq 4$  then
  | | return  $20 - n^2$ 
  | else
  | | if  $4 < n < 10$  then
  | | | return  $2^n$ 
  | | | else
  | | | | return 3
  | | | end
  | | end
  | end
end

```

Given these examples, one might guess that any $f : \mathbb{N} \rightarrow \mathbb{N}$ is computable. That is false. In fact, most functions are not computable, and we will spend the remainder of this short section proving it. This involves two steps. In the first step (Proposition 18.1, below) we show that there are uncountably many functions $f : \mathbb{N} \rightarrow \mathbb{N}$. Then we show that there are only countably many procedures. This will force us to the conclusion that there are not enough procedures to compute all the functions.

Proposition 18.1 The set of all functions $f : \mathbb{N} \rightarrow \mathbb{N}$ is uncountable.

Proof. Certainly there are infinitely many functions $f : \mathbb{N} \rightarrow \mathbb{N}$. Suppose for the sake of contradiction that this set of functions is countable. Then by Theorem 18.3, these functions can be arranged in an infinite list

$$f_1, f_2, f_3, f_4, f_5, \dots, \tag{18.3}$$

such that every function $f : \mathbb{N} \rightarrow \mathbb{N}$ is somewhere on this list. Imagine the following infinite table that tallies the values of these functions. The table is arranged so that its k th row is $f_k(1), f_k(2), f_k(3), f_k(4), \dots$, that is, each entry x_{kn} is the number $x_{kn} = f_k(n)$.

| $n :$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | \dots |
|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|
| $f_1(n)$ | x_{11} | x_{12} | x_{13} | x_{14} | x_{15} | x_{16} | x_{17} | x_{18} | x_{19} | \dots |
| $f_2(n)$ | x_{21} | x_{22} | x_{23} | x_{24} | x_{25} | x_{26} | x_{27} | x_{28} | x_{29} | \dots |
| $f_3(n)$ | x_{31} | x_{32} | x_{33} | x_{34} | x_{35} | x_{36} | x_{37} | x_{38} | x_{39} | \dots |
| $f_4(n)$ | x_{41} | x_{42} | x_{43} | x_{44} | x_{45} | x_{46} | x_{47} | x_{48} | x_{49} | \dots |
| $f_5(n)$ | x_{51} | x_{52} | x_{53} | x_{54} | x_{55} | x_{56} | x_{57} | x_{58} | x_{59} | \dots |
| $f_6(n)$ | x_{61} | x_{62} | x_{63} | x_{64} | x_{65} | x_{66} | x_{67} | x_{68} | x_{69} | \dots |
| $f_7(n)$ | x_{71} | x_{72} | x_{73} | x_{74} | x_{75} | x_{76} | x_{77} | x_{78} | x_{79} | \dots |
| $f_8(n)$ | x_{81} | x_{82} | x_{83} | x_{84} | x_{85} | x_{86} | x_{87} | x_{88} | x_{89} | \dots |
| $f_9(n)$ | x_{91} | x_{92} | x_{93} | x_{94} | x_{95} | x_{96} | x_{97} | x_{98} | x_{99} | \dots |
| \vdots | \vdots | \vdots | \vdots | \vdots | \vdots | \vdots | \vdots | \vdots | \vdots | \vdots |

The gray diagonal covers the entries $f_n(n) = x_{nn}$. These entries are the key to producing a contradiction, for they lead to a function $f_0 : \mathbb{N} \rightarrow \mathbb{N}$ that is not on the list (18.3). Simply define f_0 as

$$f_0(n) = \begin{cases} 1 & \text{if } x_{nn} = 0 \\ 0 & \text{if } x_{nn} \neq 0. \end{cases}$$

Notice that if f_n is any function on the list (18.3), then $f_n(n) = x_{nn} \neq f_0(n)$. Therefore f_n and f_0 are not equal, because they do not agree on the value n . Consequently f_0 is not equal to any of the functions f_n on the list (18.3). This contradicts the assumption we made in the first paragraph of the proof, namely that the list (18.3) contains every function $\mathbb{N} \rightarrow \mathbb{N}$.

In summary, the assumption that the set of functions $\mathbb{N} \rightarrow \mathbb{N}$ is countable leads to a contradiction, so this set is uncountable. ■

Next we will argue that, even though the set of functions $\mathbb{N} \rightarrow \mathbb{N}$ is uncountable, the set of *procedures* is *countably infinite*. To fix the discussion, consider procedures that are written in some particular programming language. Programs (procedures) in this language are written using a finite set Σ of computer keyboard symbols. (Here the sigma is a mnemonic for “symbol,” not “sum.”) The set Σ includes the “blank” space character, which we will denote as “_” (to make it visible). Thus

$$\Sigma = \{ _ , a, b, c, \dots, z, A, B, C, \dots, Z, 0, 1, 2, \dots, 9, (,), +, -, *, \$, \{, \}, /, \dots \},$$

where the blank character is listed first. Let’s say $|\Sigma| = 100$ (a value chosen for simplicity, rather than by actually counting the symbols on a keyboard).

For a fixed positive integer k , the Cartesian power $\Sigma^k = \Sigma \times \Sigma \times \dots \times \Sigma$ has cardinality 100^k , a number that can be quite large, but it is finite.

We can identify any length- k string of symbols from Σ as an element of Σ^k . For example, the string “for (i=2) to 10 do” appears in Σ^{18} as

$$(f, o, r, _, (, i, =, 2,), _, t, o, _, 1, 0, _, d, o) \in \Sigma^{18}.$$

Certainly Σ^{18} also contains some meaningless nonsense, like the encoding of “uk9*C\$aaaA2017hhhh”. But any procedure or fragment of a procedure that uses 18 or fewer characters is encoded in Σ^{18} . Likewise, any procedure that is written in k or fewer characters can be regarded an element of Σ^k .

Now consider the set

$$\Upsilon = \bigcup_{k=1}^{\infty} \Sigma^k = \Sigma^1 \cup \Sigma^2 \cup \Sigma^3 \cup \Sigma^4 \cup \dots$$

Any syntactically correct procedure is an element of this set. Granted, Υ also contains a lot of meaningless nonsense. And it contains some brilliant non-procedures, like Shakepere’s *Othello*. But the point is that Υ contains all procedures that can possibly be written.

The interesting thing about Υ is that it is countable. To verify this, we just need to show that its elements can be arranged in an infinite list. This can be done as follows. The first 100 entries of the list are the 100 symbols in Σ^1 . Follow this with the $100^2 = 10,000$ elements of Σ^2 . Then the list continues with the $100^3 = 1,000,000$ elements of Σ^3 , followed by the $100^4 = 100,000,000$ elements of Σ^4 , and so on. Therefore Υ is countable.

The set of all possible procedures is a subset of the countably infinite set Υ , so it is countable by Theorem 18.8, which states that an infinite subset of a countable set is countable. We have therefore proved the following result.

Proposition 18.2 The set of all programs (or procedures) that can be written in a given programming language is countable.

This means that the set of computable functions—those functions that can be computed with a procedure—is countable, because there are only countably many procedures to compute them. But Proposition 18.3 says that the number of functions $\mathbb{N} \rightarrow \mathbb{N}$ is uncountable. Therefore there exist functions that cannot be computed with a procedure. This is our main result.

Theorem 18.10 There exist functions that are not computable, that is, they cannot be computed by any procedure.

18.5 Solutions for Chapter 18

Section 18.1 Exercises

1. \mathbb{R} and $(0, \infty)$

Observe that the function $f(x) = e^x$ sends \mathbb{R} to $(0, \infty)$. It is injective because $f(x) = f(y)$ implies $e^x = e^y$, and taking \ln of both sides gives $x = y$. It is surjective because if $b \in (0, \infty)$, then $f(\ln(b)) = b$. Therefore, because of the bijection $f : \mathbb{R} \rightarrow (0, \infty)$, it follows that $|\mathbb{R}| = |(0, \infty)|$.

3. \mathbb{R} and $(0, 1)$

Observe that the function $\frac{1}{\pi}f(x) = \cot^{-1}(x)$ sends \mathbb{R} to $(0, 1)$. It is injective and surjective by elementary trigonometry. Therefore, because of the bijection $f : \mathbb{R} \rightarrow (0, 1)$, it follows that $|\mathbb{R}| = |(0, 1)|$.

5. $A = \{3k : k \in \mathbb{Z}\}$ and $B = \{7k : k \in \mathbb{Z}\}$

Observe that the function $f(x) = \frac{7}{3}x$ sends A to B . It is injective because $f(x) = f(y)$ implies $\frac{7}{3}x = \frac{7}{3}y$, and multiplying both sides by $\frac{3}{7}$ gives $x = y$. It is surjective because if $b \in B$, then $b = 7k$ for some integer k . Then $3k \in A$, and $f(3k) = 7k = b$. Therefore, because of the bijection $f : A \rightarrow B$, it follows that $|A| = |B|$.

7. \mathbb{Z} and $S = \{\dots, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, 16, \dots\}$

Observe that the function $f : \mathbb{Z} \rightarrow S$ defined as $f(n) = 2^n$ is bijective: It is injective because $f(m) = f(n)$ implies $2^m = 2^n$, and taking \log_2 of both sides produces $m = n$. It is surjective because any element b of S has form $b = 2^n$ for some integer n , and therefore $f(n) = 2^n = b$. Because of the bijection $f : \mathbb{Z} \rightarrow S$, it follows that $|\mathbb{Z}| = |S|$.

9. $\{0, 1\} \times \mathbb{N}$ and \mathbb{N}

Consider the function $f : \{0, 1\} \times \mathbb{N} \rightarrow \mathbb{N}$ defined as $f(a, n) = 2n - a$. This is injective because if $f(a, n) = f(b, m)$, then $2n - a = 2m - b$. Now if a were unequal to b , one of a or b would be 0 and the other would be 1, and one side of $2n - a = 2m - b$ would be odd and the other even, a contradiction. Therefore $a = b$. Then $2n - a = 2m - b$ becomes $2n - a = 2m - a$; add a to both sides and divide by 2 to get $m = n$. Thus we have $a = b$ and $m = n$, so $(a, n) = (b, m)$, so f is injective. To see that f is surjective, take any $b \in \mathbb{N}$. If b is even, then $b = 2n$ for some integer n , and $f(0, n) = 2n - 0 = b$. If b is odd, then $b = 2n + 1$ for some integer n . Then $f(1, n + 1) = 2(n + 1) - 1 = 2n + 1 = b$. Therefore f is surjective. Then f is a bijection, so $|\{0, 1\} \times \mathbb{N}| = |\mathbb{N}|$.

11. $[0, 1]$ and $(0, 1)$

Proof. Consider the subset $X = \{\frac{1}{n} : n \in \mathbb{N}\} \subseteq [0, 1]$. Let $f : [0, 1] \rightarrow (0, 1)$ be defined as $f(x) = x$ if $x \in [0, 1] - X$ and $f(\frac{1}{n}) = \frac{1}{n+1}$ for any $\frac{1}{n} \in X$. It is easy to check that f is a bijection. Next let $Y = \{1 - \frac{1}{n} : n \in \mathbb{N}\} \subseteq [0, 1]$, and define $g : [0, 1] \rightarrow (0, 1)$ as $g(x) = x$ if $x \in [0, 1] - Y$ and $g(1 - \frac{1}{n}) = 1 - \frac{1}{n+1}$ for any $1 - \frac{1}{n} \in Y$. As in the case of f , it is easy to check that g is a bijection. Therefore the composition $g \circ f : [0, 1] \rightarrow (0, 1)$ is a bijection. (See Theorem 17.2.) We conclude that $|[0, 1]| = |(0, 1)|$. ■

13. $\mathcal{P}(\mathbb{N})$ and $\mathcal{P}(\mathbb{Z})$

Outline: By Exercise 18 of Section 17.2, we have a bijection $f: \mathbb{N} \rightarrow \mathbb{Z}$ defined as $f(n) = \frac{(-1)^n(2n-1)+1}{4}$. Now define a function $\Phi: \mathcal{P}(\mathbb{N}) \rightarrow \mathcal{P}(\mathbb{Z})$ as $\Phi(X) = \{f(x) : x \in X\}$. Check that Φ is a bijection.

15. Find a formula for the bijection f in Example 18.2.

Hint: Consider the function f from Exercise 18 of Section 17.2.

Section 18.2 Exercises

1. Prove that the set $A = \{\ln(n) : n \in \mathbb{N}\} \subseteq \mathbb{R}$ is countably infinite.

Just note that its elements can be written in infinite list form as $\ln(1), \ln(2), \ln(3), \dots$. Thus A is countably infinite.

3. Prove that the set $A = \{(5n, -3n) : n \in \mathbb{Z}\}$ is countably infinite.

Consider the function $f: \mathbb{Z} \rightarrow A$ defined as $f(n) = (5n, -3n)$. This is clearly surjective, and it is injective because $f(n) = f(m)$ gives $(5n, -3n) = (5m, -3m)$, so $5n = 5m$, hence $m = n$. Thus, because f is surjective, $|\mathbb{Z}| = |A|$, and $|A| = |\mathbb{Z}| = \aleph_0$. Therefore A is countably infinite.

5. Prove or disprove: There exists a countably infinite subset of the set of irrational numbers.

This is true. Just consider the set consisting of the irrational numbers $\frac{\pi}{1}, \frac{\pi}{2}, \frac{\pi}{3}, \frac{\pi}{4}, \dots$.

7. Prove or disprove: The set \mathbb{Q}^{100} is countably infinite.

This is true. Note $\mathbb{Q}^{100} = \mathbb{Q} \times \mathbb{Q} \times \dots \times \mathbb{Q}$ (100 times), and since \mathbb{Q} is countably infinite, it follows from the corollary of Theorem 18.5 that this product is countably infinite.

9. Prove or disprove: The set $\{0, 1\} \times \mathbb{N}$ is countably infinite.

This is true. Note that $\{0, 1\} \times \mathbb{N}$ can be written in infinite list form as $(0, 1), (1, 1), (0, 2), (1, 2), (0, 3), (1, 3), (0, 4), (1, 4), \dots$. Thus the set is countably infinite.

11. Partition \mathbb{N} into 8 countably infinite sets.

For each $i \in \{1, 2, 3, 4, 5, 6, 7, 8\}$, let X_i be those natural numbers that are congruent to i modulo 8, that is,

$$\begin{aligned} X_1 &= \{1, 9, 17, 25, 33, \dots\} \\ X_2 &= \{2, 10, 18, 26, 34, \dots\} \\ X_3 &= \{3, 11, 19, 27, 35, \dots\} \\ X_4 &= \{4, 12, 20, 28, 36, \dots\} \\ X_5 &= \{5, 13, 21, 29, 37, \dots\} \\ X_6 &= \{6, 14, 22, 30, 38, \dots\} \\ X_7 &= \{7, 15, 23, 31, 39, \dots\} \\ X_8 &= \{8, 16, 24, 32, 40, \dots\} \end{aligned}$$

13. If $A = \{X \subset \mathbb{N} : X \text{ is finite}\}$, then $|A| = \aleph_0$.

Proof. This is **true**. To show this we will describe how to arrange the items of A in an infinite list $X_1, X_2, X_3, X_4, \dots$

For each natural number n , let p_n be the n th prime number. Thus $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $p_5 = 11$, and so on. Now consider any element $X \in A$. If $X \neq \emptyset$, then $X = \{n_1, n_2, n_3, \dots, n_k\}$, where $k = |X|$ and $n_i \in \mathbb{N}$ for each $1 \leq i \leq k$. Define a function $f : A \rightarrow \mathbb{N} \cup \{0\}$ as follows: $f(\{n_1, n_2, n_3, \dots, n_k\}) = p_{n_1} p_{n_2} \cdots p_{n_k}$. For example, $f(\{1, 2, 3\}) = p_1 p_2 p_3 = 2 \cdot 3 \cdot 5 = 30$, and $f(\{3, 5\}) = p_3 p_5 = 5 \cdot 11 = 55$, etc. Also, we should not forget that $\emptyset \in A$, and we define $f(\emptyset) = 0$.

