Mathematical Problem Solving for Elementary School Teachers

Dennis E. White

April 15, 2013

Copyright

Preface

These notes were written over an ten year period in conjunction with the development of a mathematics course aimed at elementary education majors. The course had its inception in an *ad hoc* committee formed to address the Mathematical Association of America's document *A Call for Change*, which itself was a response to the National Council of Teachers of Mathematics' *Curriculum and Evaluation Standards*. *A Call for Change* calls for a restructuring of how we teach and what we teach elementary education students.

Certain fundamental principles guided the content and pedagogy of these notes.

i. The mathematical content is nontrivial and nonremedial. We assume the students have basic manipulative skills. We do not teach remedial skills. We do not teach many topics in a superficial way. The problems are, for the most part, nontrivial. Some topics are explored to a depth often found in junior and senior level courses. There is little emphasis placed on drill exercises or memorization.

ii. The general topics should conform to those described in *A Call for Change*. Topics include geometry, number theory, algebraic structures, analysis, probability and statistics.

iii. As also mentioned in *A Call for Change*, special emphasis is given to the interconnection of ideas, to the communication of mathematics and to problem solving skills. Material in these notes interconnect in various ways. Many problems emphasize communicating mathematical ideas both orally and in writing. Many of the problems are open-ended. Some can be solved using a variety of techniques.

iv. The course should be given in a non-threatening environment. It is intended that these notes be used in a cooperative learning environment. It is also intended that there would be less emphasis on tests and benchmarks. The experience the students using these notes have will be taken back to their own classrooms.

To the Students

These notes are substantially different from the mathematics textbooks you may be familiar with. There are no large bodies of exercises at the end of each section. There are few “drill” exercises. There is little repetition. The text is densely written and requires close and careful reading. Later chapters frequently refer to results, exercises, and ideas from earlier chapters.

However, these notes are meant to give you a greater understanding of (and maybe appreciation for) how mathematical problems are really solved. You will often be led through a series of exercises to an understanding of some fairly deep mathematical results. It is my belief that most students, with proper mathematical skills, can learn some fairly sophisticated mathematics.

These notes will probably require more effort on your part than perhaps you have put into other mathematics courses. This is on purpose. I believe that learning mathematics takes active participation, including testing hypotheses, constructing examples, forming strategies, and organizing ideas. All these things you must do. The notes can’t do them for you; your instructor can’t do them for you.

Learning mathematics is an active process. It is not possible to learn mathematics by reading a textbook like a novel. Good mathematics students, from elementary school to graduate school, read a math book with pencil and paper in hand.

Mathematics is not a collection of independent topics. It is not “Algebra I,” “Algebra II,” “Trigonometry,” “Plane Geometry,” etc. All of mathematics is interconnected in a fundamental way. In these notes, you will find some problems which require methods from several different mathematical “areas.” Other problems have more than one solution, each solution coming from a different mathematical “area.” Ideas learned in Chapter 2 will reappear in Chapter 7, Chapter 11 and Chapter 12. Chapter 12 uses ideas from Chapter 2, Chapter 5, Chapter 6, and Chapter 10.

The topics were chosen because they are related to material that is widely found in elementary school curricula. However, these topics are taught at a substantially deeper level. It is not the purpose of these notes to teach you elementary school mathematics.

As I mentioned above, it is my belief that most students, with proper mathematical skills, can learn the material in these notes. However, students without those prerequisite skills have great difficulty. Those skills include facility at handling fractions, powers, exponents and radicals in both numeric and algebraic contexts. Students should also understand the basics of analytic geometry: graphing functions, linear and quadratic equations, the quadratic formula, etc. They should also be somewhat familiar with logarithms and with techniques of counting.

Let me conclude with a word about calculators. For the most part, I have not discouraged the use of a calculator. Some exercises explicitly call for a calculator. However, besides the mathematical skills described in the preceding paragraph, another prerequisite is an understanding of “appropriate” calculator use. A calculator is not a substitute for mathematical common sense. It should not be used to divide 24 by 6, or to decide if $\frac{1}{2}$ is larger or smaller than $\frac{1}{3}$.

To the Instructors

These notes were designed to be used in a problem-solving environment. I feel they work best in a cooperative group setting. They are not designed to be lectured from, and I don't think they work particularly well in that role. Nevertheless, lectures do have a place in this course, if they are short and appropriate.

You will surely notice the paucity of drill exercises. While some mathematical topics do require drill exercises, my concentration in these notes is on problem-solving skills. If you feel your class needs extra drill exercises in a particular area, you are welcome to design your own.

Because there are few exercises, I expect that most classes will do a sizable percentage of them. I leave it to your judgment which to omit.

Many of the exercises are not routine. Many have more than one solution method. Consequently, your classroom role is much expanded over a typical lecture-style course.

A few of the exercises have been starred. The star means two things. First, the exercise is difficult. Second, the exercise is not in the main flow of ideas, and can be omitted.

The last chapter, Chapter 13, is an alternative to Chapter 8.

Acknowledgments

I would like to thank all the instructors and teaching assistants over the years who have helped me in the many revisions of these notes. I want to thank especially Bert Fristedt (who also provided Chapter 8) and Dennis Stanton for their many useful suggestions and comments.

Contents

List of Figures

List of Tables

Chapter 1

Number Sequences

In this chapter, we will describe various kinds of sequences of numbers. We will concentrate on the two most important kinds of sequences: arithmetic and geometric. From these, we will learn the two fundamental ways of describing sequences: explicit formulas and recursions. We will also learn how to sum the terms in these sequences. Finally, we will describe some other common sequences, including the Fibonacci numbers. Many other sequences will appear in subsequent chapters.

1.1 Recursions for Arithmetic and Geometric Sequences

One of the first things we learn about in mathematics is sequences of numbers. These sequences can be very simple, for instance, the counting numbers:

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

or the even numbers:

$$\{2,\ 4,\ 6,\ 8,\ \ldots\}\,.$$

Some are more complex, such as the powers of 10:

$$\{1,\ 10,\ 100,\ 1000,\ 10000,\ \ldots\}\,,$$

the perfect squares:

$$\{1,\ 4,\ 9,\ 16,\ 25,\ \ldots\}$$

or the prime numbers:

$$\{2,\ 3,\ 5,\ 7,\ 11,\ 13,\ \ldots\}\,.$$

Some include negative numbers:

$$\{-1,\ -2,\ 3,\ 4,\ -5,\ -6,\ 7,\ 8,\ \ldots\}$$

and some include fractions:

$$\{1,\ 1/2,\ 1/3,\ 1/4,\ 1/5,\ \ldots\}\,.$$

Some can be quite difficult to understand. For instance, the digits of π:

$$\{3,\ 1,\ 4,\ 1,\ 5,\ 9,\ \ldots\}\,.$$

At this point, we should issue a warning about our notation. We have given only the first few numbers in the sequence and have left it for you to guess the pattern. In our examples thus far, this pattern has been obvious. Sometimes this is not the case. And even if the pattern seems obvious, we may not have the obvious sequence in mind. For instance, we all assume that the next number in the sequence

$$\{1,\ 2,\ 3,\ \ldots\} \tag{1.1}$$

is 4. However, suppose this sequence is really

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

or

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

or even

$$\{1,\ 2,\ 3,\ 5,\ 8,\ 13,\ 21,\ \ldots\}$$

For now, we will assume that the sequence 1.1 means the “obvious” sequence of counting numbers.

In this and the following sections, we will concentrate on a special kind of sequence and will only occasionally look at other, more general, sequences. You are already familiar with many sequences of this kind—the counting numbers:

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

the even numbers:

$$\{2,\ 4,\ 6,\ 8,\ \ldots\}\,,$$

multiples of 5:

$$\{5,\ 10,\ 15,\ 20,\ \ldots\}\,,$$

multiples of 10:

$$\{10,\ 20,\ 30,\ \ldots\}\,,$$

powers of 10:

$$\{1,\ 10,\ 100,\ 1000,\ 10000,\ \ldots\}$$

and powers of 2:

$$\{1,\ 2,\ 4,\ 8,\ 16,\ 32,\ \ldots\}\,.$$

We are going to consider these and other such sequences in a very general way. The key observation is that each of these sequences is created either by successive addition (counting numbers, even numbers, multiples of 5 or multiples of 10) or by successive multiplication (powers of 10, powers of 2).

Successive additions can give us number sequences other than just multiples of a given number. For example, the odd numbers

$$\{1,\ 3,\ 5,\ \ldots\}$$

are constructed by successively adding 2. Similarly, successive multiplications can give us number sequences other than powers of a given number. For example,

$$\{3,\ 6,\ 12,\ 24,\ 48,\ \ldots\}$$

is constructed by successively multiplying by 2.

Number sequences which are formed by successive additions of the same amount are called *arithmetic sequences*. Those which are formed by successive multiplication by the same amount are called *geometric sequences*. That is, the difference between successive numbers in an arithmetic sequence is always the same, while the quotient of successive numbers in a geometric sequence is always the same. The even numbers, the odd numbers, and the multiples of 5 are examples of arithmetic sequences, while the powers of 2, the powers of 10 and the sequence

$$\{3,\ 6,\ 12,\ 24,\ 48,\ldots\}$$

are examples of geometric sequences.

Exercise 1.1.1. Is the sequence

$$\{2,\ 10,\ 50,\ 250,\ldots\}$$

arithmetic or geometric?

Exercise 1.1.2. Is the sequence

$$\{10,\ 13,\ 16,\ 19,\ldots\}$$

arithmetic or geometric?

Exercise 1.1.3. For each of the following sequences, determine if the sequence is arithmetic, geometric, both arithmetic and geometric, or neither arithmetic nor geometric. Also, what is the next number in the sequence?

i. $\{0,\ -1,\ -2,\ -3,\ -4,\ \ldots\}$;

ii. $\{3,\ 3,\ 3,\ 3,\ \ldots\}$;

iii. $\{1,\ 1/2,\ 1/4,\ 1/8,\ \ldots\}$;

iv. $\{+1,\ -1,\ +1,\ -1,\ \ldots\}$;

v. $\{1,\ 1/2,\ 1/3,\ 1/4,\ \ldots\}$;

vi. $\{\frac{1}{2},\ 2,\ 3\,\frac{1}{2},\ 5,\ 6\,\frac{1}{2},\ \ldots\}$;

vii. $\{4/5,\ 2/15,\ -8/15,\ -6/5,\ -28/15,\ \ldots\}$;

viii. $\{\sqrt{3},\ 3,\ 3\sqrt{3},\ 9,\ 9\sqrt{3},\ \ldots\}$;

ix. $\{+1,\ -2,\ +3,\ -4,\ +5,\ \ldots\}$.

We can display number sequences in a symbolic way. We will let the letter a with subscripts represent a sequence. That is, a_1 represents the first number in the sequence, a_2 the second number, etc. (The use of a is not special. We could have chosen b or c or α.) This gives us a convenient shorthand for number sequences. We may now refer to the entire sequence by writing $\{a_n\}$. The a_n here is a "generic" member of the sequence. It refers to the nth number (called *term*) in the sequence. The letter n is called an *index*. It is also sometimes called a *subscript* or a *parameter*. There is nothing special about the use of n as the index. The sequence $\{a_k\}$ is the same as the sequence $\{a_n\}$.

Here is an example. Let $a_1 = 3$, $a_2 = 6$, $a_3 = 12$, $a_4 = 24$, etc. Then

$$\{a_1,\ a_2,\ a_3,\ \ldots\}$$

is the sequence

$$\{3,\ 6,\ 12,\ 24,\ 48,\ \ldots\}.$$

Instead of writing

$$\{3,\ 6,\ 12,\ 24,\ 48,\ \ldots\}$$

every time we wish to refer to this sequence, we now simply write $\{a_n\}$. This notation also gives us a handy way to refer to individual terms in the sequence. In $\{a_n\}$ just described, $a_1 = 3$, $a_5 = 48$ and $a_{11} = 3072$.

Exercise 1.1.4. Let $\{a_n\}$ be the sequence

$$\{2,\ 10,\ 50,\ 250,\ \ldots\}.$$

What is a_2? a_5?

Exercise 1.1.5. Let $\{b_n\}$ be the sequence

$$\{3,\ 8,\ 13,\ 18,\ \ldots\}.$$

What is b_3? b_6?

Exercise 1.1.6. Let $\{c_n\}$ be the sequence

$$\{\sqrt{3},\ 3,\ 3\sqrt{3},\ 9,\ 9\sqrt{3},\ \ldots\}.$$

What is c_3? c_7?

Every arithmetic sequence can be described as follows: the nth term is computed by adding some fixed constant (called the *common difference*) to the preceding (or $(n-1)$st) term. For example, if

$$\{w_n\} = \{1,\ 4,\ 7,\ 10,\ \ldots\},$$

then w_7 is $w_6 + 3$ (and w_6 is $w_5 + 3$, w_5 is $w_4 + 3$, etc.) and, more generally,

$$w_n = w_{n-1} + 3\,. \tag{1.2}$$

This description is called a *recursion.* A recursion is a formula for computing a term in a sequence from earlier terms in the sequence. In this example, the only earlier term we need is the preceding term.

Exercise 1.1.7. Use the recursion in Equation 1.2 to compute w_5, w_6 and w_7.

Notice that the choice of n and $n-1$ as the subscripts in the recursion is somewhat arbitrary. We are simply trying to say, using symbols, that the next term in the sequence is gotten from the previous term by adding three. We might also have written

$$w_{n+1} = w_n + 3$$

to mean the same thing.

Similarly, the nth term of a geometric sequence can be described as some fixed multiple (called the *common ratio*) of the $(n-1)$st term. For example, if

$$\{t_n\} = \{3,\ 6,\ 12,\ 24,\ 48,\ \ldots\},$$

then $t_5 = 2t_4$ (and $t_4 = 2t_3$, $t_3 = 2t_2$, etc.) and, more generally,

$$t_n = 2t_{n-1}\,. \tag{1.3}$$

As above, we might also have written

$$t_{n+1} = 2t_n\,.$$

Exercise 1.1.8. Use the recursion in Equation 1.3 to compute t_6, t_7 and t_8.

Our goal is to find a recursion for a general arithmetic sequence and for a general geometric sequence.

Exercise 1.1.9. For each of the sequences below, determine if the sequence is arithmetic or geometric, find the common difference or ratio, and find a recursion.

i. $\{u_n\} = \{2,\ 4,\ 6,\ 8,\ \ldots\}$;

ii. $\{v_n\} = \{1,\ 3,\ 5,\ 7,\ \ldots\}$;

iii. $\{s_n\} = \{1,\ 2,\ 4,\ 8,\ 16,\ \ldots\}$;

iv. $\{\alpha_n\} = \{1/2,\ 2,\ 7/2,\ 5,\ 13/2,\ \dots\}$;

v. $\{\beta_n\} = \{\sqrt[3]{2},\ 2,\ 2\sqrt[3]{4},\ 4\sqrt[3]{2},\ 8,\ \dots\}$;

vi. $\{\gamma_n\} = \{4/3,\ -1/4,\ -11/6,\ -41/12,\ -5,\ \dots\}$;

vii. $\{A_n\} = \{\pi,\ 3\pi,\ 5\pi,\ 7\pi,\ \dots\}$.

Exercise 1.1.10. Find a recursion for a general arithmetic sequence $\{a_n\}$ with common difference d.

Exercise 1.1.11. Find a recursion for a general geometric sequence $\{g_n\}$ with common ratio r.

Note that the sequences

$$\{u_n\} = \{2,\ 4,\ 6,\ 8,\ \dots\},$$

and

$$\{v_n\} = \{1,\ 3,\ 5,\ 7,\ \dots\}$$

have the same recursions, although they are different sequences. More information, besides the recursion, is needed to define the sequence unambiguously. For arithmetic and geometric sequences, that information is the value of a single term, called an *initial condition*. In most cases, that single term is the first term of the sequence. Thus the sequence $\{w_n\}$ is completely defined by the recursion

$$w_n = w_{n-1} + 3$$

and the initial condition

$$w_1 = 1\,.$$

Similarly, the sequence $\{t_n\}$ is completely defined by

$$t_n = 2t_{n-1}$$

and the initial condition

$$t_1 = 3\,.$$

Exercise 1.1.12. Write recursions and initial conditions for the sequences below

i. $\{2,\ 7,\ 12,\ 17,\ 22,\ \dots\}$;

ii. $\{2,\ 6,\ 18,\ 54,\ 162,\ \dots\}$;

iii. $\{3,\ 30,\ 300,\ 3000,\ \dots\}$.

Sequences which are both arithmetic and geometric are very special. The next two exercises classify them.

Exercise 1.1.13. Find some sequences which are both arithmetic and geometric.

Exercise 1.1.14. Describe all sequences which are both arithmetic and geometric. Give an argument justifying your description.

Arithmetic and geometric sequences can be used as building blocks for other arithmetic and geometric sequences. The next few exercises show one such kind of construction.

Exercise 1.1.15. For the sequence

$$\{v_n\} = \{1,\ 3,\ 5,\ 7,\ \dots\},$$

write down the sequence

$$\{v_1,\ v_3,\ v_5,\ v_7,\ \dots\}$$

and the sequence

$$\{v_5,\ v_8,\ v_{11},\ v_{14},\ \dots\}.$$

Are these sequences arithmetic? Do the same for the sequence

$$\{w_n\} = \{1,\ 4,\ 7,\ 10,\dots\}.$$

Exercise 1.1.16. Suppose $\{a_n\}$ is an arithmetic sequence. Show that the sequence

$$\{a_1,\ a_3,\ a_5,\ a_7,\ \dots\}$$

is also an arithmetic sequence. Show that the sequence

$$\{a_5,\ a_8,\ a_{11},\ a_{14},\ \dots\}$$

is an arithmetic sequence. State and show as general a result of this type as you can.

Exercise 1.1.17. Repeat Exercise 1.1.16, replacing the word "arithmetic" with "geometric" everywhere.

Exercise 1.1.18. In Exercise 1.1.16 we saw that by selecting some of the terms in an arithmetic sequence we get a new arithmetic sequence. Is it possible to select terms from an arithmetic sequence to get a geometric sequence? Try to do this using the even numbers as your arithmetic sequence. Find as many (if any) geometric sequences as you can. Describe all of the geometric sequences that you get.

Exercise 1.1.19. Can you select terms from a geometric sequence that produce an arithmetic sequence? Try to do this using the powers of 2 as your geometric sequence. Are there any? Why or why not? What can you say in general?

It is possible to describe many sequences, not just arithmetic and geometric, with recursions. For example, if

$$\rho_n = 2\rho_{n-2} - \rho_{n-1}, \qquad \rho_1 = 1, \quad \rho_2 = 2\,,$$

then

$$\begin{aligned} \rho_3 &= 2\rho_1 - \rho_2 = 2 \cdot 1 - 2 = 0 \\ \rho_4 &= 2\rho_2 - \rho_3 = 2 \cdot 2 - 0 = 4 \\ \rho_5 &= 2\rho_3 - \rho_4 = 2 \cdot 0 - 4 = -4\,. \end{aligned}$$

Exercise 1.1.20. Find ρ_6 and ρ_7.

Exercise 1.1.21. Write the first six terms of the sequences defined by the following recursions and initial conditions.

i. $a_n = a_{n-1}a_{n-2} - 1$ with $a_1 = 1$ and $a_2 = 2$.

ii. $b_n = b_{n-1}b_{n-2} - 1$ with $b_1 = 1$ and $b_2 = 3$.

iii. $c_n = c_{n-1} + n^2 - n$ with $c_1 = 1$.

1.2 Explicit Formulas for Arithmetic and Geometric Sequences

While a recursion is a useful description of a sequence, it will not be much help in computing, say, the 100th term in a sequence. However, we already have an intuitive idea of how to do this for arithmetic and geometric sequences.

Exercise 1.2.1. If 2 is the first even number, what is the 12th even number? If 5 is the first multiple of 5, what is the 112th multiple of 5? If 2 is the first power of 2, what is the 13th power of 2? If 3 is the first multiple of 3, what is the nth multiple of 3?

Exercise 1.2.2. If 1 is the first odd number, what is the 17th odd number? What is the 97th number in the sequence which begins

$$\{2,\ 7,\ 12,\ 17,\ 22,\ \ldots\}\,?$$

What is the 16th number in the sequence

$$\{2,\ 6,\ 18,\ 54,\ 162,\ \ldots\}\,?$$

What is the nth number in the sequence

$$\{2,\ 5,\ 8,\ 11,\ \ldots\}\,?$$

The last part of these two exercises should have convinced you that there is a formula, involving n, for the nth term in an arithmetic (or geometric) sequence. Such a formula is called an *explicit formula.* Our goal in this section is to find the explicit formulas for general arithmetic and geometric sequences.

For example, if the sequence is

$$\{w_n\} = \{1,\ 4,\ 7,\ 10, \dots\},$$

then the explicit formula is

$$w_n = 3n - 2\,.$$

To check this, note that $w_1 = 3 \cdot 1 - 2 = 1$, $w_2 = 3 \cdot 2 - 2 = 4$, etc.

If the sequence is

$$\{t_n\} = \{3,\ 6,\ 12,\ 24,\ 48,\ \dots\},$$

then the explicit formula is

$$t_n = 3 \cdot 2^{n-1}\,.$$

To check this, note that $t_1 = 3 \cdot 2^0 = 3$, $w_2 = 3 \cdot 2^1 = 6$, etc.

Exercise 1.2.3. Find explicit formulas for each of the following sequences. Arithmetically verify your formulas for $n = 1$, 2 and 3.

i. $\{u_n\} = \{2,\ 4,\ 6,\ 8,\ \dots\}$;

ii. $\{v_n\} = \{1,\ 3,\ 5,\ 7,\ \dots\}$;

iii. $\{s_n\} = \{1,\ 2,\ 4,\ 8,\ 16,\ \dots\}$.

Exercise 1.2.4. Find explicit formulas for each of the following sequences.

i. $\{2,\ 7,\ 12,\ 17,\ 22,\ \dots\}$;

ii. $\{2,\ 6,\ 18,\ 54,\ 162,\ \dots\}$;

iii. $\{3,\ 30,\ 300,\ 3000,\ \dots\}$.

Exercise 1.2.5. Write down an explicit formula for a general arithmetic sequence with common difference d.

Exercise 1.2.6. Write down an explicit formula for a general geometric sequence with a common ratio r.

Exercise 1.2.7. If a sequence has an explicit formula which follows your rule for arithmetic/geometric sequences, is it arithmetic/geometric? Why?

Exercise 1.2.8. For each of the following sequences, find an explicit formula.

i. $\{u_n\} = \{2,\ 4,\ 6,\ 8,\ \dots\}$;

ii. $\{v_n\} = \{1,\ 3,\ 5,\ 7,\ \dots\}$;

iii. $\{s_n\} = \{1,\ 2,\ 4,\ 8,\ 16,\ \ldots\}$;

iv. $\{\alpha_n\} = \{1/2,\ 2,\ 7/2,\ 5,\ 13/2,\ \ldots\}$;

v. $\{\beta_n\} = \{\sqrt[3]{2},\ 2,\ 2\sqrt[3]{4},\ 4\sqrt[3]{2},\ 8,\ \ldots\}$;

vi. $\{\gamma_n\} = \{4/3,\ -1/4,\ -11/6,\ -41/12,\ -5,\ \ldots\}$;

vii. $\{A_n\} = \{\pi,\ 3\pi,\ 5\pi,\ 7\pi,\ \ldots\}$.

Recursions and explicit formulas are the two most common ways to define precisely a number sequence.

Exercise 1.2.9. Explain the difference between a recursion and an explicit formula.

Exercise 1.2.10. Which of the following formulas is an explicit formula and which is a recursion?

$$a_n = n^2 + a_1 + a_{10}, \text{ for } n > 10,$$

$$b_k = k + b_1 + b_2 + \cdots + b_{k-1}, \text{ for } k > 1,$$

$$c_n = 1 + 2 + 3 + \cdots + n^2, \text{ for } n \geq 1.$$

The explicit formulas can be used in several ways to solve problems involving arithmetic and geometric sequences.

Exercise 1.2.11. If the sixth term in an arithmetic sequence is 100 and the first term is 3, what is the 20th term?

Exercise 1.2.12. If the nth term in an arithmetic sequence is 570, the first term is 3, and that the fifth term is 31, what is n?

Exercise 1.2.13. If second term in a geometric sequence is 9 and the fifth term is 3, what is the tenth term?

Arithmetic and geometric are only two kinds of sequences. We can think of many other number sequences. Some of these also have explicit formulas. For example, the explicit formula

$$t_n = \frac{n^2 - 1}{n^2 + 1}$$

yields the sequence

$$\{t_n\} = \{0,\ 3/5,\ 4/5,\ 15/17,\ 12/13,\ \ldots\}.$$

Exercise 1.2.14. Find an explicit formula for each of these sequences:

$$\{\frac{0}{1},\ \frac{1}{2},\ \frac{2}{3},\ \frac{3}{4},\ \ldots\},$$

$$\{0,\ 3,\ 8,\ 15,\ 24,\ 35,\ 48,\ 63,\ \ldots\}.$$

***Exercise 1.2.15.** Find an explicit formula for this sequence:

$$\{0,\ 1,\ 1,\ 2,\ 2,\ 2,\ 2,\ 3,\ 3,\ 3,\ 3,\ 3,\ 3,\ 3,\ 3,\ 4,\ \ldots\}$$

(Hint: use base 2 logarithms).

We can now summarize the recursions and explicit formulas for arithmetic and geometric sequences.

For an arithmetic sequence $\{a_n\}$ with common difference d, the recursion is

$$a_n = a_{n-1} + d$$

while the explicit formula is

$$a_n = a_1 + d(n-1)\,.$$

For a geometric sequence $\{g_n\}$ with common ratio r, the recursion is

$$g_n = r g_{n-1}$$

while the explicit formula is

$$g_n = g_1 r^{n-1}\,.$$

The term a_1 in the sequence $\{a_n\}$ refers to the first term in the sequence. That is, the sequence is

$$\{a_1,\ a_2,\ a_3,\ \ldots\}.$$

However, sometimes, as a matter of convenience, we want the first term to be indexed by 0, so that the sequence is

$$\{b_0,\ b_1,\ b_2,\ \ldots\}.$$

For example, we might describe the sequence

$$\{3,\ 6,\ 12,\ 24,\ 48,\ \ldots\}$$

as

$$\{a_1,\ a_2,\ a_3,\ \ldots\},$$

so that $a_1 = 3$, $a_2 = 6$, etc. But we could also describe it as

$$\{b_0,\ b_1,\ b_2,\ \ldots\}$$

with $b_0 = 3$, $b_1 = 6$, etc. When there could be confusion about what index is used for the first term in the sequence $\{a_n\}$, we write $\{a_n\}_{n=1,2,\ldots}$.

Exercise 1.2.16. If the sequence is

$$\{b_k\}_{k=0,1,2,\ldots} = \{4,\ 7,\ 10,\ \ldots\}\,,$$

find b_4, b_6 and b_n.

Exercise 1.2.17. If the sequence is

$$\{c_l\}_{l=0,1,2,\ldots} = \{4,\ 6,\ 9,\ 27/2,\ \ldots\}\,,$$

find c_4, c_6 and c_n.

Exercise 1.2.18. What happens to the recursion for an arithmetic sequence if the indexing begins at 0 instead of 1?

Exercise 1.2.19. What happens to the explicit formula for an arithmetic sequence if the indexing begins at 0 instead of 1?

1.3 Summing Arithmetic Sequences

Arithmetic and geometric sequences form the building blocks for other interesting sequences. For example, we can create a new sequence by adding the terms in an arithmetic sequence. Suppose $\{a_n\}$ is an arithmetic sequence. What can we say about the sequences $\{s_n\}$ where

$$\begin{aligned}
s_1 &= a_1,\\
s_2 &= a_1 + a_2,\\
s_3 &= a_1 + a_2 + a_3,\\
s_4 &= a_1 + a_2 + a_3 + a_4,\\
&\vdots \qquad ?
\end{aligned}$$

In the special case that

$$\{a_n\} = \{1, 2, 3, 4, \ldots\}\,,$$

there is a simple formula for the corresponding s_n and a nice proof. In this case,

$$\begin{aligned}
s_1 &= 1,\\
s_2 &= 1 + 2 = 3,\\
s_3 &= 1 + 2 + 3 = 6,\\
s_4 &= 1 + 2 + 3 + 4 = 10\\
\text{and} \qquad s_5 &= 1 + 2 + 3 + 4 + 5 = 15\,.
\end{aligned}$$

The formula for the sum of the first n counting numbers is

$$s_n = 1 + 2 + 3 + \cdots + n = n(n+1)/2\,. \tag{1.4}$$

Exercise 1.3.1. Check that Equation (1.4) is correct for the five values s_1, s_2, s_3, s_4, and s_5 above.

Figure 1.1 describes s_1, s_2, s_3 and s_4. The black dots in each row represent the counting numbers. The first diagram represents $s_1 = 1$. The second diagram represents $s_2 = 1 + 2$. The third diagram represents $s_3 = 1 + 2 + 3$, etc.

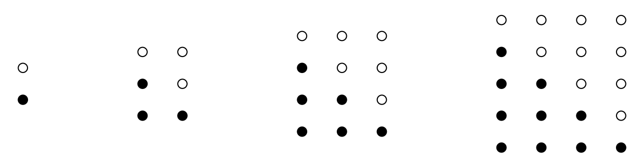


Figure 1.1: Triangular numbers

Exercise 1.3.2. Use Figure 1.1 to give a proof of Equation (1.4).

Because of the diagrams in Figure 1.1, the sequence $\{s_n\}$ is called the sequence of *triangular numbers.*

The sequence of sums can be computed for every arithmetic sequence. Here are two approaches:

i. Write the sum forwards and backwards and add corresponding terms.

ii. Use the formula for the counting sequence given above.

For example, suppose we want to sum the first twenty terms of the arithmetic sequence

$$\{9, 13, 17, \dots\}.$$

The twentieth term is $9 + 4(20 - 1) = 85$, so the sum is

$$9 + 13 + 17 + \cdots + 85.$$

Now write this sum forwards and backwards and add corresponding terms:

$$\begin{aligned} &9 + 13 + 17 + \cdots + 77 + 81 + 85 \\ &+85 + 81 + 77 + \cdots + 17 + 13 + 9 \\ &= 94 + 94 + 94 + \cdots + 94 + 94 + 94 = 94 \cdot 20 = 1880. \end{aligned}$$

So

$$2(9 + 13 + 17 + \cdots + 85) = 1880$$

or

$$9 + 13 + 17 + \cdots + 85 = 940.$$

For the second method, we will manipulate the sum so as to be able to use Equation (1.4):

$$\begin{aligned} 9 + 13 + \cdots + 85 &= (9 + 0) + (9 + 4) + (9 + 8) + \cdots + (9 + 19 \cdot 4) \\ &= 9 \cdot 20 + (4 + 8 + \cdots + 19 \cdot 4) \\ &= 180 + 4(1 + 2 + \cdots + 19) \\ &= 180 + 4\frac{19 \cdot 20}{2} \\ &= 180 + 760 \\ &= 940\,. \end{aligned}$$

Notice that Equation (1.4) was used for $n = 19$, even though the problem was to find the sum of the first twenty terms of the sequence. This is because the counting sequence which emerged in the calculation began at 0, not 1.

Exercise 1.3.3. Find the sum of the first 100 terms of the arithmetic sequence

$$\{3,\ 4,\ 5,\ 6,\ \ldots\}$$

using both methods.

Exercise 1.3.4. Find the sum of the first 75 terms of the arithmetic sequence

$$\{3,\ 6,\ 9,\ 12,\ \ldots\}$$

using both methods.

Exercise 1.3.5. Find the sum of the first 50 terms of the arithmetic sequence

$$\{5,\ 8,\ 11,\ 14,\ \ldots\}$$

using both methods.

Exercise 1.3.6. Using the first method, derive the following formula:

> The formula for the sum of the first n terms of the arithmetic sequence $\{a_n\}$ is
>
> $$s_n = \frac{n}{2}(a_1 + a_n)\,.$$

Exercise 1.3.7. From the previous exercise and the explicit formula for an arithmetic sequence, derive the following alternate formula:

> Another formula for the sum of the first n terms of the arithmetic sequence $\{a_n\}$ with common difference d is
>
> $$s_n = na_1 + d\frac{n(n-1)}{2}\,.$$

The formula for the sum of an arithmetic sequence can be combined with the explicit formula in the previous section to solve the following problems.

Exercise 1.3.8. If you were told that the nth term in an arithmetic sequence is 570, that the first term is 3, and that the fifth term is 31, what would you say is the sum of these n terms?

Exercise 1.3.9. Suppose the sum of the first 16 terms of an arithmetic sequence is 440, while the sum of the first 8 terms is 124. What is the 16th term?

Exercise 1.3.10. What is the sum of the last 100 terms in the arithmetic sequence $\{1,\ 5,\ \ldots,\ 2001\}$?

Exercise 1.3.11. What is the sum of the odd numbers between 101 and 999, including 101 and 999?

Exercise 1.3.12. Sum the even numbers from -48 to 98.

***Exercise 1.3.13.** Suppose the second term in an arithmetic sequence is 2 and the nth term is 32, while the sum of the first n terms is 715/2. Find n.

Triangular numbers are depicted in the first picture in Figure 1.2 below. For each of the following triangles we are going to count the number of dots on a side and the number of dots "enclosed" (that is, on the perimeter or in the interior) by the triangle. For the triangle ABC, these numbers are 2 on a side and 3 enclosed. For the triangle ADE, they are 3 and 6. For the triangle AFG, they are 4 and 10. Finally, for the triangle AHI, they are 5 and 15. Let's include the "triangle" A, which has 1 and 1 as its numbers. The sequence of the number of circles enclosed then begins $\{1,\ 3,\ 6,\ 10,\ 15, \ldots\}$ and is evidently the sequence of triangular numbers (since each interior number includes the previous interior number plus the number of dots on the new side).

In a similar manner, the second picture in Figure 1.2 depicts the *square numbers*. The numbers of dots on each side again are 1, 2, 3, 4 and 5, while the numbers of enclosed dots are the perfect squares 1, 4, 9, 16, and 25.

The third picture in Figure 1.2 depicts *pentagonal numbers*. They are

$$\{1,\ 5,\ 12,\ 22,\ 35,\ \ldots\}\,.$$

The first is 1, the second is $1+4$, the third is $1+4+7$, the fourth is $1+4+7+10$, etc.

Exercise 1.3.14. Use the fact that the pentagonal numbers are the sequence of sums of an arithmetic sequence to find a formula for the nth pentagonal number.

***Exercise 1.3.15.** Write down a sequence of pictures which describes hexagonal numbers. Find a formula for them. Compute the formula for the nth k-polygonal number.

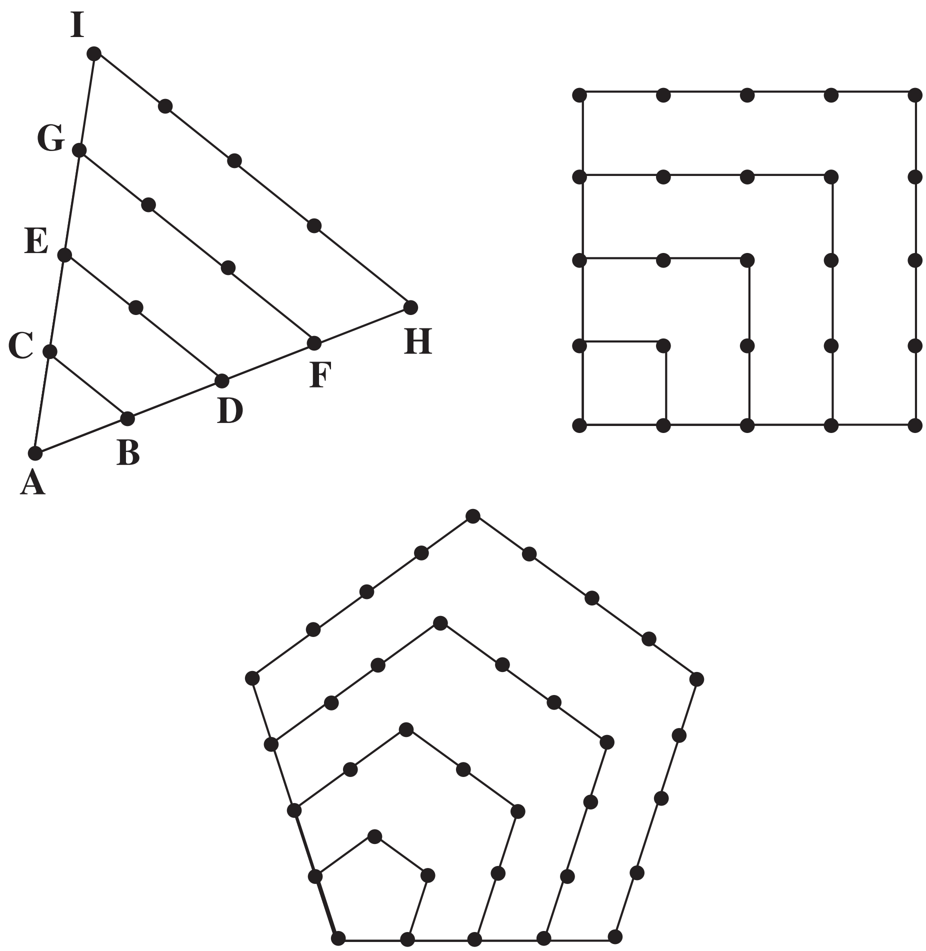


Figure 1.2: Triangular, square and pentagonal numbers

1.4 Summing Geometric Sequences

With a little bit of algebra, we can also compute the sum sequence for geometric sequences. Notice that

$$\begin{aligned}(r+1)(r-1) &= r^2-1,\\ (r^2+r+1)(r-1) &= r^3-1,\\ (r^3+r^2+r+1)(r-1) &= r^4-1\,.\end{aligned}$$

Exercise 1.4.1. Check the algebra in the above equations by doing the polynomial arithmetic.

In general,

$$(r^{n-1}+r^{n-2}+\cdots+r^2+r+1)(r-1) = r^n-1\,, \tag{1.5}$$

or, equivalently,

$$r^{n-1}+r^{n-2}+\cdots+r^2+r+1 = \frac{r^n-1}{r-1}, \quad r \neq 1\,. \tag{1.6}$$

Exercise 1.4.2. Explain why Equation (1.5) is true.

Exercise 1.4.3. Explain why Equation (1.6) follows from Equation (1.5).

Let's use Equation (1.6) to find the sum of the first 10 terms of the geometric sequence

$$\{2,\ 10,\ 50,\ 250,\ \ldots\}\,.$$

Write

$$2+10+50+\cdots+2\cdot 5^9 = 2(1+5+5^2+\cdots+5^9)$$

by factoring out the first term 2. Next, use Equation (1.6) with $r=5$ to get

$$2(1+5+5^2+\cdots+5^9) = \frac{2(5^{10}-1)}{5-1}\,.$$

Finally, simplify this last expression:

$$\frac{2(5^{10}-1)}{5-1} = \frac{5^{10}-1}{2}\,.$$

Exercise 1.4.4. Do a similar calculation to compute the sum of the first 20 terms of this sequence.

Exercise 1.4.5. Based on the preceding discussion and the previous exercise, find a formula for the sum of the first n terms of this sequence.

Exercise 1.4.6. Derive a formula for the sum of the first 20 terms of a geometric sequence whose first term is g_1 and whose common ratio is r.

Exercise 1.4.7. Derive a formula for the sum of the first n terms of a geometric sequence whose first term is g_1 and whose common ratio is r.

If the absolute value of the common ratio is less than 1, then all the terms of the geometric sequence can be added up. The next set of exercises shows how this works.

Exercise 1.4.8. Find the sum of the first 10 terms of the geometric sequence $\{1,\ 1/2,\ 1/4,\ \ldots\}$. Find the sum of the first 100 terms of the same sequence. Do the same things for the geometric sequence $\{1,\ 1/3,\ 1/9,\ \ldots\}$.

Exercise 1.4.9. Find the sum of the first n terms of the geometric sequence $\{1,\ 1/2,\ 1/4,\ \ldots\}$. Find the sum of the first n terms of the geometric sequence $\{1,\ 1/3,\ 1/9,\ \ldots\}$.

Exercise 1.4.10. What happens to $(1/2)^n$ as n grows large? What happens to the sum of the first n terms of the geometric sequence $\{1,\ 1/2,\ 1/4,\ \ldots\}$ as n grows large?

Exercise 1.4.11. What happens to the sum of the first n terms of the geometric sequence $\{1,\ 1/3,\ 1/9,\ \ldots\}$ as n grows large?

From Exercise 1.4.7 we have the following.

The formula for the sum of the first n terms of the geometric sequence $\{g_n\}$ is

$$s_n = g_1 \cdot \frac{r^n - 1}{r - 1}\,. \tag{1.7}$$

Exercise 1.4.12. Use Equation 1.7 to prove

$$s_n = g_1 \cdot \frac{1 - r^n}{1 - r}\,.$$

Exercise 1.4.13. In the equation in Exercise 1.4.12, what happens to r^n as n grows large, when $|r| < 1$? Show that the sequence of sums, $\{s_1,\ s_2,\ s_3,\ \ldots\}$, for a geometric sequence $\{g_n\}$ gets close to a certain value as n gets large, if $|r| < 1$.

The previous exercise shows that if $\{g_n\}$ is a geometric sequence with common ration r and if $|r| < 1$, then

$$g_1 + g_2 + g_3 + \ldots$$

gets close to a certain value which we will call s_∞. In fact, a consequence of this exercise is the following:

The formula for "all" the terms in a geometric sequence is

$$s_\infty = g_1 \cdot \frac{1}{1 - r}\,.$$

Exercise 1.4.14. Find the "infinite" sums

$$1 + 1/2 + 1/4 + 1/8 + \cdots$$

and

$$1 + 1/3 + 1/9 + 1/27 + \cdots .$$

Exercise 1.4.15. Find the "infinite" sums

$$3 + 2 + 4/3 + 8/9 + 16/27 + \cdots$$

and

$$1 - 1/2 + 1/4 - 1/8 + 1/16 - 1/32 + \cdots .$$

Exercise 1.4.16. Find the "infinite" sum

$$4 - \frac{4}{\sqrt{3}} + \frac{4}{3} - \frac{4}{3\sqrt{3}} + \cdots .$$

1.5 Examples of Arithmetic and Geometric Sequences

Arithmetic and geometric sequences have many applications. Here are several examples. In each example, you will have to determine whether an arithmetic or a geometric sequence is appropriate. Sometimes you will have to sum the sequence.

Exercise 1.5.1. A ladder with 15 rungs is tapered so that the top rung is 12 inches wide while the bottom rung is 18 inches wide. Find the total length of all the rungs.

Exercise 1.5.2. Puff pastry is made as follows. The dough is rolled into a rectangle. Then two-thirds of the rectangle is buttered. The unbuttered third is folded over, followed by the other buttered third (like a letter), to get a stack of two butter layers sandwiched between three dough layers. See Figure 1.3. Now this new rectangle of dough is rolled out and the process is repeated. If this buttering, folding and rolling is done six times, how many layers of dough are there in the final pastry?

Exercise 1.5.3. If a clock chimes the hour on the hour (e.g., it chimes five times at 5 o'clock), and it also chimes once on the half-hour, how many times does it chime from 12:15 p.m. to 12:15 p.m. the next day?

An important application of geometric sequences is compound interest. Suppose we invest \$2 at 5% per year. In the first year, our two dollars earns 10 cents interest. If that dime is invested along with the two dollars for the second year, the original two dollars earns another dime and the dime interest from

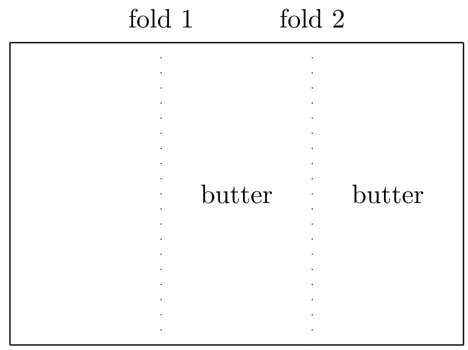


Figure 1.3: Puff pastry

the first year earns $.10 \cdot .05$. This interest on the interest is called compound interest. So after the second year, we have our original two dollars, two dimes of interest on those two dollars, and \$.005 interest on interest. This is the same as $2 \cdot 1.05 \cdot 1.05$ since

$$\begin{aligned} 2 \cdot (1 + .05) \cdot (1 + .05) &= 2 \cdot (1 + 2 \cdot .05 + .05^2) \\ &= 2 \cdot 1 + 2 \cdot .10 + 2 \cdot .0025 \\ &= 2 + .20 + .005\,. \end{aligned}$$

For the third year, we now have $2 \cdot 1.05^2$ invested, which earns 5%. So we have $\$2 \cdot 1.05^3 = \$2.31525$ after three years.

If our interest is compounded every six months, then our \$2 earns 2.5% in the first six months, and the \$2 plus this interest earns another 2.5% in the next six months. Thus, after one year, we have $\$2 \cdot 1.025 \cdot 1.025 = \$2.10125$. After two years, we will have $\$2 \cdot 1.025^4 \approx \$2.20763$. And after three years, we will have $\$2 \cdot 1.025^6 \approx \$2.31939$.

Exercise 1.5.4. Suppose in 1787 George Washington invested \$25 at 4% interest, compounded yearly. What would his descendants have today? What if the compounding was done quarterly instead of yearly? Daily? Every second?

At 6 p.m., the minute hand of a standard clock points straight up and the hour hand points straight down. Thirty minutes later, the minute hand "catches up" to where the hour hand was at 6 p.m. However, the hour hand has moved halfway between the 6 and the 7. Two and one-half minutes later, the minute hand reaches that position, but the hour hand has moved again.

Exercise 1.5.5. What time is it when the minute hand "catches" the hour hand? That is, at what time between 6 p.m. and 7 p.m. are the minute hand and the hour hand pointing in exactly the same direction? Solve this problem using an appropriate sequence. Can you find other ways to solve it?

Recall that to solve equations of the form $3^n = 10$ or $2^y = 5$ requires the use of logarithms.

Exercise 1.5.6. Solve for n: $3^n = 10$. Solve for y: $2^y = 5$.

Also note that sometimes the logarithms are particularly easy to calculate.

Exercise 1.5.7. Without using a calculator, solve $9^z = 27$ for z.

You will need to use logarithms in parts of the following exercise.

Exercise 1.5.8. A biologist is culturing a certain bacteria. Every three days the culture doubles in size. If five grams are present initially, how many grams will be present in six days? In nine days? In $3k$ days? In two days? How many days (or fraction thereof) will it take for the culture to quadruple in size? To triple in size?

Exercise 1.5.9. A pile of logs is made by stacking 40 logs in the bottom layer, 39 in the next layer (in the gaps between the 40 logs on the bottom), 38 in the next and so on. How many logs are there in all if there are ten layers in the stack?

Exercise 1.5.10. Before he can marry the princess, a potential suitor must pay a small sum to the king. On the first square of a checkerboard he must put a penny; on the second square, two pennies; on the third, four pennies; on the fourth, eight pennies; and so on. How many pennies must he pay the king? (A checkerboard is 8×8.)

Another application of geometric sequences is analyzing chain letters. Suppose you receive a chain letter which contains a list of six names. Suppose this letter instructs you to (1) send $10 to the person at the top of the list, (2) make five copies of the letter, removing the top person's name from the list, and adding your name to the bottom of the list, and (3) send the five copies to five of your friends. The letter claims that the chain has been unbroken for dozens of years. And it warns that terrible things will happen to you if you "break the chain".

Exercise 1.5.11. Suppose one person starts the process by creating such a letter with six fictitious names and sending it to twenty-five people at random. If it takes about one month to perform the above steps, how long would it be before a letter has been sent to every person on the planet? (You will have to estimate the number of people on the planet. Assume that if a person is sent a letter, that person will not be sent another. Finally, you may use logs to find your answer, although it is not necessary.)

Exercise 1.5.12. Obviously, not everyone on the planet receives such letters. What do you think happens? What about the claim that the chain has been unbroken for dozens of years? Who makes money on such schemes? Who loses money? How do you think a chain letter like this starts?

Certain fractals lead to geometric sequences. A fractal snowflake pattern is produced step by step as shown in Figure 1.4. Start with an equilateral triangle whose area is one square inch. At each stage, a new equilateral triangle is pasted onto each edge of the figure. The edges of the new triangles are 1/3 the size of the edge that it is pasted on.

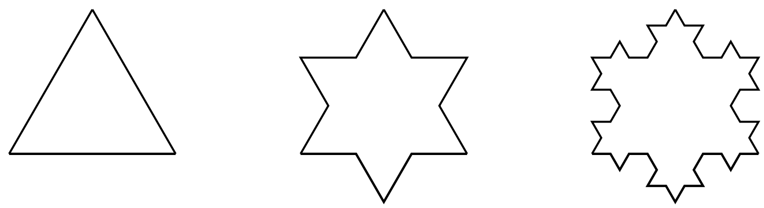


Figure 1.4: Three fractal snowflakes

***Exercise 1.5.13.** How many triangles are added at the nth stage? What is the total area of the snowflake at the nth stage? (Note: if one equilateral triangle has an edge 1/3 the size of another, its area is 1/9 the area of the other.)

***Exercise 1.5.14.** Suppose a is the length of the perimeter of the triangle in the first picture in Figure 1.4. What is the length of the perimeter in the second picture? In the third picture? At the nth stage?

These last two problems describe a fractal "path" with the property that the area enclosed is finite, while the length of the path is infinite! Figure 1.5 shows this fractal path after five steps.

1.6 Fibonacci Numbers

Of course there are many sequences of numbers other than arithmetic and geometric. Some are easily described by an explicit formula. For example, the sequence of squares is $\{1,\ 4,\ 9,\ 16,\ \ldots\}$. The nth term in this sequence is n^2. Another example is the triangular numbers, $\{1,\ 3,\ 6,\ 10,\ 15, \ldots\}$. The nth term in this sequence is $n(n+1)/2$.

Other sequences are more easily described by recursions. An example of such a sequence is the Fibonacci sequence.

In Figure 1.6, we have drawn all possible "tilings" of 2×1, 2×2, 2×3 and 2×4 rectangles, using only 2×1 dominoes. The first rectangle (on the left) has dimensions 2×1, so there is only one possible tiling. The second rectangle has dimensions 2×2, and there are two possible tilings, shown in the second

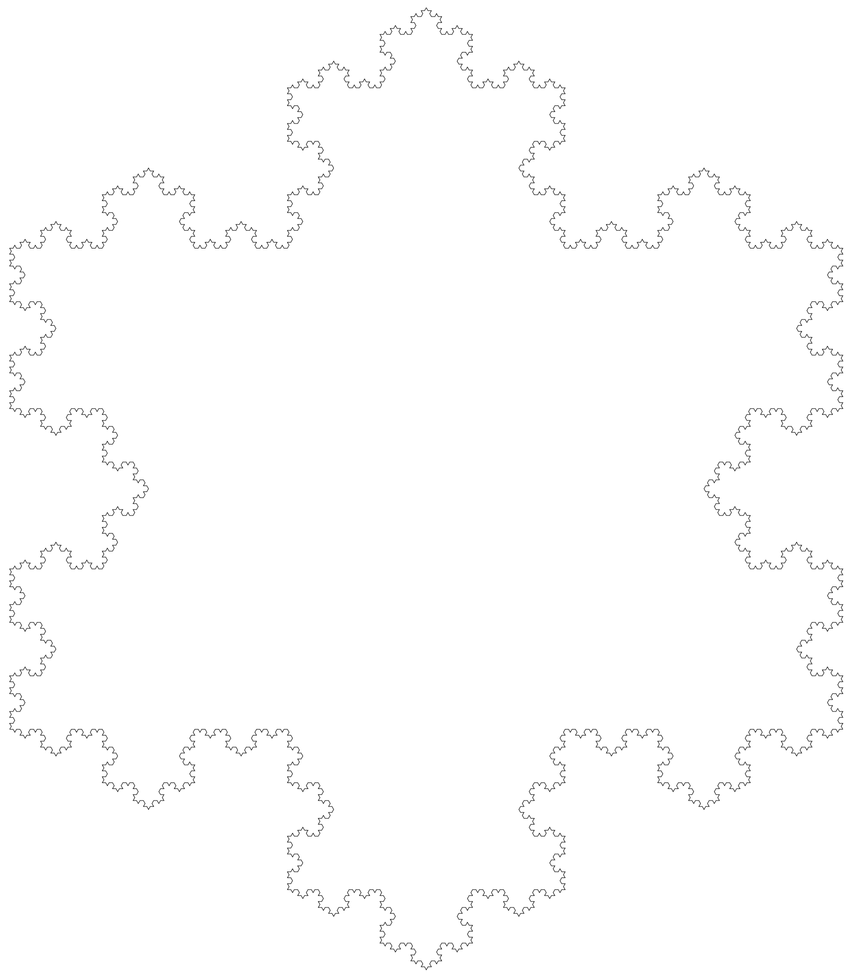


Figure 1.5: Fractal snowflake

column. The third rectangle is 2×3, and there are three possible tilings, shown in the third column. Finally, the last rectangle (on the right) has dimensions 2×4, and there are five tilings, shown in the last column.

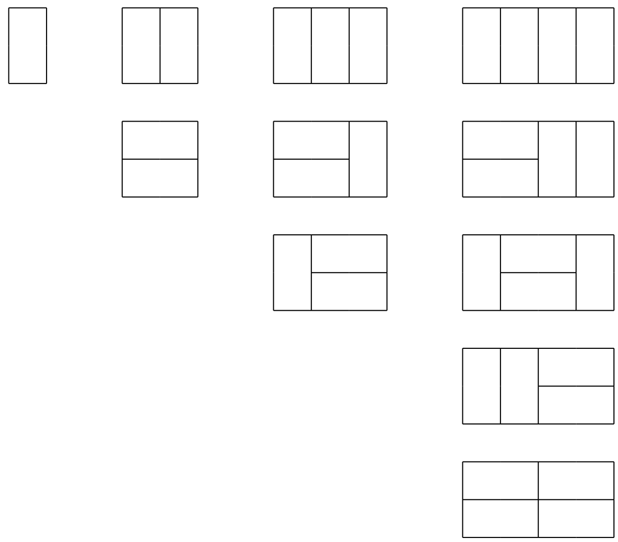


Figure 1.6: Domino tilings of 2×1, 2×2, 2×3 and 2×4 rectangles

Exercise 1.6.1. Draw all possible tilings for 2×5 and 2×6 rectangles.

Exercise 1.6.2. Let f_n denote the number of tilings for a $2 \times n$ grid. Thus, $f_1 = 1$, $f_2 = 2$, $f_3 = 3$, and $f_4 = 5$. Using Figures 1.7 and 1.8 as a guide, explain why $f_3 = f_2 + f_1$ and $f_4 = f_3 + f_2$.

Exercise 1.6.3. Generalize your arguments in the previous exercise to show that

$$f_n = f_{n-1} + f_{n-2}$$

for all $n \geq 3$, not just $n = 3$ and $n = 4$. Thus, for example, your argument should show why $f_{200} = f_{199} + f_{198}$, even though you do not know any of the values f_{200}, f_{199} and f_{198}.

Exercise 1.6.4. The sequence $\{f_n\}$ is called the *Fibonacci sequence* and the terms f_n are called Fibonacci numbers. We usually let $f_0 = 1$ and start the sequence at index 0. Why is this o.k.? What initial conditions must we have to define the sequence?

There are dozens of formulas involving the Fibonacci numbers. Here are two examples.

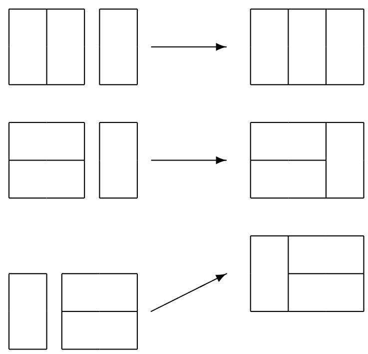


Figure 1.7: Construction of f_3

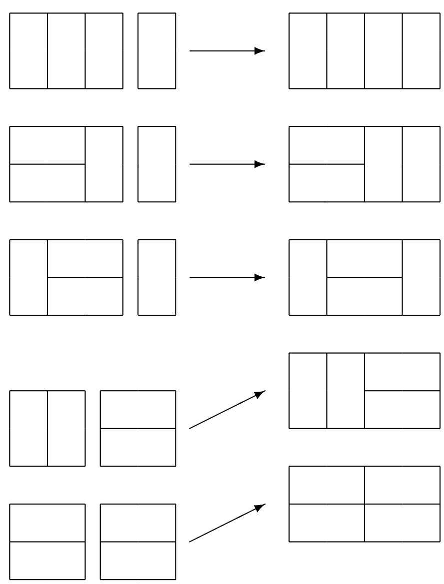


Figure 1.8: Construction of f_4

Exercise 1.6.5. Explain each step in the following calculations:

$$\begin{aligned} f_6 &= f_5 + f_4 \\ &= f_4 + f_4 + f_3 \\ &= f_4 + f_3 + f_3 + f_2 \\ &= f_4 + f_3 + f_2 + f_2 + f_1 \\ &= f_4 + f_3 + f_2 + f_1 + f_1 + f_0 \\ &= f_4 + f_3 + f_2 + f_1 + f_0 + 1\,. \end{aligned}$$

Now prove:

$$f_0 + f_1 + f_2 + \cdots + f_n = f_{n+2} - 1\,.$$

Exercise 1.6.6. Explain each step in the following calculations:

$$\begin{aligned} f_5 \cdot f_4 &= (f_4 + f_3) \cdot f_4 = f_4^2 + f_4 \cdot f_3 \\ &= f_4^2 + (f_3 + f_2) \cdot f_3 = f_4^2 + f_3^2 + f_3 \cdot f_2 \\ &= f_4^2 + f_3^2 + (f_2 + f_1) \cdot f_2 = f_4^2 + f_3^2 + f_2^2 + f_2 \cdot f_1 \\ &= f_4^2 + f_3^2 + f_2^2 + (f_1 + f_0) \cdot f_1 = f_4^2 + f_3^2 + f_2^2 + f_1^2 + f_1 \cdot f_0 \\ &= f_4^2 + f_3^2 + f_2^2 + f_1^2 + f_0^2\,. \end{aligned}$$

Now prove:

$$f_0^2 + f_1^2 + f_2^2 + \cdots + f_n^2 = f_n \cdot f_{n+1}$$

One of the most beautiful properties of the Fibonacci numbers is that the ratio of successive numbers tends to the golden mean, $(1+\sqrt{5})/2$. We begin by dividing the recursion

$$f_n = f_{n-1} + f_{n-2}$$

by f_{n-1}, to get

$$\begin{aligned} \frac{f_n}{f_{n-1}} &= 1 + \frac{f_{n-2}}{f_{n-1}} \\ &= 1 + \frac{1}{\frac{f_{n-1}}{f_{n-2}}}\,. \end{aligned}$$

Now replace f_n/f_{n-1} by a_n. That is, a_n is the ratio of two successive terms in the Fibonacci sequence. We would like to show that a_n gets close to the golden mean if n grows large.

If a_n replaces f_n/f_{n-1}, then a_{n-1} replaces f_{n-1}/f_{n-2}. So we now have

$$a_n = 1 + \frac{1}{a_{n-1}}\,. \tag{1.8}$$

Now suppose a_n gets close to some real number a as n gets large. If a_n gets close to a, then Equation 1.8 becomes

$$a = 1 + \frac{1}{a}\,. \tag{1.9}$$

Exercise 1.6.7. Solve Equation (1.9) for a.

There is also a beautiful explicit formula for the Fibonacci numbers. It is outside the scope of this chapter to derive it, but we can state it. First, let a and b be the roots of the quadratic equation $x^2 - x - 1 = 0$, with $a > b$. (Note that a is exactly the golden mean described Exercise 1.6.7.) Then

$$f_n = \frac{a^{n+1} - b^{n+1}}{\sqrt{5}} . \tag{1.10}$$

Exercise 1.6.8. Find a and b. Use Equation (1.10) to compute f_0, f_1, f_2 and f_3 and compare with the values for these numbers computed earlier in this section.