Note that $f : A \rightarrow \mathbb{N} \cup \{0\}$ is an injection: Let $X = \{n_1, n_2, n_3, \dots, n_k\}$ and put $Y = \{m_1, m_2, m_3, \dots, m_\ell\}$, and $X \neq Y$. Then there is an integer a that belongs to one of X or Y but not the other. Then the prime factorization of one of the numbers $f(X)$ and $f(Y)$ uses the prime number p_a but the prime factorization of the other does not use p_a . It follows that $f(X) \neq f(Y)$ by the fundamental theorem of arithmetic. Thus f is injective.

So each set $X \in A$ is associated with an integer $f(X) \geq 0$, and no two different sets are associated with the same number. Thus we can list the elements in $X \in A$ in increasing order of the numbers $f(X)$. The list begins as

$$\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{4\}, \{1, 3\}, \{5\}, \{6\}, \{1, 4\}, \{2, 3\}, \{7\}, \dots$$

It follows that A is countably infinite. ■

15. Hint: Use the fundamental theorem of arithmetic.

Section 18.3 Exercises

- 1.** Suppose B is an uncountable set and A is a set. Given that there is a surjective function $f : A \rightarrow B$, what can be said about the cardinality of A ?

The set A must be uncountable, as follows. For each $b \in B$, let a_b be an element of A for which $f(a_b) = b$. (Such an element must exist because f is surjective.) Now form the set $U = \{a_b : b \in B\}$. Then the function $f : U \rightarrow B$ is bijective, by construction. Then since B is uncountable, so is U . Therefore U is an uncountable subset of A , so A is uncountable by Theorem 18.9.

- 3.** Prove or disprove: If A is uncountable, then $|A| = |\mathbb{R}|$.

This is false. Let $A = \mathcal{P}(\mathbb{R})$. Then A is uncountable, and by Theorem 18.7, $|\mathbb{R}| < |\mathcal{P}(\mathbb{R})| = |A|$.

- 5.** Prove or disprove: The set $\{0, 1\} \times \mathbb{R}$ is uncountable.

This is true. To see why, first note that the function $f : \mathbb{R} \rightarrow \{0\} \times \mathbb{R}$ defined as $f(x) = (0, x)$ is a bijection. Thus $|\mathbb{R}| = |\{0\} \times \mathbb{R}|$, and since \mathbb{R} is uncountable, so is $\{0\} \times \mathbb{R}$. Then $\{0\} \times \mathbb{R}$ is an uncountable subset of the set $\{0, 1\} \times \mathbb{R}$, so $\{0, 1\} \times \mathbb{R}$ is uncountable by Theorem 18.9.

- 7.** Prove or disprove: If $A \subseteq B$ and A is countably infinite and B is uncountable, then $B - A$ is uncountable.

This is true. To see why, suppose to the contrary that $B - A$ is countably infinite. Then $B = A \cup (B - A)$ is a union of countably infinite sets, and thus countable, by Theorem 18.6. This contradicts the fact that B is uncountable.

Review of Real-Valued Functions

In Chapter 6 we saw how the efficiency of algorithms is measured by functions of the size of their inputs. For example, the sequential search algorithm (page 192) needs $f(n) = 2 + 2n$ steps (in the worst case) to search a list of length n . By contrast, the binary search algorithm (page 194) needs only $g(n) = 3 + 2\log_2(n)$ steps in the worst case.

Using functions of input size to study the performance of algorithms is important in computer science, and is a key ingredient of the final chapters of this book. The purpose of this chapter is to review the basic properties of the functions that arise most naturally in this context, namely polynomial, exponential and logarithm functions. There is nothing really new here; you have studied such functions for years. But if you are a bit rusty with, say, exponents and logarithms, then this chapter is a refresher. If you already have a good grip on the algebra of functions, then you can skip it.

Chapter 17 developed a theory of functions $f : A \rightarrow B$ from one set to another. Here we are concerned with functions $f : \mathbb{R} \rightarrow \mathbb{R}$, where A and B are the set \mathbb{R} , or perhaps intervals on the real line, as in $f : \mathbb{R} \rightarrow [0, \infty)$. Actually, the uses to which we will later apply such functions involve situations in which the domain is input size (a positive integer) and the co-domain is the number of steps executed by an algorithm (also a positive integer). In this context, they are properly viewed as functions $f : \mathbb{N} \rightarrow \mathbb{N}$. However, because $\mathbb{N} \subseteq \mathbb{R}$, we typically view the domain co-domain as sets of real numbers.

Ideas studied in Chapter 17 that play a role in this chapter include domain, range, co-domain, as well as injective, surjective, bijective and inverse functions. A certain fluency with exponents is essential too.

19.1 Exponent Review

We start at the beginning. In an expression such as a^n in which a is raised to the power of n , the number a is called the **base** and n is the **exponent**. For a number a and positive integer n ,

$$a^n = \underbrace{a \cdot a \cdot a \cdots a}_{n \text{ times}}.$$

This would be too elementary to mention except that every exponent property flows from it. For example,

$$(ab)^n = \underbrace{(ab) \cdot (ab) \cdot (ab) \cdots (ab)}_{n \text{ times}} = \underbrace{a \cdot a \cdot a \cdots a}_{n \text{ times}} \cdot \underbrace{b \cdot b \cdot b \cdots b}_{n \text{ times}} = a^n b^n,$$

that is, $(ab)^n = a^n b^n$. Also, $\left(\frac{a}{b}\right)^n = \frac{a}{b} \cdot \frac{a}{b} \cdots \frac{a}{b} = \frac{a^n}{b^n}$. And $a^m a^n = a^{m+n}$ because

$$a^m a^n = \underbrace{a \cdot a \cdot a \cdots a}_{m \text{ times}} \cdot \underbrace{a \cdot a \cdot a \cdots a}_{n \text{ times}} = a^{m+n}.$$

Assuming for the moment that $m > n$, we also get

$$\frac{a^m}{a^n} = \frac{\overbrace{a \cdot a \cdot a \cdots a}^{m \text{ times}}}{\underbrace{a \cdot a \cdot a \cdots a}_{n \text{ times}}} = \underbrace{a \cdot a \cdots a}_{m-n \text{ times}} = a^{m-n}$$

because the a 's on the bottom cancel with n of the a 's on top, leaving $m-n$ a 's on top. Also notice that $(a^n)^m = a^{nm}$ because

$$(a^n)^m = \overbrace{(a \cdot a \cdot a \cdots a) \cdot (a \cdot a \cdot a \cdots a) \cdots (a \cdot a \cdot a \cdots a)}^{m \text{ groups of } a\text{'s}} = a^{nm}.$$

We have just verified the following fundamental Laws of exponents.

Fact 19.1 Basic Laws of Exponents

$$a^1 = a \qquad (ab)^n = a^n b^n \qquad \left(\frac{a}{b}\right)^n = \frac{a^n}{b^n}$$

$$a^m a^n = a^{m+n} \qquad \frac{a^m}{a^n} = a^{m-n} \qquad (a^n)^m = a^{nm}$$

So far we have assumed n is a positive integer because in performing $a^n = a \cdot a \cdots a$ we cannot multiply a times itself a negative or fractional number of times. But there is a way to understand these rules when n is zero, negative or fractional. Trusting the above property $a^{m-n} = \frac{a^m}{a^n}$ yields

$$a^0 = a^{1-1} = \frac{a^1}{a^1} = 1, \quad (\text{provided } a \neq 0)$$

$$a^{-n} = a^{0-n} = \frac{a^0}{a^n} = \frac{1}{a^n}.$$

Notice 0^0 is undefined because $0^0 = 0^{1-1} = \frac{0^1}{0^1} = \frac{0}{0}$, which is undefined. But we can find a^n when n is 0 (and $a \neq 0$) or negative, as in $2^{-3} = \frac{1}{2^3} = \frac{1}{8}$. In essence we just multiplied 2 times itself -3 times! Also note $a^{-1} = \frac{1}{a}$.

What about fractional powers, like $a^{m/n}$ or $a^{1/n}$? If we believe $(a^n)^m = a^{nm}$, then

$$\left(a^{\frac{1}{n}}\right)^n = a^{\frac{1}{n} \cdot n} = a^1 = a.$$

In words, $a^{\frac{1}{n}}$ is a number that, if raised to the power of n , results in a . This means $a^{1/n} = \sqrt[n]{a}$. For example, $16^{1/4} = \sqrt[4]{16} = 2$ and $2^{1/2} = \sqrt{2}$. Further, $a^{\frac{m}{n}} = a^{\frac{1}{n}m} = \left(a^{\frac{1}{n}}\right)^m = \sqrt[n]{a^m} = \sqrt[n]{a^m}$. Let's summarize all of this.

Fact 19.2 Laws of zero, negative and rational exponents

$$a^0 = 1 \quad (\text{if } a \neq 0) \qquad a^{-n} = \frac{1}{a^n} \qquad a^{-1} = \frac{1}{a}$$


$$a^{\frac{1}{n}} = \sqrt[n]{a} \qquad a^{\frac{m}{n}} = \sqrt[n]{a^m} = \sqrt[n]{a^m}$$

The boxed equations hold for any rational m and n , positive or negative.

Example 19.1 Knowing the rules of exponents in the boxes above means we can evaluate many expressions without a calculator. Suppose we are confronted with $16^{-1.5}$. What number is this? We reckon as follows

$$16^{-1.5} = 16^{-3/2} = \frac{1}{16^{3/2}} = \frac{1}{\sqrt{16}^3} = \frac{1}{4^3} = \frac{1}{64}.$$

For another example, $8^{-1.5} = 8^{-3/2} = \frac{1}{8^{3/2}} = \frac{1}{\sqrt{8}^3} = \frac{1}{(2\sqrt{2})^3} = \frac{1}{2^3\sqrt{2}^3} = \frac{1}{16\sqrt{2}}$.

Also, $(-8)^{5/3} = \sqrt[3]{-8^5} = (-2)^5 = (-2)(-2)(-2)(-2)(-2) = -32$. 

Exercises for Section 19.1

Work the following exponents with pencil and paper alone. Then compare your answer to a calculator's to verify that the calculator is working properly.

1. $25^{1/2}$ 2. $4^{1/2}$ 3. $\frac{1}{4}^{1/2}$ 4. $27^{1/3}$ 5. $(-27)^{1/3}$ 6. $(27)^{-1/3}$ 7. $(-27)^{4/3}$
8. 2^{-1} 9. 2^{-2} 10. 2^{-3} 11. $\frac{1}{2}^{-1}$ 12. $\frac{1}{2}^{-2}$ 13. $\frac{1}{2}^{-3}$ 14. $\frac{1}{4}^{-1/2}$
15. $\sqrt{2}^6$ 16. $\left(\frac{4}{9}\right)^{-1/2}$ 17. $\left(\frac{\sqrt{3}}{2}\right)^{-4}$ 18. $\frac{\sqrt{3}^{100}}{\sqrt{3}^{94}}$ 19. $\left(\left(\frac{2}{3}\right)^{\frac{3}{2}}\right)^2$ 20. $\left(\frac{3^9}{3^7}\right)^{\frac{3}{2}}$ 21. $\left(\sqrt{2}\sqrt{2}\right)^{\sqrt{2}}$

19.2 Linear Functions, Power Functions and Polynomials

Some functions (and families of functions) are so elemental that they become part of our daily mathematical vocabulary. Here is a quick inventory.

We begin with linear functions. A **linear function** is a function $f : \mathbb{R} \rightarrow \mathbb{R}$ having the form $f(x) = mx + b$, where m and b are constants. The graph of this function is a straight line with slope m and y -intercept b . See Figure 19.1.

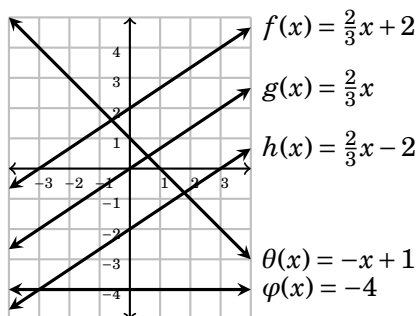


Figure 19.1. Some linear functions.

In $f(x) = mx + b$ it is of course possible that $m = 0$, giving the function $f(x) = b$. This is called a **constant function**; no matter what the input x is, the output is always the same number b . The graph of this function is a horizontal line (slope 0) passing through the point b on the y -axis. The constant function $\varphi(x) = -4$ is illustrated above. You could write it as $\varphi(x) = 0 \cdot x - 4$ and regard it as the rule *multiply x by zero and subtract 4*.

A **power function** is a function of form $f(x) = x^n$, where the exponent n is a constant. Figure 19.2 shows a few examples where n is a positive integer. It is important to *internalize* (not just memorize) these graphs. Take time to understand why the graphs look the way they do. Notice that when n is even x^n is positive for any x , so the graph lies above the x axis in those cases. By contrast, for odd n the value x^n is negative whenever x is negative; thus a portion of these graphs is below the x -axis.

It is of course possible to have power functions $f(x) = x^n$ for which n is not an integer. For example, $f(x) = x^{\frac{1}{2}} = \sqrt{x}$, and in general $f(x) = x^{\frac{a}{b}} = \sqrt[b]{x^a}$. Notice that if a and b are positive integers, then $f(x) = x^{\frac{a}{b}} = \sqrt[b]{x^a}$ grows arbitrarily large as x increases: For any positive y (no matter how large), $x > \sqrt[b]{y^b}$ implies $f(x) > \sqrt[b]{\sqrt[b]{y^b}^b} = y$. This illustrates an important fact.

Fact 19.3 If $n > 0$ then the power function $f(x) = x^n$ increases to ∞ as x increases to ∞ .

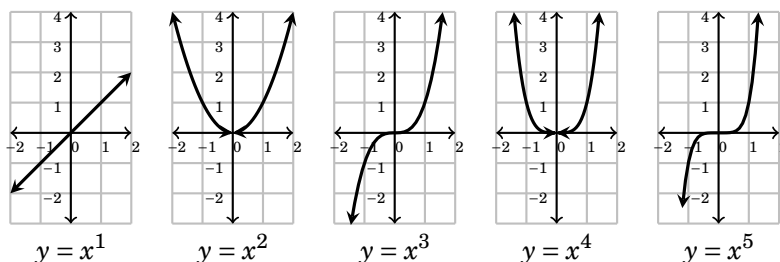


Figure 19.2. Power functions $f(x) = x^n$. In each case the domain is all real numbers, \mathbb{R} . If n is even the range is $[0, \infty)$. If n is odd the range is \mathbb{R} .