1.7 Tower of Hanoi

The Tower of Hanoi game is a puzzle which consists of three pegs and several circular disks, all of different sizes, which fit on the pegs like wheels on an axle. You are allowed to move the disks one at a time from one peg to another peg, always requiring that smaller disks be placed on top of larger ones. The puzzle is to move all the disks from one peg to a second peg in as few moves as possible.

Figure 1.9 shows the seven moves required to move three disks.

Exercise 1.7.1. How many moves are required to move four disks. Note that one way to do it is to move the top three disks to the third peg, then move the bottom disk to the second peg, and then move the top three disks to the second peg.

Exercise 1.7.2. Let T_n be the number of moves required to move n disks. Write down T_1, T_2, T_3 and T_4. Use the method outlined in Exercise 1.7.1 to show

$$T_n = 2T_{n-1} + 1 . \tag{1.11}$$

Use this recursion to compute T_n for $n = 5, 6, \ldots, 10$.

To find an explicit formula for T_n, we construct a new sequence from the sequence $\{T_n\}$. Notice that Equation 1.11 can be rewritten as

$$T_n + 1 = 2T_{n-1} + 2 \tag{1.12}$$

$$= 2(T_{n-1} + 1) . \tag{1.13}$$

This motivates us to let $A_n = T_n + 1$.

Exercise 1.7.3. Use Equation (1.12) to show $A_n = 2A_{n-1}$. What kind of a sequence is $\{A_n\}$? What is A_1 (the initial condition)? Find the explicit formula for A_n.

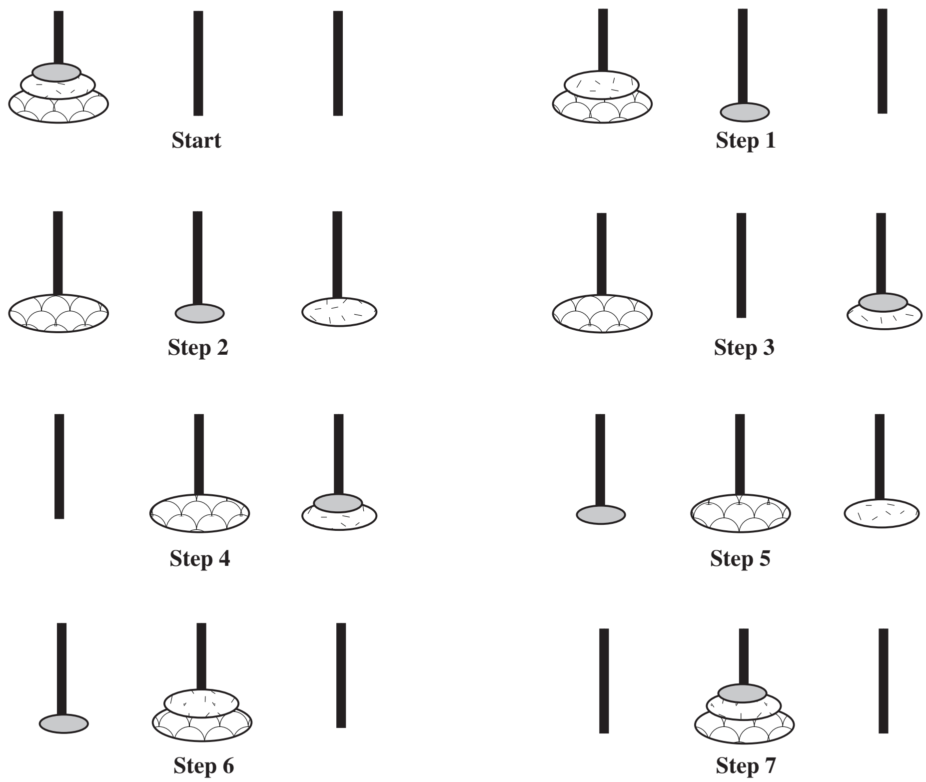


Figure 1.9: Tower of Hanoi

Exercise 1.7.4. Use the explicit formula for A_n you found in the previous exercise together with the definition of A_n above to give an explicit formula for T_n.

1.8 Divisions of a plane

If we draw a line across a plane, the plane is divided into two regions (see the first picture in Figure 1.10). If we draw a second, nonparallel, line, the plane is divided into four regions (see the second picture in Figure 1.10). If we draw a third line, not parallel to either of the first two, and not intersecting them at their intersection point, the plane is divided into seven regions (see the third picture in Figure 1.10).

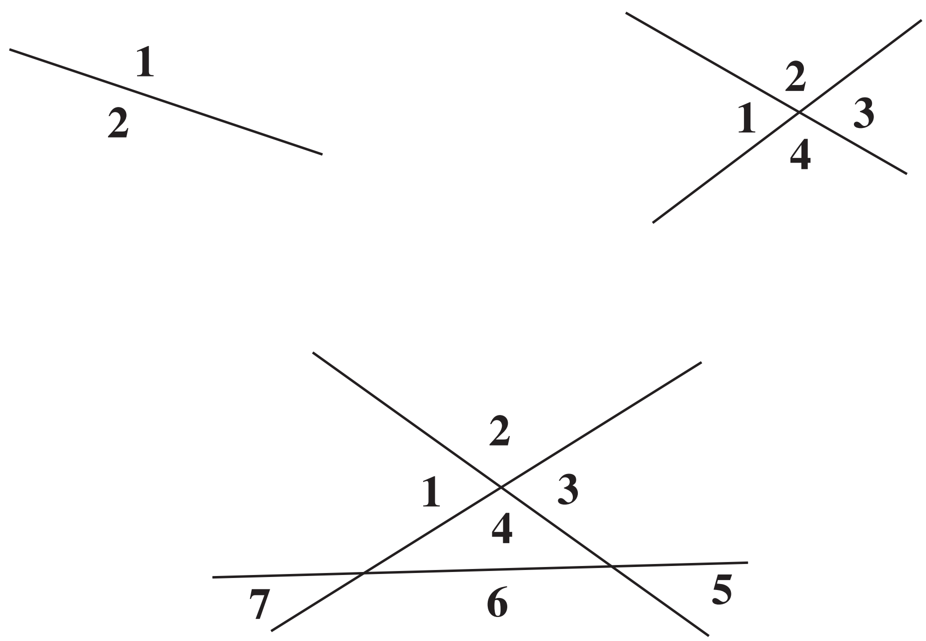


Figure 1.10: Dividing a plane

Exercise 1.8.1. Into how many regions will the plane be divided by four "general" lines? ("General" means no three intersecting at a common point and no two parallel.) Can you do five lines—don't try to draw them; instead, how many new regions are created by the fifth line?

Exercise 1.8.2. Suppose R_n is the number of regions created by n general lines. Write down R_0, R_1, R_2, R_3, R_4 and R_5. Note that

$$\begin{aligned} R_1 &= R_0 + 1 \\ R_2 &= R_1 + 2 \\ R_3 &= R_2 + 3 \\ R_4 &= R_3 + 4 \\ R_5 &= R_4 + 5\,. \end{aligned}$$

Exercise 1.8.3. Write down a recursion for R_n. Compute R_n for $n = 6, 7, \ldots, 10$.

Exercise 1.8.4. From your data in Exercises 1.8.2 and 1.8.3, guess an explicit formula (try subtracting one from each number).

Exercise 1.8.5. Explain each step in the following sequence of calculations:

$$\begin{aligned} R_6 &= R_5 + 6 \\ &= R_4 + 5 + 6 \\ &= R_3 + 4 + 5 + 6 \\ &= R_2 + 3 + 4 + 5 + 6 \\ &= R_1 + 2 + 3 + 4 + 5 + 6 \\ &= R_0 + 1 + 2 + 3 + 4 + 5 + 6 \\ &= 1 + 1 + 2 + 3 + 4 + 5 + 6 \\ &= 1 + \frac{7 \cdot 6}{2}\,. \end{aligned}$$

Use these calculations to prove your guess in the previous exercise.

Chapter 2

Counting

In this chapter, we will describe a variety of counting techniques and principles. These include the fundamental addition and multiplication principles. We will then learn how to count ordered and unordered collections of objects, and how to count collections where some or all elements are repeated. We will also learn how to use counting arguments to show two sets have the same size.

2.1 When to Add and When to Multiply

Three fundamental principles govern almost all of the counting techniques and formulas described in this chapter. These are the *Addition Principle*, the *Multiplication Principle*, and the *Principle of One-to-One Correspondences*.

The Addition Principle is especially easy. It states that the number of elements in the union of two sets which do not intersect is the sum of the number of elements in each set. That is, if A is one set and B is another, and $A \cap B$ is empty, then $n(A \cup B) = n(A) + n(B)$, where $n(A)$ is the number of elements in the set A.

This extends to unions of sets which do intersect as follows. The number of elements in the union of two sets is the sum of the number of elements in each set minus the number of elements in the intersection of the two sets. Using the set language above, $n(A \cup B) = n(A) + n(B) - n(A \cap B)$. This is because elements in the intersection set are counted in both $n(A)$ and $n(B)$. Since they have been counted twice, we must subtract them.

For example, if 13 children are blue-eyed, 6 are left-handed, and 2 are blue-eyed and left-handed, then the number of children who are either blue-eyed or left-handed is $13 + 6 - 2 = 17$.

The Multiplication Principle is harder to state, but usually easier to apply. It states that to count objects which are constructed in several steps, count the number of ways to perform each step and take the product.

For example, Minnesota license plates have three letters followed by three numbers. Therefore, by the multiplication principle, the number of possible license plates is $26 \times 26 \times 26 \times 10 \times 10 \times 10$. This is because we construct a license plate by choosing a letter for the first position, then choosing a letter for the second position, etc. There are 26 ways to perform the first step, then 26 ways to perform the second step, etc.

It is useful to remember that certain phrases or words naturally imply the use of the addition principle or the multiplication principle. The word "or" frequently means the addition principle is involved ("the number of children who are either blue-eyed *or* left-handed"). The phrases "for each" and "and then" usually mean the multiplication principle is involved. For instance, *for each* choice of 26 letters in the first position on the license plate there are 26 possible letters for the second position.

These two principles are often used together, sometimes in rather complicated ways. For example, let's count license plates which begin with **T** or **TT** (but not **TTT**). Note the connector "or." Our plan is first to count the plates that begin with **T** (but not **TT**) and then add the number of the plates that begin with **TT** (but not **TTT**). We add these numbers since we have divided the set we wish to count into these two disjoint cases.

To count each case, we apply the multiplication principle. In the first case, a **T** must be placed in the first position. There are 25 possible letters for the second position (**T** is not allowed), and for each of these choices, there are 26 possible letters for the third position. Using the multiplication principle again to put together the numbers and letters, we have $25 \times 26 \times 10 \times 10 \times 10$ plates in this case.

In the second case, **TT** must be in the first two positions. There are then 25 possible letters for the third position. By the multiplication principle, there are $25 \times 10 \times 10 \times 10$ plates in this case.

Adding the two cases gives $25 \times 27 \times 10 \times 10 \times 10$.

Alternatively, we could count all the plates which begin with **T** and subtract the ones with **TTT**. The number in the former case is $26 \times 26 \times 10 \times 10 \times 10$. The number in the latter case is $10 \times 10 \times 10$. The difference is

$$\begin{aligned}26 \times 26 \times 10 \times 10 \times 10 - 10 \times 10 \times 10 &= (26 \times 26 - 1) \times 10 \times 10 \times 10 \\ &= 25 \times 27 \times 10 \times 10 \times 10\,.\end{aligned}$$

Exercise 2.1.1. Actually in Minnesota, the license plates have three letters followed by three numbers or three numbers followed by three letters. How many possible license plates are there?

In the following exercises, we will assume that the license plates are three letters followed by three numbers.

Exercise 2.1.2. How many license plates have all distinct numbers and letters?

Exercise 2.1.3. How many license plates have a "double letter", that is, two adjacent equal letters? A "double number"? (Note: triple letters are also double letters and triple numbers are also double numbers.)

Exercise 2.1.4. How many license plates have a double letter and a double number? A double letter or a double number?

Suppose there are 15 different apples and 10 different pears. How many ways are there for Jack to pick an apple or a pear and then for Jill to pick an apple or a pear? The "or" connectors tell us that an addition is involved. The "and then" connector tells us a multiplication is involved. Jack has 25 different fruit to choose from $(15 + 10)$. Jill then has 24 different fruit to choose from (since Jack has already taken one). So the number of ways is 25×24.

In Exercises 2.1.5 to 2.1.7, pay particular attention to the conjunctions "and" and "or."

Exercise 2.1.5. How many ways are there for Jack to pick an apple and a pear and then for Jill to pick an apple and a pear?

Exercise 2.1.6. How many ways are there for Jack to pick an apple or a pear and then for Jill to pick an apple and a pear?

Exercise 2.1.7. How many ways are there for Jack to pick an apple and a pear and then for Jill to pick an apple or a pear?

How many subsets of a set of size 3 are there? For instance, if the set is $\{A, B, C\}$, the subsets are $\emptyset$, $\{A\}$, $\{B\}$, $\{C\}$, $\{A, B\}$, $\{A, C\}$, $\{B, C\}$, and $\{A, B, C\}$. Picking such a subset can be thought of as a three-step process. First decide whether A is going to be in the subset. Then decide whether B is going to be in the subset. Finally, decide whether C is going to be in the subset. There are two choices for each decision (either A is in the subset or it is not). By the multiplication principle, there are $2 \times 2 \times 2 = 8$ subsets of $\{A, B, C\}$.

Exercise 2.1.8. How many subsets of a set of size 4 are there? Of a set of size 5? Of a set of size n?

The Principle of One-to-One Correspondences states that if the elements of two sets can be placed into one-to-one correspondence, then they have the same number of elements. We will frequently use this principle when we want to show two sets are counted by the same number, even though we may not know what that number is.

As an example, Exercise 2.1.8 may be rephrased as a license plate problem. Suppose we wish to count "license plates" with only three positions and only the digits 0 and 1 are allowed. Using our previous methods, there are $2 \times 2 \times 2 = 8$ such "license plates." Now let's establish a one-to-one correspondence between these license plates and the subsets of $\{A, B, C\}$. Starting with a license plate, we construct a subset as follows. If the license plate has a 1 in the first position, put A in the subset. If the plate has a 0 in the first position, then A is not in the subset. Similarly, if the plate has a 1 in the second position, place B in the subset. If the plate has a 0 in the second position, then B is not in the subset. Finally, the third position determines whether C is in the subset. For example, the license plate 011 corresponds to the subset $\{B, C\}$. Therefore, by the principle of one-to-one correspondences, the number of subsets of a set with three elements is the same as the number of such license plates.

Exercise 2.1.9. In a similar fashion, the subsets of $\{A, B, C, D, E\}$ correspond to license plates made up of five digits, all 0's or 1's. What subset corresponds to 10011? What license plate corresponds to $\{B, C, E\}$?

This particular one-to-one correspondence will play an important role in Section 2.3

We conclude this section with a very practical "license plate" problem.

Exercise 2.1.10. At one time, every telephone area code had the properties that the first digit was any number except 0 or 1, the middle digit was always 0 or 1 and the last digit could never be the same as the middle digit. How many possible area codes were there? Recently, the restrictions on the middle digit have been removed. Now how many area codes are there?

2.2 Permutations and Ordered Selections

Permutations are ordered collections of objects. Here are some examples.

Exercise 2.2.1. How many different 5-letter words can be formed from the letters in the word SNACK, using each letter exactly once? How many 4-letter words, using each letter no more than once? How many 3-letter words, using each letter no more than once?

Exercise 2.2.2. How many different "decks" of 52 distinct playing cards are there?

Exercise 2.2.3. How many ways can five children be chosen from a group of 15, and arranged in a row?

Several different notations are generally used to represent the number of permutations of n objects k at a time. You may have seen $P(n, k)$, $P_{n,k}$ or ${}_nP_k$. Regrettably, none of these notations conform to what is used by most mathematicians, which is $(n)_k$.

Exercise 2.2.4. Give the answers to Exercise 2.2.1 in this notation.

Exercise 2.2.5. Explain why the number of permutations of 15 objects 5 at a time, $(15)_5$, is $15 \cdot 14 \cdot 13 \cdot 12 \cdot 11$.

Notice that the last term in the above product (11) is $15 - 5 + 1$.

Exercise 2.2.6. Explain why the number of permutations of n objects k at a time is $n \cdot (n-1) \cdot (n-2) \cdots (n-k+1)$. In particular, explain the $(n-k+1)$ final factor in the product.

While there may be disagreement about notation for permutations of n things k at a time, there is none when $k = n$. In this special case, $(n)_n = n! = n \cdot (n-1) \cdot (n-2) \cdots 1$, which is read n *factorial*.

Exercise 2.2.7. Compute $n!$ for all values of $n \leq 10$.

Notice that

$$\begin{aligned}(8)_3 &= 8 \cdot 7 \cdot 6 \\ &= \frac{8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1} \\ &= \frac{8!}{5!} \\ &= \frac{8!}{(8-3)!}\,.\end{aligned}$$

Exercise 2.2.8. Find a formula for $(n)_k$ as a quotient of factorials.

Notice that $5! = 5 \cdot 4!$ and $6! = 6 \cdot 5!$.

Exercise 2.2.9. Prove that $n! = n \cdot (n-1)!$. Explain why this is a recursion.

Exercise 2.2.10. How many ways can 10 children be arranged in a circle? (Two arrangements are different if some child has a different child either on the right or on the left.)

If objects are allowed to be repeated, then a somewhat different formula holds, whose derivation will be the subject of the next few exercises.

Exercise 2.2.11. How many different 5-letter words can be formed using the letters C, A and T, where the letters may be used more than once?

Exercise 2.2.12. A certain alarm company lets you determine your own alarm code. You choose any sequence of four digits, where the allowed digits are 0 through 9. How many different 4-digit alarm codes are there?

Exercise 2.2.13. How many different k-letter words can be formed using letters from a list of n letters, where the letters may be used more than once?

In summary, the number of k letter words formed from a list of n letters, no letter to be used more than once, (which is the same as the number of permutations of n things k at a time) is

$$(n)_k = n \cdot (n-1) \cdot \cdots \cdot (n-k+1) = \frac{n!}{(n-k)!}\,.$$

The number of k letter words formed from a list of n letters, where letters may be used more than once (called "permutations with repetitions") is

$$n^k\,.$$

2.3 Combinations, Subsets and Unordered Selections

Up to now, we have considered selecting objects with some order implied. Now we will simply select objects. For example, if we wish to form all the two-letter words using the letters A, B, C, or D no more than once, we know that there are $4 \times 3 = 12$ ways of doing this. These twelve two-letter words are

AB	BA	CA	DA
AC	BC	CB	DB.
AD	BD	CD	DC

However, if we want to *select* two letters from the letters A, B, C, D, then there are only six ways of doing this: A and B, A and C, A and D, B and C, B and D, and C and D. Notice that the words AB and BA are both represented by the single selection, A and B.

Selections are sometimes called *combinations*, and combinations are just another name for subsets. Since many counting problems can be rephrased in terms of combinations, it is important to recognize combinations in their various guises. We saw above that the number of ways of choosing two things out of four is six. We will see this number now in several other contexts.

In each of the following problems, construct or list the objects described. Your list should have six objects in it for each problem. Then explain why the number of objects in each problem is the same as the number of ways of choosing two things out of four. Your explanation should use the Principle of One-to-One Correspondences.

For example, here are the six different words made up of the letters of the word NOON, i.e., using two N's and two O's: OONN, ONON, NOON, ONNO, NONO, NNOO. These correspond to the subsets above in the manner described in Section 2.1. That is, the location of the N's determine which of the four letters, A, B, C, and D, are in the subset. For example, ONON corresponds to the subset B and D.

Exercise 2.3.1. List the distributions of two identical balls into four different boxes, no more than one ball per box. Give a one-to-one correspondence between these distributions and the selections of two things from four. Which distribution corresponds to the selection $\{B, D\}$?

Exercise 2.3.2. List the different routes Bill can take to work, if Bill lives two blocks south and two blocks west from where he works and he always travels either north or east. Give a one-to-one correspondence between these block-walks and the selections of two things from four. Which block-walk corresponds to the selection $\{B, D\}$?

As in the previous problems, construct or list the objects described. Then give a one-to-one correspondence between the objects in each problem and the three-element subsets of $\{A, B, C, D, E\}$.

Exercise 2.3.3. List the words from the letters of the word COOCO, i. e., using two C's and three O's. Give a one-to-one correspondence between such words and the three-element subsets of $\{A, B, C, D, E\}$. Which word corresponds to $\{B, C, E\}$?

Exercise 2.3.4. Distribute three identical balls into five different boxes, no more than one ball per box. Give a one-to-one correspondence between such distributions and the three-element subsets of $\{A, B, C, D, E\}$. Which distribution corresponds to $\{B, C, E\}$?

Exercise 2.3.5. List the different routes Bill can take to work, if Bill lives two blocks south and three blocks west from where he works and he always travels either north or east. Give a one-to-one correspondence between such block-walks and the three-element subsets of $\{A, B, C, D, E\}$. Which block-walk corresponds to $\{B, C, E\}$?

Exercise 2.3.6. Let $\{A, E, F, H\}$ be a selection of four from a set of size ten given by $\{A, B, C, D, E, F, G, H, I, J\}$. Construct a word with 10 letters, 4 C's and 6 O's, which corresponds to this selection according to the one-to-one correspondence you have discovered in the previous exercises.

Exercise 2.3.7. Find the distribution of balls into boxes which corresponds to the selection of four from ten in Exercise 2.3.6. How many balls and how many boxes are there?

Exercise 2.3.8. Find the route Bill would take to work which corresponds to the selection of four from ten in Exercise 2.3.6. How many blocks south from where he works does he live? How many blocks west?

Exercise 2.3.9. Explain why the number of objects in each of the following three sets is the same as the number of ways of choosing k things out of n.

i. The number of different words made out of n letters, where there are k of one kind of letter and $n-k$ of another kind.

ii. The number of ways of placing k identical balls into n different boxes, no more than one ball per box.

iii. The number of ways Bill can walk to work if he lives k blocks west and $n-k$ blocks south from where he works.

Each of these counting problems has as its answer the number of combinations of n things k at a time. As with permutations, there is disagreement about notation. Elementary books use $C(n,k)$, $C_{n,k}$ or ${}_nC_k$ for this number. However, the binomial coefficient notation is generally well-known, so it is what we will use.

Let's let

$$\binom{n}{k}$$

denote the number of combinations of n things k at a time, or the number of ways of choosing k things from n things. For now we won't worry about a formula for $\binom{n}{k}$. The number $\binom{n}{k}$ is read "n choose k" and is called a *binomial coefficient* (for reasons given below). Notice that the previous exercises have asked you to calculate $\binom{4}{2}$ and $\binom{5}{3}$.

We will eventually derive an explicit formula for $\binom{n}{k}$ involving factorials (a formula some of you may be familiar with). However, at this point we wish to emphasize the enumerative aspects of $\binom{n}{k}$. Our knowledge of $\binom{n}{k}$ is therefore restricted to our observation that it counts the number of selections of k things out of n things.

Exercise 2.3.10. Explain why

$$\binom{n}{k} = \binom{n}{n-k}.$$

(As mentioned in the previous paragraph, is not necessary to know a formula for $\binom{n}{k}$ to show this! Simply establish a one-to-one correspondence between objects counted by the left-hand side and objects counted by the right-hand side.)

Exercise 2.3.11. Explain why

$$2^n = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n-1} + \binom{n}{n}.$$

Hint: Show that both sides of the equation count all the subsets of a set of size n. Use Exercise 2.1.8.

Exercise 2.3.12. Write down the value of $\binom{n}{1}$, $\binom{n}{n-1}$, $\binom{4}{2}$, $\binom{5}{2}$, and $\binom{5}{3}$.

Exercise 2.3.13. Write down the value of $\binom{n}{0}$ and $\binom{n}{n}$. Give a reason for your answer.

The reason $\binom{n}{k}$ is called the binomial coefficient is that it is the coefficient of a term in the expansion of a binomial raised to a power. For instance, if we expand $(x+y)^4$, we get

$$(x+y)^4 = x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4 \,.$$

Notice that the coefficient of x^2y^2 is 6, which is $\binom{4}{2}$, the number we encountered in the first set of exercises of this section. To see this, first rewrite

$$(x+y)^4 = (x+y)(x+y)(x+y)(x+y)\,. \tag{2.1}$$

Now let's keep track of which $(x+y)$ each x and y comes from when the four $(x+y)$'s are multiplied. That is, rewrite Equation (2.1) with the four factors labeled:

$$\underset{1}{(x+y)} \quad \underset{2}{(x+y)} \quad \underset{3}{(x+y)} \quad \underset{4}{(x+y)} \tag{2.2}$$

When Expression (2.2) is expanded, we will get terms like $xyyx$, indicating that the two x's come from the first and fourth factors in Expression (2.2). Notice that this term is simply x^2y^2 in Equation (2.1).

Exercise 2.3.14. Five other terms in Expression (2.2) will have two x's and two y's. List them. Explain why the number of terms in Expression (2.2) with two x's and two y's is $\binom{4}{2}$.

Exercise 2.3.15. In a similar manner, explain why the coefficient of x^3y^2 in $(x+y)^5$ is $\binom{5}{3}$.

Exercise 2.3.16. Finally, explain why the coefficient of x^ky^{n-k} in $(x+y)^n$ is $\binom{n}{k}$.

Exercise 2.3.16 completes the proof of the binomial theorem.

Theorem 1 (The Binomial Theorem)**.**

$$\begin{aligned}(x+y)^n = \binom{n}{n}x^ny^0 + \binom{n}{n-1}x^{n-1}y^1 + \binom{n}{n-2}x^{n-2}y^2 + \cdots \\ + \binom{n}{2}x^2y^{n-2} + \binom{n}{1}x^1y^{n-1} + \binom{n}{0}x^0y^n\end{aligned} \,.$$

For example, let's expand $(3x/2 - x^2)^3$. Then

$$\begin{aligned}(3x/2 - x^2)^3 &= \binom{3}{3}(3x/2)^3(-x^2)^0 + \binom{3}{2}(3x/2)^2(-x^2)^1 \\ &\quad + \binom{3}{1}(3x/2)^1(-x^2)^2 + \binom{3}{0}(3x/2)^0(-x^2)^3 \\ &= 1 \cdot \frac{27x^3}{8} \cdot 1 + 3 \cdot \frac{9x^2}{4} \cdot (-x^2) + 3 \cdot \frac{3x}{2} \cdot (x^4) + 1 \cdot 1 \cdot (-x^6) \\ &= \frac{27x^3}{8} - \frac{27x^4}{4} + \frac{9x^5}{2} - x^6 .\end{aligned}$$

For another example, let's find the coefficient of a^9 in the expansion of $(2a^3 - b)^7$. We have to cube a^3 to get a^9, so the term containing a^9 will be

$$\binom{7}{3} \cdot (2a^3)^3 \cdot (-b)^4 = 35 \cdot (8a^9) \cdot (b^4) = 280a^9b^4 .$$

The coefficient of a^9 is then $280b^4$.

Exercise 2.3.17. Expand $(2x + 5y)^7$.

Exercise 2.3.18. Find the coefficient of x^6 in $(2x^2 + 3)^5$.

Exercise 2.3.19. Find the coefficient of s^3t^8 in $(s - 3t^2)^7$.

Exercise 2.3.20. What is the coefficient of $x^{11}y^9$ in the expansion of $(x+y)^{20}$? What is the coefficient of y^5 in the expansion of $(2 + y)^{10}$?

Exercise 2.3.21. Expand

$$\left(a^{2/3} + \frac{\sqrt{b}}{2}\right)^4 .$$

An approximation technique used by many scientists is based on the binomial theorem.

Exercise 2.3.22. Use the binomial theorem to calculate 1.001^3 by expanding $(1 + .001)^3$.

Exercise 2.3.23. Use the binomial theorem to calculate 2007^4 by expanding $(2000 + 7)^4$.

These exercises illustrated the following point. If B is much larger than z, then $(B + z)^n$ can be approximated by using only the first two terms from the binomial theorem: $B^n + nB^{n-1}z$. The higher powers of z make the contribution of the other terms insignificant.

Exercise 2.3.24. Use this technique to approximate 1.001^3 and 2007^4.

The binomial theorem is the source of many identities involving binomial coefficients. For example, if we let $x = 1$ and $y = 1$ in the binomial theorem, we get the identity in Exercise 2.3.11.

Exercise 2.3.25. By another choice of x and y in Theorem 1, show why

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots \pm \binom{n}{n-1} \mp \binom{n}{n} = 0\,.$$

The binomial coefficients satisfy an important recursion called Pascal's identity. The next four exercises lead us to this recursion.

Exercise 2.3.26. Suppose we want to choose 4 students from a group of 10 students. How many ways are there to do this if we know that one of the students (Bill) is among the four (keep your answer in terms of binomial coefficients)?

Exercise 2.3.27. Suppose we want to choose 4 students from a group of 10 students. How many ways are there to do this if we know that Bill is not among the four?

Exercise 2.3.28. Use Exercises 2.3.26 and 2.3.27 to explain why

$$\binom{10}{4} = \binom{9}{4} + \binom{9}{3}\,.$$

Exercise 2.3.29. More generally, explain why the following holds:

$$\text{Pascal's Identity:} \quad \binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}\,. \tag{2.3}$$

If we know all the binomial coefficients for a certain value of n, we may use them in Pascal's identity to compute all the binomial coefficients for the next value of n. For example, if we know that $\binom{4}{2} = 6$ and $\binom{4}{3} = 4$, then $\binom{5}{3} = \binom{4}{3} + \binom{4}{2} = 4 + 6 = 10$. Doing this kind of calculation we can compute a table of the binomial coefficients, where the rows of the table are the different $n \geq 0$ and the columns are the different k, $0 \leq k \leq n$. The entries of the table are the $\binom{n}{k}$.

For example, here is the table for $n \leq 5$:

n \ k	0	1	2	3	4	5
0	1					
1	1	1				
2	1	2	1			
3	1	3	3	1		
4	1	4	6	4	1	
5	1	5	10	10	5	1

Such a table is called *Pascal's triangle.*

Exercise 2.3.30. Complete the above table for $n \leq 10$.

There is also a simple explicit formula for binomial coefficients. In the next four exercises, we establish this formula.

Exercise 2.3.31. Suppose we want to choose 4 students from a group of 10 students, and then from these four we want to pick a chairperson, vice chairperson, secretary and treasurer. How many ways are there to do this? (Your answer should involve a binomial coefficient.)

Exercise 2.3.32. Suppose we choose a chairperson, vice chairperson, secretary and treasurer from among the 10 students. How many ways are there to do this? Is this the same as Exercise 2.3.31?

Exercise 2.3.33. Use Exercises 2.3.31 and 2.3.32 to give a formula for $\binom{10}{4}$. Verify your formula from the table computed in Exercise 2.3.30.

Exercise 2.3.34. Use Exercises 2.3.31, 2.3.32 and 2.3.33 as a model to give a formula for $\binom{n}{k}$. Use your formula to prove

$$\boxed{\binom{n}{k} = \frac{n!}{k!(n-k)!}}.$$

There are hundreds of formulas involving binomial coefficients. Here are a couple.

Exercise 2.3.35. Prove

$$k\binom{n}{k} = n\binom{n-1}{k-1}.$$

Exercise 2.3.36. More generally, prove

$$\binom{n}{k}\binom{k}{j} = \binom{n}{j}\binom{n-j}{k-j}.$$

Exercise 2.3.37. Explain the phrase "more generally" in the previous exercise. That is, show that the formula in Exercise 2.3.35 is a special case of the formula in Exercise 2.3.36.

Exercise 2.3.38. By specializing the formula in Exercise 2.3.35, prove

$$\frac{1}{n+1}\binom{2n}{n} = \frac{1}{2n+1}\binom{2n+1}{n+1}.$$

Many counting problems require binomial coefficients. Here are a few.

Exercise 2.3.39. How many ways are there to pick a 5-person basketball team from 10 possible players? How many teams if the weakest player and the strongest player must be on the team?

Exercise 2.3.40. In how many ways can the 10 basketball players split into two teams to play each other?

Exercise 2.3.41. How many ways can a committee be formed from four men and six women with at least two men and at least twice as many women as men? With four members, at least two of which are women, and Jennifer and Richard will not serve together?

Exercise 2.3.42. How many triangles can be formed by joining different sets of three corners of a regular octagon? How many triangles if no pair of adjacent corners are permitted?

Exercise 2.3.43. Suppose that in a certain northern Minnesota lake, there are N walleyes. Suppose that 100 of these have been marked. How many ways of picking a sample of 200 walleyes are there such that exactly 5 of them are marked?

Exercise 2.3.44. How many ways can Bill walk to work if he lives 10 blocks south and 8 blocks west of where he works if the east-west block which is 4 blocks north of his house and between 2 and 3 blocks east of his house is flooded by the creek? See Figure 2.1 below. (Hint: First count all block-walks, then subtract the ones which use the flooded street.)

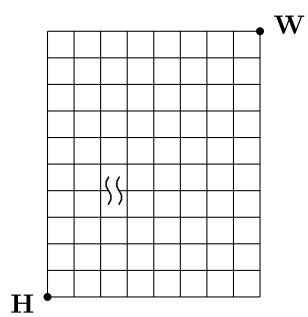


Figure 2.1: Bill's block walk

2.4 Selections with Repetitions

Sometimes we want to count permutations where some objects may be repeated a prescribed number of times. For instance, while there are six rearrangements of the letters of the word CAT (CAT, CTA, ACT, ATC, TAC, TCA), there are only three rearrangements of the letters of the word BEE (BEE, EBE, EEB).

We can compute this number as follows: first pick the position for the B. There are $\binom{3}{1} = 3$ ways to pick this position. Then pick positions for the two E's. There is $\binom{2}{2} = 1$ way to do this. So the number of such rearrangements is $3 \cdot 1 = 3$.

Exercise 2.4.1. How many rearrangements of the letters of the word MISSISSIPPI are there? Hint: Proceed as in the example above. Imagine eleven empty spaces for the letters of the word you are forming. Pick four of them and place I's. Then pick four out of the remaining seven and place S's, and so on.

Exercise 2.4.2. Use the techniques you discovered in Exercise 2.4.1 to find the number of rearrangements of the letters in the words SNACK and SYZYGY.

Exercise 2.4.3. A box contains 16 crayons, no two of the same color. In how many different ways can they be given to four children so that each child receives 4 crayons? How is this exercise similar to Exercises 2.4.1 and 2.4.2?

Exercise 2.4.4. How many ways can 12 students be divided into four groups of three? Into three groups of four? Into 2 groups of four and 2 groups of two? Be very careful in this exercise. There is an important difference between it and Exercise 2.4.3. What is that difference?

Now let's count selections where objects may be repeated. Suppose we wish to count selections of two letters from the letters A, B and C, but we can pick a letter more than once. There are six such selections: {A,A}, {A, B}, {A, C}, {B, B}, {B, C}, and {C, C}. The exercises below ask you to find one-to-one correspondences to show that other counting problems are the same as counting selections with repetitions.

Exercise 2.4.5. List the six distributions of two identical candy bars to three children, where a child may receive more than one candy bar. Give a one-to-one correspondence between these distributions and the selections of two letters from three, with repetitions allowed. What distribution corresponds to the selection $\{B, C\}$? To the selection $\{B, B\}$?

Exercise 2.4.6. List the six distributions of two identical balls into three different boxes. Give a one-to-one correspondence between these distributions and the selections of two letters from three, with repetitions allowed. What distribution corresponds to the selection $\{B, C\}$? To the selection $\{B, B\}$?

Exercise 2.4.7. List the six different solutions to the equation $x + y + z = 2$ where x, y and z are all integers ≥ 0. Give a one-to-one correspondence between these solutions and the selections of two letters from three, with repetitions allowed. What solution corresponds to the selection $\{B, C\}$? To the selection $\{B, B\}$?

Exercise 2.4.8. List all the distributions of three identical candy bars to two children, where a child may receive more than one candy bar. Give a one-to-one correspondence between these distributions and the selections of three letters from $\{A, B\}$, with repetitions allowed. What distribution corresponds to the selection $\{A, B, B\}$?

Exercise 2.4.9. List all the distributions of three identical balls into two different boxes. Give a one-to-one correspondence between these distributions and the selections of three letters from $\{A, B\}$, with repetitions allowed. What distribution corresponds to the selection $\{A, B, B\}$?

Exercise 2.4.10. List all the different solutions to the equation $x + y = 3$ where x and y are integers ≥ 0. Give a one-to-one correspondence between these solutions and the selections of three letters from $\{A, B\}$, with repetitions allowed. What solution corresponds to the selection $\{A, B, B\}$?

Exercise 2.4.11. Explain why the following numbers are the same

i. The number of ways of choosing k letters from a list of n letters, with repetition allowed.

ii. The number of distributions of k identical candy bars to n children, where a child may receive more than one candy bar.

iii. The number of distributions of k identical balls into n distinct boxes.

iv. The number of solutions to the equation

$$x_1 + \cdots + x_n = k$$

where $x_1, x_2, \ldots, x_n$ are all integers ≥ 0.

Let's look at an example of Exercise 2.4.11, part iv, in more detail. Suppose $n = 3$ and $k = 5$, so we want the number of solutions to $x_1 + x_2 + x_3 = 5$ in non-negative integers. An example of such a solution is $x_1 = 2$, $x_2 = 1$ and $x_3 = 2$. Let's create a "word", using 5 O's and 2 I's which "corresponds" to this solution, by first writing 2 O's, then an I, then 1 O, then an I, and finally 2 O's: OOIOIOO. The I's act as "separators" between the O's, and the blocks of consecutive O's have sizes 2, 1, and 2, the values of x_1, x_2 and x_3.

On the other hand, we could take any word with 5 O's and 2 I's (for example, OIIOOOO) and turn it into a solution to our equation $x_1 + x_2 + x_3 = 5$: x_1 is the number of O's before the first I; x_2 is the number of O's between the two I's; and x_3 is the number of O's after the last I. In the example OIIOOOO, $x_1 = 1$, $x_2 = 0$, and $x_3 = 4$.

Exercise 2.4.12. To what solution to the equation $x_1 + x_2 + x_3 = 5$ does the word OOIOOOI correspond?

Exercise 2.4.13. Let $\mathbf{w}$ be the word of O's and I's which corresponds to a solution to the equation

$$x_1 + \cdots + x_n = k$$

as described above. What is the relationship between the number of letters in **w** and n and k? What is the relationship between the number of O's in **w** and k?

Exercise 2.4.13 and the discussion above establishes a one-to-one correspondence between non-negative integer solutions to

$$x_1 + \cdots + x_n = k$$

and words of O's and I's.

Exercise 2.4.14. Using the Principle of One-to-One Correspondences, the discussion above, and Exercise 2.4.13, show the following:

> The number of ways of choosing k letters from n distinct letters, with repetitions allowed, and the number of solutions to the other counting problems listed in Exercise 2.4.11, is
>
> $$\binom{n+k-1}{k}.$$

Here are some problems whose solutions require counting selections with repetitions.

Exercise 2.4.15. How many different fruit baskets containing 8 pieces of fruit can be formed using only apples, oranges and pears? How many if at least one piece of each kind of fruit is used?

Exercise 2.4.16. In how many ways can 10 identical quarters be distributed to five people?

Exercise 2.4.17. Find the number of integer solutions to the equation

$$x + y + z = 13, \qquad \text{where} \qquad x \geq 1,\ y \geq 0 \text{ and } z \geq 6\,.$$

Exercise 2.4.18. How many ways can each of seven identical wine glasses be filled with one of four kinds of wine: burgundy, chablis, pinot noir and merlot. How many ways if at least one glass contains chablis? How many ways if at least one glass contains chablis and no more than two glasses contain merlot?

A pizza company is offering a special on two pizzas. Each pizza is to be made using some of the following five extra toppings: olives, pepperoni, mushrooms, onions, and sausage. The company's television advertisement claims that there are over one million possibilities. The following exercises ask you to count the number of possibilities, making various assumptions about how the toppings can be used.

Exercise 2.4.19. Suppose each pizza can have any subset of the extra toppings (so double pepperoni is not allowed, while no topping at all is allowed). How many possible pairs of pizzas are there? Hint: use the formula for the number of subsets of a set of size n you obtained in Exercise 2.1.8 to find the number of possible pizzas. Then use the formula in Exercise 2.4.14 above to count the number of pairs of pizzas.

Exercise 2.4.20. Suppose each pizza can have any five toppings (so triple pepperoni, onion and sausage would be an example, but just pepperoni would not be). Now how many pairs of pizzas are there? Hint: count pizzas by selecting five toppings from the five toppings, allowing repetitions.

Exercise 2.4.21. Suppose each pizza can have any five or fewer toppings (triple pepperoni and sausage, for example). Now how many pairs of pizzas are there? Hint: introduce a sixth "blank" topping and use the idea in the previous exercise.

2.5 Card Games

Here are some problems involving card games.

A standard deck of cards has 52 cards, broken up into four suits: hearts ($\heartsuit$), diamonds ($\diamondsuit$), clubs ($\clubsuit$), and spades ($\spadesuit$). Each suit has 13 cards each. These are 2, 3, 4, 5, 6, 7, 8, 9, 10, Jack (J), Queen (Q), King (K) and Ace (A). These thirteen cards are given an order, called *rank*. The rank order of the thirteen is specified in the list above. In particular, for our purposes, the ace has the highest rank.

Bridge is a game played by four players, each player receiving 13 cards. A bridge hand consists of a selection of 13 cards.

Exercise 2.5.1. How many bridge hands are there?

Exercise 2.5.2. How many "perfect" hands are there (all one suit)?

Exercise 2.5.3. How bridge hands have exactly 4 cards of one (unspecified) suit and exactly 3 cards in each of the other three suits? (Such a hand is said to have 4-3-3-3 distribution.)

Exercise 2.5.4. How many bridge hands are there that contain 4 diamonds and 3 of each of the other three suits?

A poker hand has five cards. The following exercises ask you to count the number of each kind of poker hand.

Exercise 2.5.5. How many total poker hands are there?

Exercise 2.5.6. A *flush* has all five cards of the same suit. How many flushes are there?

Exercise 2.5.7. A *straight* has all five cards in sequence (e.g., 3-4-5-6-7 or 8-9-10-J-Q). How many straights are there?

Exercise 2.5.8. A *straight flush* is both a straight and a flush. How many straight flushes are there?

Exercise 2.5.9. A *full house* has three of one kind and two of another kind (e.g., 5-5-5-A-A). How many full houses are there?

Exercise 2.5.10. *Four of a kind* has four of one kind (e.g., J-J-J-J-9). How many four-of-a-kinds are there?

Exercise 2.5.11. *Three of a kind* has three of one kind (but not four of a kind and not a full house). How many three-of-a-kinds are there?

Exercise 2.5.12. *Two pair* has two of one kind, two of another kind, and the fifth card of a third kind (e.g., 5-5-8-8-K). How many two pairs are there?

Exercise 2.5.13. A *pair* has two of one kind (and nothing more) (e.g., 7-7-2-K-A). How many pairs are there?

Chapter 3

Catalan Numbers

This chapter is about the Catalan numbers, a number sequence almost as famous as the Fibonacci numbers. We will give a number of problems whose solution is the Catalan numbers. We will describe the sequence of Catalan numbers by a recursion and by an explicit formula.

3.1 Several Counting Problems

In this section we will describe several different sequences of numbers. We describe these sequences as solutions to counting problems. In subsequent sections, we show that these problems are all solved by the same sequence of numbers.

The first problem is how many ways are there to triangulate a polygon. There are two ways to "triangulate" a quadrilateral. These are shown in Figure 3.1. There are five ways to "triangulate" a pentagon. These are shown in Figure 3.2.

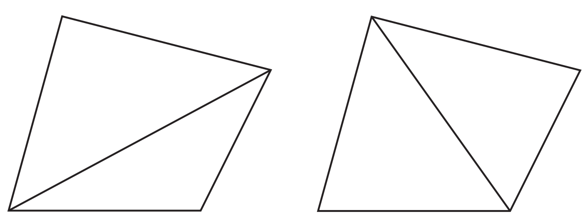


Figure 3.1: Triangulations of a quadrilateral

By "triangulate", we mean draw non-intersecting diagonals so that the interior of the polygon is partitioned into triangles. A triangulation of a hexagon is shown in Figure 3.3.

Exercise 3.1.1. Find all the ways to "triangulate" a hexagon.

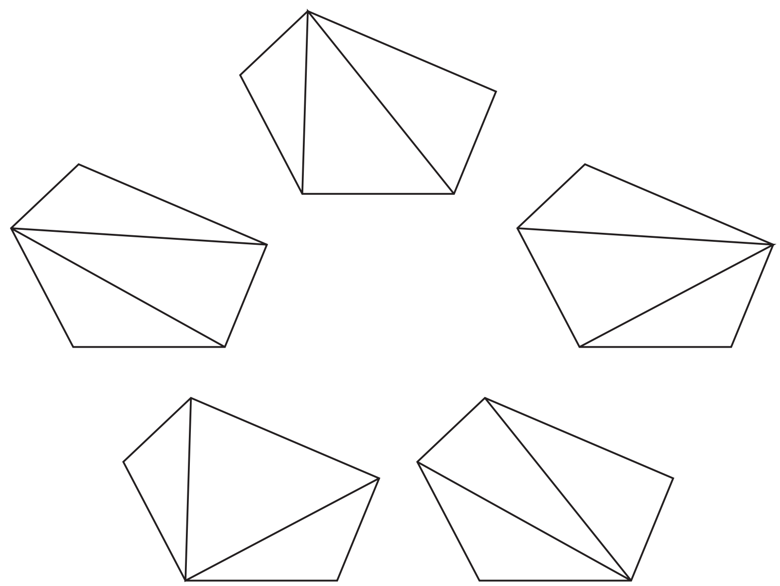


Figure 3.2: Triangulations of a pentagon

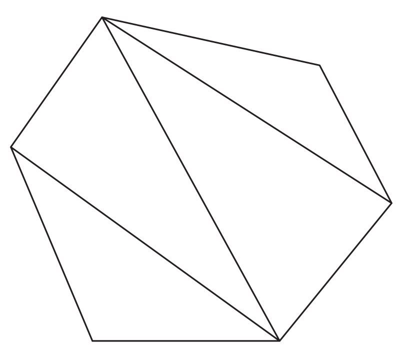


Figure 3.3: Triangulation of a hexagon

Exercise 3.1.2. Bill lives three blocks south and three blocks west from where he works. A railroad track runs diagonally from southwest to northeast, from just southeast of his house to just northeast of his work. Bill can take any of five different routes from home to work without crossing the tracks: **NNNEEE, NNENEE, NNEENE, NENNEE, NENENE** (see Figure 3.4). Find all the different routes he could take, without crossing tracks, if he lived four blocks south and four blocks west from where he works.

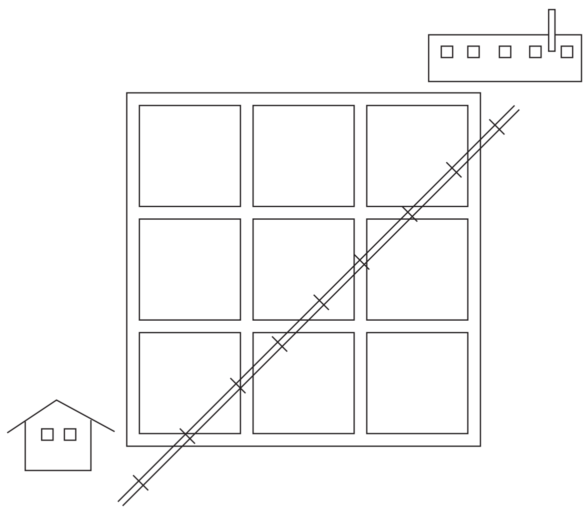
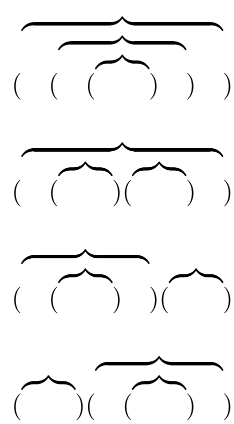


Figure 3.4: Blockwalking

Exercise 3.1.3. A sequence of parentheses is *well-formed* if every open parenthesis "(" can be paired with a closed parenthesis ")" to its right in such a way so that the parentheses pairs are "nested." There are five such sequences of 3 pairs. Here they are with the nestings indicated by braces:



$$\overbrace{(\qquad)}\overbrace{(\qquad)}\overbrace{(\qquad)}$$

Find all the sequences of 4 pairs.

Exercise 3.1.4. A sequence of parentheses is *balanced* if the number of open parentheses equals the number of closed parentheses and, at every point in the sequence, the number of open parentheses to the left of that point is greater than or equal to the number of closed parentheses to the left of that point. There are five such sequences of 3 pairs: ((())), (()()), (())(), ()(()), ()()(). Find all the sequences of 4 pairs.

Note that the well-formed sequences of parentheses and the balanced sequences of parentheses you found in Exercises 3.1.3 and 3.1.4 are the same. We will prove this in general in a later section.

Exercise 3.1.5. Alice, Brenda, Carlos, Duc, Elaine and Frank are seated in that order around a round table. They can shake hands with one another across the table, without crossing handshakes, in any one of five ways:

AB-CD-EF,
AB-CF-DE,
AD-BC-EF,
AF-BC-DE,
AF-BE-CD.

Suppose Georgia and Henry sit down at the table between Frank and Alice. Find all the ways the eight people can shake hands across the table without crossing handshakes.

Exercise 3.1.6. Here are all triples of integers (x_1, x_2, x_3) subject to the conditions that $x_1 = 0$, $x_2 = 0$ or 1, $x_3 = 0$, 1 or 2 and $x_1 \le x_2 \le x_3$:

$$(0,0,0),$$
$$(0,0,1),$$
$$(0,0,2),$$
$$(0,1,1),$$
$$(0,1,2).$$

Write down all quadruples of integers (x_1, x_2, x_3, x_4) subject to the conditions that $x_1 = 0$, $x_2 = 0$ or 1, $x_3 = 0$, 1 or 2, $x_4 = 0$, 1, 2 or 3 and $x_1 \le x_2 \le x_3 \le x_4$.

Exercise 3.1.7. Outlines contain various levels of headings. The possible outline structures for all outlines with three headings, possibly at different levels, are shown in Figure 3.5. List all the outline structures with four headings.

Six children, Aaron, Beatrice, Chen, Diana, Eduardo and Faye, are all of different heights. Suppose Aaron is taller than Beatrice, Beatrice is taller than Chen, Chen is taller than Diana, Diana is taller than Eduardo, and Eduardo is taller than Faye. Let's number the children: Aaron is 1, Beatrice is 2, Chen is

I			I			I		
II				A		II		
III			II				A	

I			I		
	A			A	
	B				1

Figure 3.5: Outlines with three headings

3, Diana is 4, Eduardo is 5 and Faye is 6. So one child is taller than another translates into its number being less than the other's.

There are 5 ways the children can be arranged in two rows and three columns so that the children decrease in height down each column and across each row, as shown in Figure 3.6. We call such an arrangement of numbers a 2×3 *tableau.* Each row and each column of a tableau is in increasing order.

Exercise 3.1.8. Now suppose Ginny and Hal join the group and Faye is taller than Ginny who is taller than Hal. Again, replace Ginny by 7 and Hal by 8. List all the ways the eight children can be arranged in two rows and four columns so that the children decrease in height down each column and across each row. That is, list all the 2×4 tableaux.

1	2	3	1	2	4	1	2	5	1	3	4	1	3	5
4	5	6	3	5	6	3	4	6	2	5	6	2	4	6

Figure 3.6: Tableaux of children

Exercise 3.1.9. For any one of Exercises 3.1.1 to 3.1.8, list all possibilities for the next case. For example, list all the possible triangulations of a heptagon (a seven-sided polygon).

Each of the objects above can be used to define a sequence of numbers. For instance, let BW_n denote the number of ways Bill can walk to work if he lives n blocks south and n blocks west of work, if he cannot walk in the region southeast of the diagonal from home to work. You have seen that $BW_3 = 5$ and $BW_4 = 14$. We will call such a block-walk a *non-crossing* block-walk.

Similarly, define $\{TR_n\}$ so that TR_3 is the number of ways to triangulate a pentagon and TR_4 is the number of ways to triangulate a hexagon.

In the same fashion, define $\{WF_n\}$, $\{BA_n\}$, $\{HS_n\}$, $\{IS_n\}$, $\{OL_n\}$, and $\{TB_n\}$. Thus, WF_3 is the number of well-formed sequences of parentheses with 3 pairs of parentheses, BA_3 is the number of balanced sequences of parentheses with 3 pairs of parentheses, and HS_3 is the number of ways 6 people seated around a table can shake hands without crossing handshakes. Also, IS_3 is the number of triples of integers described in Exercise 3.1.6, OL_3 is the number of outline structures with 3 headings, and TB_3 is the number of 2×3 tableaux.

The discussion above shows that all the sequences take the value 5 when the parameter is 3, that is,

$$TR_3 = WF_3 = BA_3 = HS_3 = IS_3 = OL_3 = TB_3 = BW_3 = 5\,.$$

Exercises 3.1.1 to 3.1.8 show that all the sequences take the value 14 when the parameter is 4.

Exercise 3.1.10. Show that all the sequences take the value 2 when the subscript is 2.

Exercise 3.1.11. Show that all the sequences take the value 1 when the subscript is 1.

Exercise 3.1.12. Describe how the parameter of the sequence relates to the parameter of the problem for each of Exercises 3.1.1 to 3.1.8. For example, in the triangulations of a polygon, what is the relationship between the n in TR_n and the number of sides of the polygon being triangulated?

We will assume that the sequences all take the value 1 when the parameter is 0. This even makes some sense: $BW_0 = 1$, for if Bill lives where he works, then he has one legal path to work—he sits still!

Thus we have seen that all eight of the sequences defined in this section begin $\{1, 1, 2, 5, 14, \dots\}$, where the initial term is indexed by 0.

The rest of this chapter will be devoted to solving the following three problems:

i. Show that all of the sequences above are the same sequence.

ii. Find a recursion for this sequence.

iii. Find an explicit formula for this sequence.

Section 3.2 will be devoted to showing

$$BW_n = BA_n = IS_n = TB_n\,, \tag{3.1}$$

and

$$WF_n = HS_n = OL_n\,. \tag{3.2}$$

The technique that we will use is the Principle of One-to-one Correspondences.

Then in Section 3.3 we will show that

$$BW_n = HS_n = TR_n\,, \tag{3.3}$$

by demonstrating that $\{BW_n\}$, $\{HS_n\}$ and $\{TR_n\}$ all satisfy the same recursion and the same initial conditions. This will complete the first two parts of our program outlined above.

Finally, the explicit formula will be derived in Section 3.4.

3.2 One-to-One Correspondences

To show Equations (3.1) and (3.2), we use the Principle of One-To-One Correspondences. For example, a balanced sequence of parentheses counted by BA_n corresponds in a very natural way to a non-crossing block-walk counted by BW_n: simply convert "(" to **N** and ")" to **E**. Thus the sequence **(())()** corresponds to **NNEENE**. The fact that the number of left parentheses is always greater than or equal to the number of right parentheses translates directly into the fact that the block-walk does not cross the diagonal, and vice versa.

The remaining correspondences are somewhat harder. We show one of these correspondences in detail and then ask you to produce the others. You should be warned, however, that each of these correspondences requires a different argument.

Let's show that the objects counted by BW_n correspond to objects counted by TB_n. Suppose we have a $2 \times n$ tableau. List all the numbers in increasing order, from 1 to $2n$. Then replace each number by **N** if the number is in the first row of the tableau, and by **E** if the number is in the second row of the tableau. Thus, the tableau in Figure 3.7 corresponds to **NNEENENNNEENENEE**.

1	2	5	7	8	9	12	14
3	4	6	10	11	13	15	16

Figure 3.7: A 2×8 tableau

We must now explain why the block-walk thus obtained does not cross the railroad track, or, equivalently, why the **N**'s always "stay ahead" of the **E**'s. Suppose for some **E**, the number of **E**'s up to that point in the block-walk exceeds the number of **N**'s. Let's say that the number of **E**'s up to that point is $k+1$, while the number of **N**'s is k. But the $k+1$ **E**'s replaced numbers in the second row of the tableau while the k **N**'s replaced numbers in the first row of the tableau. From the way we constructed the block-walk from the tableau, these $2k+1$ numbers are the $2k+1$ smallest numbers and are therefore arranged in the leftmost positions in their rows. Therefore, the $(k+1)$-st number in second row will be smaller than the $(k+1)$-st number in the first row, which does not give a legal tableau.

The preceding two paragraphs show how to assign a non-crossing block-walk to a tableau. But how do we know that some non-crossing block-walks aren't missed? And how do we know that two tableaux don't give the same block-walk under this correspondence? To answer these questions, we must reverse the identification. Starting with a non-crossing block-walk we must construct the corresponding arrangement of numbers, then verify that it is a legal tableau.

Once again, list the numbers from 1 to $2n$. Above this list, write the block-walk. The numbers below the **N**'s are placed in the first row of the tableau (in increasing order), while the numbers below the **E**'s are placed in the second row of the tableau (in increasing order).

For instance, consider this non-crossing blockwalk:

NENNNENEENEENNEE.

Write it thus:

N	E	N	N	N	E	N	E	E	N	E	E	N	N	E	E
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Then the tableau is that given in Figure 3.8.

1	3	4	5	7	10	13	14
2	6	8	9	11	12	15	16

Figure 3.8: Another 2×8 tableau

This certainly reverses the process described above, and it is clear that the numbers are arranged in order in the rows. But are they arranged in order in the columns? Suppose the number in the second row of the $(k+1)$-st column is smaller than the number in the first row of the $(k+1)$-st column. Let's say that the number in the first row is t and the number in the second row is s. Thus, $s < t$.

Then s corresponds to an **E** in the block-walk. That is, there is an **E** in the s-th position in the block-walk. The k numbers to the left of s in the tableau correspond to k **E**'s to the left of the s-th position in the block-walk. Also, no **N**'s to the left of the s-th position in the block-walk correspond either to t or to a number to the right of t in the tableau, since all these numbers are greater than s. Therefore, there cannot be more than k **N**'s to the left of the s-th position in the block-walk. Thus, the number of **E**'s is greater than the number of **N**'s at s-th position in the block-walk, and so the block-walk must cross the diagonal at (or before) the s-th position. This gives a contradiction to our assumption that we started with a non-crossing block-walk. Therefore, the assumption that the smaller s is above the larger t is wrong.

Exercise 3.2.1. Give a correspondence which shows $BW_n = IS_n$. Which integer sequence corresponds to the non-crossing block-walk **NENNEENNEE** (see Figure 3.9). Which integer sequence corresponds to the non-crossing block-walk **NENNNENEENEENNEE** in your correspondence? Which non-crossing block-walk corresponds to the integer sequence $(0, 0, 0, 1, 1, 5, 5, 6)$?

Notice that by combining the one-to-one correspondence between tableaux and non-crossing block-walks with the one-to-one correspondence in Exercise 3.2.1, we could give a one-to-one correspondence between tableaux and integer sequences.

Exercise 3.2.2. Give a correspondence which shows $WF_n = HS_n$. Which arrangement of handshakes corresponds to the sequence of well-formed parentheses ()((()())())(()) in your correspondence? Suppose **A**, **B**, **C**, **D**, **E**, **F**,

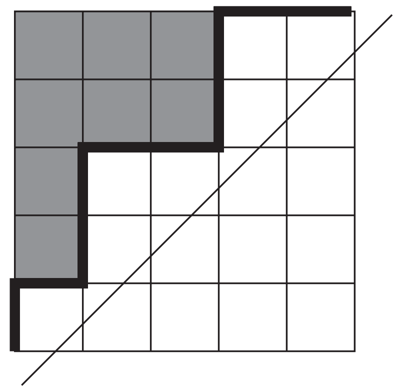


Figure 3.9: Hint: count the shaded blocks in each row

G, **H**, **I**, **J**, **K**, **L**, **M**, **N**, **O**, and **P** are seated around a round table and the following handshakes are made: **AD-BC-EL-FG-HK-IJ-MP-NO**. Give the corresponding sequence of well-formed parentheses.