A **polynomial function** is a sum of multiples of integer powers of x , plus a constant term (which could be 0). So $f(x) = x^4 - 2x^2 + \pi x + 2$ is a polynomial with constant term 2, and $g(x) = 5x^2 + 3x - 1$ is a polynomial with constant term -1 . The **degree** of a polynomial is its highest power of x , so $f(x)$ has degree 4 and $g(x)$ has degree 2. A linear function, such as $h(x) = 3x + 7$, is a polynomial of degree 1, as $h(x) = 3x^1 + 7$. We regard a constant function $f(x) = b$ as a polynomial of degree 0, as $b = bx^0$ (for $x \neq 0$).

19.3 Exponential Functions

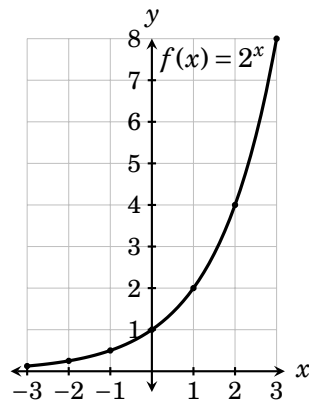
Interchanging the x and the 2 in the power function $f(x) = x^2$ gives a new function $f(x) = 2^x$. A function like this one, a constant raised to a variable power, is called an *exponential function*.

An **exponential function** is one of form $f(x) = a^x$, where a is a positive constant, called the **base** of the exponential function. For example $f(x) = 2^x$ and $f(x) = 3^x$ are exponential functions, as is $f(x) = \frac{1}{2}^x$. If we let $a = 1$ in $f(x) = a^x$ we get $f(x) = 1^x = 1$, which is, in fact, a linear function. For this reason we agree that the base of an exponential function is never 1.

Let's graph the exponential function $f(x) = 2^x$. Below is a table with some sample x and $f(x)$ values. The resulting graph is on the right.

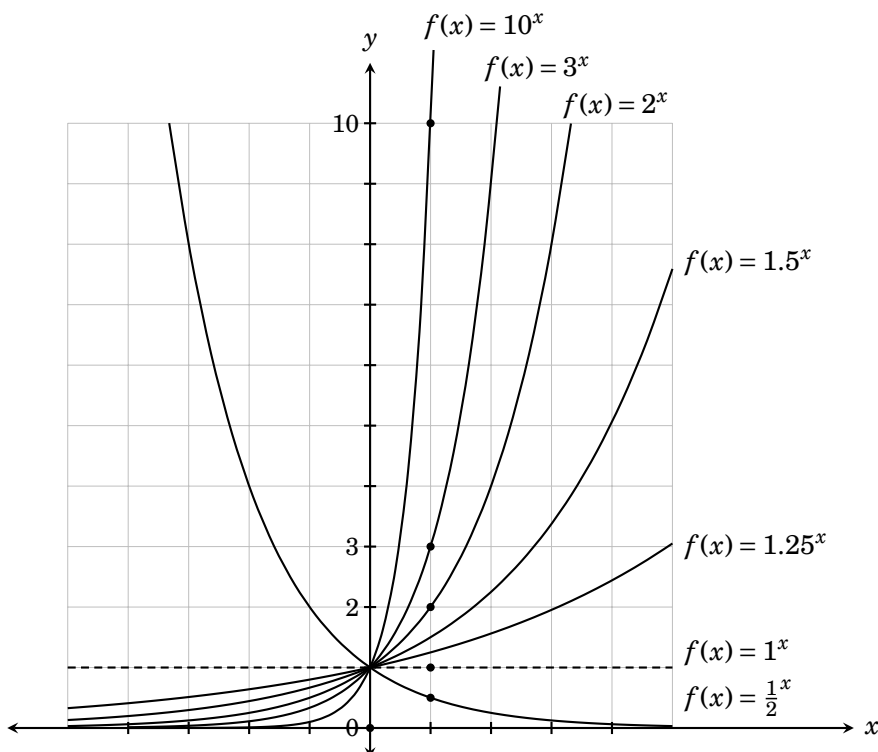
| | | | | | | | |
|--------------|---------------|---------------|---------------|---|---|---|---|
| x | -3 | -2 | -1 | 0 | 1 | 2 | 3 |
| $f(x) = 2^x$ | $\frac{1}{8}$ | $\frac{1}{4}$ | $\frac{1}{2}$ | 1 | 2 | 4 | 8 |

Notice that $f(x) = 2^x$ is positive for any x , but gets closer to zero the as x moves in the negative direction. But $2^x > 0$ for any x , so the graph never touches the x -axis.



Working with exponential functions requires fluency with the exponent properties of Section 19.1. For example, if $f(x) = 2^x$, then $f(-3) = 2^{-3} = \frac{1}{2^3} = \frac{1}{8}$ and $f\left(\frac{3}{2}\right) = 2^{\frac{3}{2}} = \sqrt{2^3} = \sqrt{2}\sqrt{2}\sqrt{2} = 2\sqrt{2}$.

Several exponential functions are graphed below. These graphs underscore the fact that the domain of any exponential function is \mathbb{R} . The range is $(0, \infty)$. The y -intercept of any exponential function is 1.



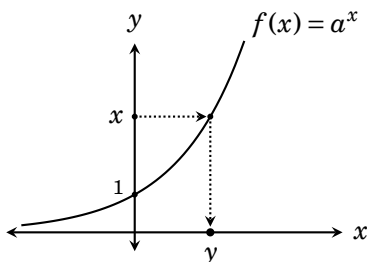
Notice that if the base of an exponential function is less than 1, like in $f(x) = \frac{1}{2}^x$, then the graph *decreases* as x increases. If in doubt, write a table for this function and graph it. (This involves using the formula $a^{-x} = \frac{1}{a^x}$.) But if the base a is greater than 1, then $f(x) = a^x$ grows very quickly as x increases.

Fact 19.4 If $a > 1$, the exponential function $f(x) = a^x$ increases to ∞ as x increases to ∞ .

Next we investigate the inverses of exponential functions, which are called *logarithms*.

19.4 Logarithmic Functions

Now we apply the ideas of Chapter 17 to explore inverses of exponential functions. Such inverses are called *logarithmic functions*, or just *logarithms*.



An exponential function $f(x) = a^x$, viewed as $f : \mathbb{R} \rightarrow (0, \infty)$, is bijective and thus has an inverse. As illustrated above, this inverse sends any number x to the number y for which $f(y) = x$, that is, for which $a^y = x$. In other words,

$$f^{-1}(x) = \left(\begin{array}{l} \text{the number } y \\ \text{for which } a^y = x \end{array} \right).$$

From this it seems that a better name for f^{-1} might be a^\square , for then

$$a^\square(x) = \left(\begin{array}{l} \text{the number } y \\ \text{for which } a^y = x \end{array} \right).$$

The idea is that $a^\square(x)$ is the number y that goes in the box so that $a^y = x$. Using a^\square as the name of f^{-1} thus puts the meaning of f^{-1} into its name. We therefore will use the symbol a^\square instead of f^{-1} for the inverse of $f(x) = a^x$.

For example, the inverse of $f(x) = 2^x$ is a function called 2^\square , where

$$2^\square(x) = \left(\begin{array}{l} \text{the number } y \\ \text{for which } 2^y = x \end{array} \right).$$

Consider $2^\square(8)$. Putting 3 in the box gives $2^3 = 8$, so $2^\square(8) = 3$. Similarly

$$\begin{array}{ll} 2^\square(16) = 4 & \text{because } 2^4 = 16, \\ 2^\square(4) = 2 & \text{because } 2^2 = 4, \\ 2^\square(2) = 1 & \text{because } 2^1 = 2, \\ 2^\square(0.5) = -1 & \text{because } 2^{-1} = \frac{1}{2} = 0.5. \end{array}$$

In the same spirit the inverse of $f(x) = 10^x$ is a function called 10^{\square} , and

$$10^{\square}(x) = \left(\begin{array}{l} \text{the number } y \\ \text{for which } 10^y = x \end{array} \right).$$

Therefore we have

$$\begin{array}{ll} 10^{\square}(1000) = 3 & \text{because } 10^3 = 1000, \\ 10^{\square}(10) = 1 & \text{because } 10^1 = 10, \\ 10^{\square}(0.1) = -1 & \text{because } 10^{-1} = \frac{1}{10} = 0.1. \end{array}$$

Given a power 10^p of 10 we have $10^{\square}(10^p) = p$. For example,

$$\begin{array}{l} 10^{\square}(100) = 10^{\square}(10^2) = 2, \\ 10^{\square}(\sqrt{10}) = 10^{\square}(10^{1/2}) = \frac{1}{2}. \end{array}$$

But doing, say, $10^{\square}(15)$ is not so easy because 15 is not an obvious power of 10. We will revisit this at the end of the section.

In general, the inverse of $f(x) = a^x$ is a function called a^{\square} , pronounced “*a* box,” and defined as

$$a^{\square}(x) = \left(\begin{array}{l} \text{the number } y \\ \text{for which } a^y = x \end{array} \right).$$

You can always compute a^{\square} of a power of a in your head because $a^{\square}(a^p) = p$.

The notation a^{\square} is nice because it reminds us of the meaning of the function. But this book is probably the only place that you will ever see the symbol a^{\square} . Every other textbook—in fact all of the civilized world—uses the symbol \log_a instead of a^{\square} , and calls it the *logarithm to base a*.

Definition 19.1 For $a > 0$ and $a \neq 1$, the **logarithm to base a** is the function

$$\log_a(x) = a^{\square}(x) = \left(\begin{array}{l} \text{number } y \text{ for} \\ \text{which } a^y = x \end{array} \right).$$

The function \log_a is pronounced “*log base a*.” It is the inverse of $f(x) = a^x$.

Here are some examples.

$$\begin{array}{ll} \log_2(8) = 2^{\square}(8) = 3 & \log_5(125) = 5^{\square}(125) = 3 \\ \log_2(4) = 2^{\square}(4) = 2 & \log_5(25) = 5^{\square}(25) = 2 \\ \log_2(2) = 2^{\square}(2) = 1 & \log_5(5) = 5^{\square}(5) = 1 \\ \log_2(1) = 2^{\square}(1) = 0 & \log_5(1) = 5^{\square}(1) = 0 \end{array}$$

To repeat, \log_a and a^{\square} are different names for the same function. We will bow to convention and use \log_a , mostly. But we will revert to a^{\square} whenever it makes the discussion clearer.

Understanding the graphs of logarithm functions is important. Recall from algebra that the graph of $f^{-1}(x)$ is the graph of $f(x)$ reflected across the line $y = x$. Because \log_a is the inverse of $f(x) = a^x$, its graph is the graph of $y = a^x$ reflected across the line $y = x$, as illustrated in Figure 19.3.

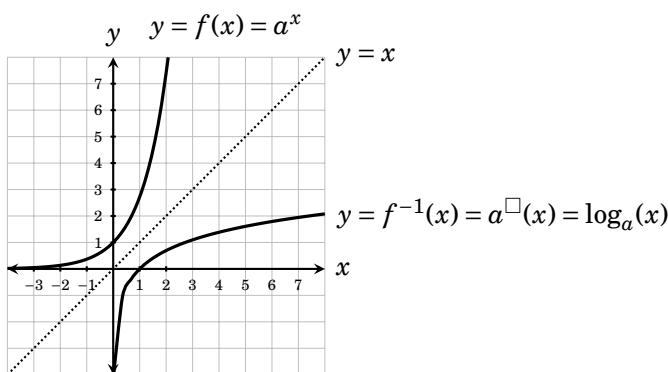


Figure 19.3. The exponential function $y = a^x$ and its inverse $y = \log_a(x)$.

Take note that the domain of \log_a is all positive numbers $(0, \infty)$ because this is the *range* of a^x . Likewise the range of \log_a is the domain of a^x , which is \mathbb{R} . Also, because $\log_a(1) = a^{\square}(1) = 0$, the x -intercept of $y = \log_a(x)$ is 1.

The logarithm function \log_{10} to base 10 occurs frequently enough that it is abbreviated as \log and called the *common logarithm*.

Definition 19.2 The **common logarithm**, denoted \log , is the function

$$\log(x) = \log_{10}(x) = 10^{\square}(x).$$

Most calculators have a $\boxed{\log}$ button for the common logarithm. Test your calculator by confirming $\log(1000) = 3$ and $\log(0.1) = -1$. The button will also tell you that $\log(15) \approx 1.17609125$. In other words $10^{\square}(15) \approx 1.17609125$, which means $10^{1.17609125} \approx 15$, a fact with which your calculator will concur.

One comment. Convention allows for $\log_a x$ in the place of $\log_a(x)$, that is, the parentheses may be dropped. We will tend to use them.

Logarithms have many important properties, which we now review. To start, for any x it is obvious that $a^{\square}(a^x) = x$ because x is what must go

into the box so that a to that power equals a^x . So we have

$$\begin{aligned} a^{\square}(a^x) &= x, \\ \log_a(a^x) &= x. \end{aligned} \tag{19.1}$$

This simply reflects the fact that $f^{-1}(f(x)) = x$ for the function $f(x) = a^x$.

Next consider the expression $a^{a^{\square}(x)}$. Here a is being raised to the power $a^{\square}(x)$, which is literally the power a must be raised to to give x . Therefore

$$\begin{aligned} a^{a^{\square}(x)} &= x, \\ a^{\log_b(x)} &= x \end{aligned} \tag{19.2}$$

for any x in the domain of a^{\square} . This is just saying $f(f^{-1}(x)) = x$.

The x in Equations (19.1) and (19.2) can be any appropriate quantity or expression. It is reasonable to think of these equations as saying

$$a^{\square}(a^{\blacksquare}) = \blacksquare \quad \text{and} \quad a^{a^{\square}(\blacksquare)} = \blacksquare,$$

where the gray rectangle can represent an arbitrary expression. Thus $a^{\square}(a^{x+y^2+3}) = x+y^2+3$ and $a^{a^{\square}(5x+1)} = 5x+1$.

Next we verify a fundamental formula for $\log_a(xy)$, that is, $a^{\square}(xy)$. Notice

$$\begin{aligned} a^{\square}(xy) &= a^{\square}(a^{a^{\square}(x)} a^{a^{\square}(y)}) \quad \dots\dots \text{because } x = a^{a^{\square}(x)} \text{ and } y = a^{a^{\square}(y)} \\ &= a^{\square}(a^{a^{\square}(x)+a^{\square}(y)}) \quad \dots\dots\dots \text{because } a^c a^d = a^{c+d} \\ &= a^{\square}(x) + a^{\square}(y) \quad \dots\dots\dots \text{using } a^{\square}(a^{\blacksquare}) = \blacksquare \end{aligned}$$

We have therefore established

$$\begin{aligned} a^{\square}(xy) &= a^{\square}(x) + a^{\square}(y), \\ \log_a(xy) &= \log_a(x) + \log_a(y). \end{aligned} \tag{19.3}$$

By the same reasoning you can also show $a^{\square}\left(\frac{x}{y}\right) = a^{\square}(x) - a^{\square}(y)$, that is,

$$\begin{aligned} a^{\square}\left(\frac{x}{y}\right) &= a^{\square}(x) - a^{\square}(y), \\ \log_a\left(\frac{x}{y}\right) &= \log_a(x) - \log_a(y). \end{aligned} \tag{19.4}$$

Applying $a^{\square}(1) = 0$ to this yields $a^{\square}\left(\frac{1}{y}\right) = a^{\square}(1) - a^{\square}(y) = -a^{\square}(y)$, so

$$\begin{aligned} a^{\square}\left(\frac{1}{y}\right) &= -a^{\square}(y), \\ \log_a\left(\frac{1}{y}\right) &= -\log_a(y). \end{aligned} \tag{19.5}$$

Here is a summary of what we have established so far.

Fact 19.5 Logarithm Laws

| | | | |
|---------------------|-----------------|--|---|
| $\log_a(a^x) = x$ | $\log_a(1) = 0$ | $\log_a(xy) = \log_a(x) + \log_a(y)$ | $\log_a(x^y) = y \log_a(x)$ |
| $a^{\log_a(x)} = x$ | $\log_a(a) = 1$ | $\log_a\left(\frac{x}{y}\right) = \log_a(x) - \log_a(y)$ | $\log_a\left(\frac{1}{y}\right) = -\log_a(y)$ |

The one law in this list that we have not yet verified is $\log_a(x^y) = y \log_a(x)$. This rule says that taking \log_a of x^y converts the *exponent* y to a *product*. Because products tend to be simpler than exponents, this property can be tremendously useful. To verify it, just notice that

$$\begin{aligned} a^{\square}(x^y) &= a^{\square}\left(\left(a^{a^{\square}(x)}\right)^y\right) \dots\dots\dots \text{because } x = a^{a^{\square}(x)} \\ &= a^{\square}\left(a^{y a^{\square}(x)}\right) \dots\dots\dots \text{because } (a^b)^y = a^{yb} \\ &= y a^{\square}(x) \dots\dots\dots \text{using } a^{\square}\left(a^{\square}\right) = \blacksquare \end{aligned}$$

Therefore $a^{\square}(x^y) = y a^{\square}(x)$, or $\log_a(x^y) = y \log_a(x)$, as listed above.

By the above laws, certain expressions involving logarithms can be transformed into simpler expressions.

Example 19.2 Simplify $\log_2(28x) - \log_2(7x)$.

To solve this we use the laws of logarithms to get


$$\begin{aligned} \log_2(28x) - \log_2(7x) &= \log_2\left(\frac{28x}{7x}\right) \\ &= \log_2(4) \\ &= 2. \end{aligned}$$



As mentioned above, the law $\log_a(x^r) = r \log_a(x)$ is extremely useful because it means taking \log_a of x^r converts the exponent r to a product. Consequently \log_a can be used to solve an equation for a quantity that appears as an exponent, as in the next example.

Example 19.3 Solve the equation $5^{x+7} = 2^x$. In other words we want to find the value of x that makes this true. Since x occurs as an exponent, we take \log_{10} of both sides and simplify with log laws.

$$\begin{aligned}\log(5^{x+7}) &= \log(2^x) \\ (x+7) \cdot \log(5) &= x \cdot \log(2) \\ x \log(5) + 7 \log(5) &= x \log(2) \\ x \log(5) - x \log(2) &= -7 \log(5) \\ x(\log(5) - \log(2)) &= -7 \log(5) \\ x &= \frac{-7 \log(5)}{\log(5) - \log(2)} \approx -12.2952955815\end{aligned}$$

where we have used a calculator in the final step. 

Example 19.4 Suppose a is positive. Solve the equation $a^y = x$ for y . The variable y is an exponent, so we take log of both sides and simplify.

$$\begin{aligned}\log(a^y) &= \log(x) \\ y \log(a) &= \log(x) \\ y &= \frac{\log(x)}{\log(a)}\end{aligned}$$


Therefore, in terms of x and a , the quantity y is the number $\frac{\log(x)}{\log(a)}$. 

Example 19.4 would have been quicker if we had used \log_a instead of \log . Let's do the same problem again with this alternative approach.

Example 19.5 Suppose a is positive. Solve the equation $a^y = x$ for y .

The variable y is an exponent, so we take \log_a of both sides and simplify.

$$\begin{aligned}\log_a(a^y) &= \log_a(x) \\ y &= \log_a(x)\end{aligned}$$


Therefore, in terms of x and a , the quantity y is the number $\log_a(x)$. 

Examples 19.4 and 19.5 say the solution of $a^y = x$ can be expressed either as $\frac{\log(x)}{\log(a)}$ or $\log_a(x)$. The first solution may be preferable, as your calculator has no \log_a button. But what is significant is that these two methods arrive at the *same* solution, which is to say $\log_a(x) = \frac{\log(x)}{\log(a)}$. To summarize:

Fact 19.6 Change of Base Formula

$$\log_a(x) = \frac{\log(x)}{\log(a)}$$

The change of base formula says that a logarithm $\log_a(x)$ to *any* base a can be expressed entirely in terms of \log_{10} .

Example 19.6 By the change of base formula, $\log_2(5) = \frac{\log(5)}{\log(2)} \approx \frac{1.698970}{0.301029} = 2.3219280$. This seems about right because $\log_2(5) = 2^{\square}(5)$ is the number y for which $2^y = 5$. Now, $2^2 = 4 < 5 < 8 = 2^3$, so y should be between 2 and 3. This example shows in fact $y = 2.3219280$, to seven decimal places. 

Exercises for Section 19.4

1. $\log_3(81) =$
2. $\log_3\left(\frac{1}{9}\right) =$
3. $\log_3(\sqrt{3}) =$
4. $\log_3\left(\frac{1}{\sqrt{3}}\right) =$
5. $\log_3(1) =$
6. $\log(1000) =$
7. $\log(\sqrt[3]{10}) =$
8. $\log(\sqrt[3]{100}) =$
9. $\log(0.01) =$
10. $\log(1) =$
11. $\log_4(4) =$
12. $\log_4(2) =$
13. $\log_4(\sqrt{2}) =$
14. $\log_4(16) =$
15. $\log_4(8) =$
16. Simplify: $\log_2(2^{\sin(x)})$
17. Simplify: $10^{\log(5x+1)}$
18. Simplify: $\log(10x^{10})$
19. Simplify: $\log(2) + \log(5)$
20. Simplify: $\log(2) + \log(2x) + \log(25x)$
21. Simplify: $\log_2(2) - \log_2(5x) + \log_2(20x)$
22. Write as a single logarithm: $5\log_2(x^3 + 1) + \log_2(x) - \log_2(3)$
23. Write as a single logarithm: $\log_2(\sin(x)) + \frac{1}{2}\log_2(4x) - 3\log_2(3)$
24. Write as a single logarithm: $2 + \log(5) + 2\log(7)$
25. Write as a single logarithm: $\log(2x) + \log(5x)$
26. Break into simpler logarithms: $\log_2(x^3(x+1))$
27. Break into simpler logarithms: $\log_2((x+5)^4 x^7 \sqrt{x+1})$
28. Break into simpler logarithms: $\log(\sqrt{x}(x+3)^6)$
29. Break into simpler logarithms: $\log_3\left(\frac{3}{5\sqrt[3]{x}}\right)$

Use the change of base formula to express the following logarithms in terms of \log .

30. $\log_2(5)$
31. $\log_3(5)$
32. $\log_4(5)$
33. $\log_5(5)$
34. $\log(8)$
35. $\log_9(10)$
36. $\log(10)$
37. $\log_2(33)$
38. $\log_3(8)$
39. $\log_3(9)$

19.5 Solutions for Chapter 19

Section 19.1

1. $25^{1/2} = \sqrt{25} = 5$
5. $(-27)^{1/3} = \sqrt[3]{-27} = -3$
9. $2^{-2} = \frac{1}{2^2} = \frac{1}{4}$
13. $\frac{1}{2}^{-3} = \frac{1}{(\frac{1}{2})^3} = \frac{1}{\frac{1}{8}} = 8$
17. $\left(\frac{\sqrt{3}}{2}\right)^{-4} = \frac{1}{\left(\frac{\sqrt{3}}{2}\right)^4} = \frac{1}{\frac{9}{16}} = \frac{16}{9}$
21. $\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\sqrt{2}} = \sqrt{2}^2 = 2$
3. $\frac{1}{4}^{1/2} = \sqrt{\frac{1}{4}} = \frac{1}{2}$
7. $(-27)^{4/3} = \sqrt[3]{-27^4} = (-3)^4 = 81$
11. $\frac{1}{2}^{-1} = \frac{1}{\frac{1}{2}} = 2$
15. $\sqrt{2}^6 = \left(\sqrt{2}^2\right)^3 = 2^3 = 8$
19. $\left(\left(\frac{2}{3}\right)^{\frac{3}{2}}\right)^2 = \left(\sqrt{\frac{2}{3}}\right)^2 = \left(\sqrt{\frac{2}{3}}\right)^3 = \left(\frac{2}{3}\right)^3 = \frac{8}{27}$

Section 19.4

1. $\log_3(81) = 3^{\square}(81) = 4$
5. $\log_3(1) = 3^{\square}(1) = 0$
9. $\log(0.01) = 10^{\square}(10^{-2}) = -2$
13. $\log_4(\sqrt{2}) = \log_4(2^{\frac{1}{2}}) = \frac{1}{2}\log_4(2) = \frac{1}{4}$
17. $10^{\log(5x+1)} = 5x + 1.$
21. $\log_2(2) - \log_2(5x) + \log_2(20x) = \log_2\left(\frac{2}{5x}\right) + \log_2(20x) = \log_2\left(\frac{40x}{5x}\right) = \log_2(8) = 3$
23. $\log_2(\sin(x)) + \frac{1}{2}\log_2(4x) - 3\log_2(3) = \log_2(\sin(x)) + \log_2\left((4x)^{\frac{1}{2}}\right) - \log_2(3^3) = \log_2(\sin(x)) + \log_2(2\sqrt{x}) - \log_2(27) = \log_2\left(\frac{2\sqrt{x}\sin(x)}{27}\right).$
25. $\log(2x) + \log(5x) = \log(2x \cdot 5x) = \log(10x^2) = \log(10) + \log(x^2) = 1 + 2\log(x)$
27. $\log_2\left((x+5)^4 x^7 \sqrt{x+1}\right) = \log_2(x+5)^4 + \log_2(x^7) + \log_2(\sqrt{x+1}) = 4\log_2(x+5) + 7\log_2(x) + \log_2\left((x+1)^{\frac{1}{2}}\right) = 4\log_2(x+5) + 7\log_2(x) + \frac{1}{2}\log_2(x+1)$
29. $\log_3\left(\frac{3}{5\sqrt[3]{x}}\right) = \log_3(3) - \log_3(5\sqrt[3]{x}) = 1 - \log_3(5) - \log_3\left(x^{\frac{1}{3}}\right) = 1 - \log_3(5) - \frac{1}{3}\log_3(x)$
31. $\log_3(5) = \frac{\log(5)}{\log(3)} \approx 1.4649$
33. $\log_5(5) = \frac{\log(5)}{\log(5)} = 1$
35. $\log_9(10) = \frac{\log(10)}{\log(9)} \approx 1.0479$
37. $\log_2(33) = \frac{\log(33)}{\log(2)} \approx 5.04438$
39. $\log_3(9) = \frac{\log(9)}{\log(3)} = 2$

Complexity of Algorithms

The goal of this chapter is to develop the language, ideas and notations that computer scientists use to analyze the speeds algorithms, and to compare and contrast the speeds of different algorithms that perform the same task. This kind of analysis is called the **time-complexity** of an algorithm, or, more often, just the **complexity** of an algorithm.

In Chapter 6 we noted that the number of steps needed for an algorithm to perform a task depends on what the input is. For example, an algorithm that puts a list into numeric order is likely to expend fewer steps on an input list that's already sorted than one that's not. Also, as a general rule, the bigger the input, the more steps the algorithm needs to process it. We introduced the idea of measuring the worst-case performance of an algorithm with a function $f(n)$, meaning that for any input of size n , the algorithm takes $f(n)$ or fewer steps to process it. Perhaps for most inputs of size n the algorithm takes fewer than $f(n)$ steps, but for some "bad" inputs the algorithm may have to take as many as $f(n)$ steps. (We will be a bit vague about what is meant by the "size" of the input, and in general this depends on context. Size could be in bytes, number of list entries, or number of vertices in an input graph, etc.)

In this chapter we will continue to measure performance of algorithms in terms of functions $f(n)$, but we will sharpen our understanding of how to compare such functions: Given two of them, we will describe rigorously when one is better than the other, or when one is just as good as the other.

To start the discussion, suppose we have two algorithms, Algorithm 1 and Algorithm 2, that do exactly the same thing. Let's say Algorithm 1 takes $f(n) = 10 + x^2$ steps (in the worst case) to process an input of size n , whereas Algorithm 2 takes $g(n) = 5 + \frac{1}{100}x^3$ steps.

Which algorithm is better?

To answer this question, we can plot the graphs of $f(x)$ and $g(x)$, as is done in Figure 20.1. In the top of the figure, they are plotted for values of n from 0 to 12. In this window it appears that $f(n)$ is bigger than $g(n)$, and is

growing much more quickly than $g(n)$. We might take this as evidence that Algorithm 2 is better, because it involves a smaller number $g(n)$ steps.

However, the bottom part of the figure takes a wider view, and plots the same two functions for $0 \leq n \leq 120$. We see that $g(n)$ overtakes $f(n)$ somewhere around $n = 100$, and thereafter $f(n) < g(n)$. Thus, contrary to the pervious paragraph's hasty conclusion, it is Algorithm 1 that is better, because it only requires $f(n)$ steps, and this is less than $g(n)$ for all of the infinitely many values of n except the first 100 or so.