Exercise 3.2.3. Give a correspondence which shows $WF_n = OL_n$. What outline corresponds to the sequence of well-formed parentheses ()((()())())(()) in your correspondence? What sequence of well-formed parentheses corresponds to the outline:

I
    A
        1
        2
    B
II
III
    A .

Material in the text above and Exercise 3.2.1 have established Equations (3.1). Exercises 3.2.2 and 3.2.3 have established Equations (3.2). What is left is to tie the three groups of sequences given by Equations (3.1), Equations (3.2), and $\{TR_n\}$ together with a common recursion. That is the goal of the next section.

3.3 The Recursion

The recursion formula for the sequences described in the previous section is harder than the recursions for arithmetic and geometric sequences, or for the Fibonacci numbers. We will demonstrate this recursion with three of the sequences described in Section 3.1.

The first sequence for which we will derive the recursion is $\{HS_n\}$.

Exercise 3.3.1. Use the values for HS_0, HS_1, HS_2, HS_3 and HS_4 that you found in Section3.1 to check arithmetically the following equations.

$$
\begin{aligned}
& HS_1 = HS_0 \cdot HS_0, \\
& HS_2 = HS_0 \cdot HS_1 + HS_1 \cdot HS_0, \\
& HS_3 = HS_0 \cdot HS_2 + HS_1 \cdot HS_1 + HS_2 \cdot HS_0, \\
\text{and} \quad & HS_4 = HS_0 \cdot HS_3 + HS_1 \cdot HS_2 + HS_2 \cdot HS_1 + HS_3 \cdot HS_0 .
\end{aligned}
$$

Exercise 3.3.2. From Exercise 3.3.1, conjecture a formula for HS_5, HS_6, and HS_7 and compute values for HS_5, HS_6, and HS_7 based on your conjecture. Compare the conjectured value for HS_5 with what you obtained in Exercise 3.1.9.

Exercise 3.3.3. From Exercises 3.3.1 and 3.3.2 guess a general formula for HS_n.

To demonstrate the derivation of this recursion, suppose there are 16 persons seated around the table. Label these 16 **A** to **P**. Now consider whom **A** shakes hands with. Suppose, for instance, it is **H**. That divides the table into two pieces. Six people are on one side of the **AH** handshake (**B** through **G**) and eight are on the other side (**I** through **P**). See Figure 3.10.

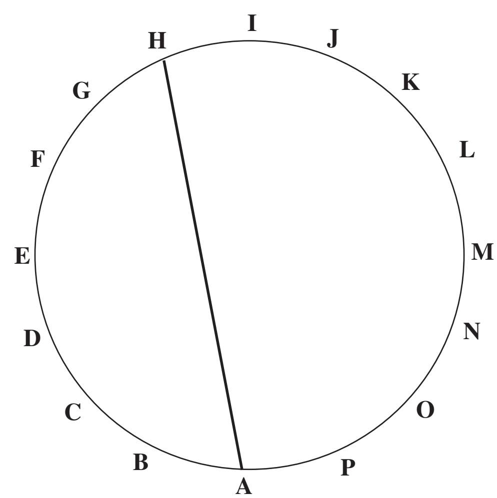


Figure 3.10: 16 people, one handshake

The six people on one side can then shake hands in HS_3 ways, while the eight on the other side can shake hands in HS_4 ways. Therefore, the total number of legal handshake arrangements among the 16, such that **A** and **H** are shaking hands, is $HS_3 \cdot HS_4$.

Exercise 3.3.4. How many legal handshake arrangements among the 16 are there such that **A** and **F** are shaking hands? Such that **A** and **B** are shaking hands? What would happen if **A** and **G** shook hands?

Exercise 3.3.5. List all the possible persons that **A** can shake hands with and give the number of legal handshake arrangements among the 16 that include that handshake. Exercise 3.3.4 is a start of this list.

Exercises 3.3.4 and 3.3.5 demonstrate that

$$HS_8 = HS_7 \cdot HS_0 + HS_6 \cdot HS_1 + HS_5 \cdot HS_2 + HS_4 \cdot HS_3 + HS_3 \cdot HS_4 + HS_2 \cdot HS_5 + HS_1 \cdot HS_6 + HS_0 \cdot HS_7 \,.$$

Exercise 3.3.6. Discuss why HS_0 was defined to be 1.

The argument described in the text above and in Exercises 3.3.4 and 3.3.5 can be made general. Suppose $2n$ people are seated around the table and that Alice is one of those people. Determine who Alice is shaking hands with. That divides the table into two groups, each of which must have a legal handshake arrangement among themselves. The sum of the number of people in the two groups is two less than the total around the table (Alice and her handshake partner are not counted). So the sum, when divided by 2, is $n-1$.

Exercise 3.3.7. Suppose 20 people, numbered from 1 to 20, are seated around a table. Suppose person 1 shakes hands with person 8. See Figure 3.11. How many ways are there for the remaining 18 people to shake hands without any handshakes crossing?

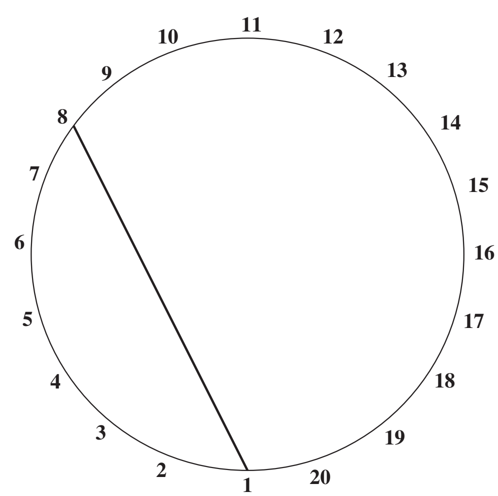


Figure 3.11: 20 people, one handshake

Exercise 3.3.8. Suppose 40 people, numbered from 1 to 40, are seated around a table. Suppose person 1 shakes hands with person 8 and person 14 shakes hands with person 29. See Figure 3.12. How many ways are there for the remaining 36 people to shake hands without any handshakes crossing?

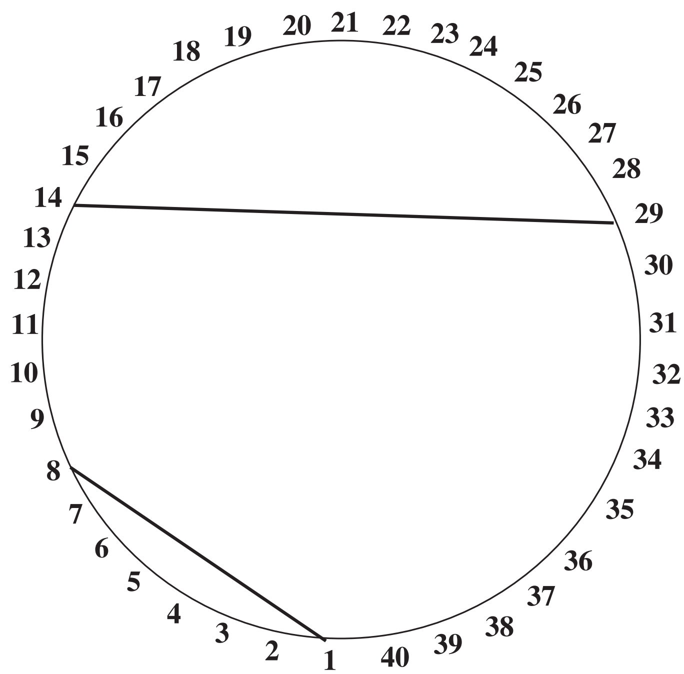


Figure 3.12: 40 people, two handshakes

Next, we show the same recursion for the sequence $\{TR_n\}$. The arguments are similar to what we just did for $\{HS_n\}$.

Exercise 3.3.9. Show how the formula

$$TR_5 = TR_0 \cdot TR_4 + TR_1 \cdot TR_3 + TR_2 \cdot TR_2 + TR_3 \cdot TR_1 + TR_4 \cdot TR_0$$

may be deduced by decomposing the triangulations of a heptagon into triangulations of two smaller polygons. The examples in Figures 3.13 and 3.14 may be of help.

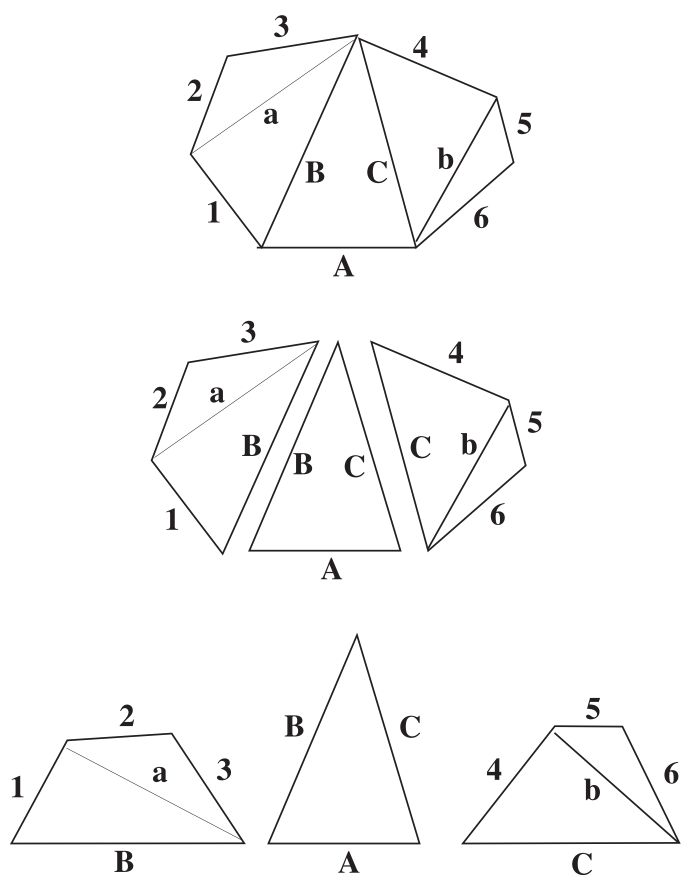


Figure 3.13: Decomposition of a triangulation

Exercise 3.3.10. Now show how the general recursion for $\{TR_n\}$ can be deduced by decomposing the triangulations of the $(n+2)$-gon into triangulations of two smaller polygons.

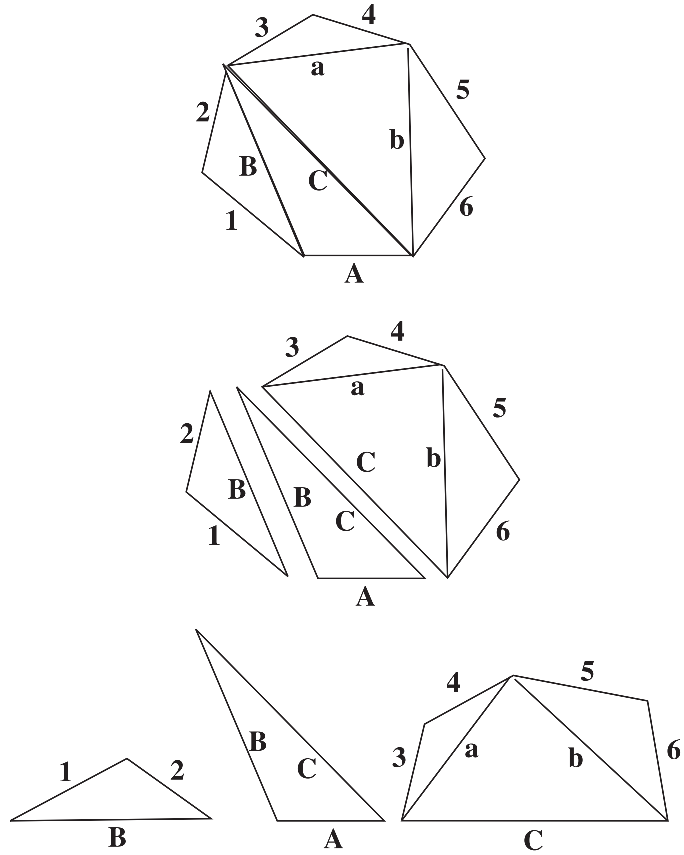


Figure 3.14: Another decomposition of a triangulation

Exercise 3.3.11. Suppose the corners of a 24-sided polygon are numbered from 1 to 24. Find the number of triangulations of this polygon which include the triangle 1-2-9. See Figure 3.15.

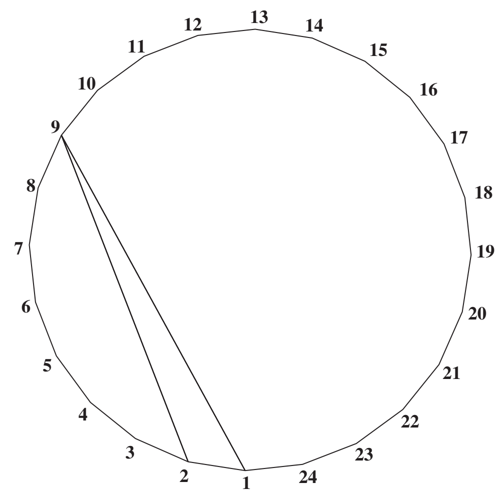


Figure 3.15: Partial triangulation of a 24-gon

Exercise 3.3.12. Suppose the corners of a 24-sided polygon are numbered from 1 to 24. Find the number of triangulations of this polygon which include the triangle 1-8-18. See Figure 3.16

Exercise 3.3.13. Suppose the corners of a 24-sided polygon are numbered from 1 to 24. Find the number of triangulations of this polygon which include the edges 1-8, 1-15 and 16-22. See Figure 3.17

Finally, we want to show that the recursion also holds for the sequence $\{BW_n\}$. In the handshake problem, we found one special handshake, removed it, and broke the remaining people up into two "smaller" tables. In the triangulation problem, we found one special triangle, removed it, and broke the remainder of the polygon into two smaller polygons. Analogously to these cases, we must find a special **N** and **E** pair, remove them, and break the non-crossing block-walk into two smaller non-crossing block-walks.

Figure 3.18 illustrates which north and east edges to remove: they are the ones marked by A and B in the figure. A is the first **N** step along the path, and B is the **E** step just before where the path first returns to the diagonal between **H** and **W**.

Figure 3.19 shows how to create the two smaller block-walks. Let $\mathbf{H}_1$ be the intersection at the north end of A. Let $\mathbf{W}_1$ be the intersection at the west end of B. Then let $\mathbf{H}_2$ be the intersection at the east end of B and let $\mathbf{W}_2$ be $\mathbf{W}$.

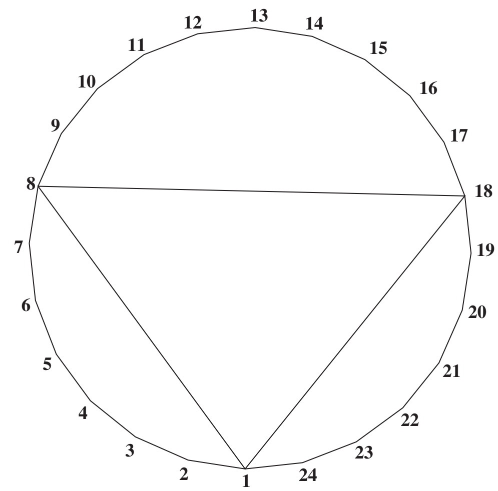


Figure 3.16: Another partial triangulation of a 24-gon

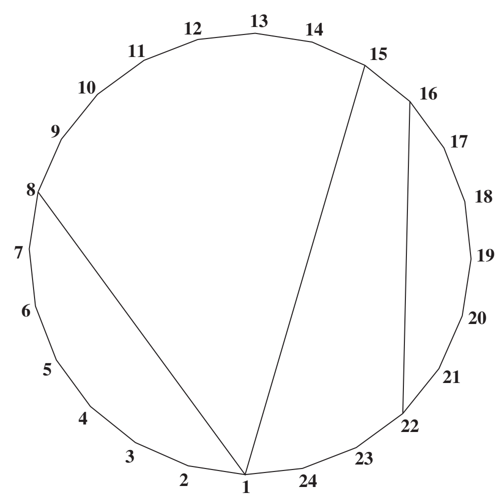


Figure 3.17: Yet another partial triangulation of a 24-gon

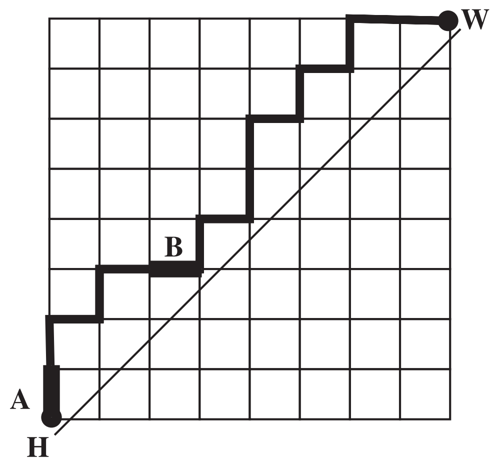


Figure 3.18: A blockwalk northwest of the tracks

Then the first smaller block walk goes from $\mathbf{H}_1$ to $\mathbf{W}_1$, while the second goes from $\mathbf{H}_2$ to $\mathbf{W}_2$. Notice that the path from $\mathbf{H}_1$ to $\mathbf{W}_1$ does not cross a new set of railroad tracks (r_1) located diagonally one block northwest of the original set of railroad tracks.

Exercise 3.3.14. Using Figures 3.18 and 3.19 as guides, write down the general recursion for the sequence $\{BW_n\}$. Prove this recursion.

Exercise 3.3.15. Suppose Bill lives 14 blocks south and 14 blocks west of work. How many non-crossing block-walks are there which first return to the H-W diagonal at location **X** in Figure 3.20?

Exercise 3.3.16. Suppose Bill lives 14 blocks south and 14 blocks west of work. How many non-crossing block-walks are there which return to the H-W diagonal at location **X** in Figure 3.20 (but may return before and after this location)?

Exercise 3.3.17. Suppose Bill lives 20 blocks south and 20 blocks west of work. How many non-crossing block-walks are there which return to the H-W diagonal at **X**, **Y** and **Z** in Figure 3.21, but nowhere else?

Exercises 3.3.10 and 3.3.14 and the discussion above about the handshake problem combine to show that all the sequences discussed in Section 3.1 are counted by the same numbers. We call those numbers *Catalan numbers*. Since all these sequences are the same, we give them a common name, $\{C_n\}$, called the *Catalan sequence*. These numbers were named after the 19th century Belgian mathematician Eugene Charles Catalan, who first discovered them in conjunction with the well-formed parentheses sequence problem.

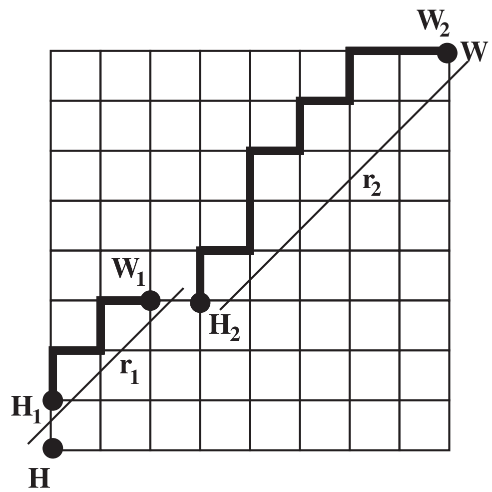


Figure 3.19: Decomposition of a blockwalk

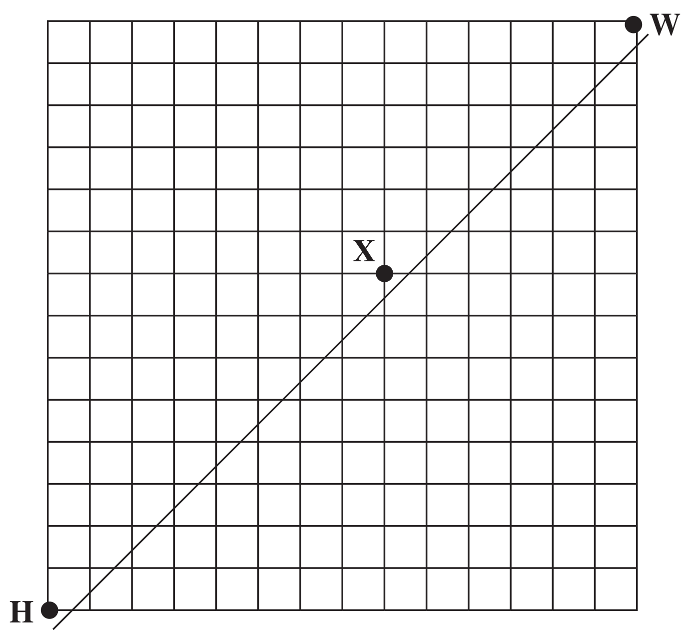


Figure 3.20: A 14-by-14 block-walking grid

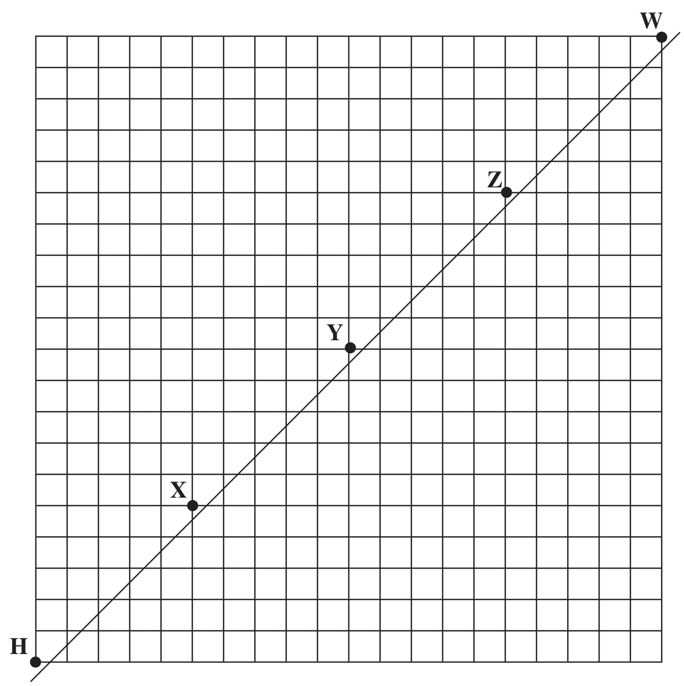


Figure 3.21: A 20-by-20 block-walking grid

Theorem 2. *The number C_n counts each of the following:*

i. *The number of ways to triangulate a polygon with $n+2$ sides.*

ii. *The number of block-walks from southwest to northeast on an $n \times n$ grid which stay northwest of the diagonal.*

iii. *The number of well-formed sequences of $2n$ parentheses.*

iv. *The number of balanced sequences of $2n$ parentheses.*

v. *The number of ways $2n$ people seated around a round table can shake hands without crossing handshakes.*

vi. *The number of n-tuples of integers, $(x_1, x_2, \ldots, x_n)$ subject to the conditions $0 \le x_i < i$ and $x_1 \le x_2 \le \cdots \le x_n$.*

vii. *The number of outlines with n different headings.*

viii. *The number of $2 \times n$ tableaux of children.*

Theorem 3. *The sequence $\{C_n\}$ satisfies the recursion*

$$C_n = C_{n-1}C_0 + C_{n-2}C_1 + \cdots + C_1C_{n-2} + C_0C_{n-1}, \text{ for } n \ge 1\,,$$

with the initial condition that $C_0 = 1$.

Although the Catalan numbers are not as famous as Fibonacci numbers, they also have a long and distinguished history, and they arise in almost as many contexts. They occur in many other settings besides the ones given here, and are also important numbers in computer science.

We conclude this section by showing why well-formed sequences of parentheses and balanced sequences of parentheses are the same.

Exercise 3.3.18. Discuss why each well-formed sequence of $2n$ parentheses is also balanced.

Exercise 3.3.19. Use Exercise 3.3.18 and Theorem 2 to show that the set of well-formed sequences of $2n$ parentheses and the set of balanced sequences of $2n$ parentheses are identical.

3.4 The Explicit Formula

The model we will use to obtain our explicit formula for C_n is the block-walking model. Any of the other counting problems in Section 3.1 could be used, but this one is the easiest.

The technique we use is a common one. Instead of counting the legal routes Bill could take, we count all possible routes and subtract the illegal ones.

Exercise 3.4.1. Suppose Bill lives 3 blocks south and 3 blocks west of work. How many different routes to work does he have (ignoring the railroad tracks) if he can only travel east and north? What if he lives 4 blocks south and 4 blocks west? n blocks south and n blocks west? n blocks south and m blocks west?

Now suppose Bill lives 4 blocks south and 4 blocks west. Let's call a path that crosses the railroad tracks a *bad path* and one that doesn't a *good path*. That is, good paths are exactly non-crossing block-walks. Let's look at one of the bad paths, for example, the one shown in the first picture in Figure 3.22. Bill's home is marked **H** and work is marked **W**. We've called the bad path **r**.

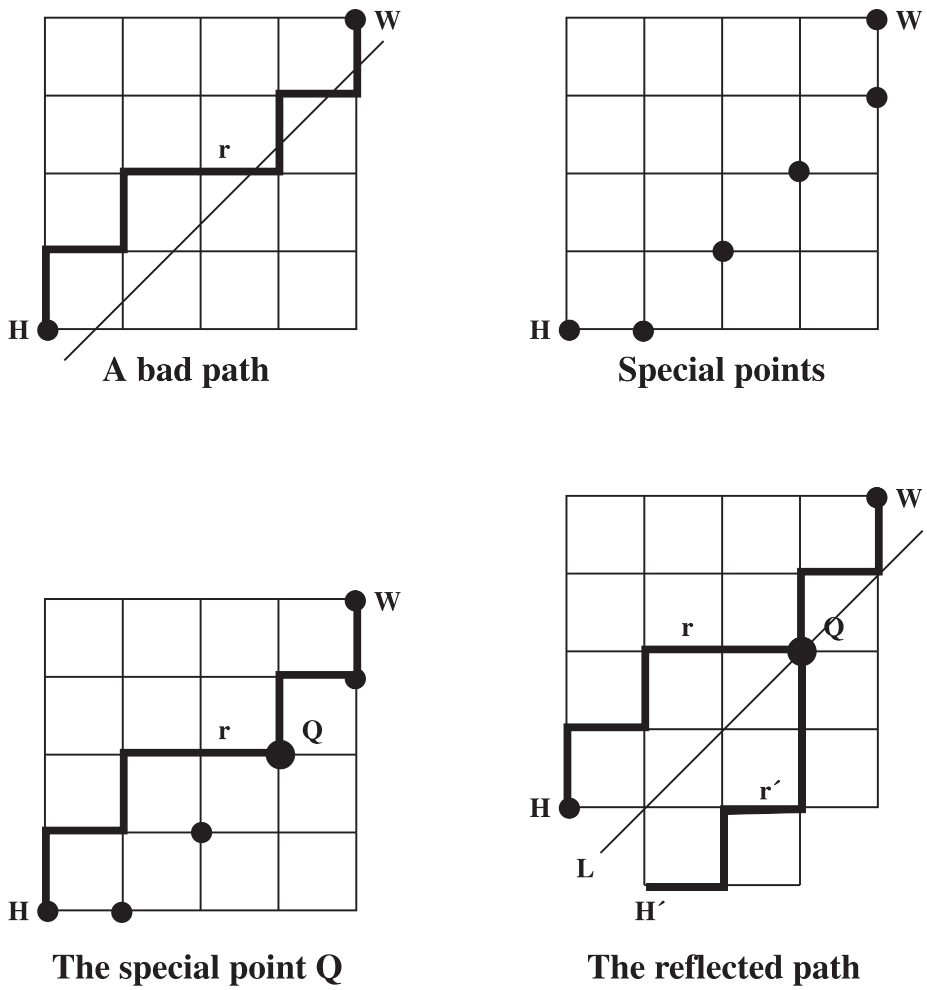


Figure 3.22: The reflection principle

Notice that every bad path must pass through at least one of 4 special intersections, shown in the second picture of Figure 3.22. Let's specially mark the special intersection which Bill encounters first on the bad path in Figure 3.22 with a **Q**. This is shown in the third picture of Figure 3.22.

Now we apply a clever trick. Reflect the part of Bill's route from his home **H** to this first special intersection **Q** through the diagonal line **L** through the special intersections. This is shown in the final picture of Figure 3.22.

What results is a new path, $\mathbf{r}'$, not from Bill's home, but from a location one block south and one block east of his home, which we will call $\mathbf{H}'$, through **Q**, all the way to his workplace.

Notice that every bad path will correspond, via such a reflection, to a different path from $\mathbf{H}'$ to **W**. Another example is shown in Figure 3.23.

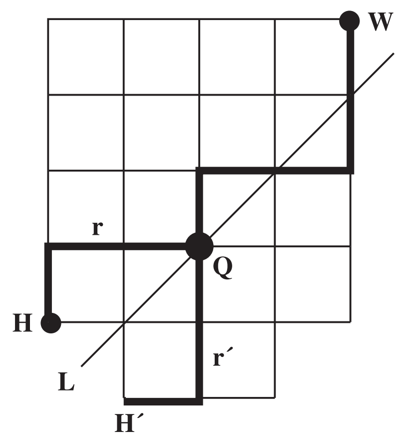


Figure 3.23: Another reflected path

Also notice that every path from $\mathbf{H}'$ to **W** is bad in the sense that it must cross the railroad tracks (the tracks are "in the way"). So every path from $\mathbf{H}'$ to **W** will correspond to a bad path: find the first special intersection along the path (it must pass through at least one, since it crosses the railroad tracks). Call this special intersection **Q**. Now reflect the portion of this path from $\mathbf{H}'$ to **Q** back across the diagonal line **L** through the special intersections. The new path is a bad path from **H** to **W**.

Therefore, the number of bad paths from **H** to **W** is the *total* number of paths from $\mathbf{H}'$ to **W**.

Exercise 3.4.2. Find the paths from $\mathbf{H}'$ to **W** which correspond to the two bad paths given in Figure 3.24.

Exercise 3.4.3. Suppose Bill lives 3 blocks south and 3 blocks west of work. Draw all the paths from home, **H**, to work, **W**, including the bad ones. Also draw all the paths from $\mathbf{H}'$, located one block south and one block east of Bill's

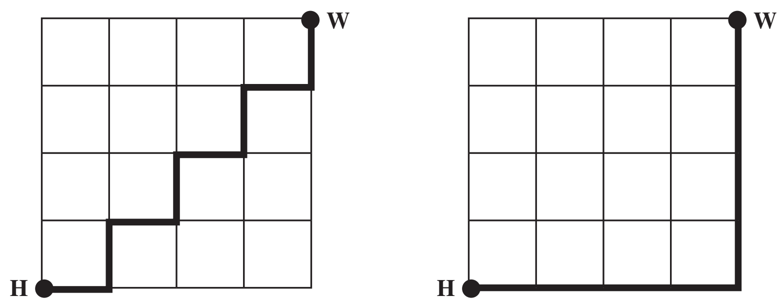


Figure 3.24: Two bad paths

home, to **W**. Now pair up the paths from **H′** to **W** with the bad ones from **H** to **W** according to the method just described.

Exercise 3.4.4. If Bill lives 4 blocks south and 4 blocks west of work, what is the number of paths from **H′** to **W**? Use this to verify that the number of good paths from **H** to **W** is 14.

Exercise 3.4.5. Now suppose Bill lives n blocks west and n blocks south of work. How many blocks west and how many blocks south of work will **H′** be? Count the number of bad paths and subtract from the total number of paths obtained in Exercise 1 to give a formula for C_n, the number of good paths.

We now state several forms for the explicit formula for the Catalan number.

Theorem 4.

$$\begin{aligned} C_n &= \binom{2n}{n} - \binom{2n}{n-1} \\ &= \frac{1}{n+1}\binom{2n}{n} \\ &= \frac{1}{2n+1}\binom{2n+1}{n}. \end{aligned}$$

Exercise 3.4.6. Algebraically manipulate the first formula in Theorem 4 to derive the second and third forms. Hint: Use Exercise 2.2.9 to show that $(n+1)! = (n+1)n!$. Then use this identity to find a convenient common denominator.

Exercise 3.4.7. Use Theorem 4 to check the values of C_0, C_1, C_2, C_3, C_4, C_5, C_6 and C_7 computed in earlier exercises.

Exercise 3.4.8. If 42 people are seated around a round table, how many ways can they shake hands without crossing handshakes?

Exercise 3.4.9. How many ways are there to triangulate a 20-sided polygon?

The ideas in this section can be used in a number of other similar situations. Here are a few examples.

Exercise 3.4.10. Use the ideas of this section to count the number of paths from **H** to **W** in Figure 3.25 which stay northwest of the railroad tracks.

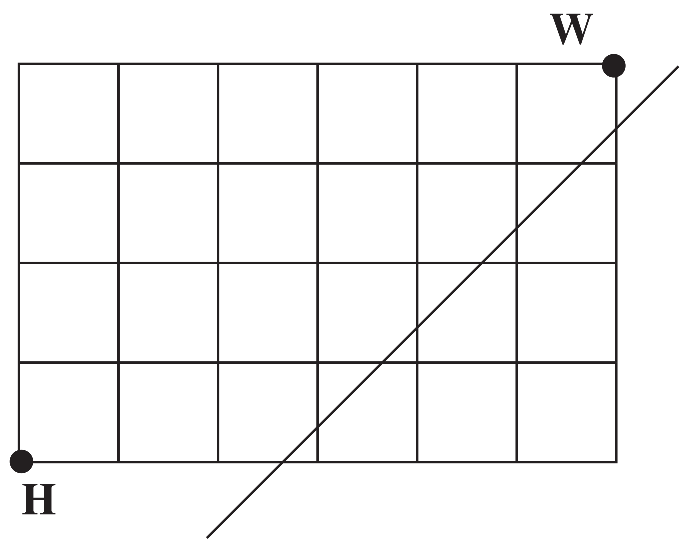


Figure 3.25: A non-square block-walk grid

Exercise 3.4.11. Count the number of paths from **H** to **W** in Figure 3.26 which stay northwest of the railroad tracks and which do not use the north-south edge which is covered by a lake.

Exercise 3.4.12. Suppose Bill leaves his home and at each intersection, he either walks east or north. If he walks a total of four blocks, how many paths does he have? How many paths does he have if he must stay northwest of the railroad tracks? (Notice that he will end up at A, B or C in Figure 3.27). An example of one such path is also shown in Figure 3.27.

Exercise 3.4.13. Answer the two questions posed in Exercise 3.4.12 if he walks a total of six blocks (see Figure 3.28 below). Find formulas for the answers to the two questions if he walks a total of $2n$ blocks. The reflection principle may be useful in the six block case and is essential in the $2n$ block case.

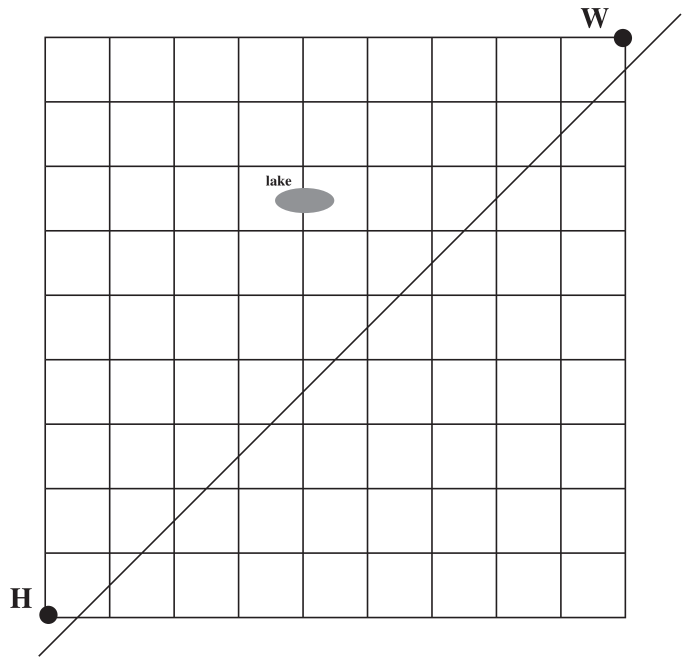


Figure 3.26: Block-walk grid with a lake

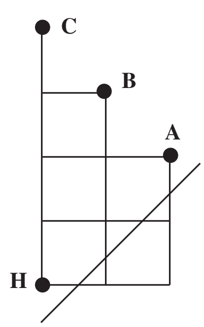


Figure 3.27: Length 4 block-walk

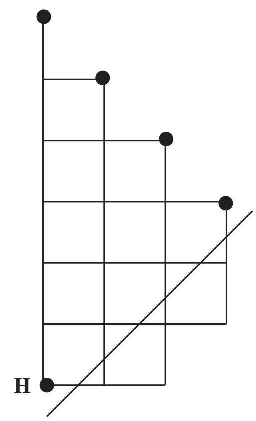


Figure 3.28: Length 6 block walk

***Exercise 3.4.14.** How many ways can Bill walk from his home at H1 to his workplace at W1 and Mary walk from her home at H2 to her workplace at W2 (see Figure 3.29)? How many of these pairs of paths are there so that the paths do not touch or cross?

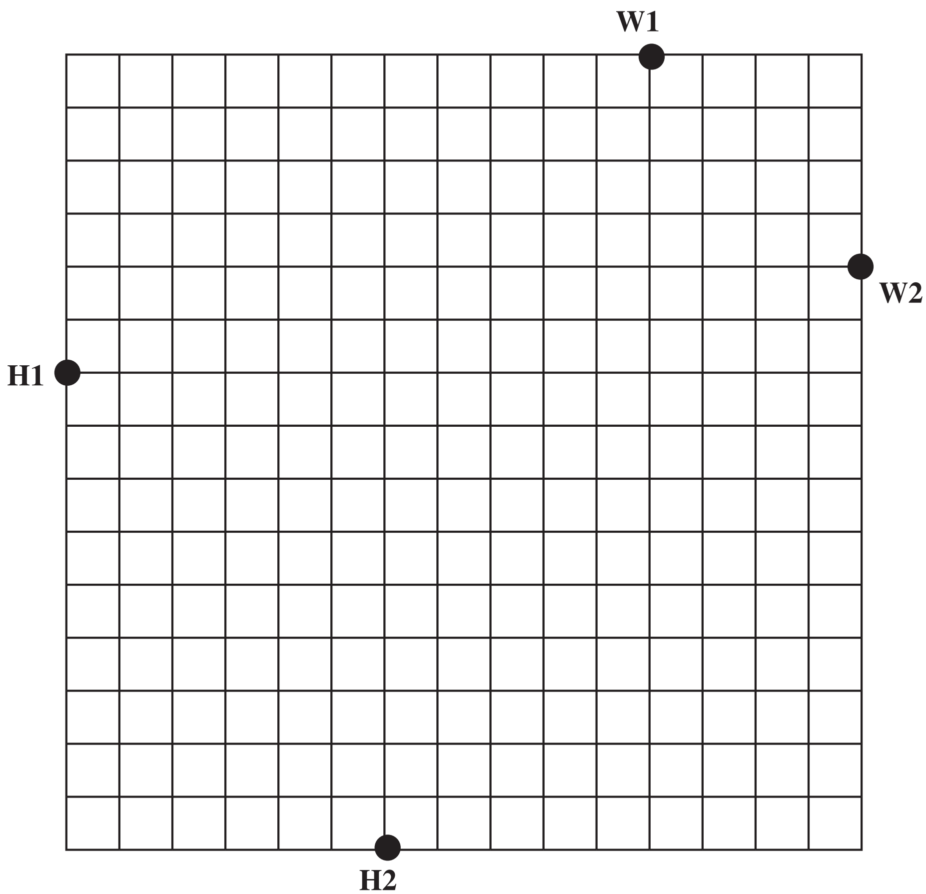


Figure 3.29: Find non-crossing paths on a grid

Chapter 4

Graphs

The graphs we discuss in this chapter are not the x-y coordinate graphs you may be familiar with from your algebra classes. The graphs here are a kind of line drawing. They are collections of points connected by lines. We will discuss some of the properties of these graphs in this chapter. For instance, when is it possible to draw such a graph on a piece of paper without lines crossing? We will also find out about several special kinds of graphs and we will classify the regular polyhedra.

4.1 Eulerian Walks and Circuits

Modern graph theory is said to have its origins in a famous old folk problem called the Königsberg Bridge Problem.

Exercise 4.1.1. The people of Königsberg often strolled around their town after dinner. See the map in Figure 4.1. Is it possible for a citizen of Königsberg to arrange her stroll so that she crosses each of the seven bridges exactly once, and finally returns to her home? Why or why not? Does the location of her home matter?

Let's replace each "land mass" with a dot (called a *vertex*, plural *vertices*), and each bridge with a line (not necessarily straight) connecting dots (called an *edge*). The Königsberg map becomes the *graph* in Figure 4.2.

The problem in Exercise 4.1.1 is then to find a *walk* through the graph in Figure 4.2, starting and ending at the same place, so that each edge is used exactly once.

A *walk* is simply an alternating sequence of vertices and edges, beginning and ending with a vertex, where each edge goes between the vertices immediately before and after in the sequence. For example, in Figure 4.3, one walk starts at vertex A, goes along edge 1 to vertex B, then along edge 4 to vertex D, along edge 7 to vertex E, along edge 8 to vertex B again, along edge 2 to vertex A again, and finally along edge 5 to vertex C.

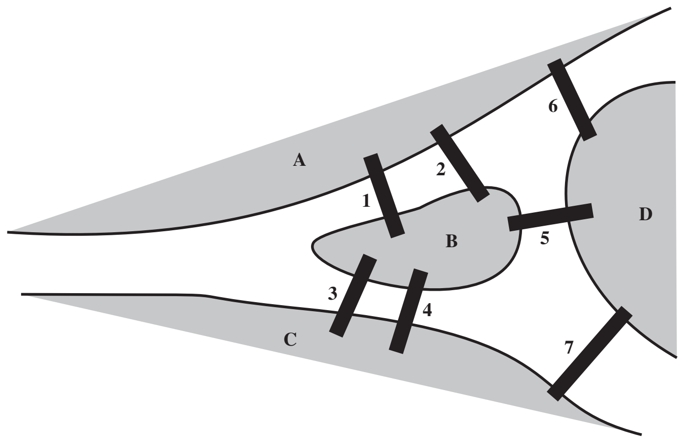


Figure 4.1: The bridges of Königsberg

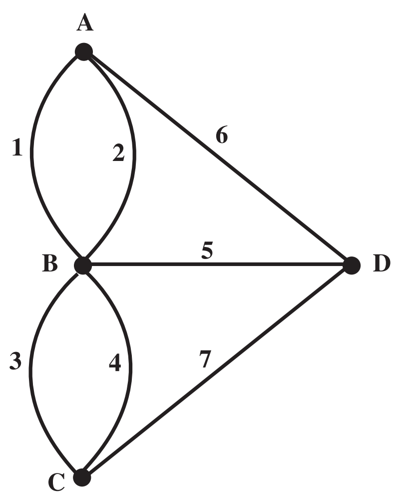


Figure 4.2: Königsberg graph

Another walk starts at D, goes along edge 7 to vertex E, then back along edge 7 to vertex D again.

We have defined walks in a very general way. Edges may be repeated, vertices may be repeated. Walks may be very long and complicated. Or they can be very short, even consisting of a single vertex and no edges. Walks may start at one vertex and end at another. Or they may start and end at the same place. We will now consider several specializations of walks.

One special kind of walk is a *closed walk*, which is a walk which begins and ends at the same vertex and has at least one edge.

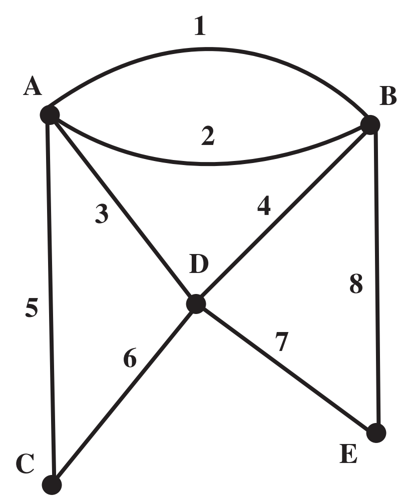


Figure 4.3: A graph with labeled vertices and edges

Exercise 4.1.2. Find two more walks in the graph in Figure 4.3. Have one of your walks start at D and end at E and visit C along the way. Have the other walk be a closed walk.

The kind of walk that occurs in the Königsberg Bridge Problem is called an *Eulerian walk*. It has the property that each edge is used in the walk exactly once. If the Eulerian walk is a closed walk, it is called an *Eulerian circuit*. The graph in Figure 4.3 has an Eulerian circuit. One such circuit is A1B2A3D4B8E7D6C5A. The graph in Figure 4.2 does not have an Eulerian circuit. The goal of this section is to find a condition on a graph that is equivalent to having an Eulerian circuit.

Exercise 4.1.3. Determine which of the graphs in Figure 4.4 have an Eulerian circuit. If the graph has such a circuit, draw it. If not, give arguments why you think no such circuit exists.

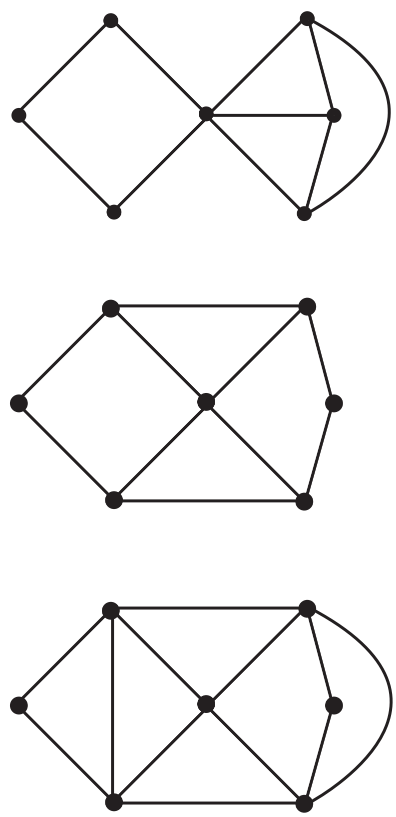


Figure 4.4: Which have Eulerian circuits?

Exercise 4.1.4. From your analysis in Exercise 4.1.3, state some property of a graph which is equivalent to having an Eulerian circuit.

Some writers on this subject allow their graphs to have *loops* and *multiple edges* (see Figure 4.5), while others do not.

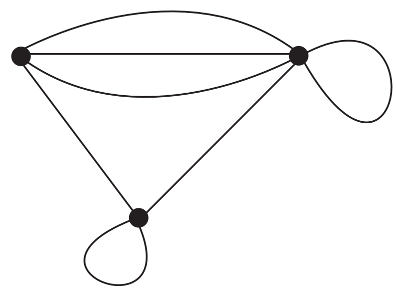


Figure 4.5: A graph with loops and multiple edges

For the purposes of this discussion of Eulerian circuits, our graphs can have multiple edges (but not loops).

Two vertices are *connected* if there is a walk from one to the other. This does not mean that there is an edge between the two vertices. For instance, in Figure 4.3 vertex C and E have no edge between them, but they are connected.

A graph is *connected* if every pair of vertices is connected. A graph which is not connected has two or more connected pieces called *connected components*. For instance, the graph in Figure 4.6 is not connected and has two connected components.

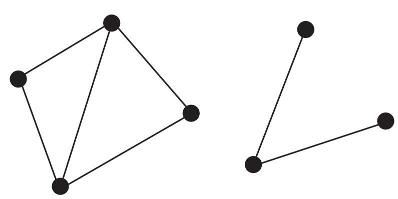


Figure 4.6: A non-connected Graph

Exercise 4.1.5. Draw a graph which is not connected and which has three connected components.

The *degree* of a vertex is the number of edges which use that vertex.

Exercise 4.1.6. Show that if a graph has an Eulerian circuit, it cannot have a vertex of odd degree.

The converse of Exercise 4.1.6 is somewhat harder to show. The next few exercises describe an algorithm for finding Eulerian circuit in a connected graph whose vertices all have even degree.

Exercise 4.1.7. The graph in Figure 4.7 has all even degrees. Find some closed walk in this graph which does not use any edge more than once. (This closed walk does not have to be an Eulerian circuit, since some of the edges may not appear in it. In fact, this closed walk may be quite simple.) Find another closed walk in this graph with three edges.

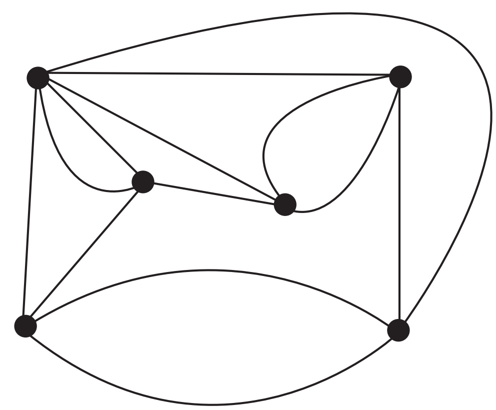


Figure 4.7: Finding an Eulerian circuit

Exercise 4.1.8. Erase the edges of the closed walk you found in Exercise 4.1.7 from this graph. (Don't erase the vertices.) What are the degrees of the vertices in this new graph? Why are they all even? Does this new graph have to be connected?

Exercise 4.1.9. Now repeat Exercises 4.1.7 and 4.1.8 for each connected component of the new graph. Continue this process until no edges remain.

Exercise 4.1.10. Now find an Eulerian circuit in the original graph by starting with the last closed walk you found in Exercise 4.1.9 and adding back the closed walks that you removed.

We can now summarize the previous group of exercises.

Theorem 5. *A connected graph has an Eulerian circuit if and only if every vertex has even degree.*

There is a similar condition for a graph to have an Eulerian walk which is not an Eulerian circuit. The next exercise asks you to find this condition.

Exercise 4.1.11. State some property of a graph which is equivalent to having an Eulerian walk from the vertex v to the vertex w, where v and w are different vertices.

The degrees of the vertices of a graph can also be used to determine the number of edges in the graph.

Exercise 4.1.12. In the graph in Figure 4.8, calculate the degrees of all the vertices and add them. How many edges are there? Try this on some more examples. Find and prove a formula which relates the number of edges in a general graph to the sum of the degrees.

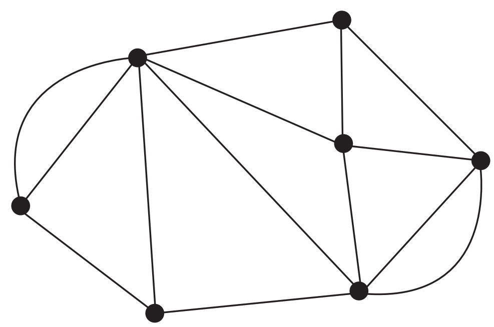


Figure 4.8: The handshake theorem

Exercise 4.1.13. Use the formula you found in Exercise 4.1.12 to show that in every graph the number of vertices of odd degree is even.

Exercise 4.1.14. Use Exercise 4.1.13 to show that at a party, the number of people who shake hands with an odd number of other people is even.

We can summarize the previous exercises with the following theorem, called the handshake theorem.

Theorem 6 (The Handshake Theorem)**.** *In a graph with E edges, the sum of the degrees of all the vertices is $2E$.*

4.2 Special Graphs

There are many “special cases” of graphs that we will find useful. Some of these will be the subjects of later chapters. Others we will find scattered throughout the rest of this chapter. These graphs will have no loops or multiple edges.

The simplest kind of graph is the *null graph*. N_n denotes the version of this graph having n vertices. It is the graph with no edges. Figure 4.9 shows N_3 and N_4.

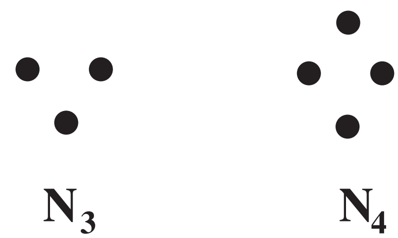


Figure 4.9: Null graphs N_3 and N_4

The most complicated kind of graph is the *complete graph*. We let K_n denote the complete graph having n vertices. In the complete graph, all possible edges are drawn (no multiple edges or loops). Figure 4.10 shows K_3 and K_4.

Figure 4.10: Complete graphs

Exercise 4.2.1. Draw K_5 and K_6. Note that you may have to "cross edges" to draw these.

Exercise 4.2.2. How many edges do K_5 and K_6 have? K_n?

Sometimes all the edges in a graph go between one set of vertices and another. Such graphs are used to model job assignment problems. The jobs make up one set of vertices, the applicants another. An edge between a job and an applicant means that that applicant is qualified for that job. These graphs are called *bipartite*. See Figure 4.11 for an example. All the edges are between the vertices in the set $\{a, b, c, d\}$ and the set $\{1, 2, 3\}$.

If every possible edge between two sets of vertices is drawn (no loops or multiple edges), what results is a *complete bipartite graph*. Such graphs have two indices—one for each set of vertices. Let $K_{n,m}$ denote the complete bipartite graph having vertex set sizes of n and m respectively. Figure 4.12 shows $K_{2,2}$ and $K_{2,3}$.

Exercise 4.2.3. Draw $K_{3,3}$ and $K_{3,4}$.

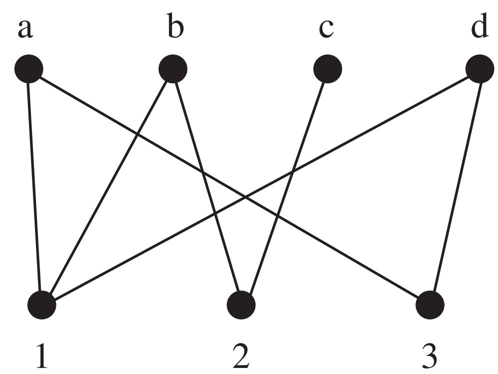


Figure 4.11: A bipartite graph

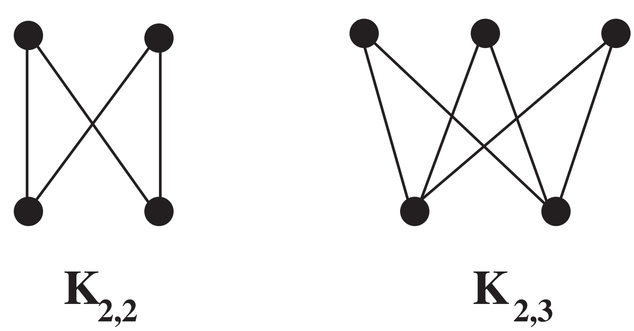


Figure 4.12: $K_{2,2}$ and $K_{2,3}$

Exercise 4.2.4. How many edges do $K_{3,3}$ and $K_{3,4}$ have? $K_{n,m}$?

Exercise 4.2.5. When does K_n have an Eulerian circuit? When does $K_{n,m}$ have an Eulerian circuit?

An important property of bipartite graphs is that every closed walk has an even number of edges.

Exercise 4.2.6. Prove that every closed walk in a bipartite graph has an even number of edges.

Graphs merely keep track of vertices and edges. The representation of these things on a piece of paper or a blackboard is purely a convenience. For example, Figure 4.13 shows three ways of drawing the same graph.

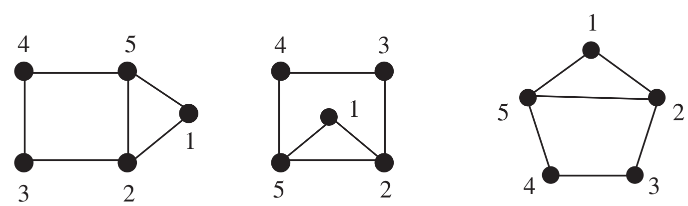


Figure 4.13: Three ways of drawing the same graph

Whenever we speak of a graph, we must differentiate between the graph (which is just a set, called vertices, and a set of pairs of vertices, called edges) and the "picture" of the graph that we draw on a page or on a blackboard. In particular, the edges may be long or short, curving or straight. They may or may not cross.

You have probably noticed, however, that graph drawings are "nicer" if edges do not cross. Figure 4.14 shows two ways of drawing K_4. The second

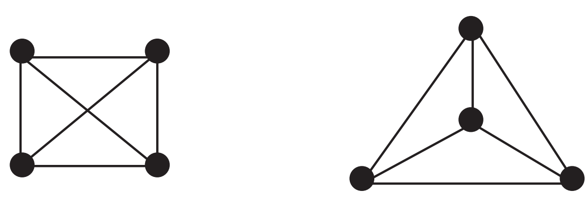


Figure 4.14: Two ways of drawing K_4

of these drawings is called a *planar representation* because the graph has been drawn on a plane with no crossing edges. Figure 4.14 shows that graphs can sometimes be drawn with a planar representation and sometimes without a planar representation. Graphs which have a planar representation are called *planar graphs*. Graphs which are not planar are *nonplanar*. Notice that the first drawing of K_4 in Figure 4.14 is a planar graph drawn in a non-planar way; it may be regarded as a planar graph in disguise.

Exercise 4.2.7. Determine which of the graphs in Figure 4.15 are planar graphs. If they are planar, draw a planar representation. If not, give whatever reasons you can why you cannot draw a planar representation.

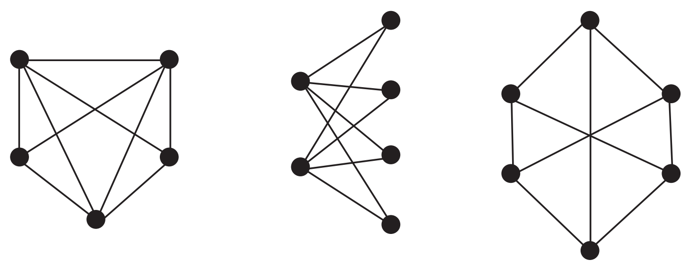


Figure 4.15: Planar graphs?

Some graphs cannot be drawn in the plane without crossing edges, no matter how hard we try. Here are two examples.

Exercise 4.2.8. Three hermits, Jake, Jed and Jethro, live in the hills, each in his own house. Located nearby are three wells. Jake , Jed and Jethro try to build paths from their houses to each well in such a way that no pair of paths cross. Is this possible?

Exercise 4.2.9. Exercise 4.2.8 asks you to try to draw a planar representation of $K_{3,3}$. Now try to draw a planar representation of K_5.

A very famous theorem states that not only are $K_{3,3}$ and K_5 nonplanar, but in a certain sense they are the *only* nonplanar graphs. The "certain sense" is that inside each nonplanar graph there is a subgraph which "looks like" $K_{3,3}$ or K_5: it may contain some vertices of degree 2, but these can be "forgotten." An example of a nonplanar graph and its "hidden" $K_{3,3}$ is given in Figure 4.16.

We will look at planar graphs in more detail in Section 4.3.

Another special kind of graph is a *tree*. To define a tree, we first define a cycle. A *cycle* is a closed walk with at least one edge and which does not repeat vertices (except for the first and last) or edges. Trees are then connected graphs (no loops or multiple edges) which have no cycles. Some examples are shown in Figure 4.17.

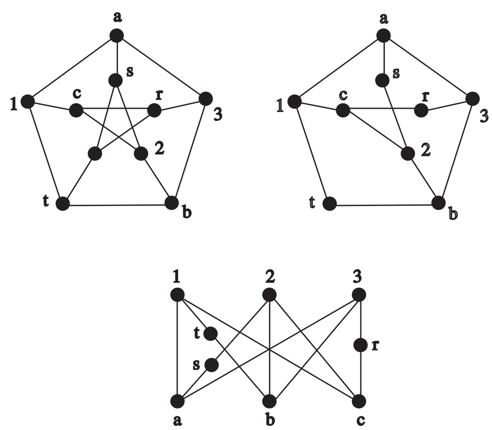


Figure 4.16: $K_{3,3}$ in the Peterson graph

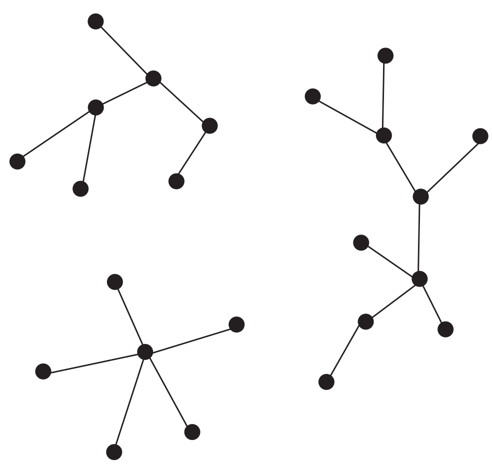


Figure 4.17: Three trees

Exercise 4.2.10. Draw some trees with four, five and six vertices. How many edges does each have? What is the relationship between the number of edges in a tree and the number of vertices?

Vertices in a tree of degree one are called *leaves* or *terminal vertices.* Notice that if a leaf and its incident edge (i. e., the edge with the leaf as one of its endpoints) are removed (*pruned*), the resulting new graph is still a tree, but with one fewer edge and one fewer vertex.

Exercise 4.2.11. Use the above argument to prove:

> The number of vertices V and the number of edges E of a tree satisfy
>
> $$E = V - 1\,. \tag{4.1}$$

Exercise 4.2.12. Is a tree a planar graph? Which of the complete graphs are trees? Which of the complete bipartite graphs are trees?

Exercise 4.2.13. Suppose you remove an edge from a tree (but not the vertices at either end of the edge). Is the resulting graph connected? What about the converse? That is, suppose you have a connected graph and you know that if you remove any edge, the graph becomes disconnected. Is the graph a tree?

Trees are used to model many real-world problems, including family trees, biological classifications, essay outlines, and computer database structures. We will look at trees in a later chapter.

4.3 Planar Graphs

Like all graphs, planar graphs have vertices and edges. But once a planar representation of such a graph is given, it also has *faces*, regions bounded on all sides by edges of the graph. One of the faces is the "infinite" outer face. This face is called the *exterior* face.

Notice that it is the planar representation that has the faces, for if we draw the graph in a non-planar way (see the left figure in Figure 4.14), we cannot determine its faces. Furthermore, if we draw two different planar representations of the same planar graph, the faces may change. For example, Figure 4.18 shows the same graph drawn in two different ways. One way has one face surrounded by 5 edges and three faces surrounded by 3 edges. The other way has two faces surrounded by 4 edges and two faces surrounded by 3 edges.

Exercise 4.3.1. In what sense are the two graphs in Figure 4.18 the same graph?

Exercise 4.3.2. On Figure 4.18, for each face indicate the number of edges around the face.

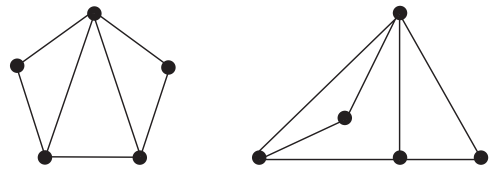


Figure 4.18: Two planar embeddings of the same graph

To keep things simple, we will take the point of view that the planar representation is the planar graph.

Suppose we are given some connected planar graph. Let's let V, E and F stand for the number of vertices, edges and faces, respectively. (When counting faces, be sure to count the exterior face.) An example is given in Figure 4.19. In this example, $F = 6$, $E = 13$ and $V = 9$.

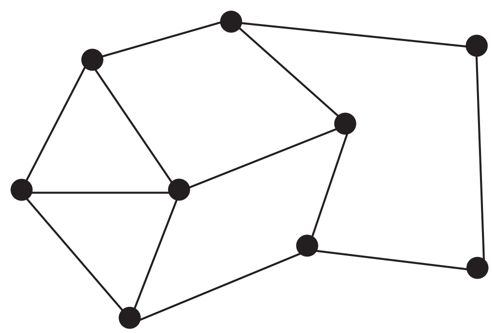


Figure 4.19: A planar graph

Exercise 4.3.3. Another example of a planar graph is given in Figure 4.20. Find V, E, and F.

The number of faces, vertices and edges of a connected planar graph are related in a fundamental way. That relationship is called Euler's formula.

Theorem 7 (Euler's Formula)**.** *In a connected planar graph with F faces, E edges and V vertices,*

$$F + V = E + 2\,. \tag{4.2}$$

In the next few exercises, we will prove Euler's formula. First, let's check it for trees.

Exercise 4.3.4. How many faces does a tree have? Use Equation (4.1) to prove Euler's formula for the special case when the planar graph is a tree.

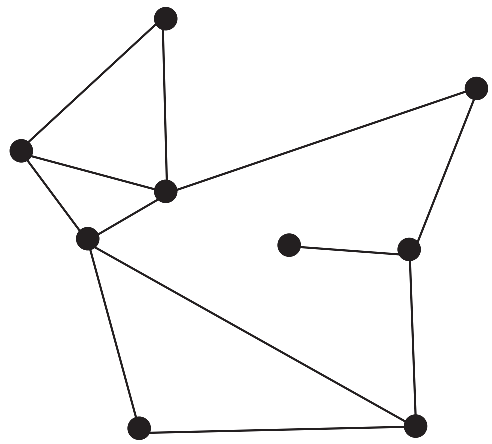


Figure 4.20: Another planar graph

Now suppose our connected planar graph is not a tree. Suppose we find an edge whose removal will not disconnect our graph. If the graph is not a tree and is connected, then Exercise 4.2.13 guarantees that such an edge exists. (Of course, if the graph is already a tree, we can't find such an edge.)

Exercise 4.3.5. If we remove this edge, what happens to the number of edges? the number of faces? the number of vertices?

Exercise 4.3.6. Suppose we remove an edge from any connected planar graph and are left with another connected planar graph. Show that $F - E + V$ does not change.

Therefore, starting with a connected planar graph, we remove edges as described above, until we are left with a tree. By Exercise 4.3.6 $F - E + V$ does not change each time we remove an edge. Therefore, $F - E + V$ will be the same for the original graph as it is for the tree. But by Exercise 4.3.4 the resulting tree will have $F - E + V = 2$. Thus we conclude that Euler's formula is satisfied by the original graph.

Exercise 4.3.7. Do some examples to figure out how the formula changes if the graph is not connected. (Hint: let C denote the number of connected components.)

One of the many consequences of Euler's formula is that planar graphs cannot have too many edges. To simplify the discussion somewhat, let's define the degree of a face. The *degree of a face* is the number of edges "around" the face. We have to be careful about graphs with faces such as the interior face in Figure 4.21. This face will have degree 8. Thus, if both sides of an edge border the same face, this edge contributes two to the degree of the face.

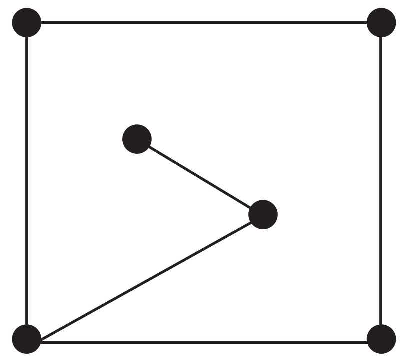


Figure 4.21: Degree of a face in a planar graph

Exercise 4.3.8. Compute the degree of each face in the graph in Figure 4.19. Then take the sum. You should get $2E$. Explain why. Do the same for the graph in Figure 4.20?

Exercise 4.3.8 demonstrates the face version of the handshake theorem, Theorem 6.

Theorem 8 (The Face Handshake Theorem)**.** *In a planar graph with E edges, the sum of the degrees of the faces equals $2E$.*

Before proving Theorem 8, let's check that the formula works when the planar graph is a tree.

Exercise 4.3.9. Check that Theorem 8 is true when the graph is a tree.

Now let's prove Theorem 8 for general planar graphs.

Exercise 4.3.10. Prove Theorem 8.

We saw in Figure 4.18 that different planar representations of the same graph can lead to different degrees of their faces. However, Theorem 8 says that the sum of these degrees must always be $2E$.

Exercise 4.3.11. Compute sums of the degrees of the faces of the two graphs in Figure 4.18. These sums should be the same.

Exercise 4.3.12. Show that the number of faces of a connected planar graph is the same regardless of the planar representation.

Let's now use the face handshake theorem and Euler's formula to show why K_5 is not a planar graph. Suppose K_5 is a planar graph.

Exercise 4.3.13. Use Euler's formula to show that if K_5 were planar, it would have 7 faces.

Exercise 4.3.14. Use Theorem 8 and the fact that if K_5 were planar, each face would have degree 3 or more to show that K_5 cannot have the 7 faces you computed in Exercise 4.3.13.

Exercise 4.3.14 shows that K_5 cannot be planar. The ideas used in this exercise can be generalized to other planar graphs.

Exercise 4.3.15. Use Theorem 8 to show the following:

> Suppose a planar graph with E edges and F faces has at least three edges around each face. Then
> $$3F \leq 2E\,. \tag{4.3}$$

We now turn our attention to $K_{3,3}$.

Exercise 4.3.16. If $K_{3,3}$ were planar, how many faces would it have?

If we assume that every face of $K_{3,3}$ has degree 3 or more, can we argue as we did for K_5 in Exercise 4.3.14?

Exercise 4.3.17. Using Exercise 4.3.14 as a model, and assuming that every face of $K_{3,3}$ has degree 3 or more and that $K_{3,3}$ has the number of faces given in Exercise 4.3.16, try to show that $K_{3,3}$ is not planar. What goes wrong?

Exercise 4.3.17 does not mean that $K_{3,3}$ is planar. It does mean that we will have to improve our arguments somewhat.

Recall from Exercise 4.2.6 that if a graph is bipartite, all its closed walks must have an even number of edges. Therefore, every face of $K_{3,3}$ must be surrounded by four or more edges, not three or more edges.

Exercise 4.3.18. Now use Theorem 8 and the fact that each face of $K_{3,3}$ must have degree 4 or more to show that $K_{3,3}$ cannot have the number of faces you computed in Exercise 4.3.16.

Exercise 4.3.19. Suppose a planar graph has at least four edges around each face. Use Theorem 8 to show
$$4F \leq 2E\,. \tag{4.4}$$

The inequalities in Exercises 4.3.13 and 4.3.16 can be used with Euler's formula to give bounds on the number of edges in a planar graph. These inequalities essentially say that the number of edges in a planar graph cannot be too big.

Exercise 4.3.20. Suppose every face of a certain connected planar graph has at least three edges around each face. Use Inequality (4.3) and Euler's formula (Equation (4.2)) to show
$$E \leq 3V - 6\,. \tag{4.5}$$

Exercise 4.3.21. Does Inequality (4.5) hold for planar graphs which are not connected? Why or why not? (Hint: a connected planar graph can be constructed from an arbitrary non-connected planar graph by inserting edges.)

Exercise 4.3.22. The graph with one vertex and no edges is planar. The graph with two vertices and one edge is planar. Check Inequality (4.5) for these two graphs. What is wrong?

Exercise 4.3.23. Suppose every face of a certain connected planar graph is surrounded by four or more edges. Use arguments similar to those in Exercise 4.3.20 and Inequality (4.4) to show that

$$E \leq 2V - 4\,. \tag{4.6}$$

4.4 Polyhedra

The method used for proving Inequality (4.5) of Section 4.3 can be used to classify polyhedra.

A *polyhedron* (plural: polyhedra) is a 3-dimensional solid body with flat, polygonal surfaces called *faces*. It may seem confusing that we are using the word "face" in two different contexts, but we shall soon see that these two versions of "faces" coincide. We will be looking at *convex* polyhedra—polyhedra without holes or indentations. An example of a convex polyhedron is a cube—see Figure 4.22.

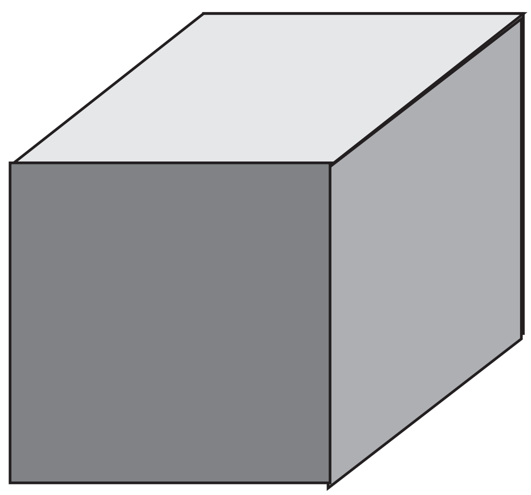


Figure 4.22: A cube

Although a polyhedron is a three-dimensional object, its topology can be reduced to a two-dimensional planar graph. Pick one of the faces of the polyhedron, and "punch a hole" in that face. Imagine that the faces are made of some stretchable material. Now stretch and spread the polyhedron out on a plane. The face of the polyhedron with the hole punched becomes the exterior face of the planar graph. The other faces of the polyhedron become the other faces of the planar graph. We sometimes say the place where we punched the hole is a "point at infinity." The face where we punched the hole is the infinite face of the planar graph. Figure 4.23 shows the tetrahedron drawn in the plane.

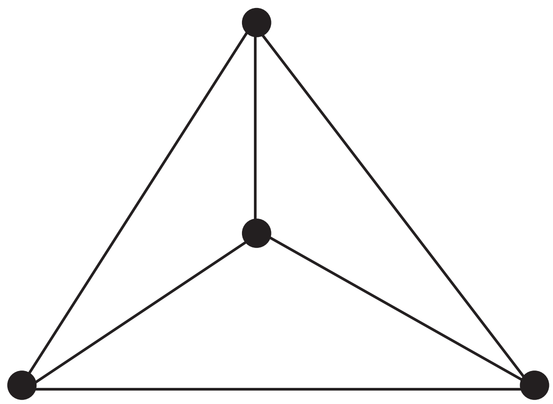


Figure 4.23: Planar view of a tetrahedron

Exercise 4.4.1. Draw a planar representation of the cube.

Since edges don't "cross" in a polyhedron, they won't cross after this stretching procedure, so the graph we get is planar. Therefore Euler's formula therefore holds for the edges, faces and vertices of a polyhedron.

If every face of the polyhedron is a regular polygon, all the faces are congruent, and every vertex has the same degree, then we say the polyhedron is *regular*. It is a remarkable fact, which is a consequence of Euler's formula, that there are only five kinds of regular polyhedra. These five are sometimes called "Platonic solids." This classification is our next goal.

When a regular polyhedron is stretched to become a planar graph, the faces are no longer regular and no longer congruent. However, all the faces have the same degree and all the vertices have the same degree. Let's say that every face has degree q and every vertex has degree p. For example, for the tetrahedron, $p = 3$ and $q = 3$. Therefore, by Theorem 6, $3V = 2E$ and by Theorem 8, $3F = 2E$.

Exercise 4.4.2. Use these two equations plus Euler's formula to find F, V and E for the tetrahedron.

Exercise 4.4.3. Use Theorems 6 and 8 to show that for the graph of a regular polyhedron $qF = 2E$ and $pV = 2E$.

Exercise 4.4.4. Use Exercise 4.4.3 and Euler's formula (Equation (4.2)) to show

> For a regular polyhedron with E edges, face degree q and vertex degree p, the following equation holds:
>
> $$\frac{1}{p} + \frac{1}{q} = \frac{1}{2} + \frac{1}{E}\,. \tag{4.7}$$

Exercise 4.4.5. Explain why $p \geq 3$ and $q \geq 3$.

Exercise 4.4.6. Find all integers p and q which satisfy Equation (4.7), subject to the inequalities in Exercise 4.4.5.

Exercise 4.4.7. For each of the solutions you found in Exercise 4.4.6, find the corresponding values of E, F and V. Your solution to Exercise 4.4.2 will be one of these solutions. Draw the polyhedral graph in each case.

> **Theorem 9.** *There are exactly five regular polyhedra. These are the tetrahedron, the cube, the dodecahedron, the octahedron and the icosahedron.*

Not all polyhedra are regular. Suppose that we only know that every face has at least q edges and that every vertex has at degree at least p.

Exercise 4.4.8. Show that the equations in Exercise 4.4.3 are replaced by the inequalities $2E \geq qF$ and $2E \geq pV$. Explain why every polyhedron satisfies $2E \geq 3F$ and $2E \geq 3V$.

Exercise 4.4.9. Show that it is impossible to construct a polyhedron entirely out of faces with six or more sides. Hint: combine the inequalities $2E \geq 3V$, obtained from Exercise 4.4.8, and $2E \geq 6F$, obtained from Theorem 8, with Euler's formula.

Exercise 4.4.10. Suppose a polyhedron is made up of four hexagons and a certain number of triangles, and is constructed so that exactly three faces meet at each vertex. Show that there must be exactly four triangles. Hint: Let x be the number of triangles. Justify each of the following equations and then combine them with Euler's formula.

$$\begin{aligned} 2E &= 3V \\ F &= 4 + x \\ 2E &= 24 + 3x \end{aligned}$$

Exercise 4.4.11. Suppose all the faces of a certain polyhedron are four-sided. Suppose 18 of its vertices have degree four and the rest have degree three. Determine the number of faces, edges and vertices of this polyhedron.

As was stated earlier, not all polyhedra are regular. We can relax the regularity rules a bit to get a larger class of polyhedra. For instance, *semi-regular polyhedra* are polyhedra whose faces are two or more types of regular polygons, and the polygons are arranged around each vertex in the same way. An example is the truncated tetrahedron, pictured in Figure 4.24. Around each vertex are two hexagons and a triangle. (The regularity of the triangles and hexagons is not apparent in this picture, because it is a planar representation of a three-dimensional polyhedron.)

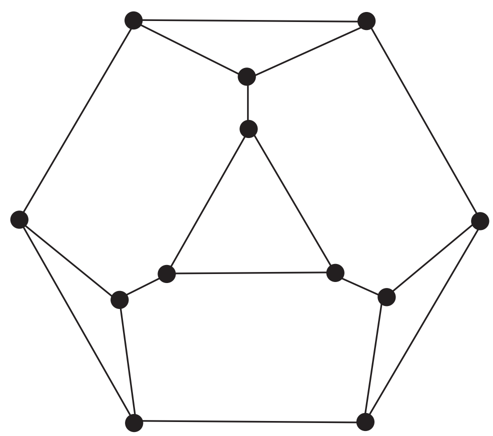


Figure 4.24: A truncated tetrahedron

There are two infinite classes of semi-regular polyhedra and 13 special ones. The truncated tetrahedron above is one of the 13 special ones. One of the infinite classes is obtained by connecting regular n-gons with squares. The planar representation of an example when the n-gon is a hexagon is shown in Figure 4.25.

Exercise 4.4.12. Find the other infinite class and as many of the other special ones as you can.

4.5 Tessellations

A *tessellation* of the plane is a subdivision of the plane into polygons. Like polyhedra, tessellations have various subcategories. One of these is regular. That means that every polygon (also called a *face*) is a regular polygon, all the polygons are congruent, every vertex has the same degree, and pairs of polygons cannot share a part of an edge. An example is pictured in Figure 4.26.

The last condition rules out pictures like Figure 4.27.

A *regular tessellation* is like an infinite planar graph. We would like to use Euler's formula, but we must be able to "extend" it to infinity. Suppose we look

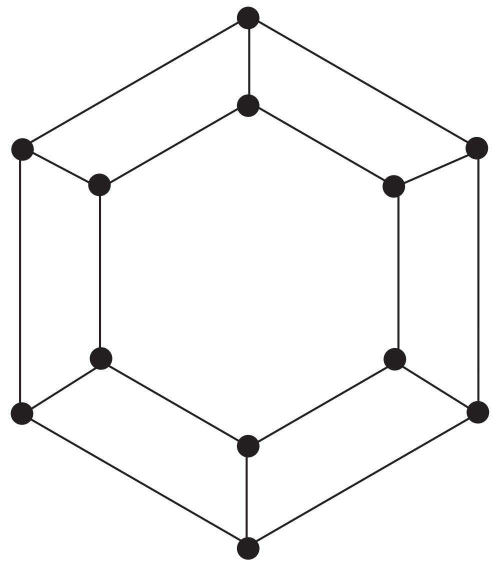


Figure 4.25: A hexagonal prism

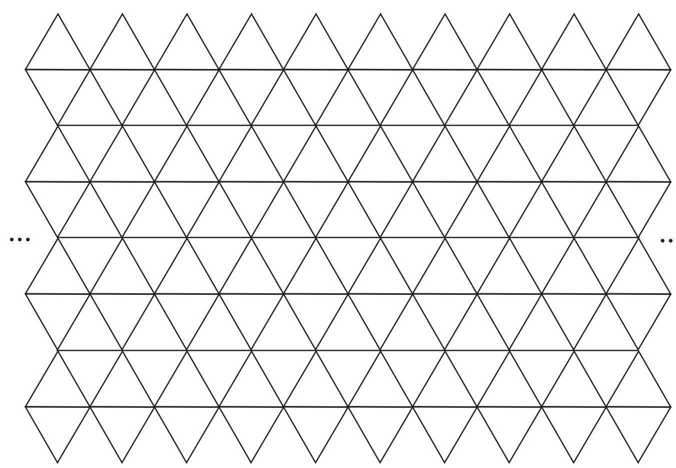


Figure 4.26: A regular tessellation

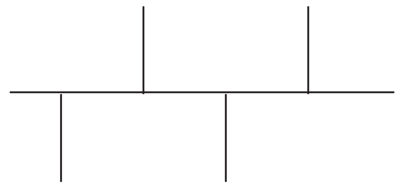


Figure 4.27: Not a regular tessellation

at a finite portion of the tessellation, which **is** a planar graph. Equation (4.7) is almost valid. It is not quite right because the formulas in Exercise 4.4.3 are not quite right.

For example, we might use the portion of the tessellation pictured in Figure 4.26 as a "partial tessellation". The vertices on the interior of this partial tessellation all have degree six. But those on the outer boundary have lower degree—some have degree five, some have degree three and some have degree two. The faces on the interior all have three edges around them, but the exterior face has many edges.

However, if we let this partial tessellation grow larger and larger, the contribution of the vertices, edges and faces on the outer boundary becomes small compared to the contributions of the vertices, edges and faces in the interior.

Furthermore, as we let the partial tessellation grow, the number of edges grows, so that Equation (4.7) becomes the following:

A regular tessellation with face degree q and vertex degree p satisfies

$$\frac{1}{p} + \frac{1}{q} = \frac{1}{2}\,. \tag{4.8}$$

Exercise 4.5.1. Use Equation (4.8) and the conditions $p \geq 3$ and $q \geq 3$ to verify that there are only three regular tessellations of the plane. Draw them.

As in the case of polyhedra not all tessellations are regular. Again we can relax the regularity rules a bit to get a larger class of tessellations.

Semi-regular tessellations are tessellations made up of two or more types of regular polygons, and the polygons are arranged at each vertex in the same way. An example is pictured in Figure 4.28

Note that each vertex has two octagons and a square around it.

Exercise 4.5.2. Suppose the degree of every vertex of a semi-regular tessellation is four and that the tessellation is made up of triangles and hexagons. How many triangles and how many hexagons meet at a vertex? Try to draw the tessellation.

There are eight semi-regular tessellations. One was drawn in Figure 4.28. One was described in Exercise 4.5.2.

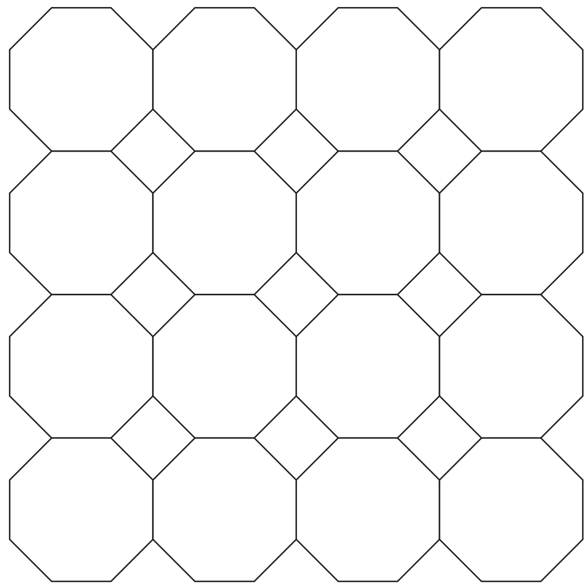


Figure 4.28: A semi-regular tessellation

Exercise 4.5.3. Find as many of the other six semi-regular tessellations as you can.

4.6 Torus Graphs

We have seen several graphs which do not have planar representations—for example, K_5 and $K_{3,3}$. It might be possible, however, to draw these graphs on the surface of more complicated three-dimensional objects without crossing edges.

For example, it might be possible to draw such a nonplanar graph on the surface of a doughnut. The surface of a doughnut is called a *torus* (see Figure 4.29). A torus can be viewed in two dimensions as a rectangle with opposite edges identified (see Figure 4.30). To convert from the rectangle to the torus, imagine rolling a rectangular piece of paper into a tube, then curling the tube up into a doughnut shape. Thus, in Figure 4.30, the point A appears in two places. Notice that the corners of the rectangle (point P in Figure 4.30) all refer to the same point.

Exercise 4.6.1. Draw $K_{3,3}$ and K_5 on the surface of a torus.

Exercise 4.6.2. Draw K_6 on the surface of a torus.

Exercise 4.6.3. Draw K_7 on the surface of a torus.

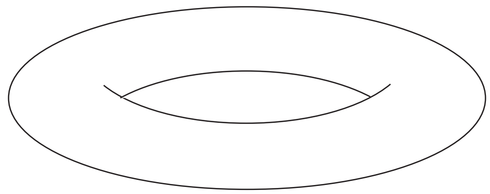


Figure 4.29: A torus

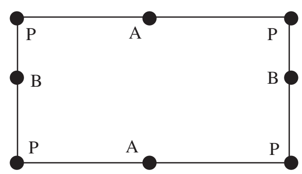


Figure 4.30: A flattened-out torus

Exercise 4.6.4. The idea of a face also makes sense for graphs on a torus. In Exercise 4.6.1 you drew K_5 and $K_{3,3}$ on the torus. Show that for these graphs, $V - E + F = 0$.

4.7 Coloring Graphs

If you tried to color the states in a map of the United States, you would find that you could use just four colors and never have two states with a common border colored alike.

The question of whether every map could be colored using four colors was unsolved for a hundred years, until the mid 1970's when Appel and Hocking proved that four colors were all that was needed.

We usually translate the map coloring problem into a graph coloring problem. The faces in the map are replaced by vertices, the common borders by edges. The map coloring problem translates into a problem of coloring the vertices of a planar graph so that no two adjacent vertices are colored alike. Figure 4.31 gives an example of this translation.

Actually, we might try to color the vertices of every graph (not just planar graphs) so that adjacent vertices are colored differently. The number of colors that are required is called the *chromatic number* of the graph. What Appel and Hocking showed was that the chromatic number of every planar graph is no more than four.

Exercise 4.7.1. What is the chromatic number of K_n? Of $K_{n,m}$?

Exercise 4.7.2. A teacher is trying to organize work groups in her classroom. She has 10 students and she wants three work groups. However the following

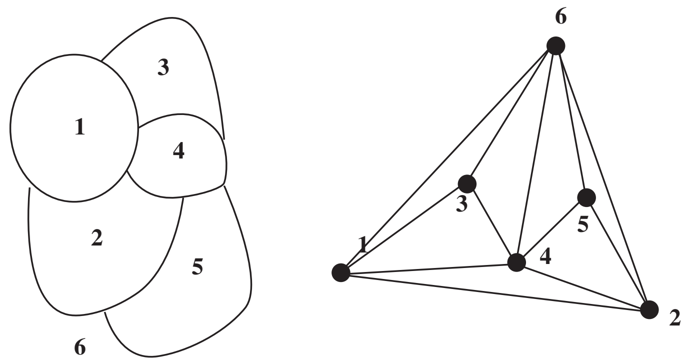


Figure 4.31: A planar map and its dual

pairs of students don't get along with each other and should not be in the same work group: Mark and Jennifer; Mark and Kristin; Mark and Lynn; Jennifer and Oliver; Oliver and Kristin; Oliver and Phil; Phil and Kristin; Phil and Lynn; Kristin and Lynn; Mark and Oliver. The other students, Ann, Bill, Cathy and Edward, get along with everyone. Restate this as a coloring problem. Can she do it?

All graphs have a number associated called the *genus*. The genus is the number of "holes" that must be punched through a sphere to create a surface upon which the graph can be drawn without crossing edges. Planar graphs have genus 0. They can be drawn on the surface of a sphere with no holes. The torus described in Section 4.6 has one hole; graphs which can be drawn on the torus but not on the sphere, like K_5, K_6 and K_7, have genus one.

Among all the graphs of a given genus, we might ask what is the largest chromatic number? For genus 0, the answer, four, was given by Appel and Hocking. For graphs of higher genus, there is a beautiful formula whose proof actually predates the four color theorem. If $g > 0$ is the genus and c is the largest chromatic number for graphs of that genus, then

$$c = \left[\frac{7 + \sqrt{1 + 48g}}{2}\right], \tag{4.9}$$

where $[x]$ means the greatest integer less than or equal to x.

Exercise 4.7.3. How many colors suffice for graphs which can be drawn on a torus? For graphs of genus 2?

Exercise 4.7.4. Although Equation (4.9) was only proved for $g > 0$, what happens in that equation if you let $g = 0$?

Although the proof of the four color theorem is certainly beyond the scope of this class (it required the computer analysis of over 1400 special cases), the proof that no more than five colors are required is sometimes given in undergraduate graph theory courses. We will show that no more than six colors are required to color the vertices of a planar graph with adjacent vertices colored differently.

The elements of this proof are actually the first steps in the proofs of the five- and four-color results.

The key to the argument is the fact that planar graphs cannot have too many edges, which was Inequality (4.5), namely, $E \leq 3V - 6$.

Exercise 4.7.5. Use this inequality to show that a planar graph must have at least one vertex of degree 5 or less.

The argument is an inductive argument. Start with a planar graph. Suppose you have a method of 6-coloring each graph with fewer vertices. Find a vertex of degree 5 or less in your graph. Remove it. Now use your method for smaller graphs to color what's left with the six colors. Then put the vertex of degree 5 back. It is adjacent to five or fewer vertices, which use five or fewer colors. Since six colors are available, this vertex can be colored the sixth color without messing up the coloring of the rest of the graph. Figure 4.32 describes the argument.

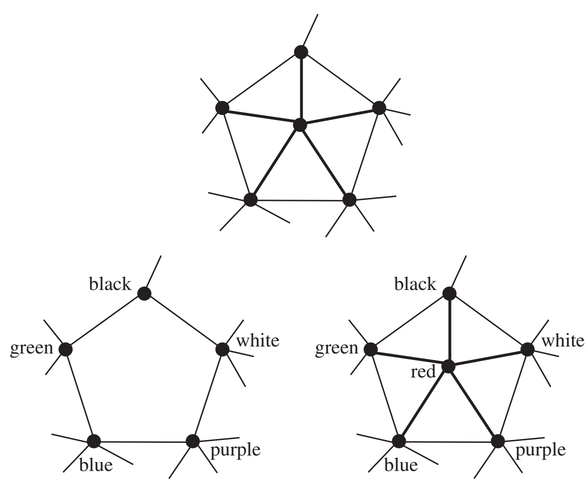


Figure 4.32: Coloring a degree 5 vertex

Exercise 4.7.6. Why doesn't this argument work for five colors instead of six?

4.8 Tournaments

In a round-robin tournament, every team plays every other team once. We can visualize the outcome of such a tournament with a special kind of graph called a *directed graph*. In a directed graph, edges have a direction ascribed, usually denoted pictorially as an arrow. In the case of a tournament, every possible edge is drawn (as in a complete graph), with the arrow pointing from the winning team to the losing team. Figure 4.33 describes a tournament with five teams, A, B, C, D and E. In this tournament, B beats A, C, D and E; A beats C and D; C beats D and E; D beats E; and E beats A.

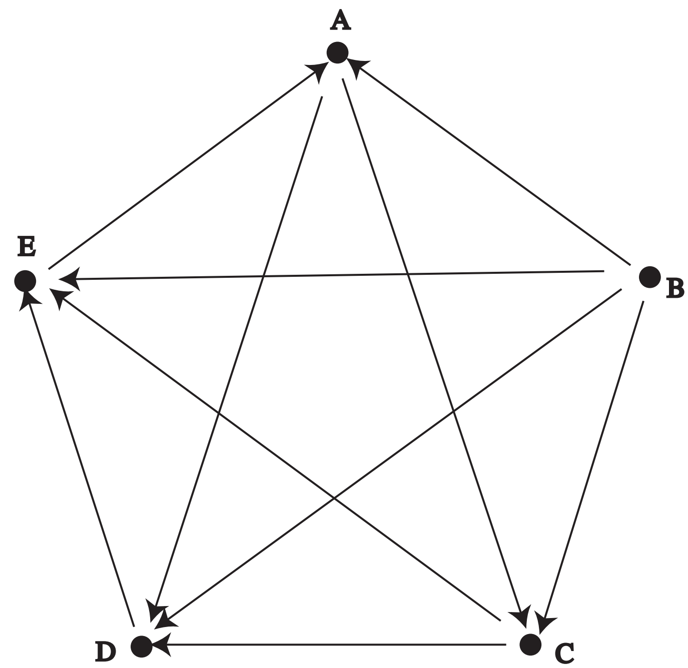


Figure 4.33: A tournament

We will begin by counting tournaments.

Exercise 4.8.1. Draw all the tournaments with three teams.

Exercise 4.8.2. How many tournaments are there with four teams? How many are there with n teams?

Some tournaments are especially well-behaved. For instance, a tournament might have the property that whenever u beats v and v beats w, then u beats w. Such tournaments are called *transitive*. If this condition does not always hold, then the tournament is called *intransitive*.

Exercise 4.8.3. Is the tournament in Figure 4.33 transitive or intransitive?

Exercise 4.8.4. Give an example of a transitive tournament with five teams.

Some tournaments might contain a *directed cycle*, i. e., a sequence of teams A, B, C, ..., K, where A beats B, B beats C, ..., and K beats A. In the above tournament, A beats C, C beats D, D beats E and E beats A.

Exercise 4.8.5. Does an intransitive tournament contain a directed cycle? Why or why not?

Notice that in the tournament in Figure 4.33, there is a 3-cycle (a directed cycle with three edges): A beats D, D beats E and E beats A.

Exercise 4.8.6. Show that if a tournament contains a directed cycle, it contains a directed 3-cycle. Conclude that if a tournament contains a directed cycle, it is intransitive.

Exercises 4.8.5 and 4.8.6 show that a tournament is transitive if and only if it has no directed cycles.

One way to describe a tournament is with its *score vector*. This is just the sequence of the number of wins for each team. For example, the tournament in Figure 4.33 has this score vector: $(2, 4, 2, 1, 1)$. This means team A won two matches, team B won four, team C won two, team D won one and team E won one.

Exercise 4.8.7. Notice that the sum of scores in the example in Figure 4.33 is 10. Give another example of a tournament with five teams. What is its score vector? What is the sum of the scores? What is the sum of the scores for a tournament with n teams? What is the largest possible score?

The score vector does not determine the tournament; there are examples of two essentially different tournaments with the same score vector. However, the score vectors of transitive tournaments are especially simple and do determine the tournament.

Exercise 4.8.8. Show that $(0, 1, 2, \ldots, n-1)$ is the score vector of some transitive tournament with n teams.

Exercise 4.8.9. Suppose T is a transitive tournament. Show that the score vector of T cannot have two equal values. Hint: Suppose two teams, A and B, have equal scores. Suppose A beats B. Now suppose B beats C. Can C beat A? Can every team that B beats beat A? Why not? Conclude that A must beat all the teams that B beats. Why is this not possible?

Exercise 4.8.10. Conclude from Exercise 4.8.9 that if T is a transitive tournament on n teams, then the score vector of T must be some rearrangement of $\{0, 1, 2, \ldots, n-1\}$.

Exercises 4.8.8, 4.8.9 and 4.8.10 show that T is a transitive tournament on n teams if and only if the score vector of T is a rearrangement of $\{0, 1, 2, \ldots, n-1\}$.

Exercise 4.8.11. How many transitive tournaments with n teams are there?

Chapter 5

Integers and Rational Numbers

In this chapter we will investigate some important properties of the integers and the rational numbers. The properties of integers include facts about primes, greatest common divisors and least common multiples, and the prime factorization theorem. We will also discuss representations of numbers and different number bases.

The integers extend quite naturally into the rationals. We will learn about decimal and other representations of rationals and about describing a number system with a collection of axioms.

5.1 Primes and Prime Factorization

Early in your mathematical life, you learned about numbers: how to count, how to add and subtract, and how to multiply and divide. You also learned that numbers come in different flavors. You probably first encountered the positive integers, $\{1, 2, 3, \ldots\}$, also called "counting numbers" or "natural numbers." When the number 0 is inserted, the set is called the nonnegative integers (in some books "whole numbers"). However, you discovered you needed negative numbers (if it warms 10 degrees from 20 below, what temperature is it?), thus forming the set of integers.

Later you learned that the inverse process of multiplication, called division, is not defined on all the integers. When one positive integer was divided by another, the result was a quotient and a remainder. Some divisions resulted in a zero remainder. Some did not. For example, when 18 is divided by 6, the remainder is 0. But if 20 is divided by 6, the remainder is 2. In order to deal with this second example, you learned about rational numbers. These will be discussed later in this chapter. In this section and the following two we will concentrate on some of the properties of the positive integers.

To express the fact that 6 divides 18 with no remainder, we write $6|18$. The symbol | is read "divides." Thus $d|n$ means d *divides* n, or d is a *divisor* of n or a *factor* of n. Every integer larger than 1 always has two divisors: 1 and itself. Some positive integers have many divisors.

Exercise 5.1.1. Write down all the divisors of 16. Of 36.

Integers larger than 1 whose divisors consist only of 1 and itself are called *primes*. Integers larger than 1 which are not prime are called *composite*. For instance, 98, 99 and 100 are composite (or composite numbers), but 97 and 101 are primes (or prime numbers).

Exercise 5.1.2. Write down all the primes smaller than 100.

Primes form the multiplicative building blocks of the positive integers. Either a positive integer is a prime or it is a product of two smaller positive integers. Now iterate this process on those two smaller positive integers: both might be primes, but if one is composite, write it as a product of two smaller positive integers. Continue this process, until the original integer is written as a product of primes. For example,

$$144 = 36 \cdot 4 = (9 \cdot 4) \cdot (2 \cdot 2) = ((3 \cdot 3) \cdot (2 \cdot 2)) \cdot (2 \cdot 2)\,.$$

Notice that there is more than one way to do this. Here is another way:

$$144 = 24 \cdot 6 = (4 \cdot 6) \cdot (2 \cdot 3) = ((2 \cdot 2) \cdot (3 \cdot 2)) \cdot (2 \cdot 3)\,.$$

A very important theorem, called the Fundamental Theorem of Arithmetic, says that regardless of how this is done, the final answer will contain the same list of primes, with the same numbers of occurrences (called *multiplicities*). In our example, 144 factors into 4 2's and 2 3's. We write $144 = 2^4 \cdot 3^2$. This is called *the prime factorization* of 144. The multiplicity of the prime 2 is 4, while the multiplicity of the prime 3 is 2

Exercise 5.1.3. Write down the prime factorizations of 1000, 192 and 196.

Determining the prime factorization of large numbers plays an important role in modern cryptography (and its applications to internet security).

Exercise 5.1.4. Find the prime factorizations of 977220 and 39463. What method are you using?

Exercise 5.1.5. Write down a three digit number. Now write down the six digit number made up of two copies the three digit number. (If your original number is *abc*, then the six digit number is *abcabc*.) Use your calculator to divide the six digit number by 13. Does it divide evenly? Explain. Now divide the quotient by 11. Does that divide evenly? Explain. Now divide that quotient by 7. Does that divide evenly? Explain.

We can use the Fundamental Theorem of Arithmetic to count the number of divisors a given number has. The next few exercises describe this method.

Exercise 5.1.6. How many divisors does 32 have? 36? 100? 144?

Exercise 5.1.7. Work out a general rule for computing the number of divisors of an integer. (Hint: use the prime factorization.) If $N = p^k q^m r^n$ where p, q and r are distinct primes and k, m and n are positive integers, how many divisors does N have?

Exercise 5.1.8. How many divisors does $2^3 \cdot 3^5 \cdot 7^2$ have? How many divisors does $6^4 \cdot 24^2 \cdot 100^2$ have?

Exercise 5.1.9. Every student in a class with 25 students is seated. Each student in the room takes a number from 1 to 25. The teacher calls off all the numbers from 1 to 25 successively. When a student hears a number called which divides her number, she stands if she is seated and sits if she is standing. After all 25 numbers have been called, what are the numbers of the students left standing? Complete and prove the following: the number of divisors of a number is odd if and only if . . . . What is the relationship between this statement and the game just described?

The Fundamental Theorem of Arithmetic says that every integer can be written uniquely as a product of primes.

Exercise 5.1.10. Since $2^3 \cdot 3 = 3 \cdot 2^3$, in what sense is the prime factorization of 24 "unique?"

Exercise 5.1.11. Suppose m and n are two integers, both ≥ 1. Is it possible that $m^2 = 2n^2$? If so, give an example, if not, give a reason.

Suppose A and B are two numbers whose product is a perfect square, $AB = C^2$.

Exercise 5.1.12. Do A and B have to be perfect squares? If not, give an example. If so, give a proof.

Now suppose A and B have no common divisor, and their product is a perfect square, $AB = C^2$.

Exercise 5.1.13. Show that A and B both have to be perfect squares.

The next two exercises demonstrate that there is no "largest" prime, just like there is no "largest" integer. We begin by assuming that there is a largest prime. Then the list of primes must be finite. We write down this list: $\{2, 3, 5, \ldots, P\}$, where P is this largest prime. The Fundamental Theorem of Arithmetic implies that every integer greater than one is a product of numbers from this list. In particular, if $N = 2 \cdot 3 \cdot 5 \cdots P$, then $N + 1$ is a product of numbers from this list.

Exercise 5.1.14. Continuing the discussion above, can 2 divide $N+1$? Can 3 divide $N+1$? Can 5 divide $N+1$? Can each of the primes in the list $\{2, 3, 5, \ldots, P\}$ divide $N+1$?

Exercise 5.1.15. Use Exercise 5.1.14 to conclude that $N+1$ is not a product of numbers from this list. Why does this mean that P is not the largest prime?

Summarizing these last two exercises, we have the following theorem.

Theorem 10. *There is no largest prime number. Equivalently, there are an infinite number of primes.*

5.2 The Euclidean Algorithm and the GCD

Suppose we wish to find a common multiple of 24 and 36. We could simply multiply 24 and 36. But in many situations we want the **smallest** such multiple. This is called the *least common multiple*, or LCM. We refer to it with LCM(24, 36).

A related problem is to find a common divisor of 24 and 36. Certainly 1 is a common divisor, but we usually want the **largest** such divisor. This is called the *greatest common divisor*, or GCD, and we refer to it with GCD(24, 36).

Exercise 5.2.1. What is GCD(24, 36) and LCM(24, 36)?

There are a couple of ways you may have learned to calculate the GCD. (We shall see that the LCM can be computed easily from the GCD.) One way is simply to find any common divisor, divide into both numbers, and repeat. When the two numbers no longer have a common divisor, take the product of all the divisors. That will be the GCD. Another way is to find the prime factorization of both numbers, then deduce the GCD from the prime factorization.

Exercise 5.2.2. Find the GCD of 96 and 144 using both methods.

Exercise 5.2.3. How can you find the LCM directly from the prime factorization? Demonstrate on 96 and 144.

Exercise 5.2.4. If we start with a perfect square (144, for instance), and factor it into a product of two numbers which do not have a common factor (like $16 \cdot 9$), then the two numbers themselves are perfect squares. Explain why.

A third way to compute the GCD, one which is very effective on large numbers and is implemented on computers, is called the Euclidean algorithm.

Notice that $\text{GCD}(24, 36) = \text{GCD}(36 - 24, 24)$. This is because each number which divides 24 and 36 also divides $36 - 24$ and 24, while each number which divides $36 - 24$ and 24 also divides 36 and 24 (since $36 = (36 - 24) + 24$). Therefore, the set of common divisors of 24 and 36 is exactly the same as the set of common divisors of $36 - 24$ and 24. In particular, the greatest common divisors will be the same.

Exercise 5.2.5. In a similar manner, show that $\text{GCD}(96, 144) = \text{GCD}(144 - 96, 96)$.

The Euclidean algorithm is based on the following fundamental fact, which generalizes the above argument.

Exercise 5.2.6. Show that if $n > m$ are positive integers, then the GCD of n and m is the same as the GCD of m and $n - m$.

The Euclidean algorithm iterates Exercise 5.2.6. For example, let's compute GCD(48, 18). By Exercise 5.2.6, we have

$$\text{GCD}(48, 18) = \text{GCD}(30, 18) = \text{GCD}(18, 12) = \text{GCD}(12, 6) = 6\,.$$

Let's demonstrate with a larger example: 14520 and 37800.

$$\text{GCD}(37800, 14520) = \text{GCD}(23280, 14520) = \text{GCD}(8760, 14520)\,.$$

Note that since division is repeated subtraction, these two steps could be replaced by the single step of dividing 14520 into 37800 and taking the remainder (8760), then replacing 37800 with 8760. Here is the complete process (using these division-remainder shortcuts):

$$\begin{aligned}\text{GCD}(14520, 37800) &= \text{GCD}(8760, 14520)\\ &= \text{GCD}(5760, 8760)\\ &= \text{GCD}(3000, 5760)\\ &= \text{GCD}(2760, 3000)\\ &= \text{GCD}(240, 2760)\\ &= \text{GCD}(120, 240)\,.\end{aligned}$$

We stop when one of the numbers is a divisor of the other. That divisor must be the GCD, so our answer is 120.

Exercise 5.2.7. Show the arithmetic in each step in the above calculation.

Exercise 5.2.8. Use the Euclidean algorithm to find the GCD of 33075 and 30030. Find the GCD of 329800 and 480249.

The fact that we could divide one number into another and get a remainder is something you probably learned in grade school, and is a fundamental arithmetic principle which we will see again. We can express this fact algebraically: for nonnegative integer n and positive integer d, there is a unique pair of nonnegative integers q and r, with $r < d$, such that

$$n = q \cdot d + r\,. \tag{5.1}$$

We can find the greatest common divisor of more than two numbers. For example, $\text{GCD}(12, 20, 30) = 2$. We can compute this by using the prime factorization. Or we can use the Euclidean algorithm repeatedly: first find the GCD of 12 and 20, then find the GCD of that number and 30.

Exercise 5.2.9. Find GCD$(504, 1120, 5670)$.

Exercise 5.2.10. Find $X =$ GCD$(504, 1120)$, $Y =$ GCD$(504, 5670)$ and $Z =$ GCD$(1120, 5670)$. Is GCD$(X, Y) =$ GCD$(504, 1120, 5670)$?

As was mentioned earlier, we may use the GCD to compute the LCM. The next two exercises demonstrate how this is done.

Exercise 5.2.11. Write down the product of 24 and 36 and also the product of GCD$(24, 36)$ and LCM$(24, 36)$.

Exercise 5.2.12. Prove that GCD$(m, n) \cdot$ LCM$(m, n) = m \cdot n$. Use this to find LCM$(14520, 37800)$.

5.3 Number Bases

We have learned to represent our numbers in a base ten positional system. We have grown so familiar with our system that it is hard for us to "pull it apart" and find out what really makes it work. We should recognize, however, that other cultures through the ages have used other number systems and even other positional systems.

Our number system is a positional system. The location of a digit within the number has a meaning. If a 3 appears in the rightmost position, it means something different than a 3 in the second rightmost position.

In fact, a 3 in the rightmost position contributes 3 to the number; in the second rightmost position it contributes 30; in the third position, it contributes 300, etc. That first position we call the 1's position, the second position the 10's position, the third position the 100's position, etc. Any digit in, say, the 10's position gets multiplied by 10. Any digit in the 1000's position gets multiplied by 1000.

So the number 12553 really means $1 \cdot 10^4 + 2 \cdot 10^3 + 5 \cdot 10^2 + 5 \cdot 10 + 3$.

In general, each nonnegative integer N written $d_n d_{n-1} d_{n-2} \cdots d_2 d_1 d_0$ means

$$N = d_n 10^n + d_{n-1} 10^{n-1} + d_{n-2} 10^{n-2} + \cdots + d_2 10^2 + d_1 10 + d_0 \,. \quad (5.2)$$

Our various arithmetic algorithms (long division, for example) exploit this notation. Because we are so familiar with the notation, it is easy to forget its real meaning, Equation (5.2) above.

As was mentioned above, our number system is not the only system used through the ages, not even the only positional system. The Mayans, in particular, used a base twenty system.

All that's required to express a number using another base is an equation like Equation (5.2), where ten is replaced by the other base.

Exercise 5.3.1. Write down the base b analog of Equation (5.2).

The first consequence of this is that the number of digit symbols changes. We need exactly b different symbols to express integers in base b. For base ten, the symbols are $0, 1, 2, 3, 4, 5, 6, 7, 8$ and 9. If b is less than ten, we usually choose $0, 1, \ldots, b-1$, although nothing says we couldn't use something different. If b is greater than ten, we usually use 0 through 9 and some other symbols. Sometimes T is used for ten and E for eleven. Of course, the problem here is what gets used for twelve? Sometimes A is used for ten, B for eleven, etc. This is what we will do.

Since we are using the same symbols to mean different things, we should give some indication of what base we are in. Let's write a subscript to indicate the base; no subscript will mean base ten. For example, 10 means the number ten, while 10_{eight} means eight and 10_{two} means two.

Another thing we notice is that as the base grows larger, the length of the numbers grows shorter. For example, if 1000 is written in base one thousand, it is 10_{thousand}. The same number in base 2 is 1111101000_{two}.

This seems to give an advantage to a large number base. But large bases come at a considerable cost: if we used base one thousand, we would need to have one thousand symbols for digits. Even worse, our multiplication tables would be one thousand by one thousand, and would therefore have one million entries! On the other hand, the symbols and arithmetic tables for base 2 are ridiculously simple:

$$\begin{aligned} 1_{\text{two}} + 1_{\text{two}} &= 10_{\text{two}}\,, \\ 1_{\text{two}} + 0_{\text{two}} = 0_{\text{two}} + 1_{\text{two}} &= 1_{\text{two}}\,, \\ 0_{\text{two}} + 0_{\text{two}} &= 0_{\text{two}}\,, \\ 1_{\text{two}} \cdot 0_{\text{two}} = 0_{\text{two}} \cdot 1_{\text{two}} = 0_{\text{two}} \cdot 0_{\text{two}} &= 0_{\text{two}} \text{ and} \\ 1_{\text{two}} \cdot 1_{\text{two}} &= 1_{\text{two}}\,. \end{aligned}$$

Exercise 5.3.2. Table 5.1 lists the first 15 counting numbers in base ten, base two, base three, base eight, base twelve and base sixteen. Write down the next fifteen counting numbers in these bases.

Exercise 5.3.3. What is the next counting number in base two after 100111_{two}? After 4677_{eight} in base eight? After $3A7F_{\text{sixteen}}$ in base sixteen?

***Exercise 5.3.4.** How many digits in base b are required to write a particular number N?

Converting numbers from one base to another is quite simple. Here is one way to take a number N from base ten to another base. Divide N by b. The remainder is the 1's digit. Now divide the quotient by b again. The remainder is the b's digit. Continue in this manner until nothing remains.

For example, if we want to write 75 in base four, divide 75 by 4 to get 18 with remainder 3. Then divide 18 by 4 to get 4 with remainder 2. Then divide 4 by 4 to get 1 with remainder 0. Finally, divide 1 by 4 to get 0 with remainder 1. The remainders are 1, 0, 2 and 3, so $75 = 1023_{\text{four}}$.

Base					
Ten	Two	Three	Eight	Twelve	Sixteen
1	1	1	1	1	1
2	10	2	2	2	2
3	11	10	3	3	3
4	100	11	4	4	4
5	101	12	5	5	5
6	110	20	6	6	6
7	111	21	7	7	7
8	1000	22	10	8	8
9	1001	100	11	9	9
10	1010	101	12	A	A
11	1011	102	13	B	B
12	1100	110	14	10	C
13	1101	111	15	11	D
14	1110	112	16	12	E
15	1111	120	17	13	F

Table 5.1: Counting Numbers

Exercise 5.3.5. Convert to bases two, three, nine and twelve: 81, 256, 1000.

Exercise 5.3.6. Explain why this method works. Use your answer in Exercise 5.3.1.

Exercise 5.3.7. Convert from base ten:

i. to base three: 4000

ii. to base five: 7293

iii. to base two: 966

iv. to base two: 1545

v. to base eight: 1276

vi. to base sixteen: 3977

One way to convert back to base ten is simply to use Exercise 5.3.1 directly. For instance,

$$\begin{aligned} 1023_{\text{four}} &= 1 \cdot 4^3 + 0 \cdot 4^2 + 2 \cdot 4^1 + 3 \cdot 4^0 \\ &= 1 \cdot 64 + 0 \cdot 16 + 2 \cdot 4 + 3 \cdot 1 = 75\,. \end{aligned}$$

Exercise 5.3.8. Convert to base ten: 100_{two}, 155_{eight}, $\text{EEFF}_{\text{sixteen}}$, $\text{A00}_{\text{twelve}}$.

Here is an alternative (and somewhat faster) method: Take the leftmost digit of the number you are converting, multiply it by b and add the next digit. Multiply that result by b and add the next digit. Continue until no digits remain.

For instance, for 1023_{four}, compute $1 \cdot 4 + 0 = 4$, then $4 \cdot 4 + 2 = 18$, then $18 \cdot 4 + 3 = 75$.

Exercise 5.3.9. Repeat Exercise 5.3.8 using this method.

Exercise 5.3.10. Use your answer in Exercise 5.3.1 to give a reason why this method works.

Exercise 5.3.11. Convert to base ten:

i. $6A0B5_{\text{twelve}}$

ii. 740433_{eight}

iii. $4FEC_{\text{sixteen}}$

iv. 2210112_{three}

v. 101110100_{two}

vi. 111011101_{two}

Some bases are more useful than others. The important ones are base two (called binary), base three (ternary), base eight (octal), base twelve (duo decimal) and base sixteen (hexadecimal).

Two is useful because binary is the language of computers. Since $16 = 2^4$, there is an especially easy way to convert back and forth between binary and hexadecimal. To go from binary to hexadecimal, group the digits four at a time, starting from the right. Each group of four digits represents a number (written in binary) from 0 to 15. These numbers correspond to the hexadecimal digits.

For example, $100110100_{\text{two}} = [0001][0011][0100] = 134_{\text{sixteen}}$.

To convert a hexadecimal number to binary, expand each digit (from 0 to F) into a four digit binary (from 0000 to 1111).

For example, $24E_{\text{sixteen}} = [0010][0100][1110] = 1001001110_{\text{two}}$.

Exercise 5.3.12. Convert from base two to base sixteen: $100010101000_{\text{two}}$; convert from base sixteen to base two: $AEE09_{\text{sixteen}}$.

Exercise 5.3.13. Explain why this method works.

Exercise 5.3.14. Convert from base three to base nine: 21211101_{three}; convert from base eight to base four: 77320_{eight} (hint: go through base 2 in an intermediate step).

Exercise 5.3.15.

i. Convert to base sixteen: 101110100_{two}

ii. Convert to base sixteen: 3320213_{four}

iii. Convert to base three: 78055_{nine}

iv. Convert to base two: $4AEF_{\text{sixteen}}$

v. Convert to base two: 6437_{eight}

vi. Convert to base two: 30321_{four}

To do arithmetic in another base, we could convert the numbers to base ten, do the arithmetic in our comfortable base ten system, then convert the answer back. However, it's usually easier to do the arithmetic in the original base. All that is necessary is the appropriate multiplication or addition table. And that need not be "memorized." It can be constructed "on the fly" from the base ten tables. For example,

$$\begin{array}{cccc} {}^{1} & 3^{1} & 5^{1} & 5_{\text{six}} \\ + & 2 & 1 & 4_{\text{six}} \\ \hline 1 & 0 & 1 & 3_{\text{six}} \end{array}$$

In the one's place, 5 plus 4 is nine, which is 13_{six}. So write the 3 and carry the 1.

In the six's place, 5 plus 1 plus the carried 1 is seven, which is 11_{six}. So write the 1 and carry the 1.

In the thirty-six's place, 3 plus 2 plus the carried 1 is six, which is 10_{six}. So write the 0 and carry the 1.

In the two hundred sixteen's place, write the carried 1.

For subtraction, borrowing in the base must take place:

$$\begin{array}{cccc} & 7 & 0 & 3_{\text{eight}} \\ - & 2 & 6 & 7_{\text{eight}} \\ \hline & 4 & 1 & 4_{\text{eight}} \end{array}$$

In the one's place, borrow an eight from the eight's place to make the 3 a 13_{eight}. Then subtract 7 from 13_{eight} to get four.

In the eight's place, borrow a sixty-four from the sixty-four's place to make the 0 a 10_{eight}. But since one was borrowed from the eight's place for the subtraction in the one's place, the 10_{eight} is reduced by one to 7. Now subtract the 6 from the seven to get 1.

Finally, in the sixty-four's place, the seven had one borrowed to leave a 6. Subtract 2 from that 6 to get 4.

Here is an example of multiplication:

$$\begin{array}{ccccc} & & 3 & 2 & 2_{\text{four}} \\ & & \times & 1 & 3_{\text{four}} \\ \hline & 2 & 2 & 3 & 2 \\ & 3 & 2 & 2 & \\ \hline 1 & 2 & 1 & 1 & 2_{\text{four}} \end{array}$$

Here is an example of division:

$$\begin{array}{ccccccccc}
 & & & & & 2 & 0 & 2 & 1_{\text{three}} \\ \cline{4-9}
2 & 1_{\text{three}} &) & 1 & 2 & 0 & 2 & 1 & 2_{\text{three}} \\
 & & & 1 & 1 & 2 & & & \\ \cline{4-6}
 & & & & & 1 & 2 & 1 & \\
 & & & & & 1 & 1 & 2 & \\ \cline{6-8}
 & & & & & & & 2 & 2 \\
 & & & & & & & 2 & 1 \\ \cline{8-9}
 & & & & & & & & 1_{\text{three}}
\end{array}$$

Exercise 5.3.16. Add in base five: 41301_{five} and 44043_{five}. Add in base two: 10011_{two} and 101001_{two}.

Exercise 5.3.17. Do the following additions:

i. $20112_{\text{three}} + 21011_{\text{three}}$

ii. $4AB7_{\text{twelve}} + 6A95_{\text{twelve}}$

iii. $1011101001_{\text{two}} + 100100111_{\text{two}}$

iv. $41557_{\text{eight}} + 36604_{\text{eight}}$

v. $44014_{\text{five}} + 20133_{\text{five}}$

vi. $110111100_{\text{two}} + 10010101_{\text{two}}$

Exercise 5.3.18. Subtract in base nine: 788_{nine} from 3504_{nine}. Subtract in base four: 313_{four} from 2021_{four}.

Exercise 5.3.19. Do the following subtractions:

i. $44733_{\text{eight}} - 31665_{\text{eight}}$

ii. $3A44_{\text{sixteen}} - 2AEF_{\text{sixteen}}$

iii. $110100010_{\text{two}} - 100110111_{\text{two}}$

iv. $143320_{\text{five}} - 44222_{\text{five}}$

v. $3200_{\text{twelve}} - 2AA9_{\text{twelve}}$

vi. $10010011_{\text{two}} - 1011110_{\text{two}}$

Exercise 5.3.20. Multiply in base twelve: $2A43_{\text{twelve}}$ by $B6_{\text{twelve}}$. Multiply in base eight: 35_{eight} by 274_{eight}.