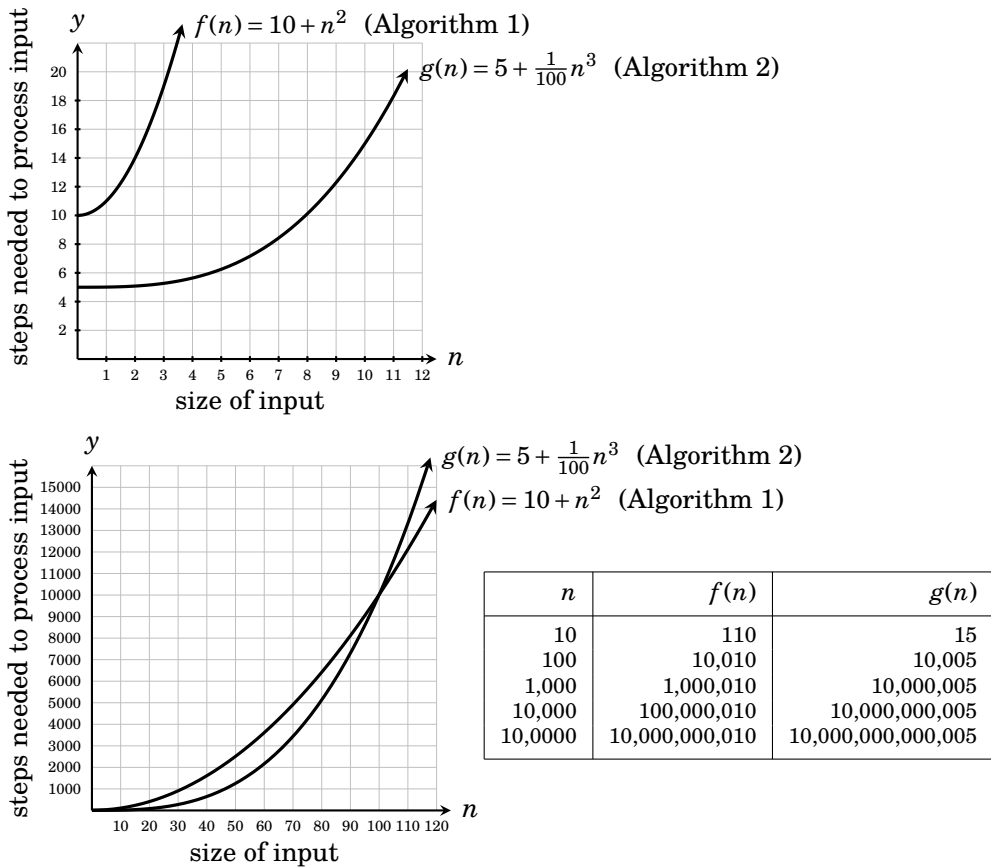


Figure 20.1. Functions $f(n)$ and $g(n)$ for $0 \leq n \leq 12$ (top) and $0 \leq n \leq 120$ (bottom). At first, $g(n) < f(n)$, but beyond about $n = 100$ the order is reversed, and $g(n) > f(n)$. The table shows why: each time n increases by a factor of 10, $f(n)$ increases about 100-fold, while $g(n)$ increases about 1000-fold. In other words, though it starts off smaller, $g(n)$ grows about 10 times faster than $f(n)$, and eventually overtakes it.

20.1 Big-O Notation

The situation in Figure 20.1 leads to the first of two guiding principles that will lead us to a meaningful formulation of algorithm complexity.

Guiding Principle A For worst-case performance, $f(n)$ is as good as or better than $g(n)$ if there exists a positive integer N for which $f(n) \leq g(n)$ whenever $n > N$.

To motivate our second guiding principle, suppose Algorithm 1 has worst-case performance $f(n)$, and Algorithm 2 has worst-case performance $g(n)$. Say there is a number A for which $f(n) \leq A \cdot g(n)$. This means Algorithm 1 takes no more than A times as many steps as Algorithm 2. So if Algorithm 1 is too slow compared to Algorithm 2, this defect can be remedied by running Algorithm 1 on a computer that is A times faster.

But if *there is no number A* for which $f(n) \leq A \cdot g(n)$ for all n , then for some n we will have $f(n) > A \cdot g(n)$, no matter how big A is. This means that for some inputs Algorithm 1 takes more time than Algorithm 2, *no matter how fast the computer it is running on is*.

Guiding Principle B For worst-case performance, $f(n)$ is as good as or better than $g(n)$ if there exists a positive number A for which $f(n) \leq A \cdot g(n)$.

These principles suggest that if $f(n)$ is “as good as or better” than $g(n)$, then it may not be true that $f(n) \leq g(n)$ for all n . Instead, $f(n)$ is “as good as or better” than $g(n)$ if there are positive numbers N and A for which $f(n) \leq A \cdot g(n)$ for all $n > N$. This leads to the chapter’s main definition, a means of comparing functions in the context of our two guiding principles.

Definition 20.1 If f and g are functions of a positive real value n , then **f is of order at most g** , written $f(n)$ is $O(g(n))$, if there exist positive numbers N and A for which

$$|f(n)| \leq A \cdot |g(n)|$$

for all $n > N$. (In this case we sometimes say “ $f(n)$ is big-O of $g(n)$.”)

Two comments: First, we usually think of n as an integer (input size), but it is a real number in the definition. This is done to make the graphs of f and g the continuous smooth curves that we are familiar with from calculus. (And it is a harmless assumption, as integers are real numbers.) Second, we tend to think of $f(n)$ and $g(n)$ as being *positive* (measuring run-time). But to make the definition useful and robust, they appear in absolute value.

Think of Definition 20.1 as giving a method of saying that one function $f(n)$ is less-than-or-equal to another function $g(n)$; a method that glosses over superfluous details and concentrates on the big picture. If $f(n)$ is $O(g(n))$, then, for all intents and purposes, this means $f \leq g$ in the sense that $f(n) \leq A \cdot g(n)$ when n is large. In other words, compared to $g(n)$, the function $f(n)$ does not grow beyond a finite, constant multiple A of $g(n)$.

In this sense, $f(n)$ being $O(g(n))$ means that the long-term growth of $f(n)$ compares favorably with that of $g(n)$. The definition gives a concise way of saying that $f(n)$ never gets “too far” beyond $g(n)$.

Notice that proving that $f(n)$ is $O(g(n))$ amounts to proving the statement


$$\exists A > 0, \exists N > 0, \forall n > N, |f(n)| \leq A \cdot |g(n)|.$$

To prove it, we must find values for A and N for which $|f(n)| \leq A \cdot |g(n)|$ is true for all $n > N$. Usually A and N will suggest themselves from f and g .

Example 20.1 Show that the polynomial $f(n) = 2 + 3n + 4n^2$ is $O(n^2)$.

Solution As long as $n > 1$ we have $n \leq n^2$ and $n^2 \leq n^3$, so

$$\begin{aligned} |f(n)| = |2 + 3n + 4n^2| &= 2 + 3n + 4n^2 \\ &\leq 2n^2 + 3n^2 + 4n^2 \\ &= 9n^2 = 9 \cdot |n^2|. \end{aligned}$$

So if $A = 9$ and $N = 1$, then $|f(n)| \leq A|n^2|$ when $n > N$. Thus $f(n)$ is $O(n^2)$. 

Next we will compare power, exponential and logarithm functions to one another. Our first result explains the relations among the power functions.

Proposition 20.1 If $1 \leq d \leq \ell$, then the power function $f(n) = n^d$ is $O(n^\ell)$. However, if $d < \ell$ then n^ℓ is not $O(n^d)$.

Proof. Suppose $\ell \geq d$. Let $A = N = 1$, and we immediately have $n^d \leq A n^\ell$ for all $n > N$, and since all terms are positive, we get $|n^d| \leq A |n^\ell|$ for all $n > N$. Thus $f(n) = n^d$ is $O(n^\ell)$ by Definition 20.1.

For the second statement, let $d < \ell$. We need to show n^ℓ is not $O(n^d)$. Suppose for the sake of contradiction that n^ℓ is $O(n^d)$. Definition 20.1 says there exist positive numbers A and N for which $|n^\ell| \leq A |n^d|$ for all $n > N$. Dropping the absolute values (as all terms are positive) and dividing both sides by n^d , we get $\frac{n^\ell}{n^d} \leq A$, so $n^{\ell-d} \leq A$ for all $n > N$. But $\ell - d$ is positive, so the power function $n^{\ell-d}$ grows arbitrarily large as n increases. Thus for large enough $n > N$ we have $n^{\ell-d} > A$, contradicting the previous sentence. \blacksquare

Let's examine this proposition in the light of graphs of some power functions. Figure 20.2 shows the graphs of $y = n^d$ for $d = 1, 2, 3, 4$ and 5. In order to give a big-picture view, the scale on the y -axis is compressed logarithmically, so that in each unit the y value doubles. This view changes the appearance of the power functions, as they "flatten out" as n increases. (Compare to this to the same functions in Figure 19.2.)

You can see that by $n = 30$, the difference between (say) n^4 and n^5 is vast, and getting vaster as n increases. This is in agreement with Proposition 20.1, which says n^5 is not $O(n^4)$; it grows beyond any finite multiple of n^4 .

It is interesting to look at the graphs of the exponential functions 2^n , 3^n and 4^n in Figure 20.2, which appear as straight lines in this compressed graph. (Compare them to Figure 19.2, which plots the same functions.) What is striking is how astronomically huge they grow, especially compared to the power functions (which "flatten out").

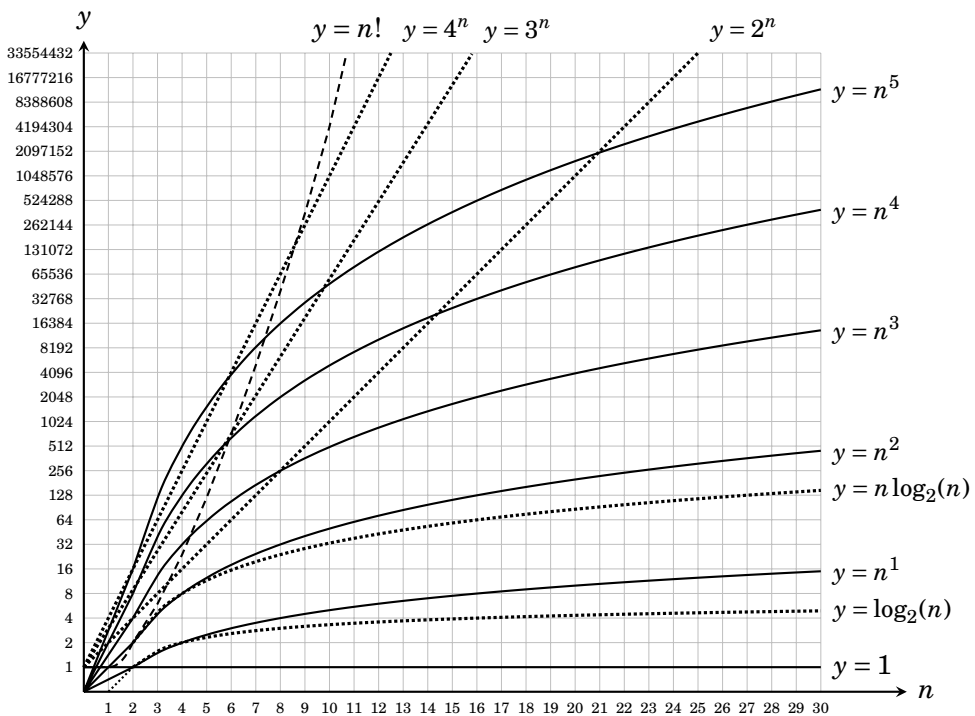


Figure 20.2. Some functions plotted on a graph where each tick on the y -axis is twice its value on the previous tick. (So the y -axis is a \log_2 scale.) Note that any power function $y = n^a$ grows vastly slower than any exponential function b^n . But $y = n!$ eventually overtakes any exponential function.

With this picture as a guide, our next task is to compare power and exponential functions in terms of Definition 20.1.

But before we do so, let's pause to lay out a road map of what we are about to do. Let's use the notation $f(x) \leq g(x)$ to mean $f(x)$ is $O(g(x))$. By $f(x) < g(x)$, we mean $f(x)$ is $O(g(x))$ but $g(x)$ **is not** $O(f(x))$. Then Proposition 20.1 implies

$$1 < n < n^2 < n^3 < n^4 < \dots$$

In the remainder of this section we are going to show

$$1 < \log_2(n) < n < n^2 < n^3 < n^4 < \dots < 2^n < 3^n < 4^n < 5^n < \dots \quad (20.1)$$

This is the content of the section's remaining propositions.

But first, a quick word about the constant function 1 that appears on the left of the chain (20.1), above. This constant function $y = f(n) = 1$ is graphed in Figure 20.2. In general, a constant function has the form $f(n) = c$, where c is some constant number. Whatever n is plugged into the function, the output is c . It is immediate that any constant function c is $O(1)$, because $c \leq A \cdot 1$ for $A = c$. Also c is $O(n)$, because clearly $c \leq A \cdot n$ for all $n > N = \frac{c}{A}$.

Now let's ponder exponential functions, at the right end of chain (20.1)

Proposition 20.2 If $1 < a < b$, then the exponential function a^n is $O(b^n)$. But b^n **is not** $O(a^n)$.

Proof. Suppose $1 < a < b$. It is immediate that a^n is $O(b^n)$, because then $a^n \leq 1 \cdot b^n$ for all $n > 0$, and Definition 20.1 applies.

Next we prove b^n not $O(a^n)$. For the sake of contradiction, say b^n is $O(a^n)$. Then Definition 20.1 says there are positive numbers A and N for which $b^n \leq Aa^n$ for all $n > N$. (We have omitted the absolute values because everything is sight is already positive.) From this $\frac{b^n}{a^n} \leq A$, which means $\left(\frac{b}{a}\right)^n < A$ for all $n > N$. This is a contradiction because $a < b$ forces $\frac{b}{a} > 1$, so the exponential function $\left(\frac{b}{a}\right)^n$ is bigger than A for all sufficiently large n . ■

Next we are going to show that any power function n^d is $O(a^n)$ if $a > 1$. For example, consider the power function n^{1000} , compared to the exponential function 2^n . For small values of n we have $n^{1000} > 2^n$. For example, $10^{1000} = 10,000 > 1024 = 2^{10}$. But you may have a sense that, because 2^n doubles each time n increases by 1, then for large enough n , we have $n^{1000} < 2^n$. If you are comfortable with your intuition and knowledge of how an exponential function eventually surpasses a power function, then you may want to skip the next proof. (But do read the statement of the proposition.)

Proposition 20.3 If $d \geq 1$ and $a > 1$, then n^d is $O(a^n)$, but a^n is not $O(n^d)$.

Proof. First we will show n^d is $O(a^n)$. To begin, note that if $n > 1$, then $\frac{n}{n-1} > 1$, because the numerator is greater than the denominator. But as n grows bigger, $\frac{n}{n-1}$ gets closer and closer to 1. The reason is that $\frac{n}{n-1} = 1 + \frac{1}{n-1}$ (check this), and the fraction $\frac{1}{n-1}$ approaches 0 as n gets bigger. (If you have had some calculus then you know to express this phenomenon as $\lim_{n \rightarrow \infty} \frac{n}{n-1} = 1$. However, we will use no calculus here.) Because $a > 1$, the number $\sqrt[d]{a}$ is greater than 1, so there is some $N > 0$ for which $n > N$ implies $\frac{n}{n-1} < \sqrt[d]{a}$. This means

$$\left(\frac{n}{n-1}\right)^d < a \quad \text{for } n > N. \quad (20.2)$$

Now let $A = N^d$. We claim that $n^d \leq Aa^n$ for all $n > N$. Indeed, if $n > N$, then

$$\begin{aligned} n^d &< (N+n)^d && \text{(because } n < N+n) \\ &= \left(\frac{N}{N}\right)^d \left(\frac{N+1}{N+1}\right)^d \left(\frac{N+2}{N+2}\right)^d \cdots \left(\frac{N+n-1}{N+n-1}\right)^d (N+n)^d && \text{(multiply by 1)} \\ &= N^d \left(\frac{N+1}{N}\right)^d \left(\frac{N+2}{N+1}\right)^d \left(\frac{N+3}{N+2}\right)^d \cdots \left(\frac{N+n}{N+n-1}\right)^d && \text{(move denominators} \\ &&& \text{one place to right)} \\ &< N^d \underbrace{a \cdot a \cdot a \cdot a \cdots a}_{n \text{ times}} && \text{(by Equation (20.2))} \\ &= Aa^n. && \text{(because } A = N^d) \end{aligned}$$

We've established $n^d \leq Aa^n$ for $n > N$, which proves n^d is $O(a^n)$.