Exercise 5.3.21. Divide in base two: 101_{two} into 100101000_{two}. Divide in base sixteen: $4E_{\text{sixteen}}$ into $3A9D_{\text{sixteen}}$.

5.4 Integers

In this section we will begin a discussion of number systems. This discussion will be continued in later chapters. We start with a discussion of the properties of the integers, including the negative integers. A common notation of this set is $\mathbb{Z}$. We are so familiar with the arithmetic and order properties of $\mathbb{Z}$ that we take them for granted. Let's write down here some of these properties.

P-1 The sum, product or difference of every two integers is another integer. However, the quotient of two integers is not always an integer.

P-2 The order in which two things are added (or multiplied) does not matter. However, the order in which they are subtracted or divided does.

P-3 Multiplication distributes through addition.

P-4 The integer 0 is special. If we add it to or subtract it from another integer, it does not change the other integer. If we multiply it by another integer, we get 0. We cannot divide by it.

P-5 The integer 1 is special. If we multiply it by another integer, we get the other integer. If we divide another integer by it, we get the other integer.

P-6 Every integer except 0 has a negative. The sum of the two is 0.

P-7 If a non-0 integer is positive, its negative is negative. If non-0 integer is negative, its negative is positive.

P-8 The integer 1 is positive. Its negative, -1, when multiplied by another integer, gives the negative of that integer.

P-9 The product of two negatives is positive. The product of two positives is positive. The product of a negative and a positive is negative.

Exercise 5.4.1. Give an illustrating example of each part of each of the properties listed above.

Exercise 5.4.2. Find at least two more such properties.

The list of properties above is chaotic. There are several difficulties with it. Let's try to sort these out. First, it is hardly complete—no such list could be complete. Second, the use of the word "negative" is confusing. It means two different things. It is the "additive inverse" in Property P-6. But in Property P-7, negative means less than 0. These two different meanings lead to confusing phrases such as "the negative of a negative is positive."

Finally, some of these properties are consequences of others. If we try to figure out which properties "define" the integers, and which can be proved from these defining properties, we come up with the following list, which we will call axioms.

Addition axioms:

A-1 (Closure). The sum of every two integers is an integer. That is, for every pair of integers n and m, $n+m$ is also an integer.

A-2 (Associative). $(k+m)+n = k+(m+n)$ for every triple of integers k, m and n.

A-3 (Commutative). The order in which things are added does not matter. That is, $m+n = n+m$ for every pair of integers m and n.

A-4 (Identity). There is a special integer, called 0, which, when added to every other integer, leaves that integer unchanged. That is, the integer 0 has the property that $0+n = n$ for every integer n.

A-5 (Inverse). Every integer has a special "twin" which, when added to it, yields 0. That is, for each integer n, there is another integer, called $-n$, such that $n+(-n) = 0$. (Some textbooks use $^{-}$ to represent $-n$. This avoids the confusion between the additive inverse and numbers less than 0.)

Multiplication axioms.

M-1 (Closure). The product of every two integers is an integer. That is, for every pair of integers n and m, $n \cdot m$ is also an integer.

M-2 (Associative). $(k \cdot m) \cdot n = k \cdot (m \cdot n)$ for every triple of integers k, m and n.

M-3 (Commutative). The order in which things are multiplied does not matter. That is, $m \cdot n = n \cdot m$ for every pair of integers m and n.

M-4 (Identity). There is a special integer, called 1, which, when multiplied by every other integer, leaves that integer unchanged. That is, the integer 1 has the property that $1 \cdot n = n$ for every integer n.

Distributive law.

D-1 (Distributive). $n \cdot (k+m) = n \cdot k + n \cdot m$ for all integers k, m, and n.

Order axioms.

O-1 (Trichotomy). For every pair of integers, one is less than the other or they are equal. That is, for integers m and n, exactly one of these holds: $m < n$, $n < m$ or $m = n$.

O-2 (Transitivity). If k, m and n are integers and if $k < m$ and $m < n$ then $k < n$.

O-3 Adding equal values to both sides of an inequality does not change the inequality. That is, if k, m and n are integers with $m < n$ then $m+k < n+k$.

O-4 The product of positive integers is positive. Thus, if m and n are integers such that $0 < m$ and $0 < n$ then $0 < m \cdot n$.

We axiomatize a number system for a several reasons. One reason is that it restores order to a list of properties such as those given earlier in this section. The axiom list strips down the number system to its essence. We retain only those axioms that we need. Other behavior displayed by our number system can be explained in terms of our axioms.

For example, all the properties described earlier can be derived from the above axioms. The formal structure of the arguments may be like those that you have seen in a plane geometry class. For example, in Property P-4, it is stated that the product of 0 with an integer is 0. That is, if n is an integer, then $0 \cdot n = 0$. Here is a proof of this statement.

$$\begin{aligned}
0 &= n \cdot 0 + (-(n \cdot 0)) && \text{A-5}\\
&= n \cdot (0 + 0) + (-(n \cdot 0)) && \text{A-4}\\
&= (n \cdot 0 + n \cdot 0) + (-(n \cdot 0)) && \text{D-1}\\
&= n \cdot 0 + (n \cdot 0 + (-(n \cdot 0)) && \text{A-2}\\
&= n \cdot 0 + 0 && \text{A-5}\\
&= 0 + n \cdot 0 && \text{A-3}\\
&= n \cdot 0 && \text{A-4}\\
&= 0 \cdot n && \text{M-3}\,.
\end{aligned}$$

Exercise 5.4.3. Here is a proof that $(-1) \cdot n = -n$ (Property P-8). As in the example above, give reasons for each step in this proof.

$$\begin{aligned}
(-1) \cdot n + n &= (-1) \cdot n + (1) \cdot n\\
&= ((-1) + (1)) \cdot n\\
&= 0 \cdot n\\
&= 0\\
\Rightarrow (-1) \cdot n &= -n\,.
\end{aligned}$$

Another reason to describe a number system by a list of axioms is that we may discover other number systems which satisfy the same list of axioms. Then we can conclude about the new system any result we were able to prove about the old system using the axioms. The beauty of this axiomatic approach is that it allows us to state and prove many common properties for widely disparate objects.

Exercise 5.4.4. Which of the axioms above does the set of even numbers satisfy? Which does the set of odd numbers satisfy?

Exercise 5.4.5. Which of the addition, multiplication and distributive axioms are satisfied by polynomials in the variable x with integer coefficients?

5.5 Rational Numbers

In this section we will show how the integers are extended to the rational numbers.

Exercise 5.5.1. Give two ways in which the integers and the rational numbers are different. That is, describe two things that you can do with rational numbers that you cannot do with integers.

Notice that in the list of axioms in the previous section, there is a "missing" axiom: an M-5 axiom. This axiom would say that every integer has a multiplicative inverse, a number such that when multiplied by the given number, gives 1.

But we know this doesn't happen: for example, 2 does not have such an inverse. Rational numbers were invented to deal with this "defect."

We may view the integers as an attempt to solve certain linear equations of the form $ax + b = 0$. However, when we are confronted with an equation like $3x + 1 = 0$, we cannot find an integer solution. The reason is the missing multiplicative inverse.

The rational numbers have this missing axiom. They satisfy all the axioms of the integers in the previous section, plus one more:

M-5 (Inverse). Every rational number except 0 has a special "twin" which, when multiplied by it, yields 1. That is, for each rational $a \neq 0$, there is another rational, called a^{-1}, such that $a \cdot a^{-1} = 1$.

***Exercise 5.5.2.** In Exercise 5.4.5 you saw that polynomials with integer coefficients satisfied the same addition, multiplication and distributive axioms as the integers. What "extension" of the polynomials will also satisfy the M-5 Axiom?

Another name for a^{-1} is $\frac{1}{a}$. We now define, for integers a and b, $a \neq 0$, $\frac{b}{a} = b \cdot \frac{1}{a}$. This definition, together with the axioms stated earlier, give us the usual arithmetic on fractions. The b is called the *numerator*, the a is called the *denominator*. The set of all numbers of the form a/b where a and b are integers is called *rational numbers*. A common notation for the rational numbers is $\mathbb{Q}$.

Exercise 5.5.3. Show that between every pair of distinct rational numbers there is a third rational number. Is the same thing true for integers? That is, is it true that for every pair of distinct integers there is a third, different, integer which lies between the first two? Explain.

We need to clarify two points about this fractional notation for rational numbers. The first point is that it is not unique. If the numerator and denominator have a common factor, that factor can be "canceled" from both parts. Thus, the fraction $\frac{6}{15}$ and the fraction $\frac{2}{5}$ both represent the same rational number. Usually, we try to reduce as much as possible, so that the numerator and denominator have no common factor.

Divide	Into	Get	Remainder
13	40	3	1
13	10	0	10
13	100	7	9
13	90	6	12
13	120	9	3
13	30	2	4
13	40	3	1

Table 5.2: Long division

Exercise 5.5.4. If the numerator and denominator have no common factor, what is their GCD?

The second point is that if n and d are positive integers with $n \geq d$, then

$$\frac{n}{d} = q + \frac{r}{d}\,, \tag{5.3}$$

where q is a positive integer and r is an integer between 0 and $d-1$. For instance, $\frac{19}{4} = 4 + \frac{3}{4}$.

Exercise 5.5.5. Explain why Equation (5.3) is just a restatement of Equation (5.1).

Fractional values can be effectively described by our positional base ten system described earlier. We represent a number by a sequence of digits, a decimal point, and a second sequence of digits. The number represented has as its integer portion the number represented by the first sequence of digits, using Equation (5.2). The fractional portion is represented by the sequence of digits to the right of the decimal point. Notice that this sequence may be infinitely long. If this sequence is $f_1 f_2 f_3 \cdots$, the fraction it represents is

$$f_1 \cdot \frac{1}{10} + f_2 \cdot \frac{1}{10^2} + f_3 \cdot \frac{1}{10^3} + \cdots\,. \tag{5.4}$$

In this format, rational numbers have a particularly simple representation. Rational numbers can always be represented as repeating or terminating decimals. Let's see how this works.

If we want to write 1/3 as a decimal, we would divide 3 into 1. Performing the long division gives $0.333\cdots$. At each stage of the division, we get a remainder of 1. When we "bring down" the 0, we are always dividing 10 by 3.

A more complicated example might by 4/13. The steps are in Table 5.2.

After the last step in Table 5.2, the process will repeat, and we will get $0.307692307692\cdots$.

A third example is 15/22. When the long division is performed, we get $15/22 = 0.61818\cdots$. Notice that the first digit does not repeat.

To save space, we will describe these *repeating* decimals with a bar over the repeating section. Thus $0.333\cdots = 0.\overline{3}$, $0.307692307692\cdots = 0.\overline{307692}$ and $0.61818\cdots = 0.6\overline{18}$.

Calculators are a poor tool to use when working with repeating decimals. Some repeating decimals don't look "repeating" on the calculator.

Exercise 5.5.6. Is 7/17 a rational number? Use your calculator to compute 7/17. Does it "look like" a rational number on your calculator? Explain.

Exercise 5.5.7. Convert to decimal: 7/17.

And some non-repeating decimals appear repeating.

Exercise 5.5.8. Use your calculator to compute

$$\sqrt{2} - \frac{1}{13861} - \frac{1}{297195528}\,.$$

Do you think this number is rational? (Remember that $\sqrt{2}$ is irrational.)

We have been discussing one kind of rational number: repeating decimals. Another kind of rational number "divides evenly." For example, $1/2 = 0.5$. These are called *terminating* decimals.

Exercise 5.5.9. Which of these rationals are repeating decimals and which are terminating: 2/5, 5/6, 4/15, 3/40? In general, which rationals are terminating and which are repeating?

Exercise 5.5.10. Why will every rational number be a repeating decimal or a terminating decimal? How long can the repeating sequence be for the fraction b/a, where b and $a \neq 0$ are integers?

The converse of the statement in Exercise 5.5.10 is also true: every repeating decimal or terminating decimal is a rational number. Here is an easy way to convert a repeating decimal to a rational. Let's demonstrate with $0.\overline{42}$

Let $x = 0.\overline{42}$. Then $100x = 42.\overline{42}$. Now subtract these two equations: $99x = 42$ or $x = 14/33$.

Exercise 5.5.11. Why did we multiply by 100 in this process?

Exercise 5.5.12. Convert to rationals: $0.\overline{4453}$, $13.\overline{221}$, $1.1\overline{12}$.

One way of seeing that every repeating decimal corresponds to a rational number is to use Equation (5.4). Again, using $0.\overline{42}$ to demonstrate, we know that $0.4242\cdots$ stands for

$$4\cdot\frac{1}{10} + 2\cdot\frac{1}{100} + 4\cdot\frac{1}{1000} + 2\cdot\frac{1}{10000} + \cdots\,.$$

This can be seen to be the sum of a geometric sequence, something we learned about in Chapter 1. The common ratio of the geometric sequence is less than one, so by the results of that earlier chapter, this "infinite" sum can be evaluated as a fraction.

Uniqueness is a thorny issue when dealing with representations of rational numbers. We have already seen that the fractional form p/q is not unique (remember $1/2 = 2/4$). The representation as repeating or terminating decimals also has its problems. For instance, is 2.4 terminating? Or is $2.4 = 2.4\overline{0}$ repeating? Even more problematic is the next exercise.

Exercise 5.5.13. What rational number does $0.\overline{9}$ represent?

Exercise 5.5.14. Find another decimal representation of $0.\overline{9}$. Find another decimal representation of $3.215\overline{9}$. Find another decimal representation of 190.

Exercise 5.5.15. Restate the following sentence so that it is true: every rational has a unique representation as a repeating or terminating decimal. Hint: Use Exercise 5.5.14 to explain what exception must be ruled out.

Exercise 5.5.16. Make a list of situations where the fraction form for rational numbers is "better," and make a list of situations where the repeating or terminating decimal form is "better." Explain what definition of "better" you are using.

We summarize our results regarding the representation of rational numbers as decimals as follows.

Theorem 11. *Every rational number has a unique representation as a terminating decimal or as a repeating decimal where the repeating section is not* $\overline{9}$.

We can write our rational numbers in other number bases, just as we wrote the integers in other bases. Instead of "decimal fractions," we have "basal fractions." Instead of a "decimal point," we use a "basal point." And just as with decimal fractions, rationals are repeating or terminating basal fractions.

For example, in binary, 0.1_{two} is one-half.

***Exercise 5.5.17.** Convert to base two, base five and base eight: 0.5, 0.2, 1/3.

***Exercise 5.5.18.** Convert to decimal fractions: 0.5_{eight}, 0.2_{three}.

***Exercise 5.5.19.** True or false (and give reasons): For each rational number, there is a number base such that the given rational number can be expressed as a terminating basal fraction in that base.

In a later chapter, we will discuss the next extension of our number system, the set of real numbers which includes irrational numbers. Irrational numbers are those whose decimal representations neither terminate nor repeat. An example is $1.6060060006\cdots$. Another is $\pi = 3.14159\cdots$.

5.6 Countability of the Rational Numbers

Everyone knows what we mean when we say a finite set has a certain number of elements. But what if the set is the set of integers? The set of integers has an infinite number of elements. Mathematicians have discovered how to compare "infinities."

Exercise 5.6.1. Make an argument that the set of even counting numbers is smaller than the set of all counting numbers. Now make an argument that the set of even counting numbers has the same size as the set of all counting numbers.

Mathematicians have resolved this paradox. Let's extend our notion of size in the following way. Two finite sets will have the same *size* if they have the same number of elements. An infinite set and a finite set never have the same size. And two infinite sets have the same size if we can establish a one-to-one correspondence between the elements of one and the elements of the other. Thus, for example, the set of positive integers and the set of all integers have the same size, because we can set up this one-to-one correspondence: $1 \to 0$, $2 \to 1$, $3 \to -1$, $4 \to 2$, $5 \to -2$, $6 \to 3, \ldots$. In general, for positive integer k, $2k \to k$ and $2k + 1 \to -k$.

Exercise 5.6.2. Show that the following sets have the same size as the positive integers: odd integers, multiples of 5, powers of 10.

Exercise 5.6.3. Suppose A, B and C are three infinite sets and A and B have the same size and B and C have the same size. Do A and C have the same size?

Exercise 5.6.2 demonstrates the fundamental paradox of sizes of infinite sets: a set can have the same size as one of its subsets! This is definitely not true of finite sets; in fact, a set is infinite if and only if it has the same size as one of its subsets!

Sets, like those in Exercise 5.6.2, which have the same size as the counting numbers, are called *countable*. To show that some infinite set is countable, one must make a sequence out of the elements of the set. For example, the positive multiples of three are countable because we can write them in a sequence: $\{3, 6, 9, 12, \ldots\}$. Also, all integers are countable, because we can write them in a sequence:

$$\{0, 1, -1, 2, -2, 3, -3, \ldots\}.$$

You've seen some examples of subsets of the integers which are countable. Now you will see that some important supersets of the integers are also countable.

Let's write the positive rational numbers in a table:

$$\begin{array}{ccccccc}
\frac{1}{1} & \frac{2}{1} & \frac{3}{1} & \frac{4}{1} & \frac{5}{1} & \frac{6}{1} & \cdots \\
\frac{1}{2} & \frac{2}{2} & \frac{3}{2} & \frac{4}{2} & \frac{5}{2} & \frac{6}{2} & \cdots \\
\frac{1}{3} & \frac{2}{3} & \frac{3}{3} & \frac{4}{3} & \frac{5}{3} & \frac{6}{3} & \cdots \\
\frac{1}{4} & \frac{2}{4} & \frac{3}{4} & \frac{4}{4} & \frac{5}{4} & \frac{6}{4} & \cdots \\
\vdots & & & & & &
\end{array}$$

Notice that numbers are repeated in this table. For example, $\frac{1}{2}$, $\frac{2}{4}$, $\frac{3}{6}$, etc. all appear.

Exercise 5.6.4. Use this table to show the positive rational numbers are countable. What did you do with the repeats, like $\frac{1}{2}$ and $\frac{2}{4}$? Does this imply that the rationals are countable? Why?

At this point you might be suspicious that **all** infinite sets are countable. We shall see in a later chapter that this is not true; in fact, there are infinitely many sizes of infinity!

Chapter 6

Modular Arithmetic

Cyclic behavior is a commonplace phenomenon. Examples can be time-related, such as days of the week, hours in a day and months of the year. Other examples include positions on a roulette wheel or points on a compass. In this chapter, we will place such behavior on a mathematical footing. We will describe the special arithmetic for such situations, called modular arithmetic, or sometimes "clock arithmetic."

6.1 Examples

We usually describe modular arithmetic or "clock arithmetic" in terms of calculating time. For instance, if it is 2:30 p.m. now, what time will it be in 40 hours? If today is Monday, what day of the week will it be in 30 days? If it is now 40 minutes past the hour, what time will it be in 45 minutes?

How might we calculate what day of the week it will be in 30 days? Thirty days consists of four weeks (of seven days each) and two extra days. So if today is Monday, in thirty days it will be Wednesday. One way to perform this calculation is to divide the 30 days by the seven days in a week. The result is the number of weeks, while the remainder is the number of extra days.

Exercise 6.1.1. If it is 2:30 p.m., what time will it be in 40 hours?

Exercise 6.1.2. If it is now 40 minutes past the hour, what time will it be in 45 minutes?

The idea of dividing and using the remainder will be a central theme in the following sections.

6.2 Rules of Modular Arithmetic

The exercises of the previous section illustrate several situations where different numbers are in some sense the same. This motivates a new kind of arithmetic where the addition, subtraction, multiplication and division is done on collections of numbers.

For example, if we add 5 hours to 6 o'clock, we get 11 o'clock, but if we add the same 5 hours to 10 o'clock, we get 15 o'clock, which is the same as 3 o'clock. Similarly, 14:00 on a University of Minnesota class schedule is the same as 2:00 on a bus schedule. We could even say that -3 o'clock is the same as 9 o'clock—after all, 9 o'clock is four hours earlier than 1 o'clock.

Notice that 10 o'clock, 22 o'clock, 34 o'clock, -2 o'clock and -14 o'clock all represent the same position on the clock. Notice also that they all differ by multiples of 12. For example, 22 and -2 differ by 24, which is twice 12. This discussion motivates the following idea.

We say that the integer a is *congruent* to the integer b mod n if $n|(b-a)$. The notation we shall use is $a \equiv b \mod n$. Sometimes we leave off the "mod n" if we know what n is. ("Mod" is short for *modulus.*) For example, $10 \equiv 22$ mod 12 because 12 divides $(22 - 10)$ and $22 \equiv -2 \mod 12$ because 12 divides $(-2 - 22)$.

Exercise 6.2.1. Verify that every two even numbers are congruent mod 2 and that every two positive numbers ending in 3 are congruent mod 10. Is 12 congruent to 20 mod 4? mod 5? Is 17 congruent to 32 mod 3? mod 4? mod 5?

Exercise 6.2.2. Prove that if $a \equiv b \mod n$, then $b \equiv a \mod n$.

Exercise 6.2.3. Prove that if $a \equiv b \mod n$ and $b \equiv c \mod n$, then $a \equiv c \mod n$.

Exercise 6.2.4. Prove that $a \equiv a \mod n$.

Exercises 6.2.2, 6.2.3 and 6.2.4 show that congruence mod n splits the integers up into n disjoint subsets, called *congruence classes.* Every number belongs to one of these classes. If two numbers are in one class, then each is congruent to the other in either direction. If two numbers are in different classes, they are not congruent to one another.

For example, for mod 12 (clock arithmetic), there are 12 congruence classes. One of the classes contains the integers -14, -2, 10, 22, and 34.

Exercise 6.2.5. Write down three other integers (besides those listed above) in the mod 12 congruence class containing 10.

Exercise 6.2.6. Write down two integers from each of the other eleven mod 12 congruence classes.

As another example, there are two mod 2 congruence classes: the even numbers and the odd numbers.

Exercise 6.2.7. Give three integers in each of the mod 3 congruence classes. Give two integers in each of the mod 6 congruence classes. Give one integer in each of the mod 10 congruence classes.

At this point, it is convenient to represent an entire mod n congruence class with a single symbol. Let's let $[k]_n$ represent the mod n congruence class containing k. For example, $[10]_{12} = \{\dots, -14, -2, 10, 22, 34, \dots\}$. When there is no confusion about the modulus, we will omit the subscript. In the example above, we would write [10]. Using this notation, we see that $[10] = [-2] = [34] = \cdots$. Thus, $[-2]$ and $[34]$ are alternate descriptions of the mod 12 congruence class [10]. The complete list of mod 12 congruence classes is [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11] and [12].

Exercise 6.2.8. Use this [ ]-notation to give another description of $[5]_{12}$.

Exercise 6.2.9. Use this notation to list the five mod 5 congruence classes. Also use it to list the two mod 2 congruence classes.

Exercise 6.2.10. Use this notation to give two descriptions of the mod 4 class containing 33. Of the mod 6 class containing 33. Of the mod 17 class containing 60. Of the mod 15 class containing 60.

Exercise 6.2.11. Is $[12]_{12} = [0]_{12}$? Is $[2]_2 = [0]_2$? Prove that $[n]_n = [0]_n$. (You will need to use the definition of congruence and congruence class in your proof.)

This notation for congruence classes is consistent with our original congruence notation. That is, $[A]_n = [B]_n$ if and only if $A \equiv B \mod n$, because both notations mean n divides the difference between A and B.

Mod n congruence classes let us "fold" all of the integers up into n symbols. In the clock example, the only numbers on the clock are $1, 2, \dots, 12$, which represent the twelve congruence classes described above.

Because we have so many ways of representing the same congruence class, it is useful to have a "standard" representation of the classes. Usually, but not always, we use $[0], [1], \dots, [n-1]$ for the mod n classes. It is especially easy to convert other forms of the class into this standard form, because of the Euclidean algorithm, which we studied in Chapter 5. We restate the key theorem here in a more general form.

Theorem 12. *If m is an integer and n is a positive integer, then there is a unique pair of integers, q and r, with $0 \le r < n$, which satisfy*

$$m = n \cdot q + r$$

or, equivalently,

$$m - r = n \cdot q\,.$$

Recall that q is the quotient when m is divided by n and r is the remainder.

For example, the standard representation of the mod 12 class [34] is [10], because if 34 is divided by 12, the remainder is 10. By Theorem 12, the difference between 34 and this remainder must be a multiple of 12.

Exercise 6.2.12. Find the standard representation for $[69]_{12}$. For $[18]_5$. For $[37]_7$. For $[14]_2$.

Theorem 12 is slightly more general than what was encountered in Chapter 5 because it allows m and q to be negative integers. Special care must be taken in applying Theorem 12 in this case. For instance, in the mod 12 world, if $m = -26$, by Theorem 12, $q = -3$ and $r = 10$, so $[-26] = [10]$. This is not computed by taking the remainder when 26 is divided by 12. (This is a mistake occasionally made by designers of computer compilers and software!) Here are two methods which work: add some multiple of 12 to -26, so that the number you get is positive, then divide by 12 and take the remainder; or take the remainder when 26 is divided by 12, but then subtract from 12 (unless the answer is 0, and then leave it alone).

Exercise 6.2.13. Find the standard representation for $[-61]_{12}$. For $[-20]_5$. For $[-10]_7$. For $[-11]_2$.

Now let's learn to do arithmetic using congruence classes instead of numbers. What enables us to do this are these two definitions:

$$[A]_n + [B]_n = [A + B]_n \,, \tag{6.1}$$

and

$$[A]_n \cdot [B]_n = [A \cdot B]_n \,. \tag{6.2}$$

What Equation (6.1) says is that if we add anything in the congruence class $[A]$ to anything in the congruence class $[B]$ we always get something in the congruence class $[A + B]$. For example, in mod 12, $[4] + [10] = [2]$ means that if we add anything in congruence class $[4]$ (say -8) to anything in congruence class $[10]$ (say 34), we get something (26) in congruence class $[2]$.

Equation (6.2) makes a similar statement about multiplication.

Addition, subtraction and multiplication are now easy: simply do usual arithmetic, and divide by the modulus and take remainders when convenient. For example, let's calculate $4 \cdot 9 + 10$ in mod 11. That is, let's find $[4 \cdot 9 + 10]_{11}$. First, take $4 \cdot 9 = 36 \equiv 3 \mod 11$. Then $3 + 10 = 13 \equiv 2 \mod 11$.

Or this can be done by doing all the arithmetic first, then dividing by 11 and taking the remainder: $4 \cdot 9 + 10 = 46 \equiv 2 \mod 11$. In either case, we get

$$4 \cdot 9 + 10 \equiv 2 \mod 11 \,,$$

or

$$[4 \cdot 9 + 10]_{11} = [2]_{11} \,.$$

As another example, in mod 2, this arithmetic translates as follows:

even plus odd is odd	$0 + 1 \equiv 1$	$[0] + [1] = [1]$,
even plus even is even	$0 + 0 \equiv 0$	$[0] + [0] = [0]$,
odd plus odd is even	$1 + 1 \equiv 0$	$[1] + [1] = [0]$,
even times even is even	$0 \cdot 0 \equiv 0$	$[0] \cdot [0] = [0]$,
even times odd is even	$0 \cdot 1 \equiv 0$	$[0] \cdot [1] = [0]$,
odd times odd is odd	$1 \cdot 1 \equiv 1$	$[1] \cdot [1] = [1]$.

Exercise 6.2.14. Find the standard class representative for these calculations:

$$7 + 9 \mod 12\,;$$

$$8 \cdot 9 \mod 11\,;$$

$$[3]_9 - [8]_9\,.$$

Exercise 6.2.15. Do the following subtractions:

$$9 - 13 \mod 6\,;$$

$$[-2]_4 - [-5]_4\,.$$

Exercise 6.2.15 shows that subtraction presents little difficulty in modular arithmetic. Division, however, is more problematic, as we shall see in the next section.

Notice that the question at the beginning of Section 6.1 can be answered quite neatly using modular arithmetic. If we number the days of the week, beginning with Sunday= 1, in 30 days it will be day $[30{+}2]_7 = [4]_7 =$Wednesday. Or even more simply, $[30]_7 = [2]_7$, so the day of the week has advanced by two days.

Exercise 6.2.16. The normal gestation period for an elephant is 22 months. If a female elephant is impregnated in November, in which month will she be due to deliver?

Exercise 6.2.17. A ship is heading 15° east of north. It turns port (left) 45° degrees. What is its new heading? (Do not use a negative number in your answer.)

Exercise 6.2.18. Some Roulette wheels have 38 "slots" on them, numbered 00, 0, then 1 through 36. The wheel is currently on the slot numbered 17. It is spun and moves 422 slots. Where is it now?

We can use modular arithmetic to calculate future days of the week in more complicated situations. For example, if today is Wednesday, June 30, 1999, what day will Christmas fall on in the year 2005? Each 365 day year will advance the day by one (since $[365]_7 = [1]_7$). Each leap year will advance the day by two. Between Christmas, 1999, and Christmas, 2005, there are two leap years and four non-leap years, so the day will advance by $[2 \cdot 2 + 4 \cdot 1]_7 = [1]_7$. What is left is to count days between June 30, 1999, and Christmas, 1999. Each 30-day month will advance the day by two days and each 31-day month will advance the day by three days. Between June 30 and November 30 there are three 31-day months and two 30-day months, thus advancing the day by $[3 \cdot 3 + 2 \cdot 2]_7 = [6]_7$. Finally, there are 25 days between November 30 and Christmas, advancing the day by $[25]_7 = [4]_7$. The final calculation is then $[6 + 4 + 1]_7 = [4]_7$, so that Christmas, 2005 falls on a Sunday.

Exercise 6.2.19. On what day of the week will July 4, 2006 fall?

Sometimes we can decide if solutions to integer equations exist by "reducing mod n". For example, the equation $6x + 9y = 5$ does not have a solution in integers, because if we reduce mod 3, we get $6x + 9y \equiv 5 \mod 3$, which is the same as $0 \equiv 2 \mod 3$.

Exercise 6.2.20. A weather forecaster has determined that there are two major cyclical temperature variations. One has a cycle of every 14 years, the other has a cycle of every 8 years. This year is the peak of the first cycle; next year is the peak of the second cycle. Will the two cycles ever peak in the same year? Explain.

6.3 Solving Equations

Recall that a linear equation, like $2x - 5 = 0$, has a single solution in our ordinary number system. Recall also, that two equations and two unknowns could have no solution, a unique single solution, or an infinite set of solutions. Also recall that a quadratic equation, like $x^2 - 3x + 2 = 0$, could have two solutions, one solution, or no solutions. We will discover similar behavior in modular arithmetic when we try to solve equations.

Exercise 6.3.1. Solve by trial and error: $[5]_6x+[2]_6 = [3]_6$. That is, determine all mod 6 congruence classes x which satisfy that equation by testing each one. In a similar way, solve $[3]_6x + [2]_6 = [5]_6$.

The strange outcome in the second part of Exercise 6.3.1 has to do with multiplicative inverses (the M-5 Axiom in our list in Chapter 5).

Let's look at another example: $3x + 8 = 4$. We will first solve this in the rational number system, then we will try to solve it in two different modular number systems.

First, let's carefully describe what we do when we solve $3x + 8 = 4$ in the rational number system.

Add the additive inverse of 8 to both sides:

$$3x + 8 - 8 = 3x = 4 - 8 = -4\,.$$

Multiply by the multiplicative inverse of 3 on both sides:

$$3^{-1} \cdot 3x = x = 3^{-1} \cdot (-4) = -4/3\,.$$

Now let's do the whole thing mod 11. That is, let's solve

$$[3]_{11}x + [8]_{11} = [4]_{11}\,.$$

Add the additive inverse of [8] (which is [3] because [8] + [3] = [0]) to both sides:

$$[3]x + [8] + [3] = [3]x = [4] + [3] = [7]\,.$$

Now comes the hard step: find the multiplicative inverse of [3] (it's not 1/3!). We can actually use the Euclidean algorithm to find it; more on that later. For now, we just systematically search. It is [4] (because $[4][3] = [12] = [1]$—remember that the inverse is that number you have to multiply by to get [1]).

So multiply both sides by [4]:

$$[4][3]x = x = [4][7] = [28] = [6]\,.$$

But what happens if we do the whole thing mod 9? Changing the modulus changes the entire problem! Add the additive inverse of [8] (which is now [1]) to both sides to get $[3]x = [5]$. But $[3]_9$ has no multiplicative inverse—we shall see why later. So we cannot solve this equation by multiplying by the multiplicative inverse of [3]. In fact, a systematic search shows that $[3]_9x + [8]_9 = [4]_9$ has no solution!

Exercise 6.3.2. What happens if the original equation is $[3]_9x + [8]_9 = [2]_9$? Be careful!

The previous exercises illustrate the necessity of finding multiplicative inverses in solving linear equations. Let's determine under what circumstances we can find such inverses.

Exercise 6.3.3. For each mod 3 congruence class, either find its multiplicative inverse, or determine that none exists. Repeat this for mod 4, mod 5, and mod 6. Make a conjecture about when congruence classes have multiplicative inverses in a given modular arithmetic.

Exercise 6.3.4. Suppose $0 < k < n$ and the GCD of k and n is not 1. Show that $[k]_n$ cannot have a multiplicative inverse.

Exercise 6.3.4 shows that if the GCD of a number with the modulus is not 1, then its congruence class cannot have a multiplicative inverse. But the following is also true: If the GCD is 1, then its congruence class does have a multiplicative inverse. In fact, we will learn how to construct the multiplicative inverse!

The construction is based on the Euclidean algorithm. To begin, let's use the example above, where we needed to find the multiplicative inverse of $[3]_{11}$. We can easily see that $\mathrm{GCD}(3, 11) = 1$, but let's go through the Euclidean algorithm:

$$\mathrm{GCD}(3, 11) = \mathrm{GCD}(2, 3) = \mathrm{GCD}(1, 2) = 1\,.$$

The first step comes from dividing 3 into 11 and taking the remainder of 2. Hence, $2 = 11 - 3 \cdot 3$.

The second step comes from dividing 2 into 3 and taking the remainder of 1, from which we obtain $1 = 3 - 1 \cdot 2$.

We can now reverse these steps to write the GCD of 3 and 11 as a multiple of 3 added to a multiple of 11. Here is how. Start with the GCD obtained in the last step, 1. Notice that in this last step, we had

$$1 = 3 - 1 \cdot 2\,, \tag{6.3}$$

that is, 1 was 1 times 3 plus -1 times 2. But in the next-to-last step, 2 was 1 times 11 plus -3 times 3. By inserting this in for the 2 in Equation 6.3, we get

$$\begin{aligned} 1 &= 3 - 1 \cdot 2 \\ &= 3 - 1 \cdot (11 - 3 \cdot 3) \\ &= 4 \cdot 3 - 1 \cdot 11\,. \end{aligned}$$

This last step comes from combining the multiples of 3. Now we have written the GCD as a multiple of 3 added to a multiple of 11. When we reduce this equation mod 11, the multiple of 11 disappears (since $[11]_{11} = [0]_{11}$), leaving $[1] = [4][3]$. This means that the mod 11 congruence classes [4] and [3] are multiplicative inverses of one another.

Let's do the harder problem of finding the multiplicative inverse of $[33]_{97}$. First trace through the Euclidean algorithm:

$$\mathrm{GCD}(33, 97) = \mathrm{GCD}(31, 33) = \mathrm{GCD}(2, 31) = \mathrm{GCD}(1, 2) = 1\,.$$

That is,

$$\begin{aligned} 31 &= 97 - 2 \cdot 33\,; \\ 2 &= 33 - 1 \cdot 31\,; \text{ and} \\ 1 &= 31 - 15 \cdot 2\,. \end{aligned}$$

Then work backwards. The final 1 is a multiple of 31 added to a multiple of 2. The 2 is a multiple of 33 added to a multiple of 31, so by putting these together, we find that 1 is a multiple of 31 added to a multiple of 33. But 31 is a multiple of 97 added to a multiple of 33, so finally, 1 is a multiple of 97 added to a multiple of 33. Here is the exact calculation.

$$\begin{aligned} 1 &= 31 - 15 \cdot 2 && \text{the last step above} \\ &= 31 - 15 \cdot (33 - 1 \cdot 31) && \text{replacing the 2} \\ &= 16 \cdot 31 - 15 \cdot 33 && \text{combining factors of 31} \\ &= 16 \cdot (97 - 2 \cdot 33) - 15 \cdot 33 && \text{replacing the 31} \\ &= 16 \cdot 97 - 47 \cdot 33 && \text{combining factors of 33}\,. \end{aligned}$$

Therefore,

$$\begin{aligned} [1] &= [-47][33] \\ &= [50][33]\,. \end{aligned}$$

Thus, $[33]_{97}$ and $[50]_{97}$ are multiplicative inverses of each other.

Exercise 6.3.5. Check directly that $[33]_{97}$ and $[50]_{97}$ are multiplicative inverses of each other. Also check directly that $[33]_{97}$ and $[-47]_{97}$ are multiplicative inverses of each other.

Exercise 6.3.6. Find a multiplicative inverse of $[17]_{23}$. Also find a multiplicative inverse of $[16]_{25}$.

The method above describes how to write $\mathrm{GCD}(m,n)$ as $ma+nb$ where a and b are integers. For example,

$$\mathrm{GCD}(27,120)=\mathrm{GCD}(12,27)=\mathrm{GCD}(3,12)=3\,,$$

according to the Euclidean algorithm. Working backwards as above,

$$\begin{aligned}3&=27-2\cdot 12\\&=27-2\cdot(120-4\cdot 27)\\&=27-2\cdot 120+8\cdot 27\\&=9\cdot 27+(-2)\cdot 120\,.\end{aligned}$$

Exercise 6.3.7. What is $\mathrm{GCD}(18,30)$? Write it as $18a+30b$.

Exercise 6.3.8. You have an unlimited supply of water, a drain, a large container, and two jugs which contain 18 cups and 30 cups respectively. Explain how you can use the jugs to put 6 cups of water into the container.

Exercise 6.3.9. You have an unlimited supply of water, a drain, a large container, and two jugs which contain 7 cups and 9 cups respectively. Explain how you can use the jugs to put one cup of water into the container.

Exercise 6.3.10. Find the solution set of the equation

$$[8]_{11}x+[9]_{11}=[6]_{11}\,.$$

Exercise 6.3.11. Find the solution set of the equation

$$[8]_{9}x+[4]_{9}=[6]_{9}\,.$$

Exercise 6.3.12. Finish this statement and explain why it is true: Every mod n congruence class, except the class $[0]$, has a multiplicative inverse if and only if . . . .

So far in this section, we have been using the congruence class notation $[k]$ to describe equations. However, we can also use the congruence notation. For instance, the following calculation describes how to solve $[2]_5x+[1]_5=[4]_5$:

$$\begin{aligned}[2]_5x+[1]_5&=[4]_5\\ [2]_5x&=[3]_5\\ [3]_5[2]_5x&=[3]_5[3]_5\\ [6]_5x&=[9]_5\\ x&=[4]_5\,.\end{aligned}$$

Using congruence notation, this becomes

$$\begin{aligned} 2x+1 &\equiv 4 \mod 5 \\ 2x &\equiv 3 \mod 5 \\ 3\cdot 2x &\equiv 3\cdot 3 \mod 5 \\ 6x &\equiv 9 \mod 5 \\ x &\equiv 4 \mod 5\,. \end{aligned}$$

Notice that our answer in the first case was $x = [4]_5$, which expresses x as a unique congruence class. In the second case, our answer was $x \equiv 4 \mod 5$, which expresses x as the infinite collection of numbers making up the congruence class $[4]_5$. Is the correct answer a single object (the congruence class) or many objects (the members of the class)? We will take the view that the answer is a single object. The notation $[k]_n$ emphasizes this fact. When we use the congruence notation $\equiv$, we will keep in mind that while $x \equiv 4 \mod 5$ means that x could be 4 or 9 or 14, etc., we will regard x as a single entity, the entire class $[4]_5$. From this point of view, the solution set of the equation $2x + 1 \equiv 2 \mod 5$ has one member, which has infinitely many names: 3, -2, 8, -7, and so forth.

Exercise 6.3.13. Find the solution set of the equation

$$2x+5 \equiv 1 \mod 7\,.$$

Exercise 6.3.14. Find the solution set of the equation

$$5x+4 \equiv 3 \mod 8\,.$$

Now let's try to solve some systems of equations. Remember that "solve" means to find the solution set, which may be empty. Also, since we have only a finite number of congruence classes, we cannot have an infinite number of solutions. For example, the equation $2x + y \equiv 1 \mod 3$ has only three pairs of congruence classes as solutions:

$$\begin{aligned} x = [0] \text{ and } y = [1]\,, \\ x = [1] \text{ and } y = [2]\,, \\ x = [2] \text{ and } y = [0]\,. \end{aligned}$$

Exercise 6.3.15. Solve the system of equations

$$\begin{aligned} x + [2]_7 y &= [4]_7\,, \\ [4]_7 x + [3]_7 y &= [4]_7\,. \end{aligned}$$

Exercise 6.3.16. Solve the system of equations

$$\begin{aligned} x + y &\equiv 3 \mod 11\,, \\ 3x + 5y &\equiv 1 \mod 11\,. \end{aligned}$$

Exercise 6.3.17. Solve the system of equations

$$\begin{aligned} x - y &\equiv 4 \mod 5\,, \\ -2x + y &\equiv -3 \mod 5\,. \end{aligned}$$

Exercise 6.3.18. Solve the system of equations

$$\begin{aligned} x + y &\equiv 1 \mod 2\,, \\ x + z &\equiv 0 \mod 2\,, \\ x + y + z &\equiv 0 \mod 2\,. \end{aligned}$$

Exercise 6.3.19. Solve the system of equations

$$\begin{aligned} x + 2y &\equiv 4 \mod 5\,, \\ 4x + 3y &\equiv 4 \mod 5\,. \end{aligned}$$

Exercise 6.3.20. Solve the system of equations

$$\begin{aligned} [2]_5 x + [3]_5 y &= [1]_5\,, \\ [4]_5 x + y &= [3]_5\,. \end{aligned}$$

Exercise 6.3.21. Solve the system of equations

$$\begin{aligned} 6x + y &\equiv 2 \mod 7\,, \\ 2x - 2y &\equiv 3 \mod 7\,. \end{aligned}$$

Next, let's try some quadratic equations. We can solve quadratic equations in one of four ways. First, we can adapt the quadratic formula from high school algebra. Remember that this formula was derived by completing the squares, so a second method is to complete the square. Third, we could find a factorization into linear factors. These three methods are the three methods we usually employ when working with quadratics in our usual algebra system. The fourth method is special to modular arithmetic: simply try all possible answers. This method is feasible because in modular arithmetic there are only a finite number of possible answers.

Here is an example. We sketch all four methods on this example. Suppose

$$x^2 + x + 3 \equiv 0 \mod 5\,. \tag{6.4}$$

To use the quadratic formula, we must evaluate

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

in mod 5. Since $2a$ is 2, we note that division by 2 in mod 5 is the same as multiplication by 3 (3 is the multiplicative inverse of 2 in mod 5). So replacing the division by 2 and substituting for a, b and c from Equation (6.4), we have

$$\begin{aligned} 3(-1 \pm \sqrt{1-12}) &\equiv 3(-1 \pm \sqrt{4}) \mod 5 \\ &\equiv 3(-1 \pm 2) \mod 5 \\ &\equiv 3, 1 \mod 5\,, \end{aligned}$$

because $-11 \equiv 4 \mod 5$ and 4 has exactly two square roots (2 and -2) in mod 5.

To complete the square, we note that half the coefficient of x (in mod 5, of course) is 3 and 3^2 is 4 in mod 5, so we need to make the constant term 4. We do this by adding 1 to both sides of Equation (6.4):

$$\begin{aligned} x^2 + x + 3 &\equiv 0 \mod 5 \\ x^2 + x + 4 &\equiv 1 \mod 5 \\ (x+3)^2 &\equiv 1 \mod 5 \\ x + 3 &\equiv 1, 4 \mod 5 \\ x &\equiv 3, 1 \mod 5\,. \end{aligned}$$

To factor, try factors whose product is 3. We immediately get

$$x^2 + x + 3 \equiv (x-1)(x-3) \mod 5\,.$$

Finally, if we plug in 0 or 4 into Equation (6.4), we get 3; if we plug in 2, we get 4; and if we plug in 1 or 3, we get 0.

Exercise 6.3.22. Solve $x^2 + [3]_{11}x + [4]_{11} = [0]_{11}$.

Exercise 6.3.23. Solve $x^2 + x + 3 \equiv 0 \mod 7$.

Exercise 6.3.24. Solve $x^2 + x + 1 \equiv 0 \mod 3$.

We can describe a Cartesian coordinate system for congruence classes. Points in the system correspond to pairs (x, y) where x and y are congruence classes. Lines are described by equations of the form

$$Ax + By = C\,,$$

where A, B and C are constant congruence classes, and A and B are not both $[0]$.

We could even "graph" points and lines by displaying the standard form for the equivalence class on a Cartesian coordinate system.

Thus, for example, in mod 2, there are four points: $([0], [0])$, $([0], [1])$, $([1], [0])$, and $([1], [1])$. We could display these as the four points in usual coordinates: $(0, 0)$, $(0, 1)$, $(1, 0)$, and $(1, 1)$.

The line $x + y = [1]$ consists of these two points: $([0], [1])$ and $([1], [0])$. There are five other lines. These are $x + y = [0]$, $y = [1]$, $y = [0]$, $x = [1]$, and $x = [0]$.

The point $([0], [1])$ lies on three of these lines: $x + y = [1]$, $x = [0]$, and $y = [1]$.

Exercise 6.3.25. How many "points" are there in the mod 3 Cartesian coordinate system? How many "lines?" How many "points" on a "line?" How many "lines" pass through a given "point?"

Exercise 6.3.26. How many "points" are there in the mod 5 Cartesian coordinate system? How many "lines?" How many "points" on a "line?" How many "lines" pass through a given "point?"

Exercise 6.3.27. Suppose p is a prime number. How many "points" are there in the mod p Cartesian coordinate system? How many "lines?" How many "points" on a "line?" How many "lines" pass through a given "point?"

Exercise 6.3.28. What points are on the mod 3 "circle" $x^2 + y^2 \equiv 1 \mod 3$?

6.4 Divisibility Tests

Recall from Chapter 5 that each non-negative integer N written

$$d_n d_{n-1} d_{n-2} \cdots d_2 d_1 d_0$$

means

$$N = d_n 10^n + d_{n-1} 10^{n-1} + d_{n-2} 10^{n-2} + \cdots + d_2 10^2 + d_1 10 + d_0\,. \qquad (6.5)$$

The following exercises can be done by reducing Equation (6.5) mod n for some particular n. For example, if Equation (6.5) is reduced mod 2, then the left hand side is N mod 2 and the right hand side is d_0 mod 2, since $10 \equiv 0$ mod 2. Therefore, a number is even if and only if its last digit is even.

Exercise 6.4.1. Find a divisibility test for divisibility 5 and prove that it works.

For divisibility by 3, we reduce Equation (6.5) mod 3. Since $10 \equiv 1 \mod 3$, we must have $10^k \equiv 1 \mod 3$ for every $k \geq 1$. Therefore, Equation (6.5) becomes

$$N \equiv d_n + d_{n-1} + \cdots + d_1 + d_0 \mod 3\,.$$

Therefore, N is divisible by 3 if and only if the sum of its digits is divisible by 3.

Exercise 6.4.2. Show that a number is divisible by 9 if and only if the sum of its digits is divisible by 9.

Exercise 6.4.3. Find similar divisibility tests for divisibility by 4, 6, 8 and 10. (Hints: for 4, look at the rightmost two digits; for 8, look at the rightmost 3 digits; 10 is similar to 2 and 5; and $6 = 2 \cdot 3$.)

Exercise 6.4.4. Show that a number is divisible by 11 if and only if the alternating sum of its digits is divisible by 11. (Alternating sum means add the first digit, subtract the second, add the third, subtract the fourth, etc.)

Exercise 6.4.5. Why do perfect squares always end in 0, 1, 4, 5, 6 or 9 in our number system?

The divisibility test for 9 leads to an old-fashioned "check" of arithmetic called "casting out nines." Suppose we add 44752833 to 95501042 and get 140253875. We can check our arithmetic by adding digits and wiping out 9's wherever we find them. For example, in 44752833, we eliminate a 4 and the 5 $(4+5=9)$ and the 7 and 2 $(7+2=9)$, leaving $4+8+3+3=18$. Now kill the 18 $(1+8=9)$, leaving 0. In 95501042, we wipe out 9, 5 and 4, leaving $5+1+2=8$. Then $0+8=8$. Finally, do the same to the answer: 140253875. Get rid of 4 and 5, 8 and 1 and 7 and 2, leaving $3+5=8$. Thus, the answer checks (which does not guarantee that the answer is correct, however).

The same technique works for multiplication, subtraction and division.

Exercise 6.4.6. Explain why casting out 9's works.

Exercise 6.4.7. What kind of errors will casting out 9's not find? Discuss.

Exercise 6.4.8. Explain "casting out 11's", based on Exercise 6.4.4. What kind of errors will casting out 11's not find? Will it find the errors not found by casting out 9's?

Exercise 6.4.9. Summing digits is a technique used in bar codes. The digit sum, called a checksum, is the last number encoded in the bar code. The bar code reader reads the numbers, then the checksum, then checks to see they correspond. For example, the Postal Service uses the sum of digits mod 9. U.P.S. and Federal Express use the sum of digits mod 7. Comment on the ability of these two schemes to detect (a) single digit errors and (b) transposition errors (adjacent numbers swapped).

Other number bases have their own collections of divisibility tests.

Exercise 6.4.10. Find tests for divisibility by 4 in base eight, by 5 in base four, by F in base sixteen.

***Exercise 6.4.11.** Show the following: a number written in base b is divisible by $b-1$ if and only if the sum of its digits is divisible by $b-1$.

***Exercise 6.4.12.** Show the following: A number written in base b is divisible by $b+1$ if and only if the alternating sum of its digits is divisible by $b+1$.

***Exercise 6.4.13.** Complete the following: Suppose $d|b$. A number written in base b is divisible by d if and only if ....

***Exercise 6.4.14.** Explain "casting out $b-1$'s" in base b arithmetic.

6.5 Nim

Number bases and modular arithmetic can be used in mathematical games. A famous example is the game of nim. In this game, between two players, a collection of sticks is placed in several rows. Each row may have many or few sticks in it. The players alternate turns. Each in her turn picks up one or more sticks from one row only. The person who picks up the last stick wins.

For example, suppose the sticks are arranged in rows with 5, 8, 8, 2, and 10 sticks, as in Figure 6.1.

```
|||||
||||||||
||||||||
||
||||||||||
```

Figure 6.1: Nim Game

The first player picks up all 10 from the last row. The second picks up 5 from the second row; the first picks up 6 from the third row; and the second picks up all 5 in the first row. The remaining three rows are shown in Figure 6.2.

```
|||
||
||
```

Figure 6.2: Continuation of Nim Game

The first player picks up all three in the first row. The second player chooses one from the second row; the first chooses one from the third row. The configuration is now shown in Figure 6.3.

```
|
|
```

Figure 6.3: Continuation of Nim Game

The second player must play, so the first player will win.

For "most" starting positions, the first player always has a winning strategy. Write the number of sticks in a row in binary notation. In our example, the rows have 101_{two}, 1000_{two}, 1000_{two}, 10_{two}, and 1010_{two} sticks, respectively. We now treat each binary digit as a mod 2 congruence class. Let's write the five binary numbers down, lining up the columns, and writing the digits as congruence classes,

$$\begin{array}{cccc} [0] & [1] & [0] & [1] \\ [1] & [0] & [0] & [0] \\ [1] & [0] & [0] & [0] \\ [0] & [0] & [1] & [0] \\ [1] & [0] & [1] & [0] . \end{array}$$

Next, find the sum of each column of congruence classes. We get

$$[1] \quad [1] \quad [0] \quad [1] .$$

If all the sums are [0], we will call the configuration *even*; if at least one of the sums is [1], we call it *odd*. This configuration is odd, since three of the sums are [1].

Exercise 6.5.1. Prove that no matter how the sticks are removed, every even configuration becomes odd.

Exercise 6.5.2. Prove that by an appropriate choice of sticks to remove from one row, every odd configuration can be made even. What choice works in the above game? (Hint: Find the leftmost [1] in the sum. Find a row of sticks for which there is a [1] in the same column. Now how would you compute the number of sticks to remove from that row in order to make the configuration even?)

Exercise 6.5.3. Assume the first player begins with an odd configuration. Describe a winning strategy for that player. What should the strategy of the first player be if the original configuration were even?

Exercise 6.5.4. How many sticks should the first player remove, and from which row, in the game given in Figure 6.4?

```
| | | | | |
| | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | |
```

Figure 6.4: Another Nim Game

Exercise 6.5.5. How many sticks should the first player remove, and from which row, in the game given in Figure 6.5?

```
| | | |
| | | |
| |
| | | | | | | | | |
| | | | | | | | |
```

Figure 6.5: Yet Another Nim Game

```
| | | | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | |
| | | | |
| | | | | | | | | |
| | | |
```

Figure 6.6: Still Another Nim Game

Exercise 6.5.6. How many sticks should the first player remove, and from which row, in the game given in Figure 6.6?

***Exercise 6.5.7.** Analyze the game if the last player to pick up a stick **loses**.

Chapter 7

Probability and Statistics, I

In this chapter we begin a study of two interrelated topics, probability and statistics. We use probability to determine the likelihood of various results based on some predetermined model. In statistics, we turn things around: we construct a model to describe events based on the results of experiments.

In this chapter we will construct probability models to describe uncertainty. We will begin with an important probability model: all possible outcomes are equally likely. This is called the equiprobable model. Another important model is the binomial model, when an experiment is repeated independently several times.

Then we will turn our attention to the topic of statistics. In particular, we will learn how to display data, or collections of numbers and information.

We will conclude the chapter with a discussion of conditional probabilities.

A solid understanding of counting techniques is essential to an understanding of probability. Therefore, it might be useful to review Chapter 2 at this time.

7.1 The Equiprobable Model

In the world of probability, sets are called *events*, elements of a set are called *sample points*, and the universal set is called the *sample space*. A *probability* is a number which is assigned to each sample point such that: (1) this number is always between 0 and 1; and (2) the sum of these numbers over all sample points is 1. These two properties are very important. Notice that no probability is ever larger than 1 nor is negative.

In more mathematical language, a *probability function* is a function from the sample space to the real interval $[0, 1]$ having the property that the sum of its values equals 1. The value it assigns to a particular sample point is the *probability* of that sample point. More generally, the *probability of an event* in the sample space is the sum of the probabilities of the sample points in the event. In particular, the event consisting of all sample points (that is, the sample space itself) has probability 1.

(1,1)	(1,2)	(1,3)	(1,4)	(1,5)	(1,6)
(2,1)	(2,2)	(2,3)	(2,4)	(2,5)	(2,6)
(3,1)	(3,2)	(3,3)	(3,4)	(3,5)	(3,6)
(4,1)	(4,2)	(4,3)	(4,4)	(4,5)	(4,6)
(5,1)	(5,2)	(5,3)	(5,4)	(5,5)	(5,6)
(6,1)	(6,2)	(6,3)	(6,4)	(6,5)	(6,6)

Table 7.1: Pair of dice outcomes

For example, if we toss a coin twice, our sample space has four sample points: **HH**, **HT**, **TH** and **TT** (For example, **HT** represents the possible outcome of heads on the first toss and tails on the second toss.) If we assume that each of these sample points is equally likely, we would assign each of them the probability $\frac{1}{4}$. Note that $\frac{1}{4}+\frac{1}{4}+\frac{1}{4}+\frac{1}{4}=1$. A typical event might be "at least one heads." We could write this event as

$$E = \{\mathbf{HH}, \mathbf{HT}, \mathbf{TH}\}.$$

Since E has three sample points in it and each of those has probability $\frac{1}{4}$, E has probability $\frac{3}{4}$.

The notation we usually use for a probability function is P. In the previous example, then, $P(\mathbf{HH}) = \frac{1}{4}$. We also use P for the probability of the various events. Again, from the previous example, $P(E) = \frac{3}{4}$.

Sometimes the assignment of probabilities to sample points can be derived from the physical setup. Examples are fair dice (each side of each six-sided die is equally likely to appear face-up), fair coins (as above, each side of each coin is equally likely), card decks (every possible order of cards is equally likely), etc. In many important examples, each sample point has the same probability, so if there are t sample points, each would have probability $1/t$. In this case, called the *equiprobable model*, an event with s sample points would have probability s/t. In effect, the equiprobable model reduces probability questions to counting questions.

The equiprobable model was used in the coin toss above. As another example, suppose we toss a pair of fair dice. The numbers from one to six are equally likely on each of the two dice. So the sample space for the equiprobable model has the sample points described in Table 7.1.

Exercise 7.1.1. Use Table 7.1 to write down the event which is described by "rolling a seven." The event "rolling doubles." The event "rolling eleven."

Exercise 7.1.2. Using the equiprobable model, compute the probabilities of the events in Exercise 7.1.1.

Exercise 7.1.3. A fair coin is tossed three times. Write down a sample space with each sample point equally likely, which describes all the possible outcomes. What is the probability that tails appears exactly twice? At least twice?

Exercise 7.1.4. Explain this sentence: "If E and F are disjoint events, then the probability of E or F occurring is the probability of E plus the probability of F." What sentence replaces this one if we omit the word "disjoint?" What aspects of Chapter 2 (Counting) are closely related to your answers to this problem?

Exercise 7.1.5. What is the probability of the empty set? The entire sample space? If the probability of E is p, what is the probability of E^c, the complement of E?

Here is another example of how probabilities can be computed from counting results. Suppose a box contains 15 golf balls and suppose 5 of these are painted red, while the remaining are white. Six of the balls are selected at random (leaving nine in the box). Let's determine the probability that exactly three of the six are painted red. First, we determine the sample space. The sample space consists of all the ways of choosing six balls out of the 15. The number of sample points in the sample space is then $\binom{15}{6}$. Each sample point is equally likely, so we use the equiprobable model.

The event in question is all the sample points consisting of a selection of six balls, three of which are painted red. The number of sample points in this event is $\binom{5}{3}\binom{10}{3}$. The first factor counts the number of ways of picking three red balls, and the second counts the number of ways of picking three white balls. The multiplication principle then requires us to take the product. Therefore the probability of our event is

$$\frac{\binom{5}{3}\binom{10}{3}}{\binom{15}{6}} = \frac{240}{1001}\,.$$

Exercise 7.1.6. Calculate the probability that exactly two of the six balls are red. Calculate the probability that none of the six balls is red.

Exercise 7.1.7. Use Exercise 7.1.5 to compute the probability that at least one of the six balls is red.

For the next two exercises, suppose that six of the fifteen balls are painted red and that four are painted green. The remaining five are white. Again, a sample of six balls is drawn.

Exercise 7.1.8. Compute the probability that exactly two are red, two are white and two are green.

Exercise 7.1.9. Compute the probability that exactly two are green and at least one is red.

In the following exercises, use the equiprobable model and counting techniques from Chapter 2 to compute the probabilities in question.

Exercise 7.1.10. Calculate the probability of being dealt the various poker hands described in Chapter 2. (Use the numbers of each kind of hand computed in that chapter. Recall that a poker hand consists of five cards from a standard deck of 52 cards.)

Exercise 7.1.11. Calculate the probability of being dealt a "perfect hand" in bridge. (Recall that a perfect hand consists of 13 cards all in one suit.)

Exercise 7.1.12. Six married couples are standing in a room. The twelve people are divided, at random, into six pairs. Find the probability that each pair is a married couple. That each pair contains a male and a female.

Exercise 7.1.13. Suppose that in a certain northern Minnesota lake, there are N walleyes. Suppose that 100 of these have been marked. What is the probability that in a sample of 200 walleyes there are exactly 5 which are marked? (Your answer should be a formula with N in it.)

***Exercise 7.1.14.** Find the number of fish N for which the probability in Exercise 7.1.13 is largest. Hint: let $\{p_N\}$ denote the sequence of probabilities computed in Exercise 7.1.13. That is, p_N is the answer you got in Exercise 7.1.13. Now compute the ratio of p_N to p_{N-1}. Show that this ratio is > 1 if N is smaller than a certain number and it is < 1 if N is larger than that number. Conclude that p_N is largest when N is that certain number. In your evaluation of the ratio of p_N to p_{N-1}, many of the factorials will cancel or partially cancel.

Exercise 7.1.15. Nine students are to be divided at random into three groups of three students. One group will work on Chapter 2, one will work on Chapter 3 and one on Chapter 4. What is the probability that Joe and Robert are in the Chapter 4 group? What is the probability that Joe and Robert are in the same group?

Exercise 7.1.16. Nine students are to be divided at random into three indistinguishable groups of three students. What is the probability that Joe and Robert are in the same group?

7.2 The General Model

When the equiprobable model does not apply, probability calculations are usually harder. For instance, in the dice model described in the previous section, we could have let each sample point represent the sum of the values on the dice. Then there would be only 11 sample points, labeled by the values 2 to 12. Since these sample points would not be equally likely, calculating probabilities of events would be more difficult. We avoided those difficulties by setting up a sample space where every sample point was equally likely.

Sometimes, however, we cannot avoid unequal probabilities. Suppose a pair of dice is tossed where each die is "loaded" so that the probability of each face is proportional to the number of dots on that face. We are going to compute several probabilities with these loaded dice.

Let's start by computing the probability of each face on a single die. Say p is the probability of the face with one dot.

Exercise 7.2.1. What (in terms of p) is the probability of the face with two dots? The face with six dots?

Exercise 7.2.2. Use Exercise 7.2.1 and the fact that the sum of the probabilities of the six faces must be 1 to compute p.

Exercise 7.2.3. Now suppose this loaded pair of dice is tossed. What is the probability that the first face has four dots and the second face has three dots?

Exercise 7.2.4. For this loaded pair of dice, find the probability of rolling seven. Of rolling doubles. Of rolling eleven. Of rolling an even number.

Exercise 7.2.5. A coin is weighted so that heads is twice as likely to appear as tails. This coin is tossed three times. What is the probability that tails appears exactly twice? At least twice?

Exercise 7.2.6. Show that Exercise 7.1.5 remains valid even if the equiprobable condition is not applicable.

Exercise 7.2.7. Prove the following formula:

If E and F are two events, then

$$P(E \cup F) = P(E) + P(F) - P(E \cap F)\,. \tag{7.1}$$

Also prove:

If E and F are disjoint events, then

$$P(E \cup F) = P(E) + P(F)\,. \tag{7.2}$$

That is, Exercise 7.1.4 remains valid even if the equiprobable condition does not hold.

Exercise 7.2.8. In the dice experiment described in Exercise 7.2.4, what is the probability that at least one die is a three? Use this exercise to illustrate Equation (7.1).

7.3 Independent Events and the Binomial Model

Two events are *independent* if the probability of one is not affected by the occurrence of the other. For instance, suppose a pair of fair dice are tossed twice. The event of rolling seven on one toss is not affected by rolling a seven on the other toss.

This informal definition of independence can be made mathematically precise by considering the probability of the intersection of the two events, called the *joint probability* of the two events.

Suppose we let E represent the event of rolling seven on the first toss, and F represent the event of rolling seven on the second toss. Let's compute the probability of rolling seven on both tosses, that is, $P(E \cap F)$. There are 36 outcomes on the first toss and 36 on the second toss. By the multiplication principle of Chapter 2, there are 36^2 total outcomes. There are 6 ways of rolling seven on the first toss and 6 ways of rolling seven on the second toss. Again, by the multiplication principle, there are 6^2 ways of rolling seven on both tosses. Using equiprobability, we then have that the probability of rolling seven on both tosses is

$$P(E \cap F) = \frac{6^2}{36^2} = \frac{6}{36} \cdot \frac{6}{36} = P(E)P(F)\,.$$

This motivates the following definition of independence.

Two events E and F are *independent* if

$$P(E \cap F) = P(E)P(F)\,. \tag{7.3}$$

If two events are not independent, they are *dependent events.*

Be careful not to confuse independent events with disjoint events. For example, tossing a seven on the first toss and tossing a six on the second toss are independent events, while tossing a seven on the first toss and tossing a six on the first toss are disjoint events. Roughly speaking, disjoint events are two events which are mutually exclusive, while independent events are two events such that one does not affect the other.

Exercise 7.3.1. For each of the following pairs of events, guess whether they are independent or dependent, without making any calculations. Then make the calculation required by Equation (7.3) to check your guess. Also, note which pairs are disjoint.

i. A coin is flipped twice. The two events are "first toss heads" and "second toss heads."

ii. A standard deck of playing cards is shuffled several times, then the top two cards in the deck are drawn. The two events are "both cards aces" and "both cards kings."

iii. Same experiment as part ii, but the two events are "both cards aces" and "at least one card is a spade."

iv. Only one card is drawn at random from the card deck. The two events are "card is a spade" and "card is an ace."

v. Two residents of Minneapolis are selected one at a time at random. The two events are "first one is blue-eyed" and "second one is blue-eyed."

vi. Nine students are to be divided at random into three groups of three students. The two events are "Joe and Robert are in a group together" and "Jenn and Julie are in a group together."

vii. Same as part vi, but the two events are “Joe and Robert are in a group together” and “Jenn and Joe are in a group together.”

Exercise 7.3.2. A fair coin is tossed ten times, and all ten times heads appears. What is the probability heads will appear on the eleventh toss?

Sometimes an experiment is repeated several times and it is assumed that the different trials are independent. This leads us to the *binomial model*.

For example, suppose a pair of fair dice is tossed four times and we want to find the probability of rolling seven exactly twice. There are $\binom{4}{2}$ choices for the two rolls that are seven. For example, the first and third rolls might be seven. These $\binom{4}{2}$ choices are disjoint events. The probability of each one of these events is easily computed from the independence assumption. For instance, the probability the first and third rolls are seven is

$$\frac{1}{6} \cdot \frac{5}{6} \cdot \frac{1}{6} \cdot \frac{5}{6} = \left(\frac{1}{6}\right)^2 \cdot \left(\frac{5}{6}\right)^2 .$$

Each of these $\binom{4}{2}$ events will have the same probability: $\left(\frac{1}{6}\right)^2 \cdot \left(\frac{5}{6}\right)^2$. Therefore, by Equation (7.2), the probability that seven occurs exactly twice will be

$$\binom{4}{2} \cdot \left(\frac{1}{6}\right)^2 \cdot \left(\frac{5}{6}\right)^2 .$$

Here are several exercises that require you to compute probabilities in the context of a sequence of independent trials.

Exercise 7.3.3. Find the probability that the fair dice come up seven at least twice in the four rolls.

Exercise 7.3.4. A pair of fair dice is tossed 10 times. Find the probability of rolling 7 exactly 4 times. At least 4 times.

Exercise 7.3.5. Repeat Exercise 7.3.4 with the loaded dice of Exercise 7.2.4.

Exercise 7.3.6. Suppose an unprepared student takes a ten-question multiple-choice exam. Each question has four possible answers, only one of which is correct. What is the probability that she can attain a passing grade of at least 80% by guessing?

Exercise 7.3.7. Suppose an experiment is repeated independently n times. Suppose each experiment has probability of success p (and probability of failure $q = 1 - p$). Use your experience from the above problems to write down a formula for the probability of exactly k successes in the n trials.

Exercise 7.3.8. Every day a class meets, the nine students in the class are divided at random into three groups of three students. The class meets 20 times. What is the probability that Joe and Robert are never in a group together? Are in a group together at least five times? Use the formula from Exercise 7.3.7

Exercise 7.3.9. Suppose a certain baseball player comes to bat and has probability 0.6 of being put out, 0.1 of getting a walk, 0.2 of getting a single, and 0.1 of getting an extra-base hit. If he comes to bat five times in a game, what is the probability that he gets a walk and a single (and three outs)? That he has a perfect day (no outs)? What independence assumption are you making? Is it a reasonable assumption?

Exercise 7.3.10. A pair of fair dice are tossed six times. What is the probability that among the six outcomes, exactly one will be a seven and exactly one will be an eleven? Exactly two will be seven, and at least one will be eleven?

Exercise 7.3.11. A card is drawn and replaced from an ordinary deck of 52 cards. How many times must this experiment be performed so that the probability of drawing at least one heart is greater than 3/4? This problem can be done both with and without logarithms. Do it both ways.

Summarizing the result in Exercise 7.3.7, we have

> If an experiment with two outcomes (success and failure) is repeated independently n times, where the probability of success on any one trial is p and the probability of failure is $q = 1 - p$, then the probability of exactly k successes in the n trials is
>
> $$\binom{n}{k} p^k q^{n-k} . \tag{7.4}$$

Exercise 7.3.12. Using the Binomial Theorem (Theorem 1) and the fact that $p + q = 1$, show that if expression 7.4 is added up for all values of k, the result is 1.

7.4 Misuse of Statistics

Statistics is a much misunderstood and misused subject. It is relatively easy to find examples of this misunderstanding and misuse merely by reading a daily newspaper or watching television news. Here are a few examples.

Exercise 7.4.1. In 1991, 45,827 persons were killed in motor vehicle traffic accidents. In that same year, there were 941 air transport fatalities. Comment on the conclusion that you are safer flying than driving. What other data may be useful?

Exercise 7.4.2. In 1970, 17.2% of the deaths in the United States were due to cancer. In 1990, that percentage was 23.9%. Explain why this percentage is increasing in spite of better treatments. What other information would you need to support your position?

Exercise 7.4.3. In 1990, of the 92,000 pedestrians injured or killed in traffic accidents, 36% were injured or killed at night. Comment on the conclusion that it is safer to walk at night.

Exercise 7.4.4. Minnesota public schools have had high school graduation rates among the top five of all the states for many years. What conclusions can you draw about the quality of public school education in Minnesota? Why?

Exercise 7.4.5. A representative of a cell phone company makes the following statement in opposition to a proposed law limiting cell phone use in automobiles: "In the last 5 years, cell phone use is up ten fold, while automobile accidents are down 5%." Is this a valid argument?

Exercise 7.4.6. Find an example of misused statistics in the newspaper or on television.

7.5 Graphs

In statistics, we try to construct a model to describe events based on the results of experiments.

The result of these "experiments" usually is a collection of numbers, called *data*. In this section we will learn about various pictorial representations of data.

Data come in two forms: numerical and categorical. For example, each of us has a height, weight, age and number of siblings (numerical data); but we also can be classified by name, sex, eye color or hair color (categorical data). Numerical data can be continuous or discrete. Continuous data would include height, weight or age; number of siblings is discrete data. We usually make continuous data into discrete data by defining ranges. For example, in measuring height, we might measure to the nearest inch. We might measure age in number of months. We will only consider discrete data.

Numerical data have an order defined—the order inherited from the ordinary order on numbers. We could, for instance, rank ourselves by height or by age or by the number of siblings. Categorical data do not usually have a natural order assigned.

One way of summarizing data is with a *frequency distribution*. We simply add up the number of occurrences of each category or number in our sample.

Table 7.2 shows a list of data for 25 students: height in inches, age in months, sex, eye color, number of siblings and G.P.A.

Exercise 7.5.1. Find the frequency distributions for sex, for eye color and for number of siblings.

We often use intervals of values to group numerical statistics to give a more useful picture. For instance, we might group the weights in 10 pound intervals.

Exercise 7.5.2. Group height, weight and age values and find their frequency distributions.

Height	Weight	Age	Sex	Eyes	Siblings	GPA
71	205	245	M	Blue	1	3.3
72	194	229	M	Blue	0	3.2
65	122	250	F	Green	1	3.4
68	153	247	M	Brown	4	3.9
62	113	369	F	Hazel	2	3.1
60	101	313	F	Blue	1	3.1
66	141	233	M	Brown	1	2.5
70	152	242	M	Blue	1	2.9
66	134	260	F	Blue	3	3.8
74	198	288	M	Hazel	1	3.3
71	177	241	M	Brown	2	3.0
70	190	220	M	Blue	2	3.6
67	139	299	F	Brown	2	2.7
67	152	248	F	Brown	0	2.1
75	212	249	M	Green	1	3.1
61	98	239	F	Brown	1	2.9
66	120	253	F	Brown	1	3.2
63	111	268	F	Blue	0	4.0
66	129	237	F	Hazel	1	3.4
69	149	270	F	Green	3	2.8
68	156	249	M	Brown	0	2.4
70	173	229	M	Brown	4	2.9
68	141	235	F	Blue	5	3.2
71	182	239	M	Blue	2	3.7
69	160	332	M	Blue	1	1.9

Table 7.2: Twenty-five students

One way of displaying data is with a bar graph, sometimes called a *histograph*. Each value of the frequency distribution is represented as a vertical bar. The height of the bar is proportional to the frequency of the corresponding value.

Exercise 7.5.3. Bar graphs are better at displaying frequency distributions of numerical data rather than categorical data. Why?

Exercise 7.5.4. Construct bar graphs for the numerical statistics in Exercises 7.5.1 and 7.5.2. Use the intervals you used in Exercise 7.5.2.

Categorical data can also be represented as a bar graph, but the use of an axis gives the false impression that order is involved. Sometimes pie charts are used to display categorical data. In a pie chart, a circle is divided into sectors corresponding to the categories, of size proportional to the frequency of the category.

Exercise 7.5.5. Draw a pie chart for eye color.

Now let's use the pool of students described in Table 7.2 to perform some sampling experiments.

Exercise 7.5.6. What is the probability that a student chosen at random from these twenty-five students has blue eyes? Has brown eyes? Is female?

When a sampling experiment is repeated, we have to decide whether the item chosen in the first experiment is to be returned to the pool of items for the subsequent experiment. If it is returned, we say the sampling is done *with replacement*; if not, the sampling is done *without replacement*. Generally speaking, sampling with replacement is somewhat easier to model, since it leads to independent trials.

Now let's repeat the experiment in Exercise 7.5.6 five times with replacement.

Exercise 7.5.7. Suppose five students are selected at random, with replacement. What is the probability that exactly three of them have blue eyes? At least three are female?

Let's see what happens when we repeat the experiment in Exercise 7.5.6 without replacement.

Exercise 7.5.8. Suppose five students are selected at random from the 25 students described in Table 7.2, without replacement. What is the probability that exactly three of them have blue eyes? At least three are female?

Next, let's compute some joint probabilities.

Exercise 7.5.9. Based on the data in Table 7.2, what is the probability that a student chosen at random is a blue-eyed male? A brown-eyed female?

Exercise 7.5.10. Are the events of being blue-eyed and of being male independent in this pool of students?

Extrapolating probabilities from small samples to large populations can be unreliable. The last exercise illustrated some of the difficulty. In our sample, the two events "blue-eyed" and "male" were not independent. But our intuition tells us that these are independent events for a general population.

In this and the previous sections, we have seen how a predetermined knowledge of a probability distribution can be used to find the probabilities of various events. Determining these probabilities is especially easy if the equiprobable model is in effect.

In real life, however, the assignment of probabilities is more problematic. If a newspaper says that 39% of the residents of Minneapolis say they will move out of the city in the next five years, does that mean the newspaper asked every resident if they would move out in five years? How can a drug company determine that a certain drug cures a disease 20% of the time? In both cases, the probability assignment was determined by experiments and sampling procedures. These issues will be dealt with in a subsequent chapter.

7.6 Conditional Probabilities

Sometimes our sample space is reduced for us by additional information. The probabilities we construct are then called *conditional probabilities*. If E and F are events in some sample space, we write $E|F$ to mean the event E **given** the event F. That is, we already know that F has happened or will happen. This effectively reduces the sample space to F and we compute all our probabilities by pretending F is the new sample space.

For example, consider the twenty-five students in Table 7.2. Suppose a student is chosen at random from among these twenty-five and that student is male. Then the probability that he has blue eyes is $6/13$. By stating that the student is male, we have effectively reduced the sample space to just the thirteen males among the twenty-five students. Of those thirteen, six have blue eyes.

Exercise 7.6.1. Suppose a student is chosen at random from among the twenty-five and that student has blue eyes. What is the probability that the student is male?

It is important to understand the difference between conditional probability and joint probability. In the Exercise 7.6.1, you were asked to find the probability that the student selected was male, *given* that the student had blue eyes. This will be different, in general, from the probability that the student selected was male *with* blue eyes (cf. Exercise 7.5.9)!

It is sometimes useful to display conditional probabilities on a "tree diagram." Beginning at the "root," paths describe the different choices. Each edge is labeled with a particular conditional probability. The end nodes are labeled with the product of the probabilities on the path from the root. These nodes represent all the possible outcomes, and their corresponding probabilities.

An example from Exercise 7.6.1 is shown in Figure 7.1. The same exercise is shown in Figure 7.2.

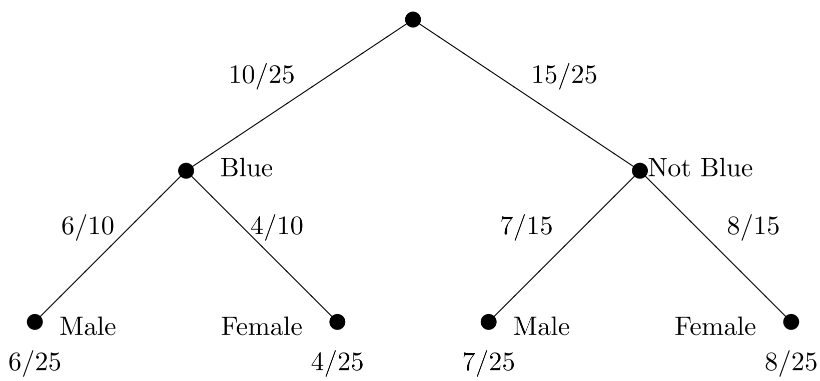


Figure 7.1: One tree diagram

Note that the trees in Figures 7.1 and 7.2 describe two views of the same situation (Table 7.2). Figure 7.1 first divides the sample space into blue-eyed and not-blue-eyed. Then it divides those two groups into male and female. Figure 7.2, on the other hand, first divides the sample space into male and female, then into blue-eyed and not-blue-eyed. Note the differing conditional probabilities. Note also that the joint probabilities at the bottoms of the trees are the same.

In the case of the data in Table 7.2, we are easily able to draw both of these trees. In many situations, however, we can draw only one of the trees, yet we need to compute the conditional probabilities of the other tree.

Exercise 7.6.2. Explain where all the probabilities in Figures 7.1 and 7.2 come from. Also, explain how to use the tree in Figure 7.1 to answer the question posed in Exercise 7.6.1.

Exercise 7.6.3. Using the data in Table 7.2, draw the trees which correspond to the following events: "blue-eyed" and "not blue-eyed," "0 or 1 sibling" and "at least 2 siblings." Calculate the various conditional and joint probabilities and write them in the appropriate places on your trees.

Tree diagrams may be used in several of the exercises in this section.

Exercise 7.6.4. A pair of fair dice is rolled. What is the probability the roll

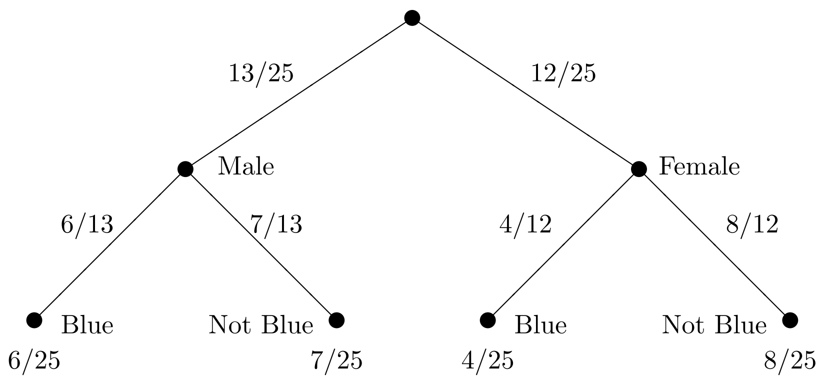


Figure 7.2: Another tree diagram

is even, given that the two numbers showing are different? If the roll is even, what is the probability the two numbers are different?

Exercise 7.6.5. Three fair coins are tossed. What is the probability exactly one is heads, given that both heads and tails appear?

Exercise 7.6.6. Three fair coins are tossed. What is the probability exactly one is heads, given that the first coin shows tails?

In the following two exercises, you will be asked to calculate some probabilities for words selected at random from all the words which may be formed using the letters of the word READER the same number of times as they appear in READER.

Exercise 7.6.7. What is the probability that the two E's are adjacent?

Exercise 7.6.8. First guess whether the probability in question is greater than, the same as, or less than the probability in Exercise 7.6.7. Then compute the probability.

i. The probability that the two E's are adjacent, given the first letter of the word is an R.

ii. The probability that the two E's are adjacent, given the first letter of the word is an E.

iii. The probability that the two E's are adjacent, given the first letter of the word is an A.

iv. The probability that the two E's are adjacent, given the first letter of the word is an D.

Exercise 7.6.9. Nine students are to be divided at random into three groups of three students. What is the probability that Jenn and Julie are in the same group, given that Joe and Robert are in a group together? What is the probability that Jenn and Joe are in the same group, given that Joe and Robert are in a group together?

The fundamental formula in the calculations of conditional probabilities is the following.

If E and F are two events, then

$$P(E|F) = P(E \cap F)/P(F)\,. \tag{7.5}$$

Equivalently,

$$P(E \cap F) = P(F)P(E|F)\,. \tag{7.6}$$

Exercise 7.6.10. Check these formulas for the events in Exercise 7.6.1 above.

Exercise 7.6.11. Prove the following, using Equation (7.5) and Equation (7.3): if E and F are independent events, then $P(E|F) = P(E)$.

Even conditions which seem to differ little can change the conditional probabilities, as the next two exercises show. In each of these, compute the require probabilities by considering the sample space.

Exercise 7.6.12. A small deck of four cards consists of two aces (ace of spades and ace of hearts) and two deuces (deuce of spades and deuce of hearts). Two cards are selected without replacement. What is the probability both are aces? Both are aces given that at least one is an ace? Both are aces given that one is the ace of spades?

Exercise 7.6.13. The same experiment is performed as in the previous exercise. What is the probability that at least one card is a heart? What is the probability that at least one card is a heart, given that at least one card is a spade? What is the probability that at least one card is a heart, given that one card is the ace of spades?

Conditional probabilities can be used to solve the famous birthday paradox, whose solution you are asked to find in the next exercise.

Exercise 7.6.14. What is the probability that at least two persons in our classroom have the same birthday? Assume each year has 365 days and each birthday is equally likely. Solve this problem in two different ways. For one method, compute the complement probability by using the equiprobable model and counting possible birthdays. For the second method, compute the complement probability by using Equation (7.6) repeatedly.

In many of the following exercises, you will be computing the conditional probabilities you "don't know" from the conditional probabilities you "do know." This involves finding the "other tree" described in the discussion before Exercise 7.6.2.

Let's use the trees in Figures 7.1 and 7.2 as an example. Suppose we did not know any of the probabilities on Figure 7.2. How could we compute them? We can find the probability attached to the male branch (13/25) by adding the probabilities of male-and-blue joint outcome (6/25) to the male-and-not-blue joint outcome (7/25) from Figure 7.1. Similarly, we can find the probability attached to the female branch (or we can subtract the probability on the male branch from one). From these, we can use Equation (7.5) to compute the conditional probabilities. For instance, the blue-given-male conditional is 6/25 divided by 13/25.

Here is another example. Suppose one box of golf balls contains 10 balls, six are painted red and the remaining four white. Another box contains eight balls, five painted red and the remaining three white. A ball is selected at random from the first box and moved to the second (but its color is not observed). Then a ball is drawn from the second box. The tree in Figure 7.3 describes the situation. Note that the joint probability that the first ball moved is white and that the second ball selected is also white is $\frac{2}{5} \cdot \frac{4}{9} = \frac{8}{45}$. This follows from Equation 7.6, where E is the event that the second ball is white and F is the event that the first ball is white.

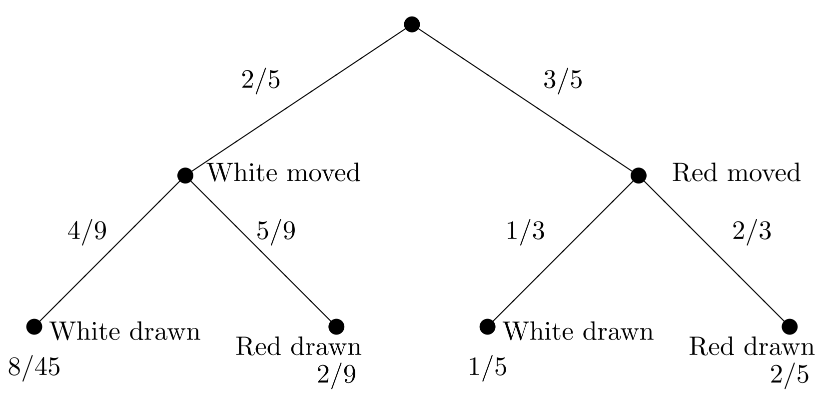


Figure 7.3: First golf ball tree

From Figure 7.3 we can compute the probability that the second ball is white by adding the two joint probabilities where the second ball is white. This probability is $1/5 + 8/45 = 17/45$.

Thus we can construct the "other" tree, conditioning on the second event. This tree is drawn in Figure 7.4. From this tree, using Equation 7.5, we can compute these new conditional probabilities. For instance, the probability that the first ball was white, given that the second was white, is $\frac{8}{45}/\frac{17}{45} = \frac{8}{17}$.

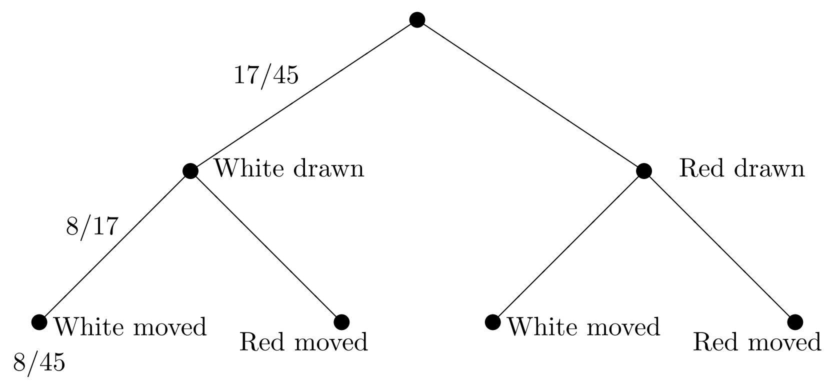


Figure 7.4: Second golf ball tree

Exercise 7.6.15. Using the information given in Figure 7.3, fill in the remaining conditional and joint probabilities on the tree in Figure 7.4. In particular, find the probability that the first ball was red, given that the second was red.

The following exercises require you to use these examples as a model to find the required probabilities.

Exercise 7.6.16. Suppose that the probability of a left-handed person getting a passing score on a certain math test is $1/4$, while for a right-handed person, the probability is $1/5$. If left-handed people make up 10% of the population, what is the probability that a person passing the test is left-handed? (Assume everyone is either left-handed or right-handed.)

Exercise 7.6.17. A game show host offers a contestant a choice of three doors. Behind one door is a new car. Behind the other two doors is billy goat. The contestant chooses door #2. The host then opens door #1 revealing a goat. The host then offers the contestant the choice of

i. keeping her choice of door #2, or

ii. changing her choice to door #3.

What should she do? Again, state what assumptions you are making.

Exercise 7.6.18. A newspaper article announces a new test for a certain kind of cancer. The article trumpets that the test is “90% effective”. Later in the article, you learn that “90% effective” means that the probability that someone tests positive will be 0.9 if they have the disease. Further along in the article, you find out that doctors are worried about a “false positive” of 5%. That means that if a person does not have the disease, the test will be positive with probability 0.05. Finally, in the second continuation of the article, on the back of the sports section, you learn that the overall rate of this disease is 0.01%, i. e., in the general population, the probability of someone having the disease is 0.0001.

A friend of yours tests positive. What is the probability she has the disease? Suppose your friend is a member of a “high risk” population, where the overall disease rate is 0.05%. Now what is the probability she has the disease, given a positive test. Can you make other suggestions about the use of this test?

Genetics is the study of traits passed on from one generation to the next. In the simplest model, a certain trait is determined by a pair of genes, and each gene may be one of two types, say G and g. An individual may have genetic type (called *genotype*) GG, Gg, or gg. Often the types GG and Gg are physically indistinguishable; we say *G dominates g*. The gene G is called *dominant.* The gene g is called *recessive.*

Individuals inherit one such gene from each of their parents. The gene inherited is chosen at random. Thus, if the parents' genotypes are both Gg, one-quarter of their offspring will have genotype GG, one-half will have genotype Gg, and one-quarter will have genotype gg. Three-quarters will therefore display the dominant physical characteristic.

Exercise 7.6.19. Check that the numbers of the previous paragraph are correct.

Let's assume that eye color is controlled by a single gene, that the gene B is dominant and the gene b is recessive. Also, let's assume brown eyes is the dominant physical characteristic and blue eyes is the recessive physical characteristic. Therefore, BB and Bb genotypes are brown-eyed and bb genotype is blue-eyed, and these are the only possible eye colors.

We will also assume that mating is done randomly, independent of eye color.

Finally, let's assume that the genotype distribution is *stable.* That means that each generation displays the same ratio of genotypes (BB:Bb:bb) as the preceding generation.

The stability of the genotype distribution and random mating leads us to an equation. Let p denote the percentage of BB genotype and q the percentage of Bb genotype. Random mating implies that the probability that both the

		Father		
		BB	Bb	bb
Mother	BB	1.00	0.50	0.00
	Bb	0.50	0.25	0.00
	bb	0.00	0.00	0.00

Table 7.3: Offspring genotype = BB

father and the mother are BB genotype will be p^2, that both the father and the mother are Bb genotype will be q^2, and that one parent is genotype BB and one is Bb will be $2pq$. (The factor 2 comes from the fact that either parent could be the BB genotype.)

Table 7.3 describes the probability of a BB genotype offspring, given the father and mother genotypes:

Table 7.3 plus random mating gives us this expression for the percentage of BB genotype in the offspring population: $p^2 + pq + q^2/4$. The stability of the genotype distribution then gives this equation:

$$p^2 + pq + q^2/4 = p\,.$$

For the remaining exercises, we will assume that people with BB genotype make up 64% of the population, that is, $p = 0.64$.

Exercise 7.6.20. What percentage has Bb genotype?

We now assume that the mother of a child is blue-eyed. We wish to compute the probability that the father is blue-eyed, subject to conditions on the eye color of a child. Again, we draw the two relevant trees in Figure 7.5 and Figure 7.6. We use the notation C-Bb to denote the child has genotype Bb, and F-bb to denote the father has genotype bb. Note that certain branches are missing because they are impossible. For instance, since the mother is blue-eyed, the child cannot have BB genotype.

Exercise 7.6.21. Fill in the probabilities on these trees. Use your results from Exercise 7.6.20.

Exercise 7.6.22. Suppose a blue-eyed child has a blue-eyed mother. What is the probability the child's father is blue-eyed?

Exercise 7.6.23. What is the probability that the child's sibling is blue-eyed? (You may have to draw yet another tree to solve this problem.)

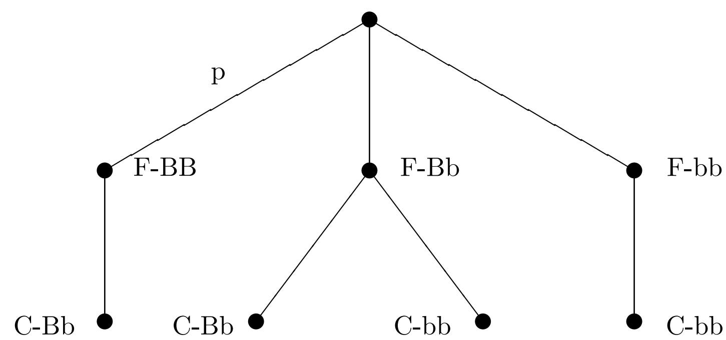


Figure 7.5: Conditional probability tree for genetics

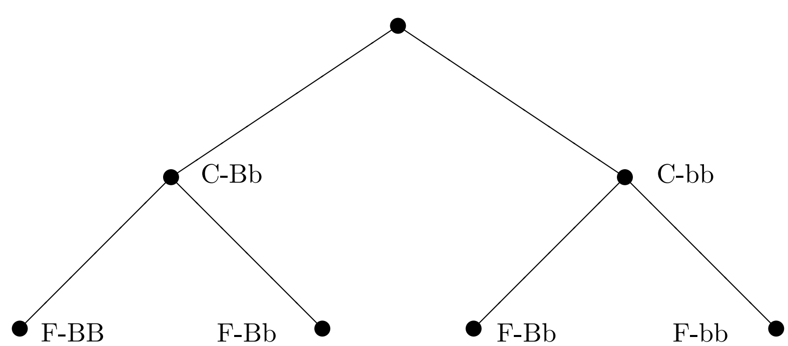


Figure 7.6: Second conditional probability tree for genetics

Chapter 8

Vector Geometry

In this chapter, algebraic methods are used to solve geometric problems, but we begin with a non-algebraic review of some aspects of geometry. In the second and subsequent sections, we treat lines and segments in a manner that is probably different from what you have seen before, and include applications to various geometric figures. Section 5 treats some aspects of geometry in three dimensions. A special topic connected with the Pythagorean Theorem is the content of Section 6.

8.1 Review of some plane geometry

Exercise 8.1.1. Position two congruent right triangles as shown in Figure 8.1, with the point $A = B'$ lying on the segment with endpoints C and C'. Prove that $\angle BAA'$ is a right angle.

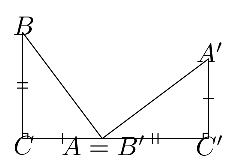


Figure 8.1: Two congruent right triangles

Exercise 8.1.2. Explain why the shaded portion of the large left square in Figure 8.2 has the same area as the shaded portion of the large right square.

The preceding exercise is preparation for a proof of the following famous theorem credited to Pythagoras from approximately 500 B.C.

Theorem 13 (Pythagorean Theorem)**.** *The square of the length of the hypotenuse of a right triangle is equal to the sum of the squares of the lengths of the other two sides.*

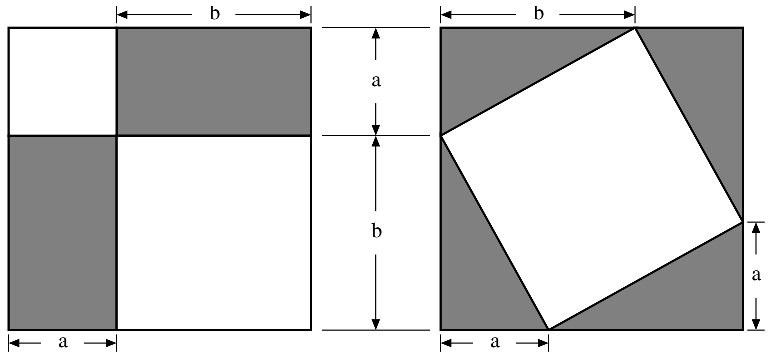


Figure 8.2: The Pythagorean Theorem via comparison of areas

Exercise 8.1.3. Use Exercise 8.1.2 to prove the preceding theorem.

Exercise 8.1.4. Explain how the picture in the left side of Figure 8.2 can be used to prove the algebraic identity

$$(a+b)^2 = a^2 + 2ab + b^2\,. \tag{8.1}$$

The right side of Figure 8.2 and the algebraic identity (8.1) can be used to give a slightly different proof of the Pythagorean Theorem that does not involve the left side of Figure 8.2. Using both sides of the figure is a device for avoiding all algebra in the proof except for the addition and subtraction of areas. Another variation of the proof was given by James A. Garfield when he was a member of the United States House of Representatives, about 5 years before he became the twentieth president of the United States. His proof using a trapezoid and the algebraic identity (8.1) is described on page 161 of Volume 3 (1876) of The New England Journal of Education, alphabetized in the University of Minnesota library as 'Journal of Education' (and is not the only journal with that name). [Actually, General Garfield (as he was known from civil war days) does not claim credit for the proof but says it arose out of discussions with other members of Congress.]

Exercise 8.1.5. Let c denote the length of the hypotenuse of a right triangle and let a and b denote the lengths of the other two sides. Two of these three numbers are given and you are to find the third number. For instance if $a = 2$ and $c = 8$ are given, you should obtain $b = \sqrt{60}$, or preferably $b = 2\sqrt{15}$, but not $b = 7.746$.

i. $a = 5$, $b = 12$

ii. $a = 3$, $b = 3$

iii. $a = 1$, $c = 2\sqrt{5}$

iv. $b = 51$, $c = 149$

A *segment* (which some insist should be called a *line segment*) consists of two points P and Q together with all the points between them; P and Q are the *endpoints* of the segment. A segment with endpoints P and Q is a subset of the line passing through the points P and Q.

The *perpendicular bisector* of a segment is a line that passes through the midpoint of the segment and is perpendicular to the segment. Here is a standard high school geometry problem.

Exercise 8.1.6. Prove that the perpendicular bisectors of two sides of a triangle meet at a point that is equidistant from all three vertices of the triangle. Then deduce that the perpendicular bisector of the third side also passes through that point.

The point where the three perpendicular bisectors of the sides of a triangle meet is called the *circumcenter* of the triangle. Since it is equidistant from all three vertices, there exists a circle centered there passing through all three vertices.

Exercise 8.1.7. Draw three pictures showing circumcenters of triangles, one for an acute triangle, one for a right triangle, and one for an obtuse triangle.

Given any line l and any point P, there exists a unique line m through P perpendicular to l. The distance from P to the intersection of l and m is also called the *distance* from P to l.

Exercise 8.1.8. Draw a picture illustrating the preceding paragraph.

A *ray* consists of all points on a line to one side of some point Q on that line. The point Q itself is considered to be part of the ray, and the ray is said to *emanate* from Q. Two rays emanating from the same point Q are said to form an *angle* at Q, and the rays are called *sides* of the angle. Since each of two segments having a common endpoint Q can be viewed as part of a ray emanating from Q, we also speak of the *angle* formed by two such segments.

Exercise 8.1.9. Draw pictures illustrating the preceding paragraph.

Here is another standard high school geometry problem.

Exercise 8.1.10. Prove that any point on the bisector of an angle is equidistant from the two sides of the angle. Then deduce that the angle bisectors of a triangle meet in a point equidistant from the three sides of the triangle.

The point where the three angle bisectors of a triangle meet is called the *incenter* of the triangle. Because it is equidistant from the three sides of the triangle, there exists a circle centered there that is tangent to the three sides of the triangle.

Exercise 8.1.11. Draw three pictures showing incenters of triangles, one for an acute triangle, one for a right triangle, and one for an obtuse triangle.

A *median* of a triangle is a line passing through a vertex of the triangle and the midpoint of the opposite side. A substantial problem in high school geometry is to prove that the medians of a triangle meet in a common point. A proof not typically given in high school is a topic later in this chapter. The point where the medians meet is called the *centroid* of the triangle.

Exercise 8.1.12. Draw three pictures showing centroids of triangles, one for an acute triangle, one for a right triangle, and one for an obtuse triangle.

An *altitude* of a triangle is a line that passes through a vertex and is perpendicular to the side (possibly extended) opposite that vertex. It develops, as we will see later in this chapter, that the altitudes of a triangle meet in a common point; it is the *orthocenter* of the triangle.

Exercise 8.1.13. Draw three pictures showing orthocenters of triangles, one for an acute triangle, one for a right triangle, and one for an obtuse triangle.

8.2 Parametric representations of lines

Recall that points in a plane can be represented by ordered pairs (x, y) of numbers. The origin must be specified as well as the directions for the two axes and a unit of measurement. An ordered pair of numbers is sometimes called a *point.*

Sometimes we will use a single capital letter to denote a point. Thus, we might write $P = (x, y)$. If we want to emphasize the distinction between geometry and arithmetic, we might avoid the equals symbol and say that P is a point with *coordinates* (x, y); x is the *first coordinate* and y is the *second coordinate.* In case several points are to be discussed, subscripts can be used to distinguish them. For instance, the vertices of a triangle could be denoted by $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, and $P_3 = (x_3, y_3)$.

Exercise 8.2.1. Let $P_1 = (0, 0)$, $P_2 = (0, 3)$, $P_3 = (1, \frac{5}{2})$, $P_4 = (-2, 0)$, and $P_5 = (\sqrt{5}, -1)$. Locate these points on a coordinate system. Then sketch the line passing through P_1 and P_2, the line passing through P_3 and P_4, and the line passing through P_5 and P_1.

Exercise 8.2.2. Suppose someone starts at the origin and moves on a line at constant speed, arriving at the point $(0, 3)$ after 2 hours. Where is she 4 hours after starting from the origin? 5 hours after? 1 hour after? 1/2 hour after? $\sqrt{7}$ hours after? t hours after, for an arbitrary positive number t?

Exercise 8.2.3. Suppose someone starts at the point $(1, \frac{5}{2})$ and moves on a line at constant speed, arriving at the point $(-2, 0)$ after 1 hour. Where is he t hours after starting at $(1, \frac{5}{2})$.

We have already seen that ordered pairs of real numbers are called points. Another name for an ordered pair of real numbers is *vector.* We use this term when certain arithmetical operations are performed with the ordered pairs; *addition* of vectors and *multiplication* of a vector by a real number are defined by

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2\ ,\ y_1 + y_2)$$

and

$$k(x, y) = (kx, ky)\,,$$

respectively. It is standard practice never to use a symbol such as $\times$ or $\cdot$ to denote this multiplication.

Exercise 8.2.4. Calculate $(3, -2) + (4, 1)$. Draw a picture of a quadrilateral with vertices at $(0, 0)$, $(3, -2)$, $(4, 1)$, and $(3, -2) + (4, 1)$. What kind of quadrilateral does it appear that you have obtained? (Later in this section you will learn how to check whether you have been deceived by appearances on this issue.)

Exercise 8.2.5. Let $P = (-2, 4)$. Calculate $2P$, $(-2)P$, $0P$, $1P$, $\frac{1}{2}P$, and $(-\frac{1}{3})P$. Place all these points on a coordinate system. Then make some relevant comments.

Notice that when working with vectors, parentheses get used for more than one purpose. For instance, in the expression

$$(4 + 5)(3, -1)$$

the first set of parentheses plays the usual grouping role and the second, in conjunction with the comma, indicates a vector. Some parentheses playing a grouping role can be omitted without creating ambiguity. For a vector P, one would usually write $-2P$ rather than $(-2)P$ and $-P$ instead of $(-1)P$ or $-1P$.

Exercise 8.2.6. Simplify the following three expressions:

i. $(4 + 5)(3, -1)\,;$

ii. $-2(3, -1)\,;$

iii. $-(-4, -5)\,.$

Exercise 8.2.7. Perform the following calculations:

i. $2(4, 3) - \frac{1}{3}(24, 18)\,;$

ii. $0(5, 6) + 5(0, 0)\,;$

iii. $[(5, -3) - (-2, 2)] + (-4, -1)\,;$

iv. $(5, -3) + [-(-2, 2) + (-4, -1)]\,;$

v. $(5, -3) - [(-2, 2) + (-4, -1)]\,;$

vi. $4(3, -1) + 5(3, -1)$ (compare with (i) of Exercise 8.2.6)

vii. $\frac{1}{3}[6(2,-3)]$.

Exercise 8.2.8. For each of the following equations decide whether there is a solution for k and if so, find it. For those that do not have a solution, give a proof that there is no solution.

i. $(4,3) = k(-12,-9)$

ii. $(4,3) = k(8,7)$

iii. $(0,0) = k(8,7)$

iv. $(8,0) = k(0,0)$

v. $(\sqrt{3}-1,1) = k(2,\sqrt{3}+1)$

Letters other than P are often used for vectors and letters other than x and y for their coordinates. A vector Q is said to be a *multiple* of a vector P if $Q = kP$ for some real number k.

Exercise 8.2.9. Use your answers for Exercise 8.2.8 to conclude that certain vectors are multiples of certain other vectors, and also to identify some vectors that are not multiples of certain other vectors.

Suppose that Laura starts at $(-1,-2)$, walks in a straight line at constant speed, and goes through the point $(2,0)$ after 1 minute. Since $(2,0)-(-1,-2) = (3,2)$, we see that Laura moves 3 units in the x-direction and 2 units in the y-direction every minute. Thus after t minutes she will have moved $3t$ units in the x-direction and $2t$ units in the y-direction. Therefore, after t minutes Laura is at the point

$$(-1+3t,-2+2t)\,,$$

which we could also write as

$$(-1,-2)+t(3,2)\,.$$

In particular, after $\frac{3}{2}$ minutes Laura is at the point $(\frac{7}{2},1)$. If we imagine that Laura was already walking when she was at the point $(-1,-2)$, but only then did we start a timing device, it would be meaningful to ask for Laura's position at time -3. It would be

$$(-1,-2)-3(3,2) = (-1,-2)+(-9,-6) = (-10,-8)\,.$$

Laura's path is shown in the left side of Figure 8.3. The same path is shown in the right side of the figure where times at which Laura is at various points are also shown. An arrow representing the vector $(3,2)$ is shown in both sides of the figure. It indicates the direction in which Laura is moving, and its length indicates her speed.

By placing the arrow with its tail at $(0,0)$ we emphasize that the direction and speed of travel can be specified without regard to the actual path of travel.

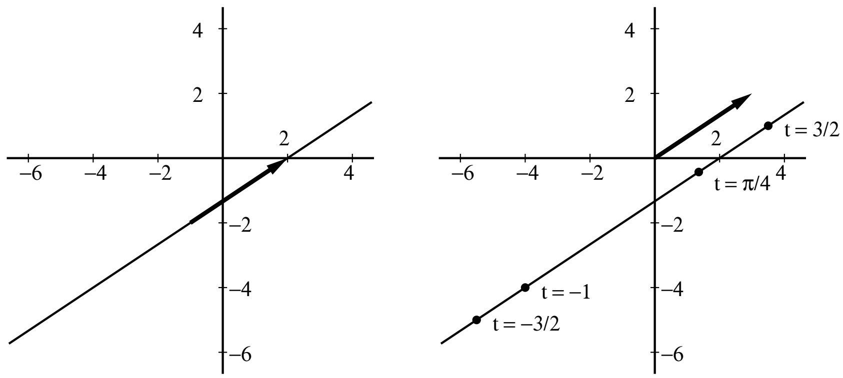


Figure 8.3: A line represented parametrically

By placing the arrow on the path of travel we convey additional information, but give the somewhat misleading impression that an arrow of the same length and direction placed elsewhere would have a different meaning.

Sometimes the terms ‘point’ and ‘vector’ are used in the same discussion. Even though both words refer to ordered pairs of real numbers, they tend to be used for different geometric interpretations. The best picture of a point is usually a dot, whereas an arrow is often the best when the word ‘vector’ is used.

Exercise 8.2.10. For each of Exercise 8.2.3 and the last question of Exercise 8.2.2 do the following. Write your answer in the form $A+tD$ for appropriate vectors A and D. Draw a picture of the path of travel. Show D as an arrow with its tail at $(0, 0)$.

Exercise 8.2.11. Bus schedules often have a picture of the path of travel, but do not place times along side the picture. Rather names are attached to various places along the path, and then a separate list is given with name and corresponding time. Why are bus schedules written in the manner just described rather than in the apparently simpler way of just placing times along side the picture of path of travel?

Let A be any point and D any vector different from $(0, 0)$. The set

$$\{A + tD \colon t \text{ any real number}\}$$

is the *line* through A in the *direction* determined by D. The vector D is called a *direction indicator* of the line, t is called the *parameter,* and the formula itself is called a *parametric representation* of the line. Notice that the parameter itself does not appear on the graph of the line. Of course, letters other than t may used, although t is a common choice because it can be useful to view it as representing time as in Exercises 8.2.2 and 8.2.3. The different roles of A and the direction indicator D can be highlighted by using the word 'point' for A and the word 'vector' for D. Often the set notation is omitted; so for instance, one speaks of the line

$$(3,5) + t(-2,-5)\,, \quad t \text{ a real number}\,, \tag{8.2}$$

or, more briefly,

$$(3,5) + t(-2,-5)\,. \tag{8.3}$$

Exercise 8.2.12. Find five points on the line $(3,5)+t(-2,-5)$, exactly one of which corresponds to an integer t, exactly three of which correspond to negative t, and exactly two of which correspond to irrational t.

Exercise 8.2.13. Prove that the line with equation $y = \frac{5}{2}x - \frac{5}{2}$ is the line of the preceding exercise.

Exercise 8.2.14. Draw pictures of the following lines on a common coordinate system:

i. $(1,2) + t(2,3)\,;$

ii. $t(2,3)\,;$

iii. $(-1,-1) + t(2,3)\,;$

iv. $(3,-4) + t(4,6)\,;$

v. $(5,0) + t(-2,-3)\,.$

Calculate the slopes of each of these lines, and then write point-slope equations for each of the lines.

Exercise 8.2.15. Draw pictures of the following lines on a common coordinate system:

i. $t(0,-3)\,;$

ii. $(5,0) + t(0,3)\,;$

iii. $(-3,0) + t(0,-3)\,;$

iv. $(0,-7) + t(0,6)\,.$

Exercise 8.2.16. Explain why A and $A+D$ are two points on the line described parametrically as $A + sD$.

Exercise 8.2.17. Explain why $B-A$ is a direction indicator of the line passing through two points A and B. Explain why $2(B-A)$ and $3(A-B)$ are also direction indicators of this line.

Exercise 8.2.18. Find two points on each of the following two lines and then represent the lines parametrically.

i. $y = -x + 4$;

ii. $y = \frac{5}{7}x - \frac{3}{4}$.

Exercise 8.2.19. Explain with pictures why the slope of a line with direction indicator (u, v) equals v/u. Also, discuss the case $u = 0$ in which case division by u is not possible.

Exercise 8.2.20. In each part of this problem find all points of intersection of the given pairs of lines:

i. $(1, 1) + s(4, -2)$, $(0, 1) + t(3, 0)$;

ii. $(4, 4) + r(2, 1)$, $(0, 0) + s(-6, -3)$;

iii. $(3, -1) + s(-2, -5)$, $(5, 4) + s(4, 10)$.

Comment on how to approach such problems when the same symbol is used for the parameter for both given lines.

Exercise 8.2.21. We will not give a proof of the theorem following this exercise, but many of the preceding exercises give us reasons to believe that it is true. Explain how some of the preceding exercises illustrate the theorem.

Theorem 14. *Let D denote a direction indicator of a line l passing through a point A, and E a direction indicator of a line m passing through a point B. Then:*

- *l and m intersect in exactly one point if E is not a multiple of D;*
- *$m = l$ if E and $(B - A)$ are both multiples of D;*
- *m is parallel to l if E is a multiple of D but $(B - A)$ isn't a multiple of D.*

Exercise 8.2.22. Create three problems to which a classmate should apply the preceding theorem: one where the answer is that the two lines are the same, one where there is no point of intersection, and one where there is exactly one point of intersection whose coordinates are not integers.

Exercise 8.2.23. Prove that the quadrilateral with vertices $(4, -3)$, $(3, 0)$, $(5, 2)$, and $(6, -1)$ is a parallelogram. Also, represent the diagonals parametrically.

Exercise 8.2.24. Let P and Q be two points neither of which is a multiple of the other. Prove that the quadrilateral with vertices $(0, 0)$, P, $P + Q$, and Q is a parallelogram and obtain parametric representations for its diagonals.

Exercise 8.2.25. Why in the preceding exercise was it important to assume that neither P nor Q is a multiple of the other?

Often a diagonal of a parallelogram is regarded as a segment rather than a line.

For an example (not connected with parallelograms) on how to treat segments parametrically, let us consider the segment with endpoints $(-4,2)$ and $(3,-2)$. A direction indicator of the line through these points is $(7,-4)$, and a parametric representation of the line is

$$(-4,2)+t(7,-4)\,.$$

Notice that we get one endpoint of the segment by setting $t=0$ and the other endpoint by setting $t=1$. The values of t between 0 and 1 give the other points on this segment. Therefore, a parametric representation of the segment is

$$(-4,2)+t(7,-4)\,,\quad 0\le t\le 1\,.$$

The formulas

$$(3,5)+t(-2,-5)\,,\quad t\ge 0\,,$$

and

$$(3,5)+t(-2,-5)\,,\quad t\le 0\,,$$

describe two rays emanating from the point $(3,5)$.

Exercise 8.2.26. Give a parametric description of a third ray emanating from $(3,5)$. Draw a picture of this ray and of the two rays described above. On the same coordinate system, but in different colors, also draw pictures of the line

$$(3,5)+t(-2,-5)$$

and the segment

$$(3,5)+t(-2,-5)\,,\quad 0\le t\le 1\,.$$

Exercise 8.2.27. Use Theorem 14 to decide how many points are in the intersection of the following two lines.

$$\begin{aligned}&(3,4)+t(2,-2)\,;\\&(3,-2)+t(4,5)\,.\end{aligned}$$

Then find all such points. Check your answer by drawing a picture.

Exercise 8.2.28. How, if at all, does your answer to the preceding problem change if the lines are replaced by the rays

$$\begin{aligned}&(3,4)+t(2,-2)\,,\quad t\ge 0\,;\\&(3,-2)+t(4,5)\,,\quad t\ge 0\,?\end{aligned}$$

Suppose these two parametric formulas represent the motion of two runners. Will they collide.

Exercise 8.2.29. How, if at all, does you answer to Exercise 8.2.27 change if the lines are replaced by the segments

$$(3,4)+t(2,-2)\,, \quad 0 \le t \le 1\,;$$
$$(3,-2)+t(4,5)\,, \quad 0 \le t \le 1\,?$$

Check your answer by drawing a picture.

Exercise 8.2.30. Find the intersection of the ray emanating from $(3,5)$ having direction indicator $(-2,-3)$ and the segment having endpoints $(-1,-1)$ and $(6,\frac{19}{2})$.

8.3 Distances and norms

The distance of a point $P=(x,y)$ from the origin can be calculated by using the Pythagorean Theorem. It equals

$$\sqrt{x^2+y^2}\,.$$

Two notations are commonly used to express this notion. Since on the real line, absolute value denotes distance from the origin, the same symbol is sometimes used to denote distance from the origin. However, we will use the other possible notation. Thus

$$\|P\| = \sqrt{x^2+y^2}\,.$$

If we are using vector terminology, we call $\|P\|$ the *norm* of the vector P. Notice that Pythagorean Theorem shows that the distance between two points P and Q is the norm of their difference, that is, $\|Q-P\|$.

Exercise 8.3.1. Draw a picture illustrating the use of the Pythagorean Theorem to show the distance from a point P to the origin is $\|P\|$. Draw a picture illustrating the use of the Pythagorean Theorem to show that the distance between two points P and Q is $\|Q-P\|$.

Exercise 8.3.2. Calculate the norms of the four vectors $(12,-5)$, $(-6,7)$, $(6,2)$, and $(\sqrt{5}-2,\sqrt{5}+2)$. Also, use some of your calculations to show that it is not always true that $\|P+Q\| = \|P\|+\|Q\|$. *Hint:* Do not confuse norms of vectors with absolute values of numbers.

Exercise 8.3.3. Prove that $\|kP\| = |k|\,\|P\|$ for every real number k and every vector P. *Hint:* Do not confuse norms of vectors with absolute values of numbers.

Theorem 15. *Let t_1 and t_2 be two arbitrary real numbers, let A be a point, and let D be a vector different from $(0,0)$. Then the distance between the points $A+t_1D$ and $A+t_2D$ equals $|t_2-t_1|\,\|D\|$. If the parametric representation $A+tD$ corresponds to motion with t denoting time, then the speed of travel equals $\|D\|$.*

Proof. The distance between the two points equals

$$\|(A + t_2D) - (A + t_1D)\| = \|(t_2 - t_1)D\|,$$

which by the preceding exercise, equals $|t_2 - t_1| \, \|D\|$, as desired. Since the distance traveled between any two times is the absolute value of the difference between those two times multiplied by $\|D\|$, the speed of travel is $\|D\|$.

Exercise 8.3.4. Suppose that $(9, 11) + t(-4, 7)$ represents Joe's travel along a line. How far does he travel in 3 units of time?

Exercise 8.3.5. Consider the segment with endpoints A and B represented parametrically by

$$A + tD, \quad 0 \le t \le 1.$$

Fix a value of t between 0 and 1; call this fixed value t_0. Show that the quotient obtained by dividing the distance from A to the point $A + t_0D$ by the distance from B to the point $A + t_0D$ equals $t_0/(1 - t_0)$. Then use the fact to show that the midpoint of the segment is $\frac{1}{2}A + \frac{1}{2}B$.

Exercise 8.3.6. Find the midpoint of the segment connecting the points $(\frac{13}{3}, \frac{5}{2})$ and $(\frac{5}{3}, -\frac{7}{4})$. Also find the point on this segment whose distance from $(\frac{13}{3}, \frac{5}{2})$ is half its distance from $(\frac{5}{3}, -\frac{7}{4})$.

Exercise 8.3.7. Find parametric representations of the medians of a triangle with vertices at A, B, and C. Find an appropriate value of the parameter for each median in order to show that each of the medians passes through the point $\frac{1}{3}A + \frac{1}{3}B + \frac{1}{3}C$.

It is natural to call $\frac{1}{3}A + \frac{1}{3}B + \frac{1}{3}C$ the *average* of the points A, B, and C. Thus the preceding exercise is a request for you to prove that every triangle has a centroid and that the centroid is the average of the vertices.

Exercise 8.3.8. Find the centroid of the triangle with vertices at the points $(0, 0)$, $(1, 3)$, and $(4, 0)$, and illustrate with a picture.

Exercise 8.3.9. Find the centroid of the triangle with vertices at the points $(2, 0)$, $(-1, \sqrt{3})$, and $(-1, -\sqrt{3})$, and illustrate with a picture.

Exercise 8.3.10. Use vector methods to prove that the diagonals of a parallelogram bisect each other.

8.4 Orthogonality and perpendicularity

We have learned how to multiply a number by a vector, getting a vector as an answer. Now we will learn how to multiply two vectors to obtain a number as an answer. We will use a dot '·' to denote this multiplication; moreover, unlike the situation for multiplication of numbers, we will never omit the dot. The *dot product* of two vectors $D = (b, c)$ and $E = (u, v)$ is defined by the formula

$$D \cdot E = bu + cv.$$

Before treating geometric issues we must learn a little more about the dot product from an algebraic point of view.

Exercise 8.4.1. Illustrate and then prove the distributive law for the dot product and sum of vectors. You may of course use the distributive law for numbers.

Exercise 8.4.2. Illustrate and then prove the following formula relating the norm of a vector and the dot product of that vector with itself:

$$\|P\|^2 = P \cdot P\,.$$

Exercise 8.4.3. Prove that

$$k(P \cdot Q) = (kP) \cdot Q = P \cdot (kQ)$$

for all vectors P and Q and all numbers k.

Recall that $\|Q - P\|$ is the distance between the points P and Q. The following theorem gives a formula for the square of this distance in terms of norms of P and Q separately and their dot product.

Theorem 16. *For any points P and Q*

$$\|Q - P\|^2 = \|Q\|^2 + \|P\|^2 - 2(P \cdot Q)\,.$$

Proof. We use Exercises 8.4.1 and 8.4.2 together with the easily proved commutativity of the dot product:

$$\begin{aligned}
\|Q - P\|^2 &= (Q - P) \cdot (Q - P) \\
&= Q \cdot (Q - P) - P \cdot (Q - P) \\
&= Q \cdot Q - Q \cdot P - P \cdot Q + P \cdot P \\
&= \|Q\|^2 - 2(P \cdot Q) + \|P\|^2\,,
\end{aligned}$$

as desired.

Exercise 8.4.4. Fill in the blank in the following formula

$$\|P + Q\|^2 = \|P\|^2 + \|Q\|^2 \underline{\hspace{6cm}}\,.$$

Two vectors are said to be *orthogonal* if their dot product equals 0.