Next we show that a^n is not $O(n^d)$. Suppose for the sake of contradiction that a^n is $O(n^d)$. Then there are positive numbers A and N for which

$$a^n \leq An^d \quad \text{when } n > N. \quad (20.3)$$

Because $1 < a$, there is a number b for which $1 < b < a$. By the first part of the proof, we know n^d is $O(b^n)$, so there exist positive A' and N' for which

$$n^d \leq A'b^n \quad \text{when } n > N'. \quad (20.4)$$

Combining inequalities (20.3) and (20.4) yields $a^n \leq An^d \leq AA'b^n$. Dividing this by b^n gives $\frac{a^n}{b^n} \leq AA'$, or $\left(\frac{a}{b}\right)^n \leq AA'$, if n is bigger than both N and N' . This is a contradiction, as the fact $1 < b < a$ ensures $\frac{a}{b} > 1$, so the exponential function $\left(\frac{a}{b}\right)^n$ actually exceeds AA' for all sufficiently large n . ■

What about logarithm functions? For fixed bases a and b , the change of base formula (Fact 19.6 on page 449) says

$$\frac{\log_a(n)}{\log_b(n)} = \frac{\frac{\log_{10}(n)}{\log_{10}(a)}}{\frac{\log_{10}(n)}{\log_{10}(b)}} = \frac{\log_{10}(b)}{\log_{10}(a)}.$$

Thus $\log_a(n) = \frac{\log_{10}(b)}{\log_{10}(a)} \log_b(n) = A \log_b(n)$ for a fixed constant $A = \frac{\log_{10}(b)}{\log_{10}(a)}$. This implies $\log_a(n)$ is $O(\log_b(n))$ regardless of the bases a and b . In other words, $\log_a(n) \leq \log_b(n)$ and $\log_b(n) \leq \log_a(n)$, for a and b . Let's adopt the notation $f(n) \simeq g(n)$ to mean that both $f(n) \leq g(n)$ and $g(n) \leq f(n)$ hold. Then we have, for instance,

$$\log_2(n) \simeq \log_3(n) \simeq \log_4(n) \simeq \log_5(n) \simeq \dots$$

In other words, any two logarithm functions have the *same order*.

Since a logarithm's base has no bearing on its order, we will finish our investigation using \log_2 .

Proposition 20.4 The function $\log_2(n)$ is $O(n)$, but n is not $O(\log_2(n))$. Also, the constant function 1 is $O(\log_2(n))$, but $\log_2(n)$ is not $O(1)$.

Proof. Observe that $n < 2^n$ holds for all positive integers n . (This should be obvious, or you can prove it with induction.) Therefore, for all $n > 2$ we have

$$\begin{aligned} 2 &< n < 2^n \\ \log_2(2) &< \log_2(n) < \log_2(2^n) \\ 1 &< \log_2(n) < n. \end{aligned}$$

(In taking logs in the second step here, we used the fact that $\log_2(n)$ is an *increasing* function, that is, $x < y$ implies $\log_2(x) < \log_2(y)$. Thus taking \log_2 did not reverse any $<$.) Note that $1 < \log_2(n)$ for $n > 2$ means 1 is $O(\log_2(n))$, and $\log_2(n) < n$ means $\log_2(n)$ is $O(n)$.

But n is **not** $O(\log_2(n))$ because if it were, there would be a positive A for which $n \leq A \log_2(n)$ for all $n > N$, for some N . From this we would get $2^n \leq 2^{A \log_2(n)}$ for all $n > N$. This becomes $2^n \leq (2^{\log_2(n)})^A = n^A$ for all $n > N$, meaning 2^n is $O(n^A)$, which contradicts Proposition 20.3.

To see that $\log_2(n)$ is not $O(1)$, suppose it were. Then $\log_2(n) \leq A \cdot 1$ for all sufficiently large n . But this is a contradiction, for as long as $n > 4^A$, we have $\log_2(n) > \log_2(4^A) = A \log_2(4) = 2A > A$. ■

The previous four propositions confirm the chain (20.1) on page 456, repeated here for emphasis:

$$1 < \log_2(n) < n < n^2 < n^3 < n^4 < \dots < 2^n < 3^n < 4^n < 5^n < \dots < n! < n^n.$$

(Actually, two new entries $n!$ and n^n have been slipped in on the right. Regarding them, see the exercises 6 and 7 below.)

Regarding the functions $f(n)$ that appear on this list, if $f(n)$ is the worst-case performance of an algorithm, we would want $f(n)$ to be as far to the left as possible, for efficiency improves the further left we can go. An algorithm whose worst-case performance was $f(n) = n!$ or $f(n) = n^n$ would be a very bad algorithm, usable only for small values of n . We will continue to develop these ideas in the remaining sections of the chapter.

Exercises for Section 20.1

1. Show that $f(n) = 3 + n + 2^n$ is $O(2^n)$.
2. Show that $f(n) = 2n^4 + n^2 - n - 3$ is $O(n^4)$.
3. Show that $f(n) = 25 + 8n + \log_2(n)$ is $O(n)$.
4. Show that $f(n) = \log_2(n) \cdot n^3$ is $O(n^4)$.
5. Show that $f(n) = n \log_2(n)$ is $O(n^2)$, but n^2 is not $O(n \log_2(n))$. (See Figure 20.2.)
6. Show that the function $f(n) = n!$ is $O(n^n)$, but n^n is not $O(n!)$.
7. Show that the function $f(n) = 2^n$ is $O(n!)$, but $n!$ is not $O(2^n)$. (See Figure 20.2.)
8. Two different algorithms, Algorithm 1 and Algorithm 2, accomplish the same task. Algorithm 1 has worst-case performance $f(n)$ and Algorithm 2 has worst-case performance $g(n)$ (where n is the input size). Say these algorithms run on two different computers: Computer 1 and Computer 2, respectively.
 - (a) Suppose $f(n)$ is $O(g(n))$. Show that there exists a number B such that if Computer 1 is B times faster than Computer 2, then Algorithm 1 will always finish before Algorithm 2 when each is run on the same input.
 - (b) Suppose $f(n)$ is **not** $O(g(n))$. Show that no matter how fast Computer 1 is, there are some inputs for which Algorithm 1 is slower than Algorithm 2.
9. Show that the relation $<$ (defined on page 456) is a transitive relation on the set of all real-valued functions on $(0, \infty)$. That is, show that $f(n) < g(n)$ and $g(n) < h(n)$ implies $f(n) < h(n)$.
10. On page 458 we defined $f(n) \simeq g(n)$ if both $f(n)$ is $O(g(n))$ and $g(n)$ is $O(f(n))$. Prove that \simeq is an equivalence relation on the set of real-valued functions on $(0, \infty)$.

20.2 Polynomial Algorithms

Big-O notation is useful for measuring the efficiency of algorithms. Suppose an algorithm has worst-case performance $f(n)$ steps to process an input of size n . If $f(n)$ is $O(g(n))$, we say that the **algorithm is $O(g(n))$** . In practice, the function $f(n)$ can be fairly complex, as it is based on the idiosyncrasies of the particular algorithm. But usually a $g(n)$ can be found that is a simple function (such as a power or exponential function). Then $g(n)$ is a simple, meaningful generic measure of the algorithm's complexity.

To help transform $f(n)$ to a simpler $g(n)$, we have the following.

Proposition 20.5 If $f(n) = f_1(n) \pm f_2(n) \pm \dots \pm f_k(n)$ and each $f_i(n)$ is $O(g(n))$, then $f(n)$ is $O(g(n))$.

Proof. (Direct) Suppose each $f_i(n)$ is $O(g(n))$. This means there exist positive numbers A_1, A_2, \dots, A_k and N_1, N_2, \dots, N_k , such that, for each index i , the inequality $|f_i(n)| \leq A_i |g(n)|$ holds for all $n \geq N_i$. Put $A = A_1 + A_2 + \dots + A_k$. Let $N = \max\{N_1, N_2, \dots, N_k\}$, that is, N is the largest of the N_i . If $n > N$, then

$$\begin{aligned} |f(n)| &= |f_1(n) \pm f_2(n) \pm \dots \pm f_k(n)| \\ &\leq |f_1(n)| + |f_2(n)| + \dots + |f_k(n)| \\ &\leq A_1 |g(n)| + A_2 |g(n)| + \dots + A_k |g(n)| \\ &\leq (A_1 + A_2 + \dots + A_k) \cdot |g(n)| \\ &\leq A \cdot |g(n)|. \end{aligned}$$

This means $f(n)$ is $O(g(n))$. ■

Proposition 20.6 Suppose $f_1(n)$ is $O(g_1(n))$ and $f_2(n)$ is $O(g_2(n))$. Then the product $f_1(n)f_2(n)$ is $O(g_1(n)g_2(n))$.

Proof. (Direct) Suppose $f_1(n)$ is $O(g_1(n))$ and $f_2(n)$ is $O(g_2(n))$. Definition 20.1 says there exist positive numbers A_1 and N_1 , and A_2 and N_2 , such that $|f_1(n)| \leq A_1 \cdot |g_1(n)|$ for all $n \geq N_1$, and $|f_2(n)| \leq A_2 \cdot |g_2(n)|$ for all $n \geq N_2$. Let $A = A_1 \cdot A_2$ and let $N = \max\{N_1, N_2\}$. Then if $n > N$, the following holds:


$$\begin{aligned} |f_1(n)f_2(n)| &= |f_1(n)| \cdot |f_2(n)| \\ &\leq A_1 \cdot |g_1(n)| \cdot A_2 \cdot |g_2(n)| \\ &\leq A_1 \cdot A_2 \cdot |g_1(n)g_2(n)| \\ &\leq A \cdot |g_1(n)g_2(n)|. \end{aligned}$$

This means $f_1(n)f_2(n)$ is $O(g_1(n)g_2(n))$. ■

Example 20.2 Show that the function $f(n) = 5n^3 - n^2 \log_2(n) + 8$ is $O(n^3)$.

Solution: Our strategy is to show that each functions $5n^3$, $n^2 \log_2(n)$ and 8 is $O(n^3)$, for then Proposition 20.5 implies $5n^3 - n^2 \log_2(n) + 8$ is $O(n^3)$.

First, the constant function 5 is $O(1)$, and n^3 is $O(n^3)$, so Proposition 20.6 implies $5n^3$ is $O(n^3)$. Second, Proposition 20.4 says $\log_2(n)$ is $O(n)$, so by Proposition 20.6, $n^2 \log_2(n)$ is $O(n^2 n) = O(n^3)$. Finally, the constant function 8 is clearly $O(n^3)$.

Our strategy is successful, so $f(n) = 5n^3 - n^2 \log_2(n) + 8$ is $O(n^3)$. 

The methods used to solve this example also work to establish two simple corollaries. First, any polynomial $f(n) = a_0 + a_1 n + a_2 n^2 + \dots + a_d x^d$ is $O(n^d)$.

Corollary 20.1 Any polynomial $f(n)$ of degree d is $O(n^d)$.

Corollary 20.2 If $f(n)$ is $O(g(n))$, and c is a constant, then $cf(n)$ is $O(g(n))$.

Now we arrive at two significant definitions. An algorithm is called a **polynomial-time algorithm** if its worst-case performance for input size n is $f(n)$, where $f(n)$ is $O(g(n))$, for some polynomial $g(n)$. (Equivalently, an algorithm is a polynomial-time algorithm if $f(n)$ is $O(n^d)$, for some power function n^d .)

An algorithm is called an **exponential-time algorithm** if it is not a polynomial algorithm, and its worst-case performance for input size n is $f(n)$, where $f(n)$ is $O(a^n)$, for some exponential function a^n .

Figure 20.2 suggests that polynomial-time algorithms are much quicker than exponential-time algorithms. In fact, computer scientists regard exponential-time algorithms as little better than useless, at best. For example, if an algorithm's worst-case performance is $f(n) = 2^n$, then even with a modest input size of $n = 60$, the number 2^{60} of steps needed to finish is so great that even on the fastest computer it could need over 3 centuries to finish. And even if we got a computer that was twice as fast, and it only needed 1.5 centuries to finish, consider that all we'd have to do is give it an input of size 61, and we are back to 3 centuries!

By contrast, a polynomial-time algorithm will get a job done in a negligible (or reasonable) amount of time, even when the input is quite large. For this reason, it is important to analyze the time-complexity of the algorithms we use or write. Always aim for polynomial-time.

The next two sections examine two case studies.

20.3 Case Study: Sequential Search Versus Binary Search

Let's use our new knowledge to compare the time-complexity of sequential search (Algorithm 8 on page 192) with that of binary search (Algorithm 9 on page 194). These two different algorithms accomplish the same thing: Determine whether a certain number z appears as an entry of a length- n list X of numbers in numeric order.

Recall that sequential search merely traverses the list from left to right, stopping only when it encounters an entry equal to z , or reaches the end of the list without finding z . In the worst case, it might have visit all n entries; indeed, on page 192 we computed its worst-case performance as $f(n) = 2 + 2n$ steps. As this is a polynomial of degree 1, Corollary 20.1 says $f(n)$ is $O(n)$. In our new parlance, the sequential search algorithm is an $O(n)$ polynomial algorithm.

The binary search algorithm (page 194) is more complex, but faster than sequential search. Recall that it jumps to the middle of the list, compares z to the middle entry, and then ignores either the left- or right-half of the list, depending on whether the middle entry is less than or greater than z . Then it repeats this procedure on the new half-sized list, etc., until it encounters z or finds that it is not in the list. At the end of Section 6.6 we found that its worst-case performance is $3 + 2\lceil \log_2(n) \rceil$ steps. Although there is nothing problematic about rounding the logarithm up here, it is not quite a perfect fit for Proposition 20.4. To remedy this, note that $\log_2(n) \leq \lceil \log_2(n) \rceil \leq \log_2(n) + 1$, so we are safe in saying that the algorithm takes no more than $f(n) = 3 + 2(\log_2(n) + 1) = 5 + 2\log_2(n)$ steps.

Then $f(n) = 5 \cdot 1 + 2 \cdot \log_2(n)$. Here the functions 1 and $\log_2(n)$ are both $O(\log_2(n))$, by Proposition 20.4, so Proposition 20.5 with Corollary 20.2 imply that $f(n)$ is $O(\log_2(n))$. Consequently, the binary search algorithm is $O(\log_2(n))$. This is better than the $O(n)$ sequential search algorithm, as $\log_2(n) < n$.

Here is a significant point. Even though binary search is $O(\log_2(n))$, and $\log_2(n)$ is not a polynomial, we still consider binary search to be a polynomial algorithm. The reason for this is that its worse case run-time $f(n) = 5 + 2\log_2(n)$ is also $O(n)$, by Proposition 20.4, Proposition 20.5 and Corollary 20.2. But although we classify it as a polynomial algorithm, we say that its time-complexity is $O(\log_2(n))$, because this is an order of magnitude better than $O(n)$.

20.4 Case Study: Bubble Sort Versus Merge Sort

At the end of Section 6.3, we devised the bubble sort algorithm (Algorithm 5, page 182). It inputs a list of numbers and sorts them into numerical order. For example, with input $X = (5, 3, 5, 7, 4)$, the output is $X = (3, 4, 5, 5, 7)$. For convenience, the code from page 182 is repeated here. (You may want to quickly review the discussion and explanation preceding page 182.)

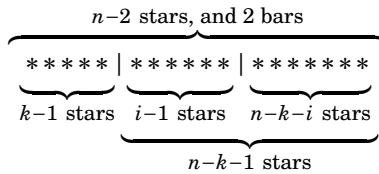
Algorithm 5: bubble sort

```

Input: A list  $X = (x_1, x_2, \dots, x_n)$  of numbers
Output: The list sorted into numeric order
begin
  for  $k := 1$  to  $n - 1$  do
    for  $i := 1$  to  $n - k$  do
      if  $x_i > x_{i+1}$  then
         $temp := x_i$  ..... temporarily holds value of  $x_i$ 
         $x_i := x_{i+1}$ 
         $x_{i+1} := temp$  ..... now  $x_i$  and  $x_{i+1}$  are swapped
      end
    end
  end
  output  $X$  ..... now  $X$  is sorted
end

```

Let's analyze the performance of this algorithm. The if-statement inside the nested for loops is executed once for each pair (k, i) of integers with $1 \leq k \leq n - 1$, and $1 \leq i \leq n - k$. In other words, once for each pair (k, i) with $0 \leq k - 1 \leq n - 2$, and $0 \leq i - 1 \leq n - k - 1$. We can model such pairs as lists of length n , made of $n - 2$ stars and 2 bars. There are $k - 1$ stars before the first bar, and $i - 1$ stars between the two bars.



For example, suppose $n = 8$. Then $***|*|**$ corresponds to $(k, i) = (4, 2)$, whereas $**||***$ corresponds to $(k, i) = (4, 1)$. Also $|*****|$ means $(k, i) = (1, 7)$, and $||*****$ is $(k, i) = (1, 1)$. The number of such lists is $\binom{n}{2} = \frac{n(n-1)}{2} = \frac{1}{2}n^2 - \frac{1}{2}n$, the number of ways to choose 2 out of n spots for the bars. So the if-statement gets executed $\frac{1}{2}n^2 - \frac{1}{2}n$ times, and at worst it executes 3 statements. Thus the worst-case performance of bubble sort is $\frac{3}{2}n^2 - \frac{3}{2}n$ steps. Consequently bubble sort is an $O(n^2)$ polynomial algorithm.

Now, $O(n^2)$ is not bad. But there is another sort algorithm that is better. It is called **merge sort**. It is also polynomial, but its worst-case performance is $O(n \log_2(n))$. (Note $O(n \log_2(n))$ is better than $O(n^2)$ by Exercise 20.1.5.)

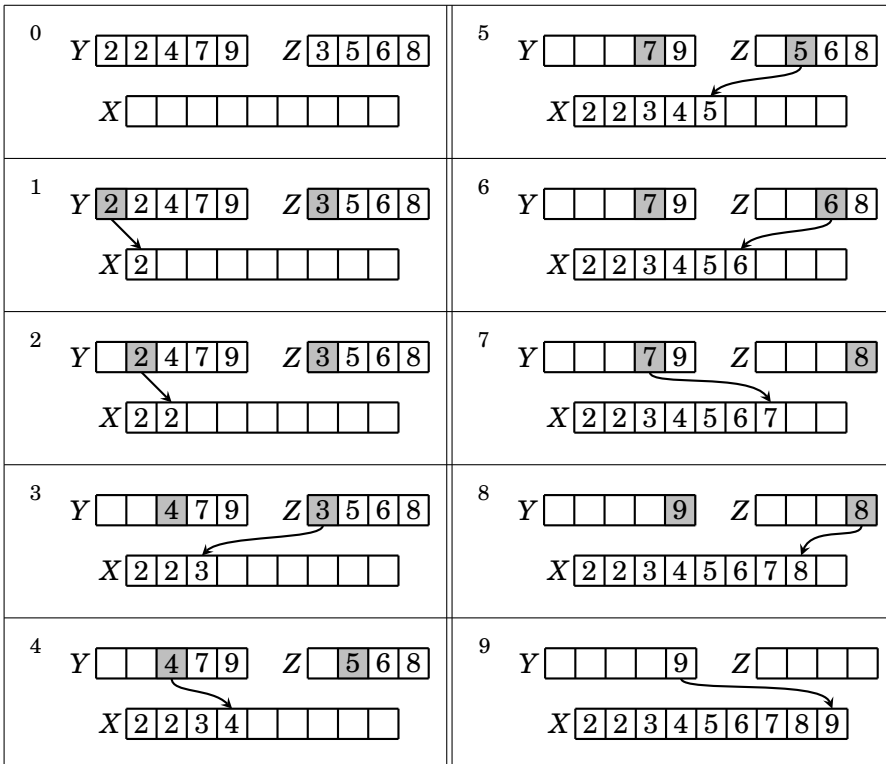
A big piece of the merge sort algorithm involves “merging” two sorted lists Y and Z into a single sorted list X . The idea is to start with $X = ()$, then continually compare the left-most entries of Y and Z , always removing the smaller one and appending it to the end of X , until Y and Z are used up.

To illustrate, say $Y = (2, 2, 4, 7, 9)$ and $Z = (3, 5, 6, 8)$. Step 1 compares the first entries of both Y and Z . The first entry 2 of Y is smaller than the first entry 3 of Z . So remove 2 from Y and make it the first entry of X , so $X = (2)$. Now Y is one entry shorter than it was previously.

Step 2 compares the first entries of Y and Z . Again, the first entry 2 of Y is smaller than the first entry 3 of Z . So remove 2 from Y and make it the next entry of X . Now $X = (2, 2)$ and Y has been shortened once again.

For step 3, compare the first entries of both Y and Z . This time the first entry 3 of Z is smaller than the first entry 4 of Y . So remove 3 from Z and make it the next entry of X . Now Z has been shortened.

Repeat until all entries of Y and Z have been removed and put onto X , as shown below. In the end, X is a sorted merging of Y and Z .



In the example above, notice that after step 8 all the entries of Z have been removed. At this point we attach whatever entries are left on Y to the end of X . Likewise, if at some point all the entries of Y had been removed, then we'd append the remaining entries of Z to X .

Here is pseudocode for merging sorted lists Y and Z into a sorted list X . It is a procedure called `Merge` whose input is the two lists Y and Z , and whose output is the merged list X . Rather than actually removing entries from Y and Z , it maintains two indices i and j that indicate the current "first" entries of Y and Z , respectively. Initially $i = j = 1$. Then every time an entry of Y is "removed," i increases by 1. Every time an entry of Z is "removed," j increases by 1.

```

Procedure Merge( $Y, Z$ ).       $Y$  and  $Z$  are sorted lists to be merged


---


begin
   $i := 1$  ..... index for list  $Y = (y_1, \dots, y_\ell)$ , initially  $y_i = y_1$ 
   $j := 1$  ..... index for list  $Z = (z_1, \dots, z_m)$ , initially  $z_j = z_1$ 
   $k := 0$  ..... index for merged list  $X = (x_1, \dots, x_{\ell+m})$ 
  while  $(i \leq \ell) \vee (j \leq m)$  do
     $k := k + 1$  ..... advance to fresh entry of  $X$ 
    if  $(i \leq \ell) \wedge (j \leq m)$  then
      if  $y_i \leq z_j$  then
         $x_k := y_i$  .....  $x_k$  gets  $y_i$  because  $y_i \leq z_j$ 
         $i := i + 1$  ..... move to next entry of  $Y$ 
      else
         $x_k := z_j$  .....  $x_k$  gets  $z_j$  because  $z_j < y_i$ 
         $j := j + 1$  ..... move to next entry of  $Z$ 
      end
    else
      if  $i > \ell$  then
         $x_k := z_j$  } ..... if reached,  $Y$  is used up;
         $j := j + 1$  } ..... use entries of  $Z$ 
      else
         $x_k := y_i$  } ..... if reached,  $Z$  is used up;
         $i := i + 1$  } ..... use entries of  $Y$ 
      end
    end
  end
end

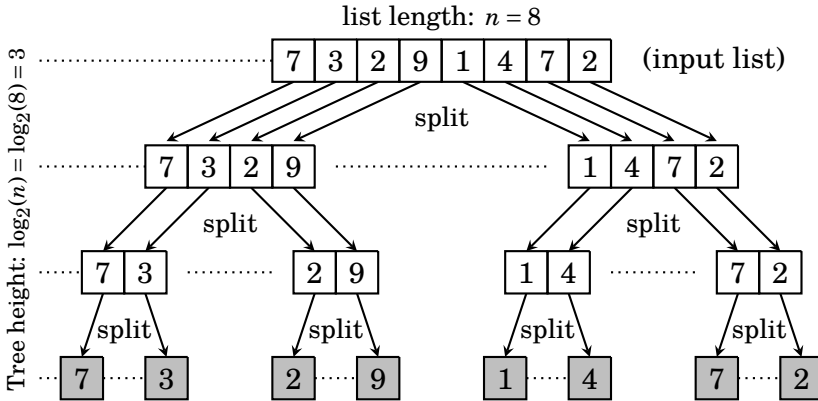

---



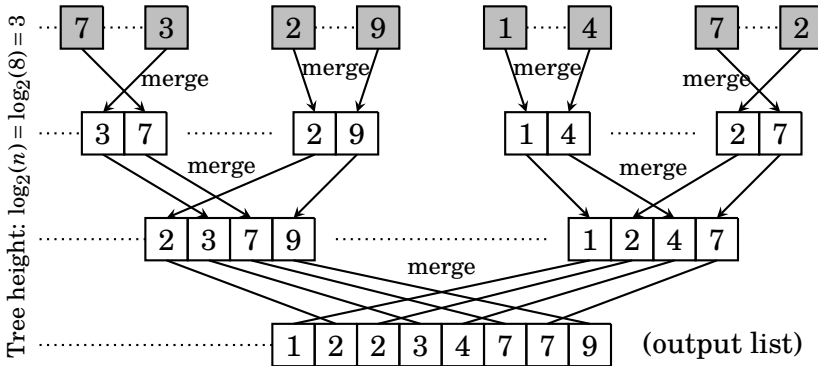
```

Notice that if Y has ℓ entries and Z has m entries, then `Merge` merges them in $3 + 2(\ell + m)$ steps, so it is $O(\ell + m)$.

Now that we can merge two sorted lists into one sorted list with Merge, we can explain MergeSort, an algorithm that sorts a length- n list in $O(n \log_2(n))$ time. For simplicity, first consider a list whose length is a power of 2, like $n = 2^3 = 8$. Imagine that its entries are written on movable cards. Begin by splitting the list in half, into two smaller lists. Then split these half-lists in half, and continue until you can't split any further.

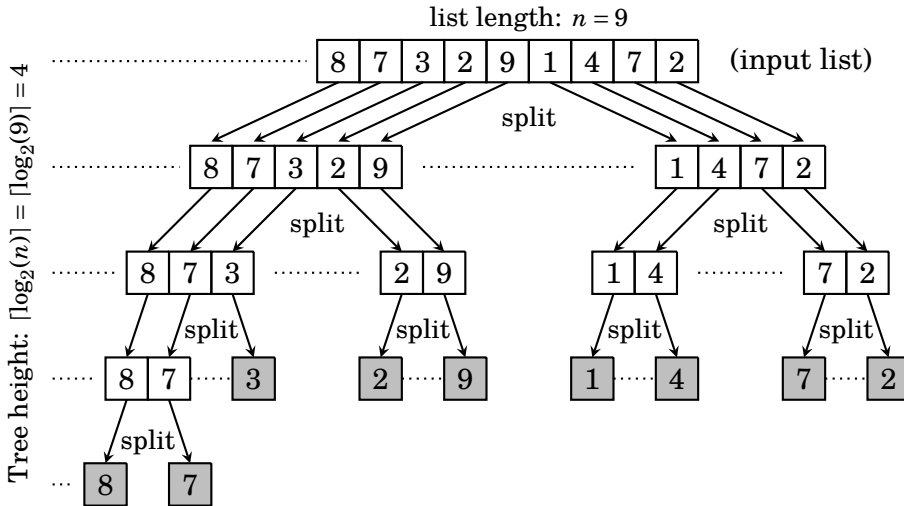


Now we have 8 lists of length 1, and each one is already sorted by default! Next merge these with Merge in the reverse order in which they were split.

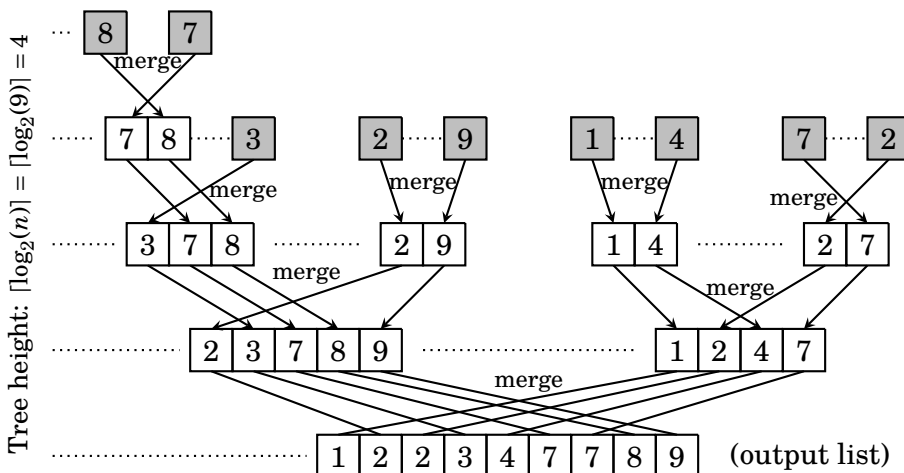


This is our sorted list. We will shortly write the MergeSort procedure to follow these steps. But first, let's count the number of steps (card movements) made in sorting the above example list of length $n = 2^k$. The first list-splitting phase made an inverted tree of height $\log_2(n) = \log_2(2^k) = k$ (in our example, $k = 3$). At each level of the tree we had to move all n cards, so the total number of moves in the "splitting" phase is $n \log_2(n)$. In the second "merging" phase we had to make another $n \log_2(n)$ moves. Summary: You can sort a list of length $n = 2^k$ cards with $2n \log_2(n)$ card movements.

The previous page's example was simplified by the assumption that the list's length was a power of 2. If this is not the case, then not every splitting operation will result in two equal-sized half-lists. You may have to split into two lists of lengths $\lceil \frac{n}{2} \rceil$ and $\lfloor \frac{n}{2} \rfloor$, respectively. This is illustrated below with a list of length 9.



We had to go an extra level down to fully split our list into length-1 lists. The tree height increased to $\lceil \log_2(n) \rceil = \lceil \log_2(9) \rceil = 4$. The total number of card movements in this splitting phase is never more than n card moves per level, that is, $n \lceil \log_2(n) \rceil$. Reversing this process—but merging instead of splitting—gives our final sorted list in just $2n \lceil \log_2(n) \rceil$ card movements.