Theorem 17. *A necessary and sufficient condition for two lines to be perpendicular is that their direction indicators be orthogonal.*

Partial Proof. (The proof of a theorem that says "necessary and sufficient" or "if and only if" often requires two separate arguments going in opposite directions. For this theorem we will skip the proof of sufficiency, but comment that one approach to proving sufficiency is to first prove a converse of the Pythagorean Theorem—namely, that if the square of one side of a triangle equals the sum of the squares of the other two sides, then the triangle is a right triangle.)

Suppose that two lines are perpendicular at a point A. Let D and E denote direction indicators of the two lines. Then the triangle with vertices A, $A+D$, and $A+E$ has a right angle at A. It is now left for the reader, in the following exercise, to complete the proof that D and E are orthogonal.

Exercise 8.4.5. Use the Pythagorean Theorem to finish the above proof of necessity.

Because of Theorem 17, 'orthogonal' and 'perpendicular' are often treated as synonyms, although usually 'orthogonal' is used in conjunction with vectors and 'perpendicular' in conjunction with lines.

In the first section of this chapter it was mentioned that the the altitudes of any triangle intersect in a common point called the orthocenter of the triangle. We will now prove this fact.

We will use an important fact in 2-dimensional geometry, a fact which will not be proved here. It is that if a line m is perpendicular to a line k and a line n is perpendicular to a line l, then a necessary and sufficient condition for m and n to meet in a single point is that k and l meet in a single point. Two sides of a triangle are parts of lines that do meet in a single point. Hence, any two altitudes of a triangle meet in a single point.

Let F denote the intersection of the altitudes from A and B in a triangle with vertices at A, B, and C. Using the relation between perpendicularity of lines and orthogonality of vectors, we obtain

$$\begin{aligned}(F-A)\cdot(C-B) &= 0\,;\\ (F-B)\cdot(A-C) &= 0\,.\end{aligned}$$

We use the distribution law to rewrite these two equalities:

$$\begin{aligned}F\cdot(C-B) &= A\cdot(C-B)\,;\\ F\cdot(A-C) &= B\cdot(A-C)\,.\end{aligned}$$

We rewrite once more:

$$\begin{aligned}F\cdot(C-B) &= A\cdot C-A\cdot B\,;\\ F\cdot(A-C) &= B\cdot A-B\cdot C\,.\end{aligned}$$

Now we add the two equalities, again using the distributive law:

$$F\cdot(A-B)=A\cdot C-B\cdot C\,,$$

which is equivalent to

$$F\cdot(A-B)=C\cdot(A-B)\,,$$

Subtract $C\cdot(A-B)$ from both sides to get

$$(F-C)\cdot(A-B)=0$$

Therefore, the line through F and C is perpendicular to the line through A and B; that is, F is on the altitude from C. So all three altitudes meet at F.

Exercise 8.4.6. The words in the preceding discussion are somewhat misleading in case the triangle of interest is a right triangle, but the essentials of the argument are valid for such a triangle. Explain.

Exercise 8.4.7. Find the orthocenter of the triangle with vertices at $(1, 0)$, $(3, 5)$, and $(-4, 4)$. Then draw a picture showing your answer. *Hint:* Let the coordinates of the orthocenter be (x, y) and find two equations that x and y must satisfy.

Exercise 8.4.8. Use vector methods to prove that the diagonals of a rhombus are perpendicular to each other. *Hint:* It might be helpful to place the coordinate system so that one vertex of the rhombus is at $(0, 0)$.

Exercise 8.4.9. Use vector methods to prove that the sum of the squares of the lengths of the diagonals of a parallelogram equals the sum of the squares of the lengths of the four sides. *Hint:* See the hint for the preceding exercise.

8.5 Three-dimensional space

One of the great advantages of vector methods for the study of geometry is that they work for three-dimensional geometry, not just for the two-dimensional geometry that we have been studying. Moreover, they provide one approach to understanding geometry in four and more dimensions. When treating 3-dimensional geometry, vectors are ordered triples rather than ordered pairs. For 4-dimensional geometry, vectors are ordered 4-tuples, and for n-dimensional geometry, vectors are ordered n-tuples.

Lines, rays, and segments can be defined parametrically in n dimensions just as in two dimensions. The concept of 'parallelism' requires some attention. We say that two distinct lines are *parallel* if their direction indicators are multiples of each other. The following exercise concerns three lines that are not parallel, two of which also do not meet.

Exercise 8.5.1. For each pair of the three lines $t(1, 2, 3)$, $t(-3, -1, -3)$, and $(1, 1, 1) + t(2, 1, 2)$ decide if they meet and if so, where.

The *norm* of a vector $P = (x, y, z)$ in 3-dimensional space is defined by

$$\|P\| = \sqrt{x^2 + y^2 + z^2}\,,$$

the *distance* between points P and Q equals $\|Q - P\|$, and the *dot product* of vectors $D = (a, b, c)$ and $E = (u, v, w)$ is defined by

$$D \cdot E = au + bv + cw\,.$$

As for two-dimensional geometry, $\|P\|^2 = P \cdot P$.

Exercise 8.5.2. Let $A = (0\,,\,0\,,\,3)$, $B = (2\sqrt{2}\,,\,0\,,\,-1)$, $C = (-\sqrt{2}\,,\,\sqrt{6}\,,\,-1)$ and $D = (-\sqrt{2}\,,\,-\sqrt{6}\,,\,-1)$. Find the distances between each pair of these points. Also find the average of these four points.

A *tetrahedron* is a polyhedron made up of four triangular faces, four vertices and six edges, with three triangles meeting at each vertex. Recall that the regular tetrahedron was one of the five platonic solids encountered in Chapter 4. A *median* of a tetrahedron is a line through one vertex and the centroid of the opposite face.

Exercise 8.5.3. Prove that all four medians of an arbitrary (not necessarily regular) tetrahedron meet at the average of the four vertices of the tetrahedron. This point is called the *centroid* of the tetrahedron.

A *parallelepiped* is a polyhedron with six parallelogram faces, eight vertices and twelve edges, with three parallelograms meeting at each vertex. Furthermore, opposite parallelograms lie in parallel planes. The cube, one of the five platonic solids in Chapter 4, is a parallelepiped.

By placing the $(0, 0, 0)$ at one vertex of a parallelepiped and naming the vertices adjacent to that vertex as U and V and W, the names of the other four vertices become $U + V$, $V + W$, $W + U$, and $U + V + W$. A *diagonal* of a parallelepiped is a segment connecting two vertices and not lying in any face of the parallelepiped.

Exercise 8.5.4. How many diagonals does a parallelepiped have?

Exercise 8.5.5. Prove that all the diagonals of a parallelepiped bisect each other.

8.6 Pythagorean triples

Exercise 8.1.5 makes it clear that if the lengths of two sides of a right triangle are integers, it is possible that the length of the third side is an integer, and it is also possible that it is irrational. We will focus the remainder of this section on right triangles whose three side lengths are all integers. A triple (a, b, c) of positive integers for which $c^2 = a^2 + b^2$ is called a *Pythagorean triple.*

Exercise 8.6.1. Which of the following triples are Pythagorean triples?

i. $(7, 24, 25)$

ii. $(6, 8, 10)$

iii. $(7, 4, 8)$

iv. $(21, 20, 29)$

v. $(105, 100, 145)$

Exercise 8.6.2. From which of the Pythagorean triples in the preceding exercise can other Pythagorean triples be obtained by dividing each member of the Pythagorean triple by the same integer?

The preceding exercise indicates why it is natural to focus attention on Pythagorean triples (a, b, c) having the additional property that $\mathrm{GCD}(a, b, c) = 1$. Such a Pythagorean triple is said to be *primitive.*

Exercise 8.6.3. Let (a, b, c) be a Pythagorean triple. Prove that

$$\mathrm{GCD}(a, b, c) = \mathrm{GCD}(a, b) = \mathrm{GCD}(a, c) = \mathrm{GCD}(b, c)\,.$$

Exercise 8.6.4. Prove that if (a, b, c) is a Pythagorean triple, then

$$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1\,.$$

Moreover, use the preceding exercise to show that if (a, b, c) is primitive, then $\frac{a}{c}$ and $\frac{b}{c}$ are fractions in lowest terms.

Recall that the equation of the circle of radius 1 centered at $(0, 0)$ has the equation $x^2 + y^2 = 1$. The preceding exercise shows how to obtain a point on the quarter circle $x^2 + y^2 = 1$, $x > 0$, $y > 0$, from a Pythagorean triple, a point with the additional property of being a *rational point,* that is, a point both of whose coordinates are rational. Moreover, no reduction to lowest terms is required if the Pythagorean triple is primitive. Conversely, according to the following exercise both coordinates of any rational point on the quarter circle $x^2 + y^2 = 1$, $x > 0$, $y > 0$, have the same denominator when written in lowest terms and a primitive Pythagorean triple can be obtained from it by using the numerators as the first two members of the triple and the common denominator as the third member.

Exercise 8.6.5. Substantiate the assertions made in the preceding sentence by first describing how to get some Pythagorean triple from any rational point on the quarter circle $x^2 + y^2 = 1$, $x > 0$, $y > 0$. Then use Exercise 8.6.3 to prove that both coordinates of the rational point have the same denominator when written in lowest terms.

The preceding exercises and discussion show that the problem of describing all primitive Pythagorean triples is essentially the same as the problem of describing all rational points on the quarter circle $x^2 + y^2 = 1$, $x > 0$, $y > 0$. We will proceed to describe all such rational points by a clever device, the first discoverer of which must have felt very proud. A one-to-one correspondence between rational points on the quarter circle $x^2 + y^2 = 1$, $x > 0$, $y > 0$, and rational numbers between 0 and 1 will be obtained.

Here is how to obtain the rational number t corresponding to a rational point $(\frac{a}{c}, \frac{b}{c})$ on the quarter circle $x^2 + y^2 = 1$, $x > 0$, $y > 0$. Set

$$t = \frac{a}{b + c}\,.$$

It is obvious that t is rational and positive. Furthermore, since a, b and c form the three sides of a triangle, it follows that $t < 1$. Therefore t is a rational number between 0 and 1.

The following exercise shows that the process can be reversed.

Exercise 8.6.6. Let (a, b, c) be a primitive Pythagorean triple. Substitute $\frac{a}{b+c}$ for t in the formula

$$\left(\tfrac{2t}{1+t^2}, \tfrac{1-t^2}{1+t^2}\right), \tag{8.4}$$

and simplify to show that the rational point $\left(\frac{a}{c}, \frac{b}{c}\right)$ is obtained.

Suppose that we start with a rational t between 0 and 1 that we do not know in advance comes from a rational point on the quarter circle $x^2 + y^2 = 1$, $x > 0$, $y > 0$. Clearly, (8.4) gives a rational point in the first quadrant. The following exercise completes the proof that it is on the quarter circle.

Exercise 8.6.7. Prove the following algebraic identity:

$$\left(\tfrac{2t}{1+t^2}\right)^2 + \left(\tfrac{1-t^2}{1+t^2}\right)^2 = 1\,.$$

Exercise 8.6.8. Find many rational points on the quarter circle $x^2 + y^2 = 1$, $x > 0$, $y > 0$, and the corresponding primitive Pythagorean triples by using the following values for t in (8.4):

i. 1/2

ii. 1/3

iii. 1/5

iv. 2/3

v. 2/7

vi. 3/8

vii. 3/20

Hint: Do not use your calculator for any divisions. Do not let decimal representations get into your work.

Exercise 8.6.9. The formula (8.4) with the restriction $0 < t < 1$ can be viewed as a parametric representation of the quarter circle $x^2 + y^2$, $x > 0$, $y > 0$. If this representation is regarded as representing travel, does the travel proceed in the clockwise direction or in the counterclockwise direction? Explain. If the restriction $0 < t < 1$ is omitted, what curve is then represented parametrically by (8.4)?

Exercise 8.6.10. The triple $(5, 12, 13)$ is Pythagorean and primitive. Use it to find several Pythagorean triples that are not primitive.

Exercise 8.6.11. Check that each of the triples (a, b, c) is primitive Pythagorean:

i. $(7, 24, 25)$

ii. $(16, 63, 65)$

iii. $(20, 21, 29)$

iv. $(180, 19, 181)$

Then for each, calculate the corresponding rational number between 0 and 1.

Exercise 8.6.12. Find the side lengths of some right triangle whose side lengths are whole numbers having greatest common divisor equal to 1 and the length of whose hypotenuse has at least four digits.

You might enjoy reading the short article about Pythagorean triples beginning on page 160 of Volume 1 (1875) of the above-mentioned The New England Journal of Education. On the positive side, a relationship with triangular numbers is described. On the negative side, the author seems unaware of the comprehensive solution that probably was obtained by the Pythagorean school over 2000 years ago.

Chapter 9

Trees

The special kind of graph called a tree plays an important role in many areas of mathematics and in many fields outside mathematics. In this chapter, we will learn about two important algorithms associated with trees. The first, called the Prüfer correspondence, is used to count trees. The second is used to find the minimal spanning tree in a graph.

9.1 Counting Trees

A commuter airline wishes to establish a network of three towns, Emily, Crosby and Brainerd. To accomplish this, it will link certain pairs of towns with nonstop service. However, it wants to do this so that:

- It is possible to travel between every pair of towns (perhaps changing planes).
- It has as few nonstop flights as necessary.

For example, it could establish nonstop service between Emily and Crosby and between Emily and Brainerd. Then to travel between Brainerd and Crosby, one would have to change planes in Emily. Or it could establish nonstop service between Emily and Crosby and between Crosby and Brainerd. Or it could establish nonstop service between Emily and Brainerd and between Brainerd and Crosby. These are the only three possibilities. We show them in Figure 9.1 below. Note that in each case, two nonstop flights are required.

These graphs are each trees as defined in Chapter 4. That is, they are connected graphs with no cycles, no loops and no multiple edges. We will call such a network of cities a *tree network*.

If the airline network had only two cities, then there is only one possible tree network and one nonstop flight, as shown in Figure 9.2

In Figure 9.3 we show two such tree networks for four cities.

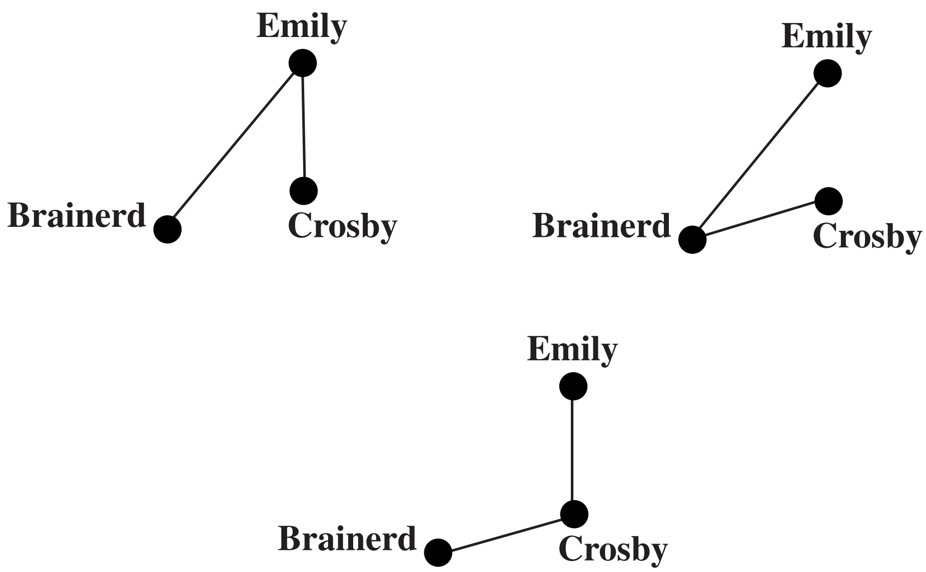


Figure 9.1: Three tree networks with three cities

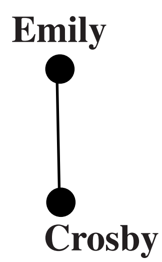


Figure 9.2: Two-city tree network

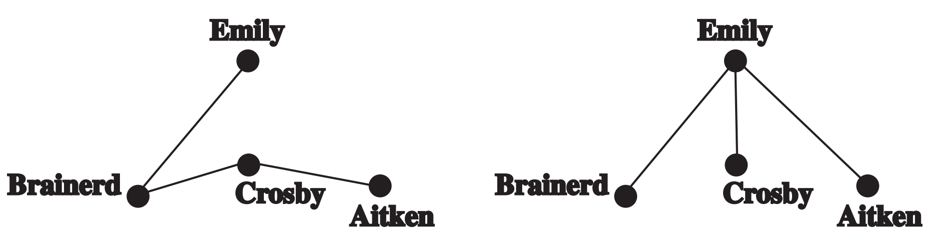


Figure 9.3: Two tree networks with four cities

Exercise 9.1.1. List all possible tree networks between the four towns, Emily, Crosby, Brainerd and Aitken. How many nonstop flights are there in each of these tree networks?

Exercise 9.1.2. Find at least six different tree networks between the five towns, Emily, Crosby, Brainerd, Aitken and Duluth. How many nonstop flights will each tree network require?

For five towns there are in fact 125 different tree networks.

Exercise 9.1.3. Make a conjecture for the number of tree networks between n towns. How many nonstop flights will each tree network require? For the second part of this exercise, recall from Chapter 4 that a tree with n vertices has $n-1$ edges.

We are now going to describe a way to "take apart" one of these tree networks. When we are finished, we will have a list of cities, instead of a tree network of connections between cities. But we will still be able to reconstruct our original tree network! The method for disassembling the tree network has much in common with the idea of "pruning," described in Chapter 4.

Let's look at the particular tree network on the five cities, Aitken, Brainerd, Crosby, Duluth and Emily shown in Figure 9.4.

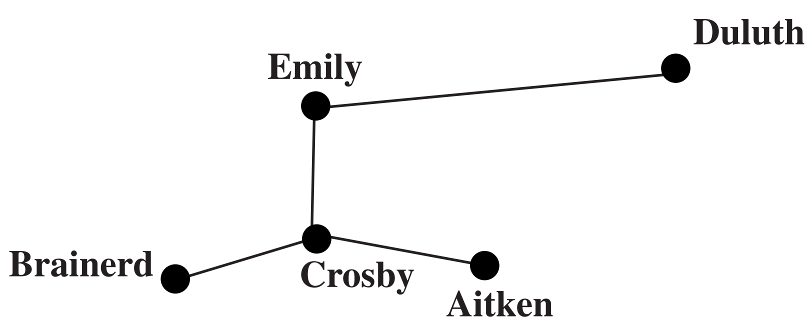


Figure 9.4: A five-city tree network

We know that this tree network is a tree, so there are terminal vertices, that is, towns connected to only one other town. Let's call these towns *terminal towns*. Let's find the alphabetically last terminal town: Duluth. We remove Duluth from the tree network and we write down in our list the town that was connected to Duluth: Emily. We now have a new tree network, shown in Figure 9.5.

Our list of cities so far consists of just Emily.

Now we repeat this process on the new tree network. The alphabetically last terminal town in the tree network in Figure 9.5 is now Emily. We remove

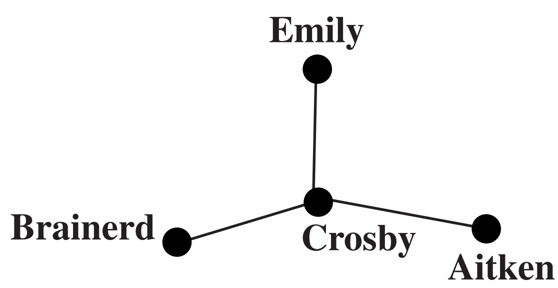


Figure 9.5: The reduced tree network

Emily and write down Crosby (the town Emily connects to). The new network is shown in Figure 9.6.

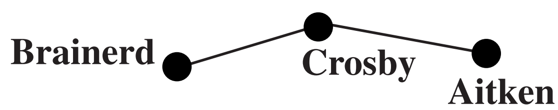


Figure 9.6: Further reduced tree network

The list of towns is now (Emily, Crosby).

We do this again with Figure 9.6, removing Brainerd and writing down Crosby. We now have the tree network in Figure 9.7 and the list of towns (Emily, Crosby, Crosby).

Figure 9.7: Final reduced tree network

We now have enough to reconstruct the entire network. In fact, all we need is the list (Emily, Crosby, Crosby). Here is why. Notice that the degree of each town is exactly one more than the number of times that town appears in the list. (Recall from Chapter 4 that the *degree* of a vertex is the number of edges at that vertex.) For example, Emily appears once in the list and has degree two. Aitken doesn't appear in the list and has degree one.

Exercise 9.1.4. Explain why the degree of each town is exactly one more than the number of times that town appears in the list.

So let's begin by drawing the towns and indicating their degrees, as in Figure 9.8.

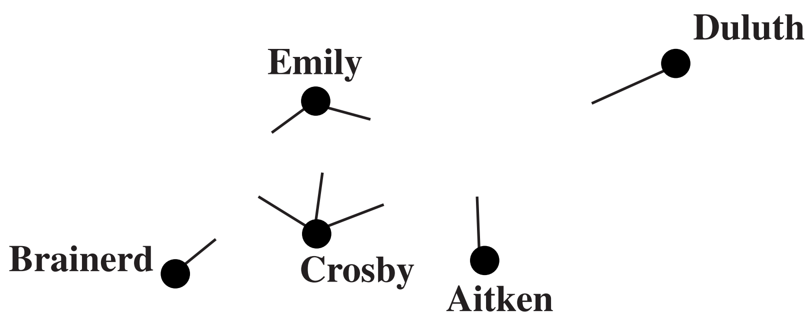


Figure 9.8: Degrees of cities

The alphabetically last terminal town (degree equal to 1) will be Duluth and from the way we constructed the list we know it must be connected to the first town in the list: Emily. So let's draw that connection in Figure 9.9.

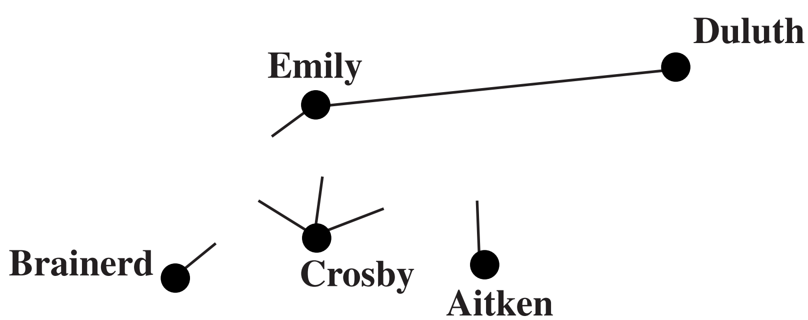


Figure 9.9: First edge

This uses up one of Emily's two connections. Emily now has one free connection, so it is now a terminal town, in fact, the alphabetically last terminal town. It must be connected to the next town in the list, Crosby. We draw that connection in Figure 9.10.

That reduces Crosby's free connections to two, so the alphabetically last terminal town is Brainerd, and it connects to the last town in the list, Crosby, as shown in Figure 9.11.

There are still two terminal towns left: Crosby (whose degree was reduced from three to two to one) and Aitken. So they must be connected, giving Figure 9.12, which is the tree network we started with.

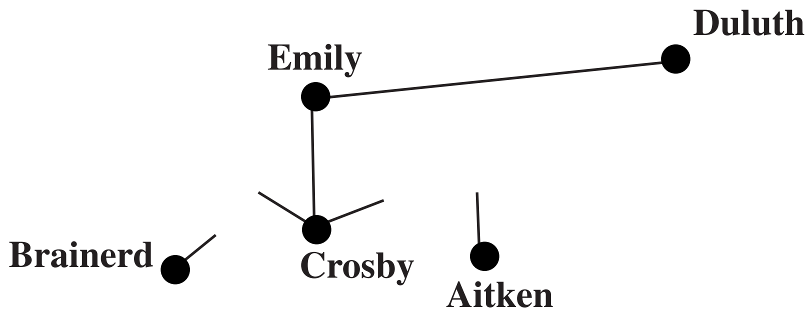


Figure 9.10: Two edges

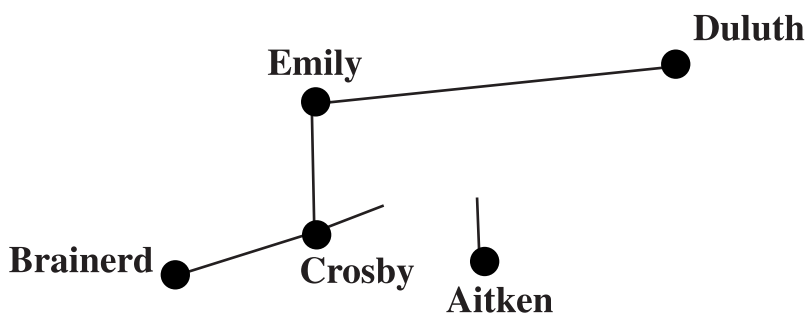


Figure 9.11: Three edges

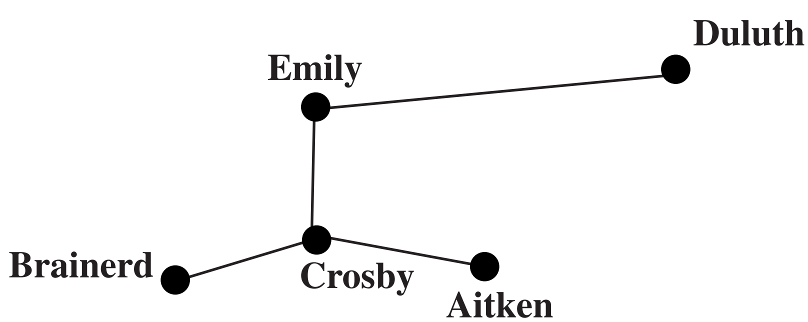


Figure 9.12: All edges restored

Here is another example, using six towns, Aitken, Brainerd, Crosby, Duluth, Emily, and Fargo. We start with a list of four towns (remember that when we stripped down the network, we stopped when two towns were left): (Crosby, Fargo, Emily, Fargo). Since Fargo appears twice in the list, Fargo must have degree three in the tree. Similarly, Brainerd has degree one, and so on. Our starting tree network is shown in Figure 9.13.

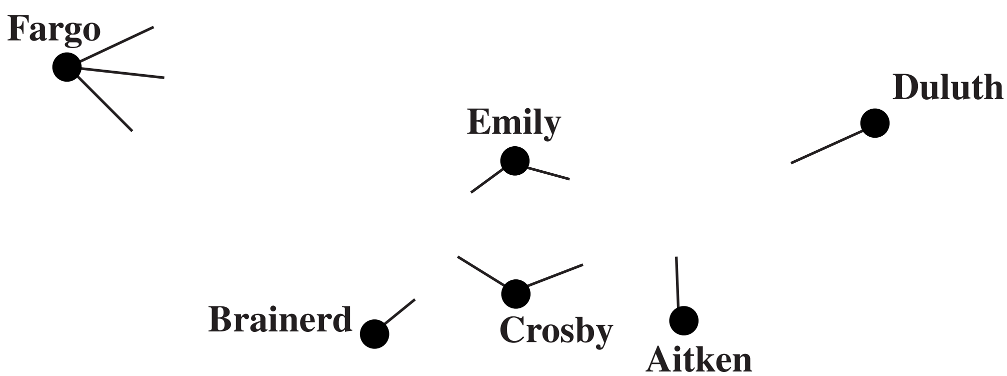


Figure 9.13: Towns with degrees

The last terminal town is Duluth, which must connect to Crosby, as shown in Figure 9.14.

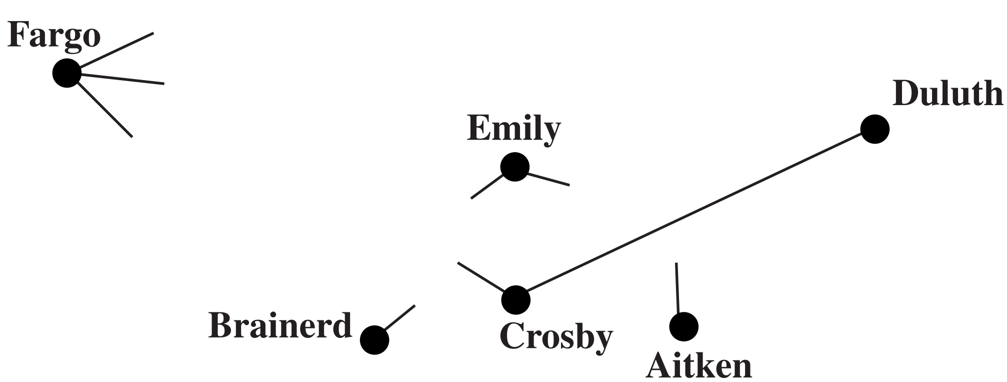


Figure 9.14: First edge

Crosby is now a terminal town. It is also the last terminal town. Crosby must connect to Fargo, which now has degree two, as shown in Figure 9.15.

Now the last terminal town is Brainerd, which must connect to Emily. Emily now has degree one, shown in Figure 9.16.

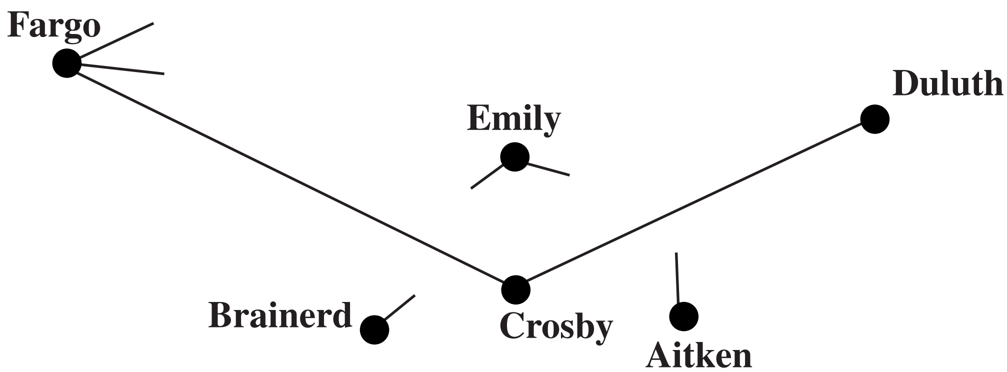


Figure 9.15: Second edge

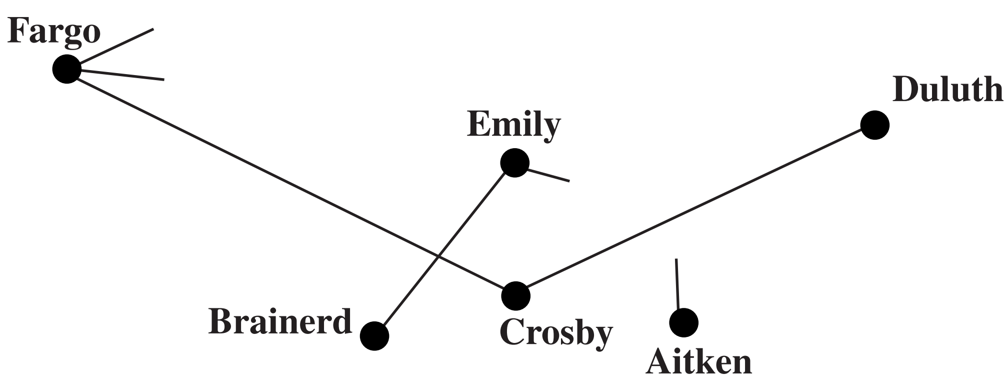


Figure 9.16: Third edge

The last terminal town is now Emily, and it connects to Fargo. Fargo now has degree one. See Figure 9.17.

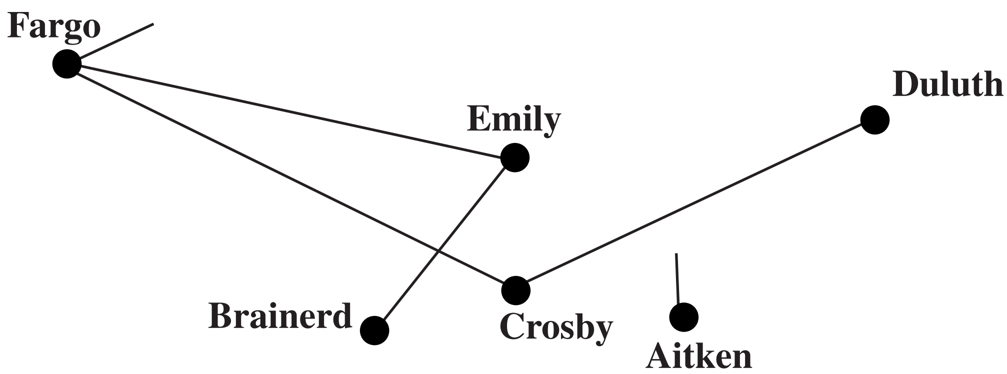


Figure 9.17: Fourth edge

The only two terminal towns left are Fargo and Aitken, so we connect them, as shown in Figure 9.18.

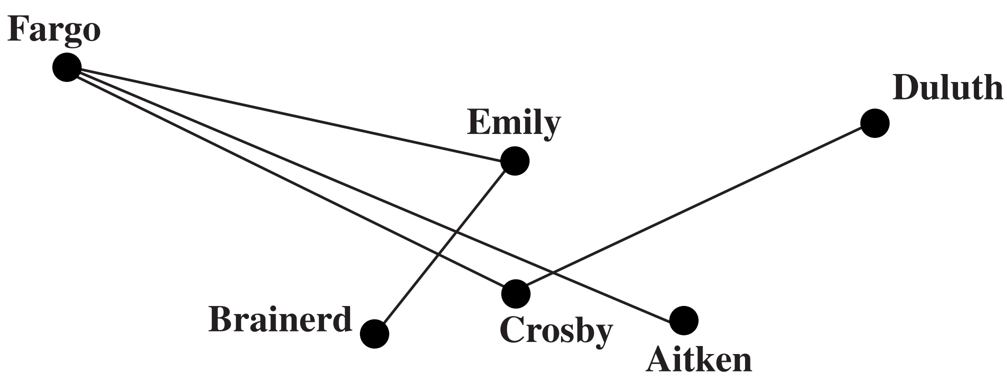


Figure 9.18: Final tree network

Exercise 9.1.5. Figure 9.19 shows a tree network on 8 towns. Construct the corresponding list of six towns.

Exercise 9.1.6. Figure 9.20 shows another tree network on 8 towns. Construct the corresponding list of six towns.

Exercise 9.1.7. Figure 9.21 shows yet another tree network on 8 towns. Construct the corresponding list of six towns.

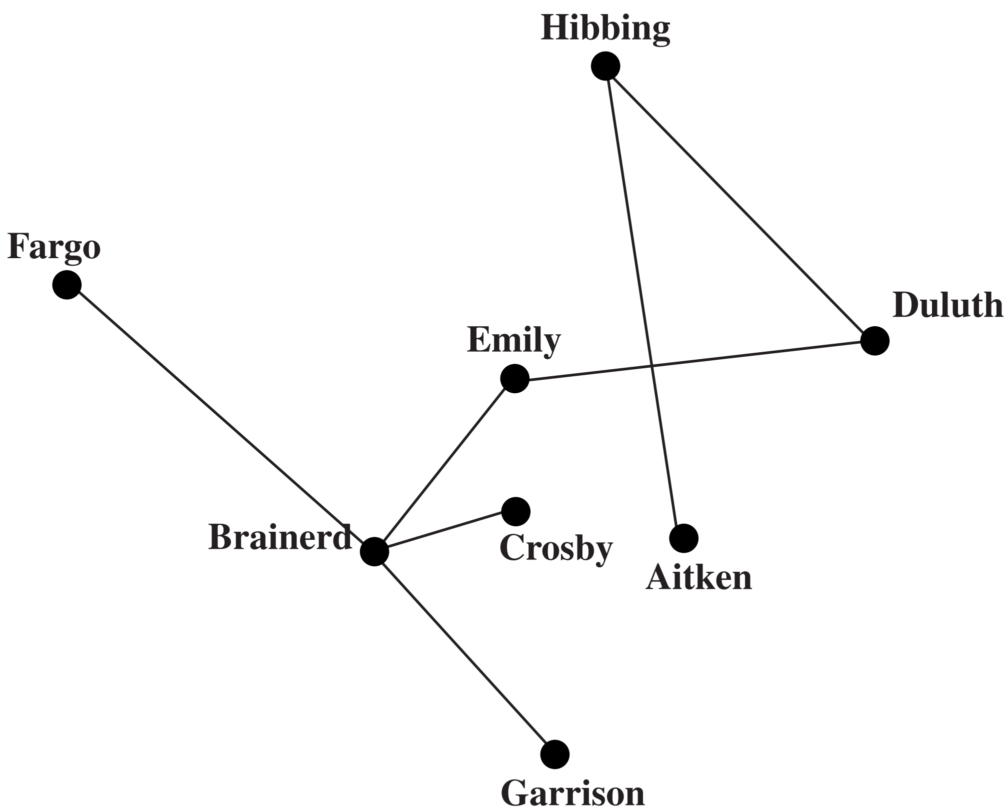


Figure 9.19: Another tree network

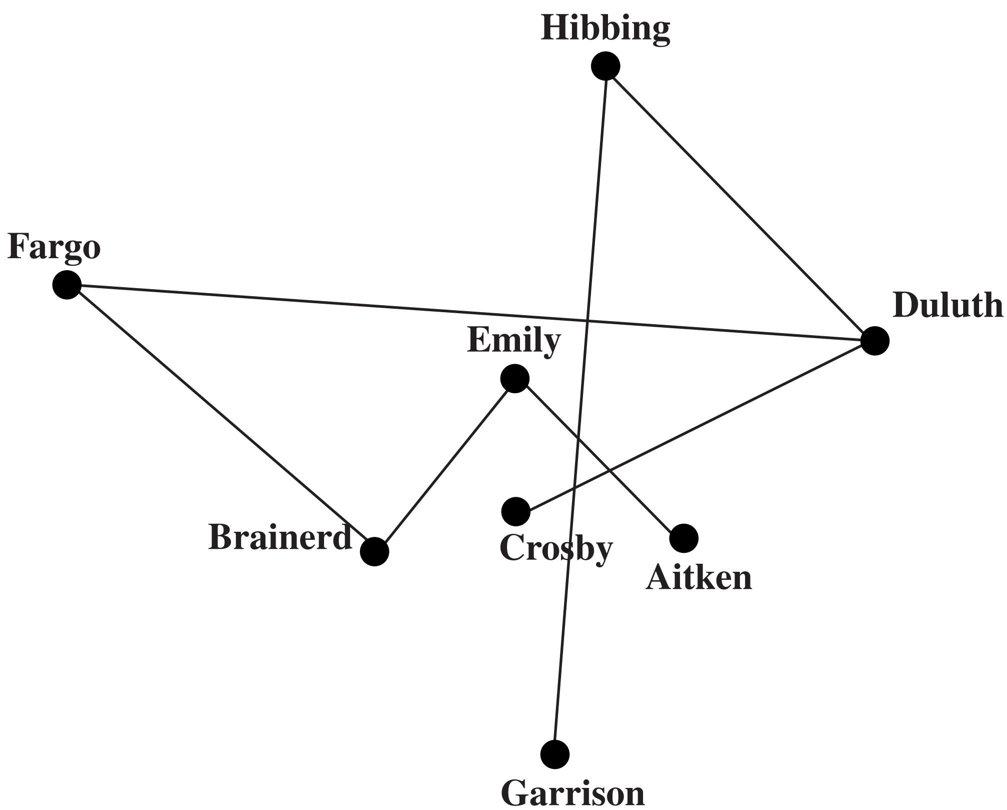


Figure 9.20: Still another tree network

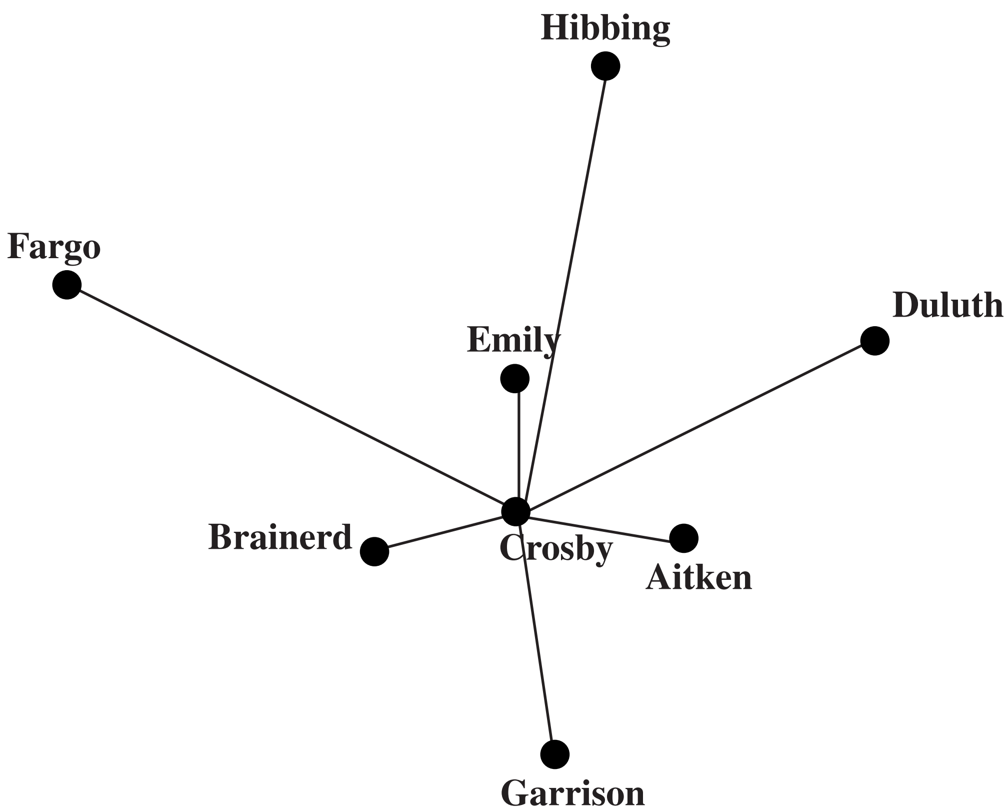


Figure 9.21: Yet another tree network

Exercise 9.1.8. Figure 9.22 shows another tree network on 8 towns. Construct the corresponding list of six towns.

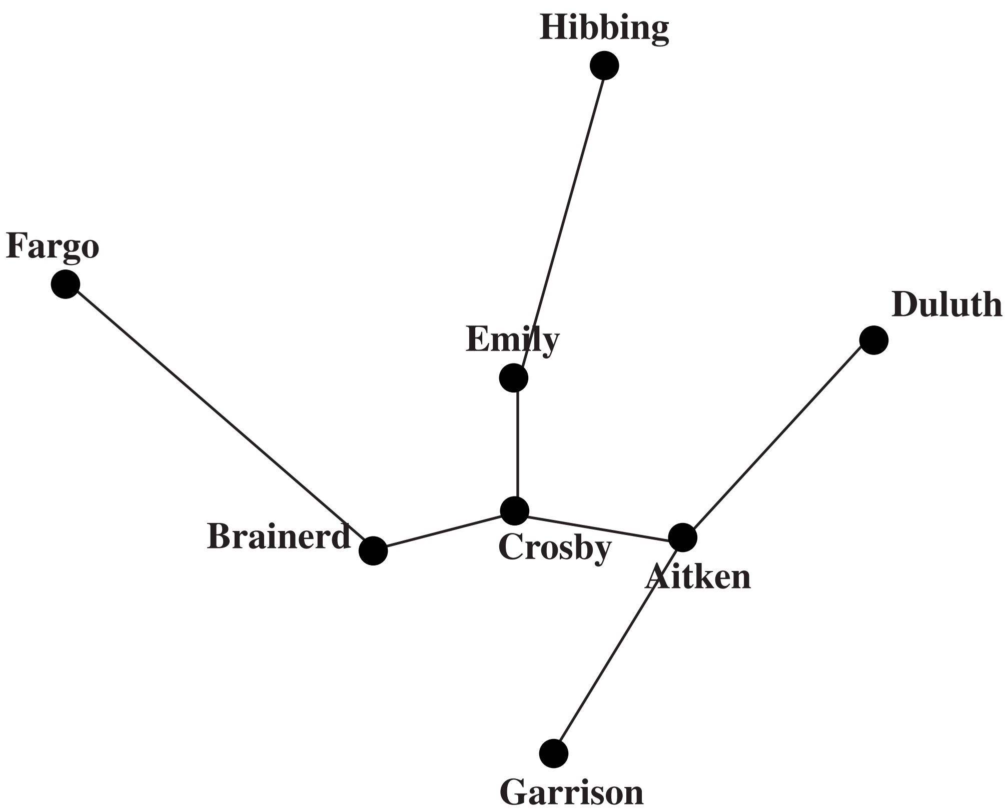


Figure 9.22: Another tree network

Exercise 9.1.9. Here is a list of six towns: (Emily, Fargo, Fargo, Hibbing, Duluth, Fargo). Construct the corresponding tree network on the eight towns, Aitken, Brainerd, Crosby, Duluth, Emily, Fargo, Garrison and Hibbing.

Exercise 9.1.10. Here is a list of seven towns: (Hibbing, Hibbing, Fargo, Hibbing, Emily, Fargo, Isle). Construct the corresponding tree network on the nine towns, Aitken, Brainerd, Crosby, Duluth, Emily, Fargo, Garrison, Hibbing and Isle.

Exercise 9.1.11. Here is a list of six towns: (Duluth, Brainerd, Fargo, Aitken, Garrison, Fargo). Construct the corresponding tree network on the eight towns, Aitken, Brainerd, Crosby, Duluth, Emily, Fargo, Garrison and Hibbing.

Exercise 9.1.12. How many tree networks are there on the eight towns Aitken, Brainerd, Crosby, Duluth, Emily, Fargo, Garrison and Hibbing? Hint: count lists of towns instead of tree networks.

Exercise 9.1.13. How many of the tree networks on eight towns Aitken, Brainerd, Crosby, Duluth, Emily, Fargo, Garrison and Hibbing are there in which Emily has degree 3? Hint: if Emily has degree 3, how many times does it appear in the list?

Exercise 9.1.14. How many of the tree networks on the eight towns Aitken, Brainerd, Crosby, Duluth, Emily, Fargo, Garrison and Hibbing are there in which Emily and Garrison have degree 3, Crosby and Brainerd have degree 2, and the remaining towns are terminal towns?

Exercise 9.1.15. How many of the tree networks on the eight towns Aitken, Brainerd, Crosby, Duluth, Emily, Fargo, Garrison and Hibbing are there in which two towns have degree 3, two towns have degree 2, and the remaining four towns are terminal towns?

Exercise 9.1.16. How many of the tree networks on the eight towns Aitken, Brainerd, Crosby, Duluth, Emily, Fargo, Garrison and Hibbing are there in which Emily has degree at least 3?

Exercise 9.1.17. How many of the tree networks on the eight towns Aitken, Brainerd, Crosby, Duluth, Emily, Fargo, Garrison and Hibbing are there in which Emily and Garrison each have degree at least 3?

Tree networks are called *labeled trees* because the vertices have labels (the names of the towns, in our case). The number of labeled trees is given by Cayley's formula.

Theorem 18 (Cayley's Formula)**.** *The number of labeled trees with n vertices is n^{n-2}.*

The correspondence between labeled trees and lists of vertices is called the *Prüfer correspondence.*

Exercise 9.1.18. Use the ideas above to prove Cayley's formula. Hint: count label-lists instead of trees.

Exercise 9.1.19. Use the Prüfer correspondence to find a formula for the number of labeled trees on n vertices where one particular vertex has degree k.

9.2 Minimum Spanning Trees

Airlines pick their tree networks usually based around a hub city where their facilities are located. In other contexts, networks are chosen to minimize the total distance within the network. For example, we might wish to lay out an electrical network which minimizes the amount of wire we use. Here is another example.

Figure 9.23 shows a street map of Snowtown, Minnesota. The numbers on the edges reflect the relative cost of plowing that street after a snowstorm.

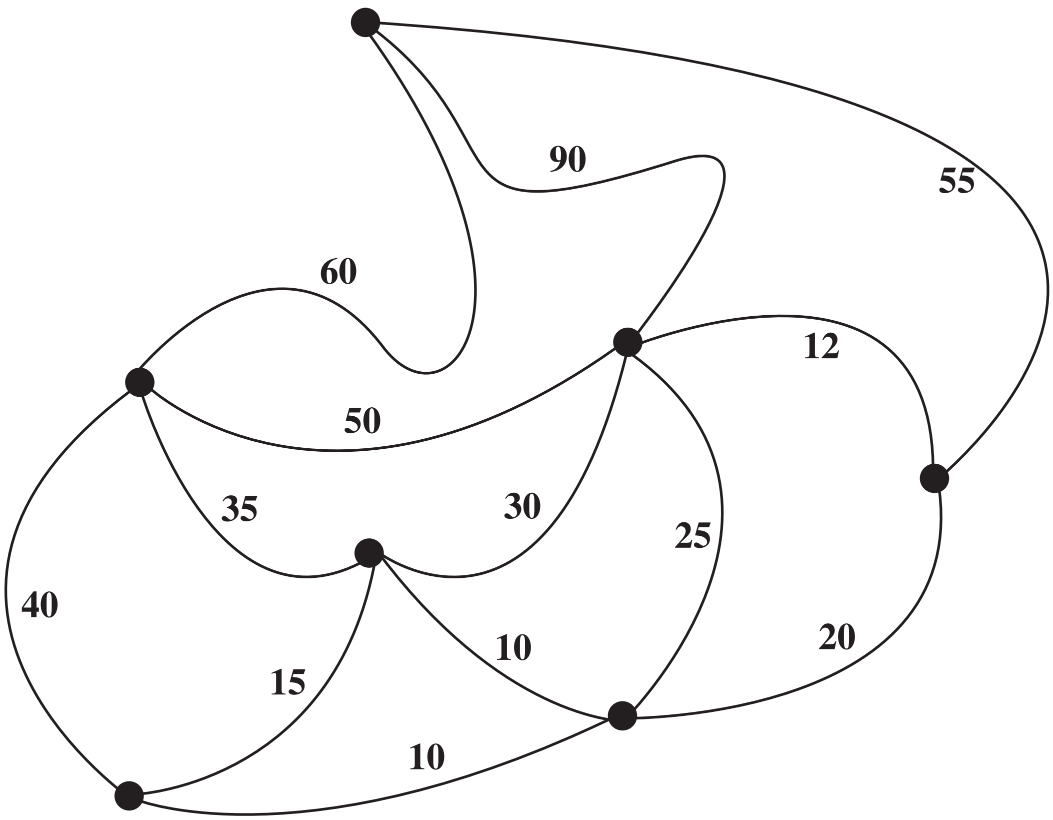


Figure 9.23: Snowtown, Minnesota

After a snowstorm, the snowplows only plow enough of the streets so that every intersection is reachable from every other intersection. For example, Figure 9.24 shows one possible way the streets could be plowed. The total cost of plowing the streets in this way is 192.

Exercise 9.2.1. Find another way of plowing the streets which is cheaper than 192.

Exercise 9.2.2. Find the cheapest way of plowing the streets so that every intersection is reachable from every other intersection.

A *spanning tree* is a subgraph of a connected graph which is a tree. For

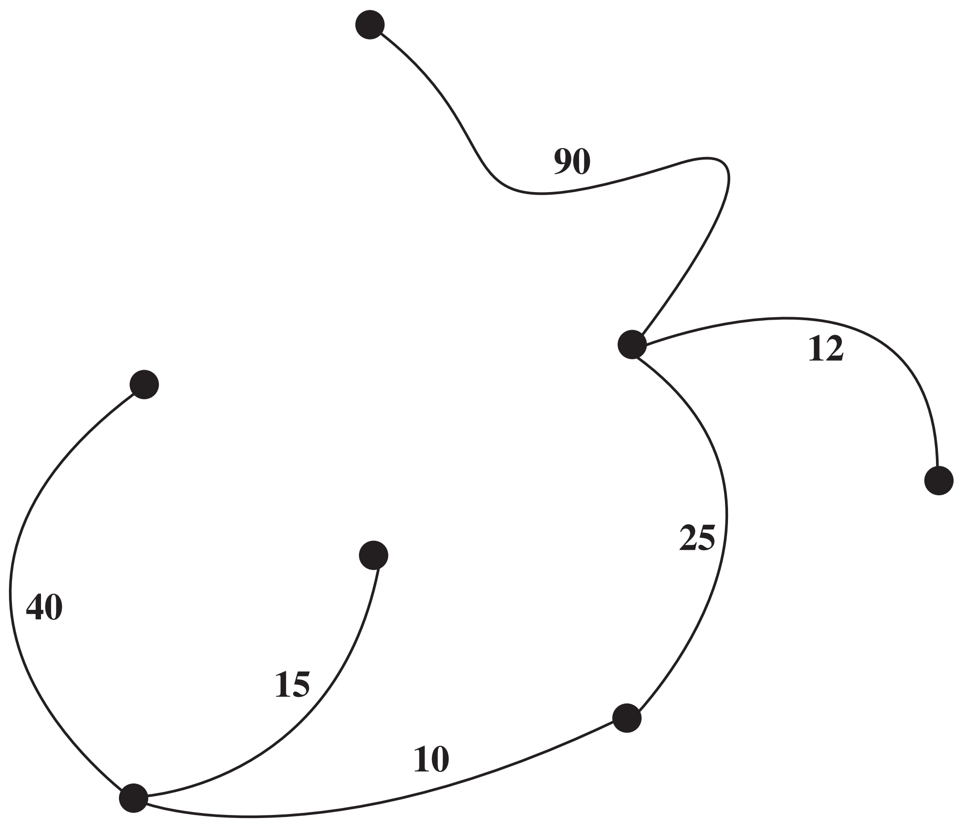


Figure 9.24: Streets plowed in Snowtown, Minnesota

example, the snowplowed streets in Figure 9.24 form a spanning tree of the graph in Figure 9.23. Your solutions to Exercise 9.2.1 and Exercise 9.2.2 were also spanning trees.

There are several methods for finding a cheapest (or *minimum cost*) spanning tree. The most direct is called the *greedy algorithm*. This algorithm proceeds as follows. First, the cheapest edge is found and put into the spanning tree. Then, the next cheapest edge is added (assuming its addition does not create a cycle). Then the next cheapest, again assuming its addition does not create a cycle. This continues until a tree is formed.

For example, in Figure 9.25, the edges with costs 1, 2, 3, 5 and 9 are added, in that order.

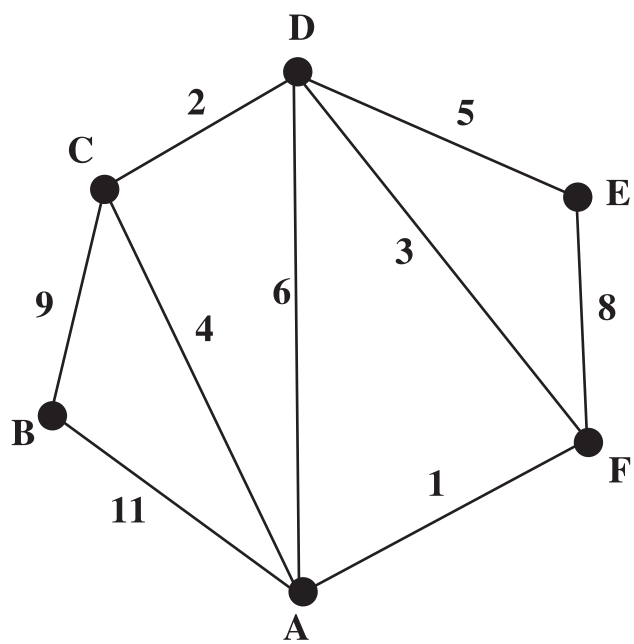


Figure 9.25: A graph with costs

Exercise 9.2.3. Apply the greedy algorithm to Figure 9.23. You should get the same spanning tree that you obtained in Exercise 9.2.2.

Although it may seem reasonable that the greedy algorithm produces a minimum cost spanning tree, this does requires proof. While we will not go through this proof, the following exercise gives an idea of the kind of arguments involved.

Exercise 9.2.4. If all the edges in a graph have different costs, prove that the minimum cost spanning tree must use the cheapest edge. Hint: argue by contradiction. Suppose the minimum cost spanning tree does not use the cheapest edge. Show that some edge in the minimum cost spanning tree can be replaced by the cheapest edge to obtain an even cheaper spanning tree.

Exercise 9.2.5. Use the greedy algorithm to find a minimum cost spanning tree in the graph in Figure 9.26.

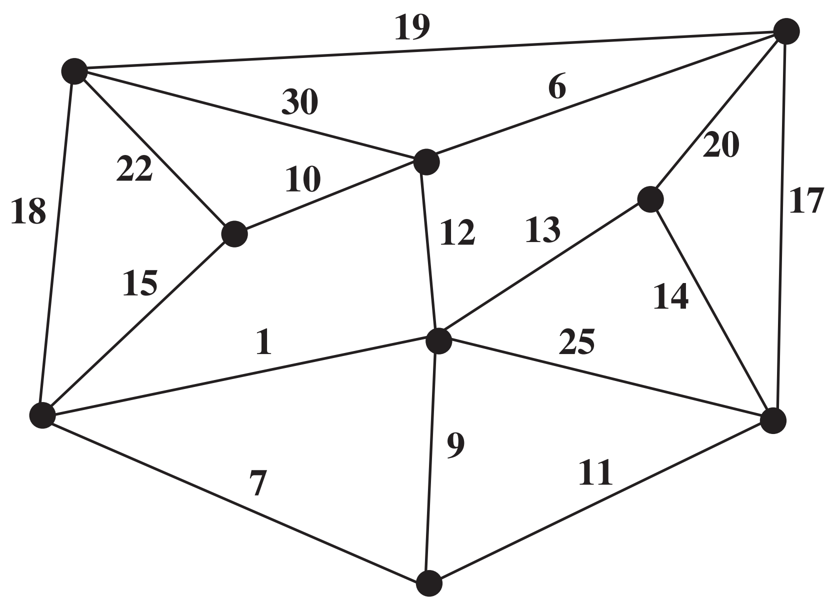


Figure 9.26: Another graph with costs

Exercise 9.2.6. Starting with the complete graph K_n, with vertices labeled 1, 2, ..., n, place costs on the edges as follows. If e is the edge between vertex i and vertex j, then the cost of e is $|i - j|$. For example, K_4 with costs is shown in Figure 9.27. Describe the minimum spanning tree for K_n with these weights.

Exercise 9.2.7. Starting with the complete graph K_n, with vertices labeled 1, 2, ..., n, place costs on the edges as follows. If e is the edge between vertex i and vertex j, then the cost of e is $i + j$. For example, K_4 with costs is shown in Figure 9.28. Describe the minimum spanning tree for K_n with these weights.