Summary: You can sort n cards with $2n \lceil \log_2(n) \rceil$ or fewer card moves.

Now we implement this idea and actually write `MergeSort`, a procedure that takes an input list X of numbers and returns X sorted into numeric order. That is, `MergeSort`(X) is a rearrangement of X into numeric order.

`MergeSort` uses the procedure `Merge`, described on page 465. But it is also recursive, calling itself. If the input list X happens to have length 0 or 1, then X is automatically already sorted, so `MergeSort`(X) just returns X . Otherwise `MergeSort` splits $X = (x_1, x_2, \dots, x_n)$ into two lists $Y = (x_1, x_2, \dots, x_{\lceil \frac{n}{2} \rceil})$ and $Z = (x_{\lceil \frac{n}{2} \rceil + 1}, \dots, x_{n-1}, x_n)$ that are each no longer than half the length of X . Then it returns `Merge`(`MergeSort`(Y), `MergeSort`(Z)).

```

Procedure MergeSort( $X$ ).            $X = (x_1, x_2, \dots, x_n)$  is list to be sorted


---


1 begin
2   if  $\ell \leq 1$  then
3     |   return  $X$    .....  $X$  has length 1 or 0, so it is already sorted
4   else
5     |    $Y := (x_1, x_2, \dots, x_{\lceil \frac{n}{2} \rceil})$  .....  $Y$  is half of  $X$ 
6     |    $Z := (x_{\lceil \frac{n}{2} \rceil + 1}, \dots, x_{n-1}, x_n)$  .....  $Z$  is other half
7     |   return Merge( MergeSort( $Y$ ), MergeSort( $Z$ ) )
8   end
9 end

```

Proposition 20.7 For any list X of numbers, `MergeSort`(X) really does return X sorted into numeric order.

Proof. We use strong induction on n to prove that `MergeSort` does indeed sort its input correctly. For the basis case, if $n = 0$ or $n = 1$, then its pseudocode reveals that `MergeSort`(X) returns X , unchanged, in line 3. This is the correct result, because as a list of length 0 or 1, X is already sorted.

For the inductive step we need to show that if $k > 1$ and `MergeSort` correctly sorts any list of length shorter than k , then `MergeSort` correctly sorts any list of length k .

We use direct proof. Suppose $k > 1$ and `MergeSort` correctly sorts any list of length shorter than k . Let X be a list of length k . Note that in this case `MergeSort`(X) splits X into two shorter lists Y and Z (lines 5 and 6), and then returns `Merge`(`MergeSort`(Y), `MergeSort`(Z)) in line 7. Now, Y and Z each has length shorter than k , so by the induction hypothesis, `MergeSort`(Y) and `MergeSort`(Z) are correct sortings of the two halves Y and Z of X . Thus the returned list `Merge`(`MergeSort`(Y), `MergeSort`(Z)) is a correct sorting of X . ■

Next we prove that MergeSort is $O(n \log_2(n))$. (You may already believe this, based on the diagrams from several pages back.) The proof is a good illustration of strong induction and logarithm properties.

Proposition 20.8 MergeSort(X) is $O(n \log_2(n))$, where X has length n .

Proof. Our strategy is to show that if X has length n , then MergeSort(X) sorts X in no more than $f(n) = 1 + 5n \log_2(n)$ steps. This will imply that MergeSort(X) is $O(n \log_2(n))$, because if $n > 1$, then $1 \leq n \log_2(n)$, so

$$1 + 5n \log_2(n) \leq n \log_2(n) + 5n \log_2(n) = 6n \log_2(n),$$

and therefore $|f(n)| \leq A \cdot |n \log_2(n)|$ for $A = 6$ and $n \geq N = 1$.

So to complete the proof, we now prove that MergeSort(X) sorts X in no more than $f(n) = 1 + 5n \log_2(n)$ steps. The proof is by strong induction on n .

For the basis step, if $n = 1$, then X has length 1, and MergeSort(X) returns X in 1 step. As $f(1) = 1 + 1 \log_2(1) = 1 + 1 \cdot 0 = 1$, we see that indeed MergeSort(X) sorts X in no more than $f(1)$ steps.

Now for the inductive step. Let $n > 2$. Suppose that if X has length $k < n$, then MergeSort(X) takes no more than $f(k)$ steps. Now assume X has length n . We must show that MergeSort(X) takes no more than $f(n)$ steps.

Case 1. Say n is even. Let's count steps for MergeSort(X). The procedure goes straight to lines 5 and 6, and creates lists Y and Z , each of length $\frac{n}{2}$. It takes $\frac{n}{2} + \frac{n}{2} = n$ steps to fill in these new lists (one assignment per entry). Next comes line 7, which returns Merge(MergeSort(Y), MergeSort(Z)). By the inductive hypothesis, MergeSort(Y) and MergeSort(Z) each take no more than $f(\frac{n}{2})$ steps, and then Merge takes $3 + 2(\frac{n}{2} + \frac{n}{2}) = 3 + 2n$ steps (by the remark at the bottom of page 465). Therefore MergeSort(X) makes a total of $n + 2f(\frac{n}{2}) + 3 + 2n = 3n + 3 + 2f(\frac{n}{2})$ steps. This number of steps is

$$\begin{aligned} 3n + 3 + 2f\left(\frac{n}{2}\right) &= 3n + 3 + 2\left(1 + 5 \cdot \frac{n}{2} \log_2\left(\frac{n}{2}\right)\right) && \text{(definition of } f) \\ &= 3n + 3 + 5n \log_2\left(\frac{n}{2}\right) \\ &= 3n + 3 + 5n(\log_2(n) - \log_2(2)) && \text{(log property)} \\ &= 3n + 3 + 5n(\log_2(n) - 1) && \text{(log property)} \\ &= (1 + 5n \log_2(n)) + (4 - 2n) \\ &= f(n) + (4 - 2n) && (f(n) = 1 + 5n \log_2(n)) \\ &\leq f(n). && \text{(because } 4 - 2n \leq 0) \end{aligned}$$

We have just shown that MergeSort(X) takes no more than $f(n)$ steps.

Case 2. Suppose n is odd. The procedure goes straight to lines 5 and 6, and creates lists Y and Z . This time Y has length $\frac{n+1}{2}$ and Z has length $\frac{n-1}{2}$. It takes $\frac{n+1}{2} + \frac{n-1}{2} = n$ steps to fill in these new lists (one assignment per entry). Next comes line 7, which returns $\text{Merge}(\text{MergeSort}(Y), \text{MergeSort}(Z))$. By the inductive hypothesis, $\text{MergeSort}(Y)$ takes no more than $f(\frac{n+1}{2})$ steps, and $\text{MergeSort}(Z)$ takes no more than $f(\frac{n-1}{2})$ steps, and then Merge takes $3 + 2(\frac{n+1}{2} + \frac{n-1}{2}) = 3 + 2n$ steps. Therefore $\text{MergeSort}(X)$ makes a total of $n + f(\frac{n+1}{2}) + f(\frac{n-1}{2}) + 3 + 2n = 3n + 3 + f(\frac{n+1}{2}) + f(\frac{n-1}{2})$ steps. Applying the definition of f , this number of steps is

$$\begin{aligned}
& 3n + 3 + \left(1 + 5 \cdot \frac{n+1}{2} \log_2 \left(\frac{n+1}{2}\right)\right) + \left(1 + 5 \cdot \frac{n-1}{2} \log_2 \left(\frac{n-1}{2}\right)\right) \\
&= 3n + 5 + \frac{5}{2} \left[(n+1) \log_2 \left(\frac{n+1}{2}\right) + (n-1) \log_2 \left(\frac{n-1}{2}\right) \right] \\
&< 3n + 5 + \frac{5}{2} \left[(n+1) \log_2 \left(\frac{n+1}{2}\right) + (n+1) \log_2 \left(\frac{n-1}{2}\right) \right] \\
&= 3n + 5 + \frac{5}{2} \left[n \left(\log_2 \left(\frac{n+1}{2}\right) + \log_2 \left(\frac{n-1}{2}\right) \right) + \left(\log_2 \left(\frac{n+1}{2}\right) - \log_2 \left(\frac{n-1}{2}\right) \right) \right] \\
&= 3n + 5 + \frac{5}{2} \left[n \log_2 \left(\frac{n+1}{2} \cdot \frac{n-1}{2}\right) + \log_2 \left(\frac{n+1}{n-1}\right) \right] \\
&= 3n + 5 + \frac{5}{2} n \log_2 \left(\frac{n^2-1}{4}\right) + \frac{5}{2} \log_2 \left(\frac{n+1}{n-1}\right) \\
&= 3n + 5 + \frac{5}{2} n (\log_2(n^2-1) - \log_2(4)) + \frac{5}{2} \log_2 \left(\frac{n+1}{n-1}\right) \\
&= -2n + 5 + \frac{5}{2} n \log_2(n^2-1) + \frac{5}{2} \log_2 \left(\frac{n+1}{n-1}\right) \\
&= (1 + 5 \log_2(n)) + 4 - 2n - \frac{5}{2} 2 \log_2(n) + \frac{5}{2} n \log_2 \left(\frac{n^2-1}{4}\right) + \frac{5}{2} \log_2 \left(\frac{n+1}{n-1}\right) \\
&= f(n) + 4 - 2n - \frac{5}{2} \log_2(n^2) + \frac{5}{2} n \log_2(n^2-1) + \frac{5}{2} \log_2 \left(\frac{n+1}{n-1}\right) \\
&= f(n) + 4 - 2n + \frac{5}{2} n \log_2 \left(\frac{n^2-1}{n^2}\right) + \frac{5}{2} \log_2 \left(\frac{n+1}{n-1}\right) \\
&\leq f(n)
\end{aligned}$$

In the last step we dropped $4 - 2n + \frac{5}{2} n \log_2 \left(\frac{n^2-1}{n^2}\right) + \frac{5}{2} \log_2 \left(\frac{n+1}{n-1}\right)$ because it is negative, and replaced the equality with \leq . (That the expression is negative is left to you to verify. Consider using calculus to show that it is a decreasing function that is negative for $n \geq 3$.) We have now shown that $\text{MergeSort}(X)$ takes no more than $f(n)$ steps. \blacksquare

20.5 Solutions for Chapter 20

1. Show that $f(n) = 3 + n + 2^n$ is $O(2^n)$.

Solution: As long as $n > 2$ we have $3 \leq 2^n$ and $n \leq 2^n$, so $|f(n)| = |3 + n + 2^n| \leq |2^n + 2^n + 2^n| = |3 \cdot 2^n| = 3 \cdot |2^n|$. Therefore, for $n > N = 2$ and $A = 3$ we have $|f(n)| \leq A \cdot |2^n|$, so by definition $f(n)$ is $O(2^n)$.

3. Show that $f(n) = 25 + 8n + \log_2(n)$ is $O(n)$.

Solution: If $n > 4$, then $25 \leq 8n$ and $\log_2(n) \leq 8n$, so $|f(n)| = |25 + 8n + \log_2(n)| \leq |8n + 8n + 8n| = |24n| = 24 \cdot |n|$. Therefore, for $n > N = 4$ and $A = 24$ we have $|f(n)| \leq A \cdot |n|$, so by definition $f(n)$ is $O(n)$.

5. Show that $f(n) = n \log_2(n)$ is $O(n^2)$, but n^2 is not $O(n \log_2(n))$.

Solution: If $n > 1$, then $n \leq 2^n$, so $\log_2(n) \leq \log_2(2^n) = n$. Hence $n \log_2(n) \leq n \cdot n = n^2$. Thus for $n > N = 1$ and $A = 1$, we have $|n \log_2(n)| \leq A \cdot |n^2|$, so $n \log_2(n)$ is $O(n^2)$.

Next, suppose for the sake of contradiction that n^2 is $O(n \log_2(n))$. Then there are positive numbers N and A for which $n^2 \leq A n \log_2(n)$ whenever $n > N$. So if $n > N$, then $n \leq A \log_2(n)$. Thus n is $O(\log_2(n))$, contradicting Proposition 20.4.

7. Show that the function $f(n) = 2^n$ is $O(n!)$, but $n!$ is not $O(2^n)$.

Solution: If $n > N = 2$, then $|2^n| = \underbrace{2 \cdot 2 \cdots 2}_{n \text{ times}} \leq \underbrace{n(n-1)(n-2) \cdots 3 \cdot 2 \cdot 1}_{n \text{ factors}} = 1 \cdot |n!|$. This

means 2^n is $O(n!)$. Next, suppose for the sake of contradiction that $n!$ is $O(2^n)$. Then there are positive numbers N and A for which $n! \leq A \cdot 2^n$ whenever $n > N$. So if $n > N$, then $n! \leq A \cdot 2^n$, and thus $A \geq \frac{2 \cdot 2 \cdots 2}{n(n-1)(n-2) \cdots 3 \cdot 2 \cdot 1} < \frac{2 \cdot 2 \cdots 2}{n \cdot n \cdots n} = \left(\frac{2}{n}\right)^n$. Now, if $n > \frac{2}{A}$, then $\frac{2}{n} < A$. Further, if $n > 2$, then $\frac{2}{n} < 1$, and so $\left(\frac{2}{n}\right)^n < \frac{n}{2}$. Consequently, if $n \geq \max\{N, \frac{2}{A}, 2\}$, then $\left(\frac{2}{n}\right)^n < A$. This contradicts the fact (established above) that $A < \left(\frac{2}{n}\right)^n$ for all $n > N$.

9. Show the relation $<$ is a transitive relation on the set of all real-valued functions on $(0, \infty)$. That is, show that $f(n) < g(n)$ and $g(n) < h(n)$ implies $f(n) < h(n)$.

Suppose $f(n) < g(n)$ and $g(n) < h(n)$. This means $f(n)$ is $O(g(n))$ but $g(n)$ is not $O(f(n))$, and $g(n)$ is $O(h(n))$ but $h(n)$ is not $O(g(n))$. Because $f(n)$ is $O(g(n))$, there are positive numbers N_1 and A_1 for which $|f(n)| \leq A_1 \cdot |g(n)|$ for all $n > N_1$. Because $g(n)$ is $O(h(n))$, there are positive numbers N_2 and A_2 for which $|g(n)| \leq A_2 \cdot |h(n)|$ for all $n > N_2$. Now put $N = \max\{N_1, N_2\}$ and $A = A_1 A_2$. Then for $n > N$ we have $|f(n)| \leq A_1 \cdot |g(n)| \leq A_1 \cdot A_2 \cdot |h(n)| = A \cdot |h(n)|$. Therefore $f(n)$ is $O(h(n))$.

To show that $f(n) < h(n)$, it remains to show that $h(n)$ is not $O(f(n))$. Suppose to the contrary that $h(n)$ is $O(f(n))$. Then there are positive numbers N and A for which $|h(n)| \leq A \cdot |f(n)|$ for all $n > N$. In particular, for $n > \max\{N, N_1\}$ we have $|h(n)| \leq A \cdot |f(n)| \leq A A_1 \cdot |g(n)|$. This means that $h(n)$ is $O(g(n))$, a contradiction.