9.3 Rooted Trees and Forests

If we decide that one of the vertices of a tree is special, the tree becomes *rooted*. The special vertex is called the *root*. Some books draw rooted trees with the

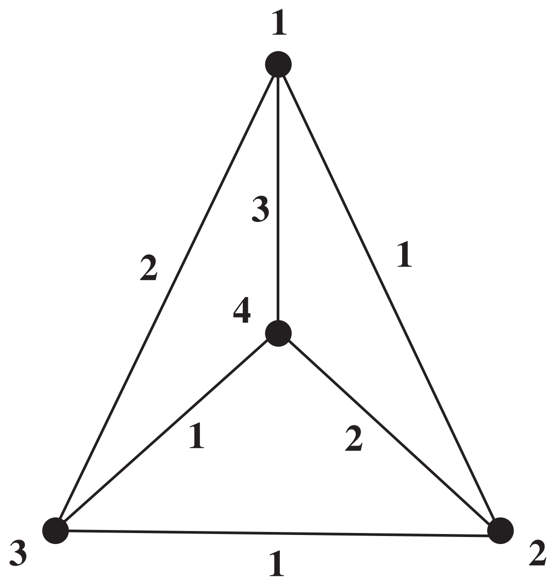


Figure 9.27: K_4 with costs

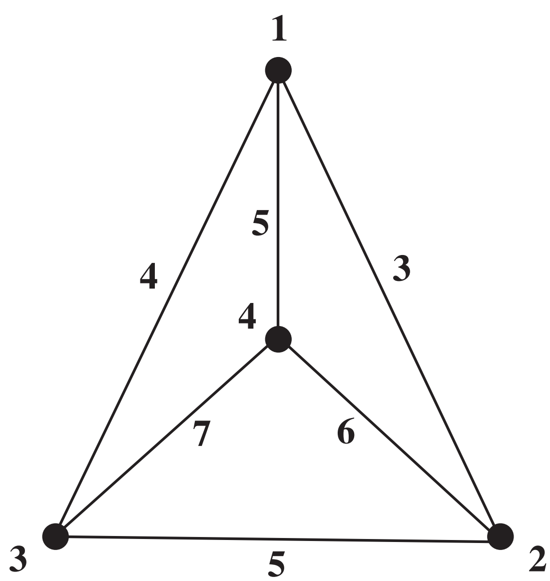


Figure 9.28: Another K_4 with costs

root at the bottom (like a real tree). Others "grow" their trees from left to right. We will place the root at the top and grow the tree downward. An example is shown in Figure 9.29.

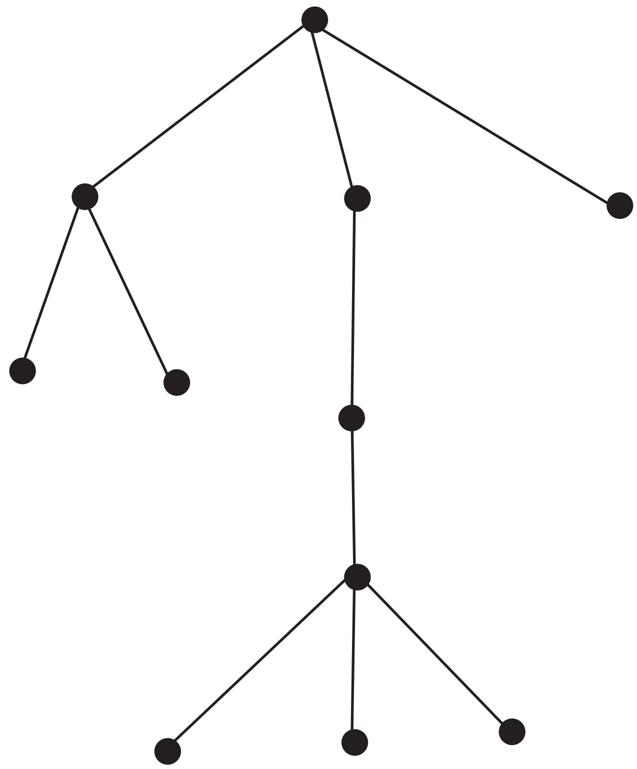


Figure 9.29: Rooted tree

You are probably already familiar with such trees. Family trees are an example of rooted trees. In fact, we use family terminology when we refer to vertices in a rooted tree. Thus, we call vertices *children*, *parents*, or *siblings* of other vertices.

We also use "tree" terminology: *leaves* and *branches*. A collection of rooted trees is called a *forest*.

One of the most familiar examples of rooted trees is outline structures. Consider, for example, this partial outline of mushrooms:

I Non-gilled
    A Sac Fungi
        1 Morels
            a Morchella Esculenta
            b Morchella Conica

        2 Lorchels
        3 Cup Fungi
    B Club Fungi
        1 Chanterelles
        2 Boletes
            a Boletes Edulis
            b Boletes Mirabilis
            c Slippery Jack
II Gilled
    A Club Fungi
        1 Amanitas
            a Amanita Francheti
            b Amanita Mirabilis
            c Amanita Phalloides
            d Amanita Muscaria
        2 Agaricus
        3 Inkycaps
III Puffballs
    A Gastromycetes
        1 Stinkhorns
        2 Puffballs

This corresponds to the rooted tree in Figure 9.30.

This leads to the following question about rooted trees: are the two trees in Figure 9.31 the "same" or "different?"

For outline structures, usually we want these trees to be different. Such trees are called *planar rooted trees.* In some other applications, we consider them the same, and then they are called simply rooted trees. In Figure 9.32 are shown all the planar rooted trees with four vertices.

Exercise 9.3.1. Draw all the planar rooted trees with five vertices.

Exercise 9.3.2. Show that the number of planar rooted trees on n vertices is C_{n-1}, the Catalan number given in Chapter 3. Hint: establish a one-to-one correspondence between planar rooted trees and outlines.

Planar forests consist of one or more planar rooted trees, with the trees drawn left-to-right, and where a different order of trees gives a different planar forest. One example of a planar forest is shown in Figure 9.33. The planar forest in Figure 9.34 is different, even though it has the same planar rooted trees in it.

Exercise 9.3.3. Show that the number of planar forests on n vertices is the same as the number of planar rooted trees on $n+1$ vertices. Hint: remove the root of the planar rooted tree.

If all the vertices of a rooted tree have labels (see Figure 9.35), the tree is called *a labeled rooted tree.*

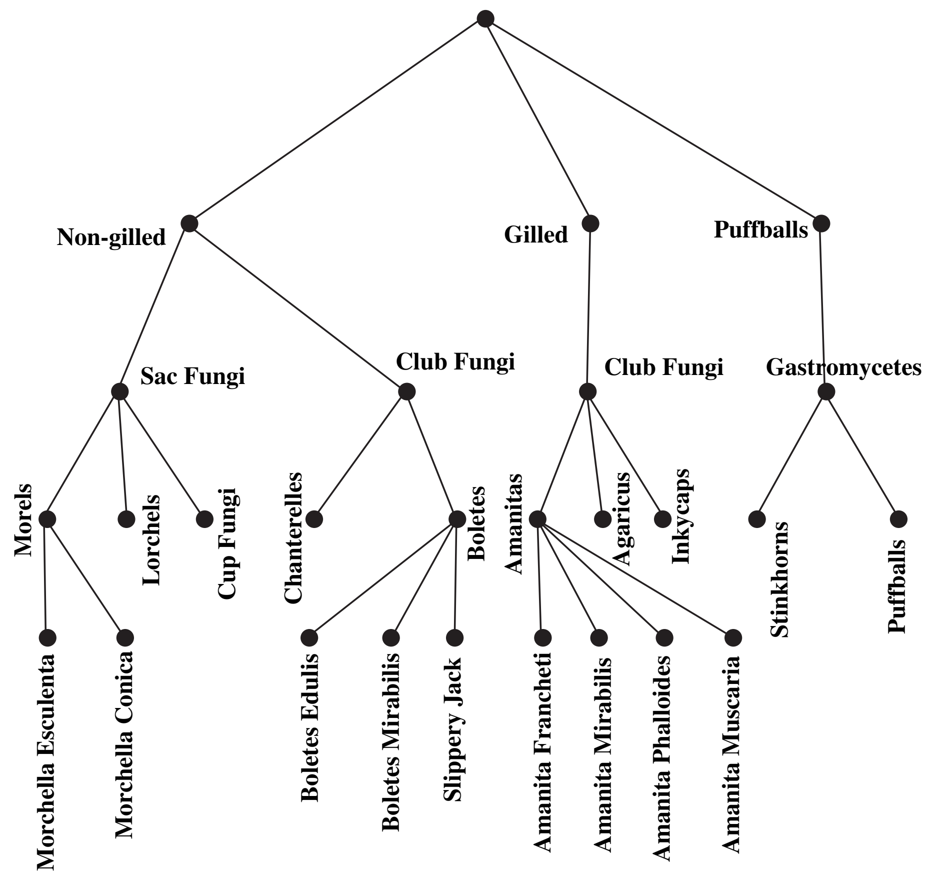


Figure 9.30: Tree of mushrooms

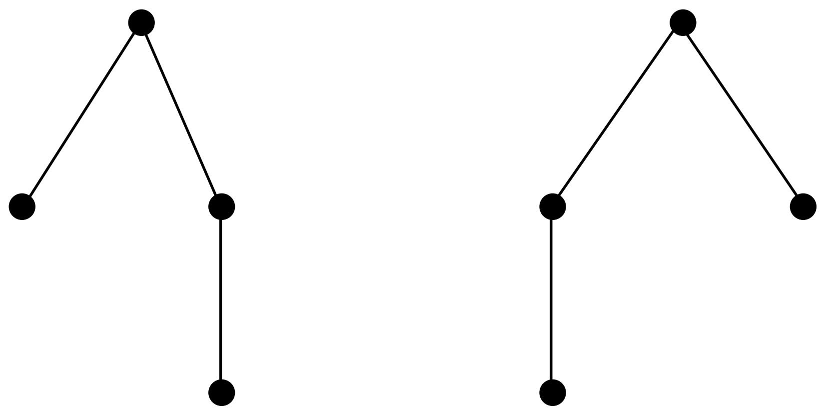


Figure 9.31: Same tree?

Exercise 9.3.4. Use Cayley's formula (Theorem 18) for labeled trees to show that the number of labeled rooted trees on n vertices is n^{n-1}.

A *labeled forest* is a collection of one or more labeled rooted trees, where all the labels are different. An example of a labeled forest is shown in Figure 9.36. Unlike planar forests, the order of the trees in a labeled forest is not important.

Exercise 9.3.5. Use Cayley's formula (Theorem 18) for labeled trees to show that the number of labeled forests on n vertices is $(n+1)^{n-1}$. Hint: establish a one-to-one correspondence between labeled trees and labeled forests by removing the vertex with the largest label.

Exercise 9.3.6. How many labeled forests are there with 12 vertices and 3 trees?

A special kind of planar rooted tree is a *binary tree.* Every vertex of a binary tree has either zero or two children. Binary trees appear in many computer science settings. For example, they organize data keys for rapid access and sorting. Such trees are sometimes called "search trees." You are probably most familiar with binary trees in tournament settings. For instance, the 1994 Super bowl Tournament was described by the binary tree in Figure 9.37

Exercise 9.3.7. Show that the number of leaves in a binary tree is one more than the number of non-leaves. Hint: in a tournament, every game has a loser and every team except one loses exactly one game.

Exercise 9.3.8. Explain why binary trees always have an odd number of vertices.

Figure 9.38 shows all the binary trees with seven vertices.

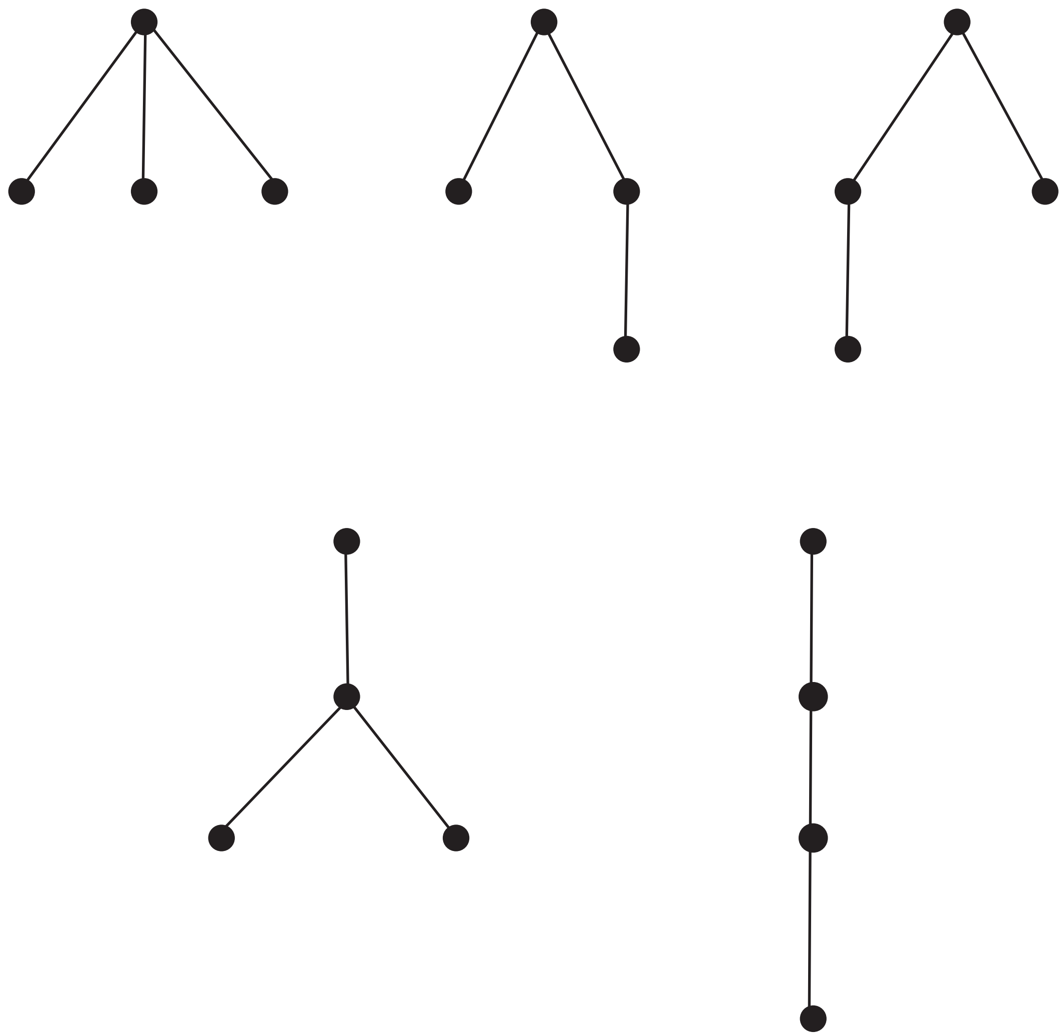


Figure 9.32: Planar rooted trees

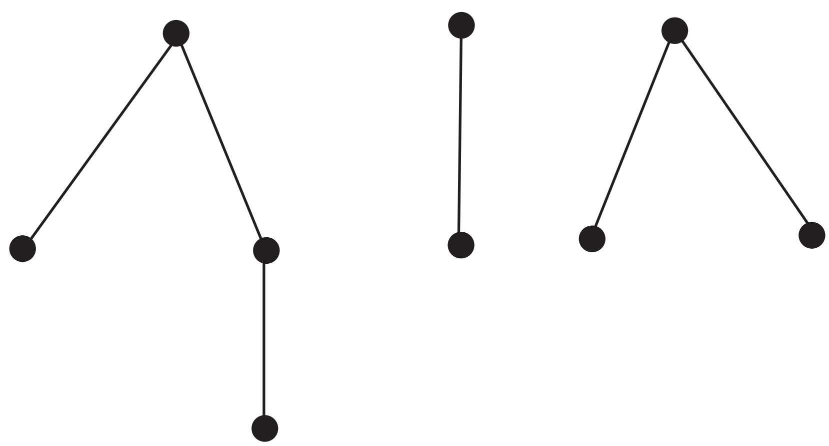


Figure 9.33: A planar forest

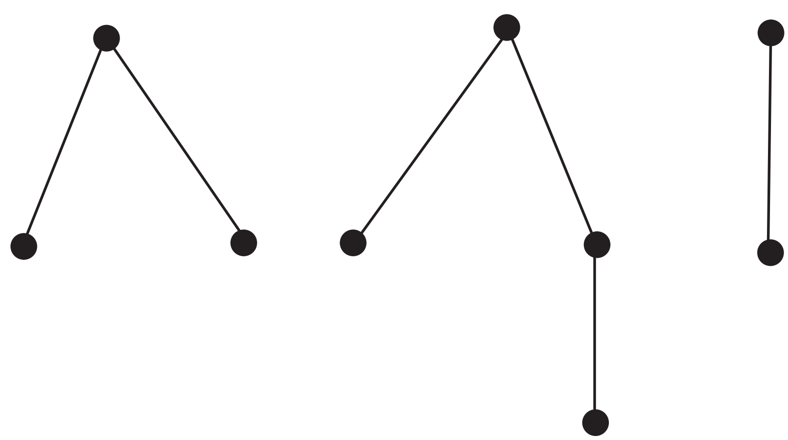


Figure 9.34: A different planar forest

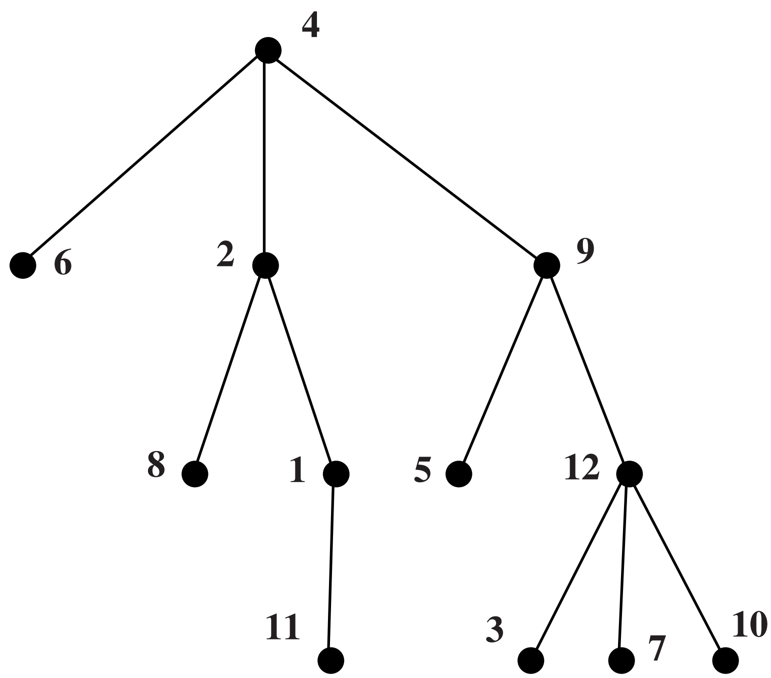


Figure 9.35: Labeled rooted tree

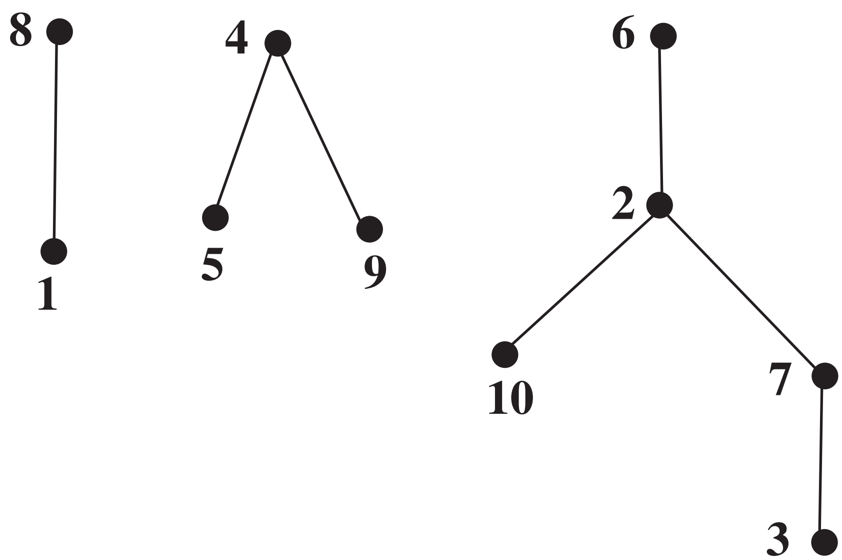


Figure 9.36: A labeled forest

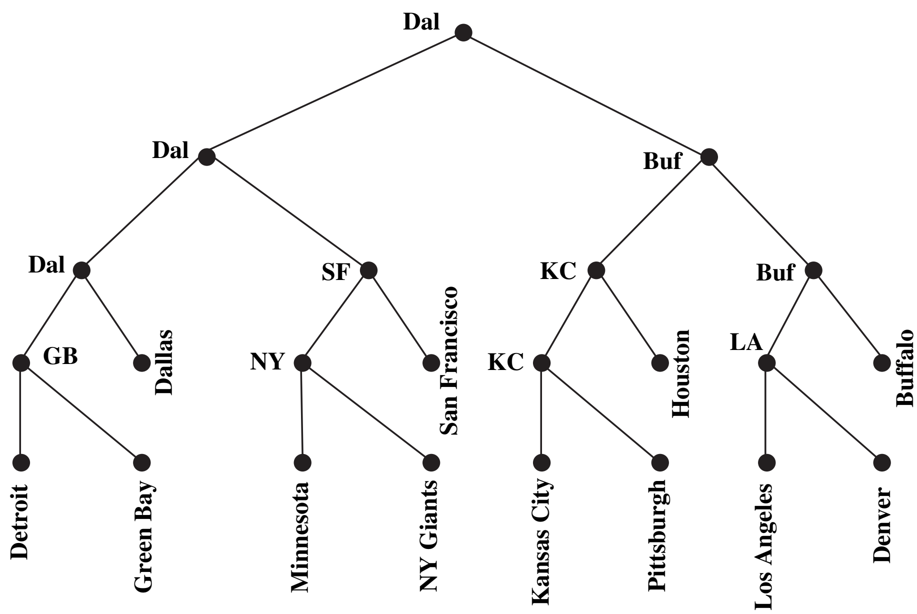


Figure 9.37: Superbowl tournament

Exercise 9.3.9. Draw all the binary trees with nine vertices.

Exercise 9.3.10. Show that the number of binary trees with $2n+1$ vertices is C_n, a Catalan number. Hint: establish a one-to-one correspondence between binary trees and polygon triangulations (described in Chapter 3).

Rooted trees provide a good way of organizing information for problem-solving. For example, suppose we wish to solve this problem: we want to form a committee of five people, by choosing from four women and six men. We want the committee to have at least two women, and Fred and Deb will not serve on the committee together. This situation is described in Figure 9.39.

By summing the number of possibilities at each leaf, we get our answer.

Exercise 9.3.11. Use the tree in Figure 9.40 to help you solve this counting problem: A certain math class has 12 women and 8 men. Two of the women and two of the men are left-handed. How many ways can you select 6 students so that exactly one is left-handed and at least four are women?

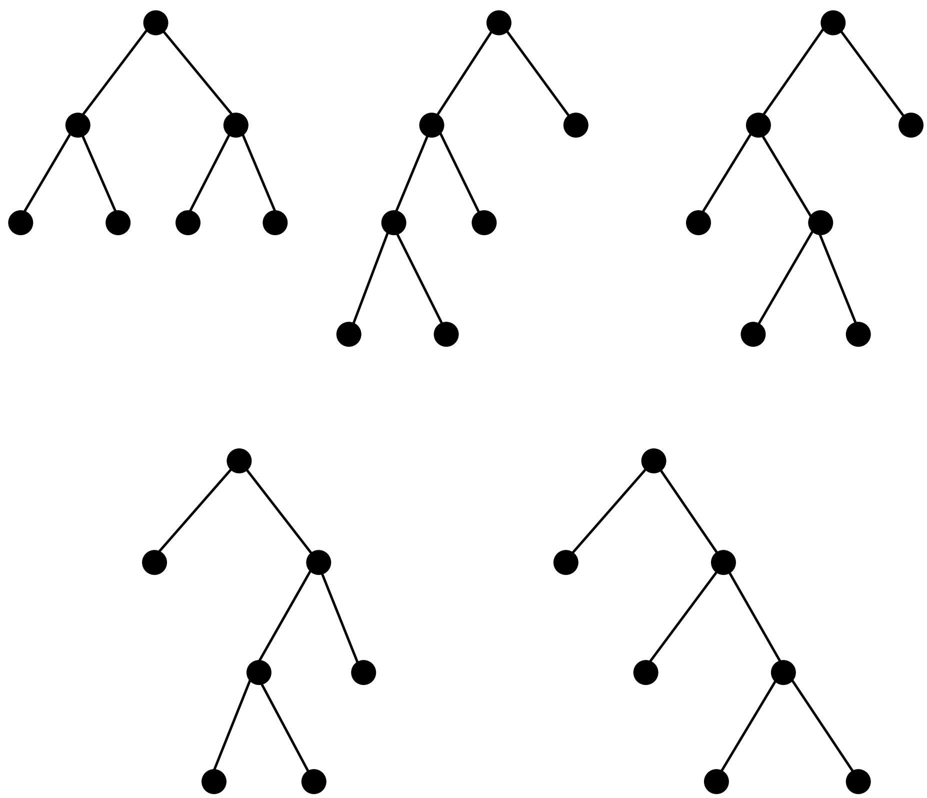


Figure 9.38: Binary trees

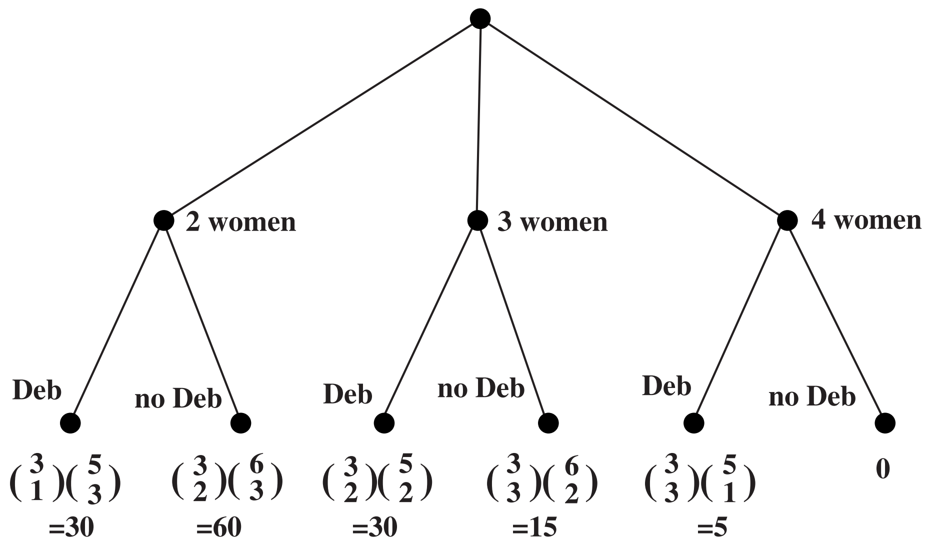


Figure 9.39: A counting problem

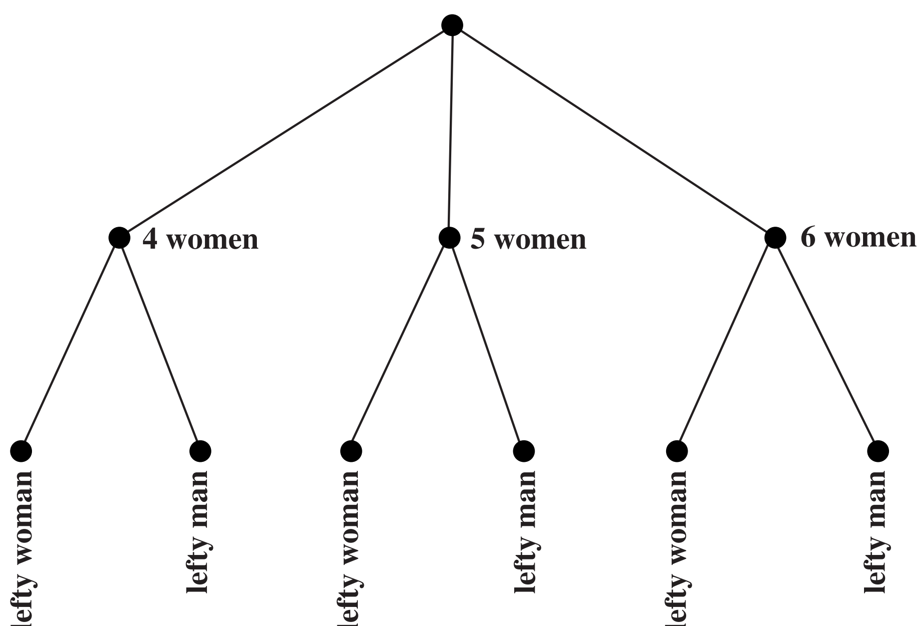


Figure 9.40: Another counting problem

Chapter 10

Real and Complex Numbers

In this chapter we present some of the important properties of the real and complex numbers. We include some of the things which distinguish the real numbers from the integers and the rationals. We describe various sizes of “infinity.” We show how to extend number systems into larger systems. Finally we state some classical non-constructibility results.

10.1 Irrational Numbers

Let’s start by reviewing some of the results from Chapter 5. In that chapter we learned how the integer number system was expanded to include quotients. We called that new number system the *rational numbers*, and we used $\mathbb{Q}$ to denote them. In that chapter, we learned that rational numbers can be represented in one of two ways:

i. A number is a rational number if it can be written in the form a/b, where a and b are integers.

ii. A rational number can be represented as a repeating or terminating decimal.

We also saw in Chapter 5 that the rational numbers satisfied a list of axioms. Each number system which satisfies Axioms A-1 to A-5, M-1 to M-5 and D-1 is called a *field*. We have already seen several examples of fields. For example, $\mathbb{Q}$ is a field. Also, expressions of the form polynomial divided by polynomial make up a field. The integers and polynomials (even with real coefficients) are not fields—they both lack Axiom M-5, the multiplicative inverse axiom.

Exercise 10.1.1. Complete the following: arithmetic mod n is a field if and only if . . . .

Fields which also satisfy the order axioms O-1 to O-4 are called *ordered fields*. The rationals are an ordered field.

Exercise 10.1.2. Find a rational number between 3/4 and

$$3/4 + 1/1000000000000000.$$

Exercise 10.1.3. Show that between any two rational numbers there is another rational number.

Exercise 10.1.3 shows that the rational numbers are "dense." Nevertheless, it is easy to construct numbers which are not rational.

Suppose we take the point of view that we want our number system to consist of all possible (infinite or finite) decimal representations. Let

$$x = 0.12112111211112\ldots,$$

where the "..." means that the strings of 1's are separated by single 2's, and that the next string of 1's is one longer than the preceding string.

Exercise 10.1.4. By showing that x does not have a repeating sequence and does not terminate, explain why x is not rational.

Exercise 10.1.5. Find at least two other numbers which are not rational.

Exercise 10.1.6. Find a number which is not rational and which lies between 3/4 and

$$3/4 + 1/1000000000000000.$$

We will call all the numbers which have a representation as an infinite or finite decimal the *real numbers*. Be very careful with the word "real." It has a specific mathematical meaning when used in this context. We denote the set of real numbers with $\mathbb{R}$.

Real numbers which are not rational are called *irrational*. Since we can add, subtract, multiply and divide (by nonzero amounts) real numbers, the real numbers form a field, in fact, an ordered field, which include the rational numbers as a *subfield*. However, the irrationals do not form a subfield, as will will note shortly.

If we write $\mathbb{I}$ to denote the irrational numbers, then, symbolically,

$$\mathbb{R} = \mathbb{Q} \cup \mathbb{I}.$$

Exercise 10.1.7. What kind of numbers do calculators produce, rational or irrational?

That there are real numbers which are not rational is transparent from our definition of reals as numbers having a decimal representation, and from the description of rationals as those numbers with repeating or terminating decimal representations. Not surprisingly, from this point of view, there are many more irrationals than rationals, a fact which will be proved in Section 10.7. But also surprisingly, showing *specific* numbers are irrational can be quite difficult.

The mathematical constant π was not shown to be irrational until the 18th century, and its proof only appears in advanced mathematics courses. The natural log base, e, is also irrational, a fact which is sometimes proved in a calculus class.

An important class of irrational numbers are certain roots, and more generally, zeros of polynomials. For instance, $\sqrt{2}$ is irrational. This fact has a famous proof, which we now outline.

Let's look at the equation $x^2 = 2$. If x were a rational number, say $x = \frac{m}{n}$, then $m^2 = 2n^2$. Let's look again at an exercise from Chapter 5.

Exercise 10.1.8. Suppose m and n are two integers, both ≥ 1. Is it possible for $m^2 = 2n^2$? Explain why this means x cannot be rational.

Exercise 10.1.9. Use a similar argument to show $\sqrt{3}$ is not rational. Show $\sqrt[3]{2}$ is not rational.

Exercise 10.1.10. Show $\sqrt{2} + \sqrt{3}$ is not rational. Hint: if $\sqrt{2} + \sqrt{3}$ were rational, then its square would be rational.

As noted earlier, both the rationals and the reals are fields.

Exercise 10.1.11. Is the sum of two irrationals always irrational? If they are, give a reason. If not, give an example of two irrationals which add to a rational.

Exercise 10.1.12. Is the product of two irrationals always irrational? If they are, give a reason. If not, give an example of two irrationals which multiply to a rational.

Exercise 10.1.13. Do the irrationals form a subfield of the reals? Why or why not?

Exercise 10.1.14. Is the sum of a rational and an irrational (a) always rational, (b) always irrational, or (c) either rational or irrational. If your answer is (a) or (b), give a reason. If it is (c), give examples of each case.

Exercise 10.1.15. Is the product of a non-zero rational and an irrational (a) always rational, (b) always irrational, or (c) either rational or irrational. If your answer is (a) or (b), give a reason. If it is (c), give examples of each case.

Exercise 10.1.16. Make a list of everything that you can think of that the real numbers and the rational numbers have in common. Then make a list of all the things about the reals and the rationals which are different. For example, "both are fields" should be on your first list, while "rationals can be represented as an integer divided by an integer, but not all reals can" should be on your second list.

10.2 Rational Approximations

As was noted in Exercise 10.1.7, calculators produce rational numbers. Therefore, when $\sqrt{2}$ is produced by a calculator, what is displayed is not the square root of 2, but a rational approximation to the square root of 2.

The reason we can find rational approximations to irrational numbers is because of the "density" of the rationals that we observed earlier.

Exercise 10.2.1. Construct a rational number between $\sqrt{2}$ and $\sqrt{2}+10^{-5}$.

Exercise 10.2.2. Show that between every two distinct real numbers there is a rational number. Hint: use the fact from Chapter 5 that rational numbers have repeating or terminating decimal expansions.

Methods for approximating irrationals with rationals exploit Exercise 10.2.2. By repeatedly applying this exercise, we can form a sequence of rational numbers which get successively closer to a given irrational number.

For example, there is an old-fashioned algorithm, similar to long division, for approximating square roots. Each step of this algorithm produces one more digit in the decimal expansion of the square root. We will not discuss this algorithm further.

Here is another method for approximating square roots. We will describe its use to approximate $\sqrt{2}$.

Start with a rational number which is "close" to $\sqrt{2}$. For instance, begin with 3/2. Find that number x such that $\frac{3}{2}\cdot x = 2$. That is, divide 3/2 into 2. We get $x = 4/3$, which is also close to $\sqrt{2}$. Now take the average of 4/3 and 3/2. That is 17/12. Notice that 17/12 is a better approximation to $\sqrt{2}$ than 3/2. That is, $2 < (17/12)^2 < (3/2)^2$.

Exercise 10.2.3. Arithmetically verify that $2 < (17/12)^2 < (3/2)^2$.

Now let's repeat this process, using 17/12 as the starting approximation.

Exercise 10.2.4. Compute

$$x = \frac{2}{17/12}\,.$$

Do not use your calculator! Your answer should be a rational number of the form integer/integer.

Exercise 10.2.5. Find the average of x and 17/12. Again, don't use your calculator. Your answer should be another rational number y.

Exercise 10.2.6. Verify that

$$\sqrt{2} < y < \frac{17}{12}$$

by showing

$$2 < y^2 < (\frac{17}{12})^2\,.$$

More generally, suppose a is a positive rational number such that $2 < a^2$. The number a may be very "close" to $\sqrt{2}$. Let b be $2/a$ (so that $a \cdot b = 2$). If we think of a as an approximation to $\sqrt{2}$, then b is also an approximation to $\sqrt{2}$, but "on the other side," i.e., $b^2 < 2$. Notice that b is also rational. Now let c be the average of a and b: $c = (a+b)/2$. Again, c is rational.

Exercise 10.2.7. Using

$$c = \frac{a+b}{2}$$

and

$$b = \frac{2}{a},$$

show

$$c^2 - 2 = \left(\frac{a-b}{2}\right)^2.$$

Exercise 10.2.8. Again using

$$c = \frac{a+b}{2}$$

and

$$b = \frac{2}{a},$$

show

$$a^2 - c^2 = \frac{1}{4}(a-b)(3a+b).$$

From Exercise 10.2.7 it follows that $c^2 - 2$ is positive, so that $c^2 > 2$. From Exercise 10.2.8 it follows that $a^2 - c^2$ is positive, so that $c^2 < a^2$. Therefore, the rational number c is a "better" approximation to $\sqrt{2}$ than a was.

We may now repeat this, letting c play the role of a. We get a sequence of rational numbers which get closer and closer to $\sqrt{2}$. That this sequence actually converges to $\sqrt{2}$ requires further calculations, which we omit here.

The basic idea behind this algorithm is that we can get as close as we like to $\sqrt{2}$ by a sequence of rationals.

This method is based on an important algorithm for numerical approximation, called Newton's method.

Exercise 10.2.9. Use a calculator to approximate $\sqrt{2}$ by, beginning with 2, successively divide into 2 and taking the average. So the first step would be $(2 + 2/2)/2 = 3/2$ and the second step would be $(3/2 + 4/3)/2 = 17/12$. The third step will give the rational number y you computed in Exercise 10.2.5. How many steps does it take before $\sqrt{2}$ has been computed to the accuracy of your calculator?

Exercise 10.2.10. Write down the number your calculator tells you is $\sqrt{2}$. Now find a rational number which is closer to $\sqrt{2}$ than this number.

10.3 The Intermediate Value Theorem

Some mathematics courses take an axiomatic point of view in the development of the real numbers. Since both the rationals and the reals satisfy all the axioms in Chapter 5, there must be some other axiom which distinguishes them. This axiom is called the Least Upper Bound Axiom. (An *upper bound* of a set of numbers is a number which is larger than all the numbers in the set.)

L-1 (LUB Axiom). Every collection of real numbers with an upper bound has a least upper bound.

Notice that the rational numbers do not satisfy Axiom L-1. For example, let S be the set of all rational numbers which are less than $\sqrt{2}$. All such numbers are certainly less than 1.5, so S has an upper bound. However, it has no least upper bound among rationals, for suppose m is such a rational least upper bound. Then by Exercise 10.2.2, between m and $\sqrt{2}$ there is another rational number. This rational number is larger than m but less than $\sqrt{2}$, so m is not the least upper bound of S. However, if we look for a least upper bound outside the rationals, we can find it: namely, $\sqrt{2}$.

Our interest in the least upper bound axiom is limited to one of its important consequences, the intermediate value theorem. We will omit its proof, which is quite difficult.

Theorem 19 (The Intermediate Value Theorem)**.** *If f is a continuous real-valued function on the real interval $[a, b]$, and if $f(a) < m$ and $f(b) > m$, then there is some number c such that $a < c < b$ and $f(c) = m$.*

Theorem 19 states that continuous real-valued functions on closed intervals take on all the intermediate values between $f(a)$ and $f(b)$. Although this theorem seems very natural and almost obvious, observe that if we limit ourselves to rational numbers, it is not true! The function $x^2 - 2$ is positive for all rational numbers bigger than $\sqrt{2}$ and negative for all rational numbers between 0 and $\sqrt{2}$. However, there is no rational number c such that $c^2 - 2 = 0$. Therefore, a fundamental piece of the proof of the intermediate value theorem is the least upper bound property of the real numbers.

Let's look at a couple of consequences of Theorem 19. The first is that it provides a "root-finder" for real-valued functions. For example, consider the polynomial $x^3 - 6$. When $x = 1$, the value of this polynomial is -5. When $x = 2$, its value is 2. Since $-5 < 0$ while $2 > 0$, the intermediate value theorem tells us that there is some value c, $1 < c < 2$, such that $c^3 - 6 = 0$.

Exercise 10.3.1. Use the intermediate value theorem to show the polynomial $x^5 - x^4 - x^2 + 2$ has at least one real zero between -1 and 0.

Exercise 10.3.2. Use your calculator and the intermediate value theorem to show the function $2^{-x} + \sqrt{x+3} - 3$ has at least one real zero between -0.55 and -0.5 and at least one real zero between 5.5 and 6.

Exercise 10.3.3. Use your calculator and the intermediate value theorem to show the function $(e^x/x) - 2^x$ has at least one real zero between 1 and 2 and at least one real zero between 5 and 6. (e is the base of natural logarithms. You should find the function e^x on your calculator.)

Exercise 10.3.4. For the zero of the function $(e^x/x) - 2^x$ between 1 and 2 discovered in the previous exercise, determine if that zero is between 1 and 1.5 or between 1.5 and 2. If the former, then determine if it is between 1 and 1.25 or between 1.25 and 1.5. If the latter, determine if it is between 1.5 and 1.75 or if it is between 1.75 and 2.

Exercise 10.3.5. Use the intermediate value theorem to prove that every polynomial $p(x)$ with real coefficients and of odd degree has at least one real zero. Hint: assume that the coefficient of the highest power term of $p(x)$ has positive sign. What happens to $p(x)$ when x grows large and positive? What happens to $p(x)$ when x grows large and negative?

Exercise 10.3.6. What goes wrong with the argument in Exercise 10.3.5 when $p(x)$ has even degree? Give an example of a polynomial with even degree which does not have any real zeros.

The intermediate value theorem can be used to show the existence of certain points and lines related to convex sets.

A set in the plane is called a *convex set* if, for every two points P and Q in the set, the line segment PQ joining them is also in the set. The interiors of circles, ellipses, triangles, parallelograms and regular polygons are all examples of convex sets. Figure 10.1 shows an example of a convex set and a set which is not convex.

A set in the plane is called a *bounded set* if there is some circle which encloses it. For example, the half-plane described by $x > 0$ is not bounded.

Suppose K is a bounded convex set and l is a line in the plane. We are going to show that there is a line parallel to l which cuts K into two pieces of equal area.

Place K in the first quadrant of a Cartesian coordinate system and orient the coordinate system so that l is parallel to the y-axis. Let b be the value of x such that all of K lies to the left of the vertical line through b. Now for each x, draw a vertical line through x and let $f(x)$ be the area of K to the left of this line. See Figure 10.2

Exercise 10.3.7. What is $f(0)$? What is $f(b)$? Use the intermediate value theorem to show that there is a c, $0 < c < b$, such that $f(c)$ is half the area of K.

Exercise 10.3.8. Jed and Jethro are two hermits standing on opposite sides of a convex lake. The distance around the lake between the two hermits is the same in either direction. Jed and Jethro begin walking around the lake clockwise at the same speed. Use the intermediate value theorem to show there is a point

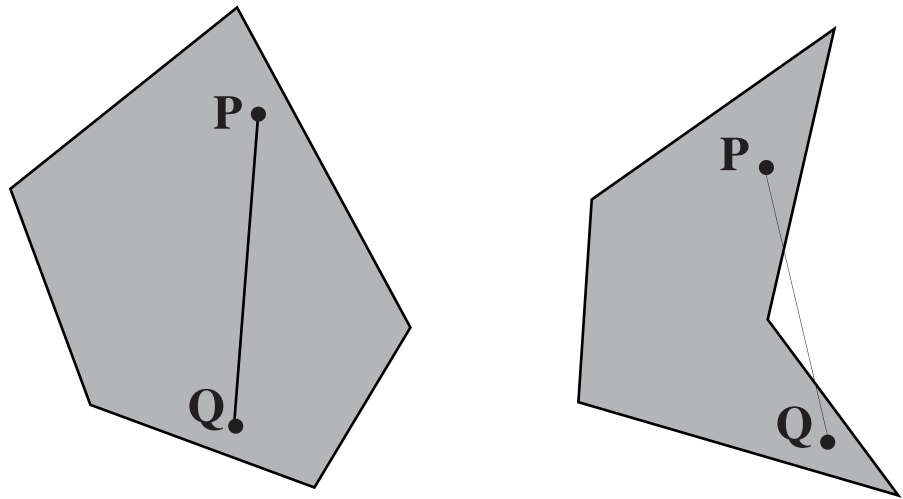


Figure 10.1: A convex set and a non-convex set

at which the line across the lake between Jed and Jethro cuts the lake into two pieces of equal area.

10.4 Complex Numbers

In this section we address the problem of solving polynomial equations.

We start with the simple equation $x^2 + 1 = 0$, which has no real solution. What we do to resolve this issue is remarkable and will be used in a later chapter on finite fields: we invent a solution! Let i stand for the solution to this equation. This i is sometimes called an imaginary number, although it exists as surely as $\sqrt{2}$ exists.

Next we form all possible expressions of the form $a + bi$ where a and b are real numbers. There is an arithmetic for these expressions: we multiply and add just like polynomials in the variable i, except that whenever we encounter i^2, we replace it with -1. For example, $(1 + i) \cdot (2 - i) = 2 + i - i^2 = 3 + i$.

Exercise 10.4.1. Compute $(2 - 4i)(-3 - i)$ and $(1.2 - \frac{3i}{4})(3.5 + \frac{i}{2})$.

Exercise 10.4.2. Compute $(\frac{2}{3} + i\sqrt{3})(\sqrt{5} + (7.61)i)$.

Exercise 10.4.3. Let $z = 3 + 4i$. Show that $z^2 = -7 + 24i$. Find z^3 and z^4. Find a connection between these complex numbers and Pythagorean triples.

From these exercises, we can see that these new numbers are closed under addition and multiplication. It is also straightforward to show that they satisfy the commutative, associative and distributive axioms.

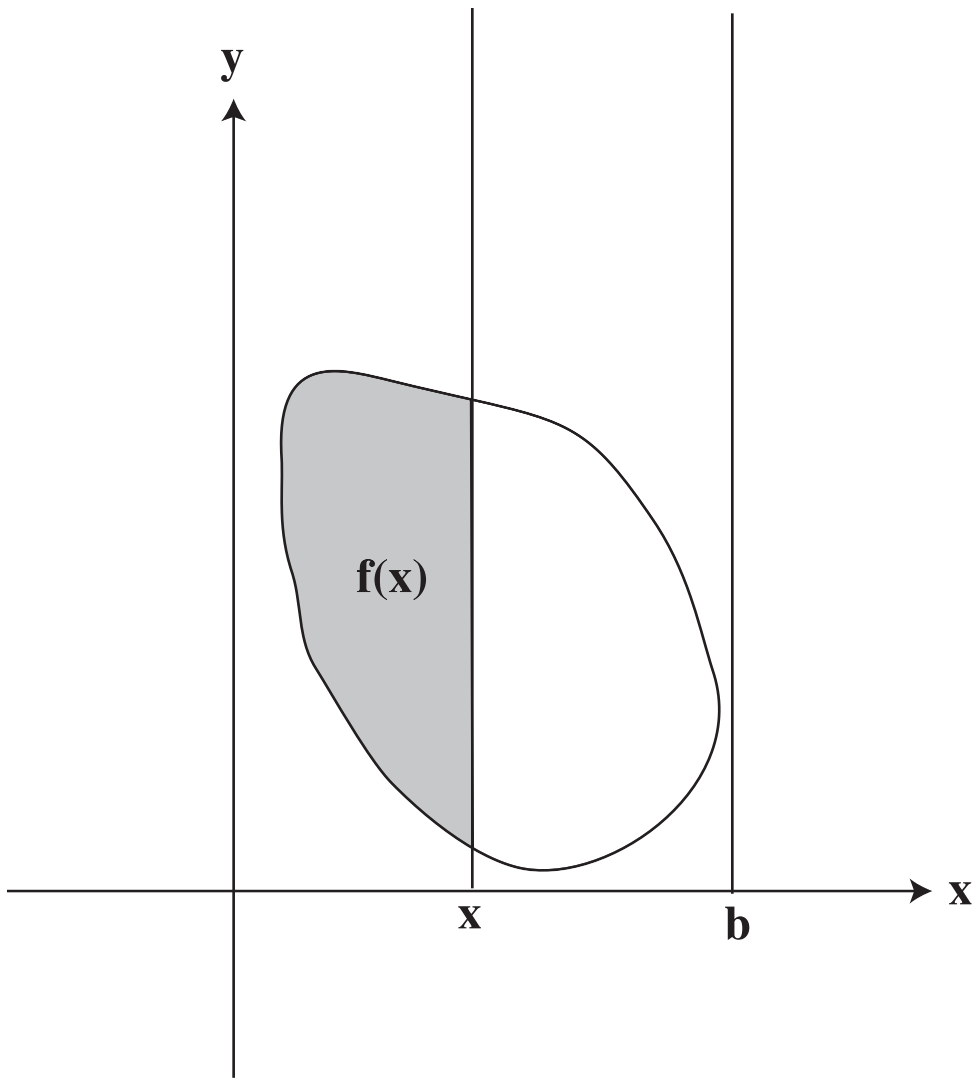


Figure 10.2: Slicing a convex set

Exercise 10.4.4. What is the additive identity for these numbers? What is the multiplicative identity? What is the additive inverse of the number $2 - 6i$? What is the additive inverse of the number $a + bi$?

We shall see below that these numbers also have multiplicative inverses, and thus satisfy all the axioms of a field described in Chapter 5. These numbers are called *complex numbers.* A common notation for the set of complex numbers is $\mathbb{C}$. The reals are a subfield of the complex numbers—they are the complex numbers $a + bi$ where $b = 0$.

***Exercise 10.4.5.** Show the complex field is not an ordered field. Hint: assume it is. By trichotomy, $i < 0$, $i = 0$, or $i > 0$. In the first case, $-i > 0$. What happens if you multiply $i < 0$ by $-i$? In the second case, what happens if you multiply $i = 0$ by i? And in the third case, what happens if you multiply $i > 0$ by i?

Division, i.e., finding multiplicative inverses, in the complex field is a little tricky. It is accomplished by multiplying the numerator and denominator by the *complex conjugate* of the denominator. If $a + bi$ is a complex number, then $a - bi$ is its complex conjugate. For example, the complex conjugate of $3 - 5i$ is $3 + 5i$.

Exercise 10.4.6. Find the complex conjugates of $1 - i$. Of i. Of $-2 - 6i$.

Multiplying a complex number by its complex conjugate yields a real number. For example, $(3-5i)\cdot(3+5i) = 9-25i^2 = 9+25 = 34$. So we can compute the multiplicative inverse of $3 - 5i$ by multiplying numerator and denominator by $3 + 5i$:

$$\begin{aligned}\frac{1}{3-5i} &= \frac{3+5i}{(3-5i)(3+5i)}\\ &= \frac{3+5i}{34}\\ &= \frac{3}{34} + \frac{5}{34}i.\end{aligned}$$

In each of the following exercises, your answer should be of the form $A + Bi$ where A and B are real numbers.

Exercise 10.4.7. Compute

$$\frac{2-4i}{-3-i}$$

and

$$\frac{1.2 - \frac{3i}{4}}{3.5 + \frac{i}{2}}.$$

Exercise 10.4.8. Compute

$$\frac{\sqrt{2}+\frac{3}{2i}}{\sqrt{5}-\frac{\sqrt{2}i}{3}}.$$

Exercise 10.4.9. Compute

$$\frac{2-i}{1+i}+\frac{2+\sqrt{3}i}{6-\sqrt{2}i}.$$

Exercise 10.4.10. Compute i^3, i^4, i^5 and i^6.

Exercise 10.4.11. Compute $(1+i)^5$.

Exercise 10.4.12. Show that the complex conjugate of the complex conjugate is the original complex number.

Pairs of numbers which are complex conjugates of one another are called *complex conjugate pairs.*

10.5 Zeros of Polynomials

In this section, we will discuss the relationship between the zeros of a polynomial and the kind of coefficients of the polynomial.

First, let's do a short review of some basic facts about polynomials. Recall that a polynomial $p(x)$ has the form

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \tag{10.1}$$

with $a_n \neq 0$. For example,

$$2x^3 - x^2 - 4x + 3/2 \tag{10.2}$$

is a polynomial. The numbers $a_n, a_{n-1}, \ldots, a_1, a_0$ in Equation 10.1 are called the *coefficients*. In expression (10.2), 2, -1, -4 and $3/2$ are the coefficients. We call a polynomial *rational*, *real* or *complex*, according to whether the coefficients are all rational, all real or all complex. Rational polynomials will also be real and complex. Real polynomials will also be complex polynomials. The example polynomial is a rational polynomial. The number n in Equation 10.1 is called the *degree* of the polynomial. In expression (10.2), the degree is 3.

Suppose $p(x) = q(x)r(x)$, where $q(x)$ and $r(x)$ are two polynomials with coefficients in the same number system as $p(x)$, and where the degrees of q and r are both at least 1. We then say $p(x)$ *factors over* that number system into $q(x)$ and $r(x)$. Expression (10.2) factors over the rationals into $x^2+x-1/2$ and $2x-3$.

As a somewhat more complicated example, the polynomial

$$x^4 - x^2 - 2$$

factors into

$$(x^2 - 2)(x^2 + 1) \qquad \text{over the rationals,}$$

into

$$(x - \sqrt{2})(x + \sqrt{2})(x^2 + 1) \qquad \text{over the reals,}$$

and into

$$(x - \sqrt{2})(x + \sqrt{2})(x - i)(x + i) \qquad \text{over the complex numbers.}$$

A factor of degree 1 is called a *linear factor* and a polynomial of degree 1 is called a *linear polynomial*. Polynomials of degree 2 are called *quadratic polynomials*. Polynomials of degrees 3, 4 and 5 are called *cubic*, *quartic* and *quintic*, respectively. (Polynomials of degree 0 are called constant polynomials, and are really just the field elements.)

A *zero* of a polynomial, $p(x)$, is a number a such that $p(a) = 0$. Zeros of polynomials are also called *roots*. In expression (10.2), $3/2$ is a zero because $2(3/2)^3 - (3/2)^2 - 4(3/2) + 3/2 = 0$. If a factor of a polynomial has the zero a, then the polynomial has the zero a. Since linear polynomials have exactly one zero, which is easily computed, finding linear factors of a polynomial is equivalent to finding zeros of the polynomial. That is, a is a zero of $p(x)$ if and only if $(x - a)$ is a linear factor of $p(x)$.

One consequence of this is that a polynomial of degree n with coefficients in some field will never have more than n zeros in that field. This is because the polynomial cannot have more than n distinct (up to constant multiple) linear factors.

Exercise 10.5.1. Let

$$p(x) = x^4 - x^2 - 4x - 4.$$

What is the degree of $p(x)$? Is $p(x)$ rational? Is it real? Is it complex? Find at least one linear factor of $p(x)$ over the rationals and at least one rational zero of $p(x)$.

If a polynomial is complex, then an important theorem, called the the "Fundamental Theorem of Algebra," states that the polynomial factors completely into linear factors.

Theorem 20 (The Fundamental Theorem of Algebra)**.** *If $p(x)$ is a complex polynomial of degree n, then $p(x)$ factors into n complex linear factors.*

For example, the polynomial $x^2 - ix - 1 + i$ factors into $(x - 1)(x + 1 - i)$. This example was concocted by picking two linear factors and multiplying them together. It is generally quite hard to start with an arbitrary complex polynomial and find the linear factorization.

The Fundamental Theorem of Algebra is a very deep result whose proof is quite difficult.

If the polynomial is real, then the zeros will either be real or will come in complex conjugate pairs. We will outline a proof of this fact shortly. First, let's look at what happens in the special case that the polynomial is real quadratic.

If $p(x)$ is a real quadratic polynomial, $p(x) = ax^2 + bx + c$, then the well-known quadratic formula tells us how to find the zeros:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

The number under the square root symbol is called the *discriminant.* If the discriminant is positive, $p(x)$ has two distinct real zeros. If the discriminant is zero, $p(x)$ has one real zero. If the discriminant is negative, $p(x)$ has a complex conjugate pair of zeros.

Exercise 10.5.2. Solve the following equations:

i. $2x^2 - 4x + 5 = 0.$

ii. $2x^2 = 3x - 1.$

iii. $3x^2 - 2x + 1/3 = 0.$

Exercise 10.5.3. Find all the zeros of the polynomial:

$$2x^3 - x^2 - 4x + 3/2.$$

Factor this polynomial into a product of three linear factors.

Is there a formula for the roots of cubic polynomials? For quartic polynomials? For quintic polynomials? The answers to these questions are quite surprising and took mathematicians hundreds of years to resolve. There is indeed a formula for cubic polynomials, considerably more complicated than the quadratic formula. This formula has been known since the sixteenth century. There is also a formula for quartic polynomials. This formula has been known since the seventeenth century. However, no formula (using only addition, subtraction, multiplication, division and roots) is possible for the general degree five or higher polynomial. This famous result was proved in the early nineteenth century by Abel.

The following exercises give a proof of the fact that real polynomials have zeros which are real or complex conjugate pairs. First, we need a bit of notation.

If z is a complex number, then let $\overline{z}$ stand for its complex conjugate. A complex number and its conjugate have certain properties:

P-1 If a is real then $\overline{a}$ is real.

P-2 $z\overline{z}$ is real.

P-3 $\overline{\overline{z}} = z.$

P-4 If z and w are complex numbers, then $\overline{z+w} = \overline{z} + \overline{w}$.

P-5 If z and w are complex numbers, then $\overline{zw} = \overline{z} \cdot \overline{w}$.

Property P-1 is obvious. Property P-2 is the property we used to find the multiplicative inverse of complex numbers. Property P-3 is the same as Exercise 10.4.12. For property P-4, suppose $z = a + bi$ and $w = c + di$. Then

$$\begin{aligned}\overline{z+w} &= \overline{(a+c) + (b+d)i} \\ &= (a+c) - (b+d)i\end{aligned}$$

and

$$\begin{aligned}\overline{z} + \overline{w} &= \overline{a+bi} + \overline{c+di} \\ &= a - bi + c - di \\ &= (a+c) - (b+d)i.\end{aligned}$$

Exercise 10.5.4. Prove property P-5 above. (Hint: let $z = a+bi$ and $w = c+di$, then do the algebra.)

These properties can be used to verify that the complex roots of polynomials with real coefficients come in complex conjugate pairs. For example, the polynomial

$$p(x) = x^5 - 4x^4 + 6x^3 - 3x^2 + x + 5$$

has one complex root $2 - i$.

Exercise 10.5.5. Algebraically verify that

$$(2-i)^5 - 4(2-i)^4 + 6(2-i)^3 - 3(2-i)^2 + (2-i) + 5 = 0.$$

Now take the complex conjugate of this equation. We get

$$\overline{(2-i)^5 - 4(2-i)^4 + 6(2-i)^3 - 3(2-i)^2 + (2-i) + 5} = \overline{0}.$$

Use properties P-1, P-4 and P-5 to distribute the complex conjugate through the sum on the left side and use property P-1 on the right side:

$$(2+i)^5 - 4(2+i)^4 + 6(2+i)^3 - 3(2+i)^2 + (2+i) + 5 = 0.$$

But the left side is now $p(2+i)$, so $2+i$ is also a solution to $p(x) = 0$.

The next three exercises ask you to do this calculation in general. Suppose $p(z)$ is a polynomial in z with real coefficients:

$$p(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0.$$

Exercise 10.5.6. Use properties P-1, P-4 and P-5 to show $p(\overline{z}) = \overline{p(z)}$.

Polynomial	over rationals	over reals	over complex
$x^2 - 2$	irreducible	not irreducible	not irreducible
$x^2 - 1$	not irreducible	not irreducible	not irreducible

Table 10.1: Irreducible polynomials?

Exercise 10.5.7. Suppose $p(z) = 0$. Use Exercise 10.5.6 and property P-1 to show $p(\overline{z}) = 0$.

Exercise 10.5.8. Conclude that the roots of $p(z)$ are either real or come in complex conjugate pairs.

We write this last exercise as the following theorem.

Theorem 21. *If $p(z)$ is a polynomial with real coefficients, then the roots of $p(z)$ are either real or come in complex conjugate pairs.*

Exercise 10.5.9. Suppose $p(x)$ is a real polynomial and suppose $p(2-3i) = 0$. What is $p(2+3i)$?

Exercise 10.5.10. Prove that any real polynomial factors into a product of real linear and real quadratic polynomials. Hint: Recall that if a and b are two zeros of $p(x)$, then $(x-a)(x-b)$ is a factor of $p(x)$. What kind of coefficients does the polynomial $(x-a)(x-\overline{a})$ have? What is its degree?

10.6 Algebraic Extensions and Zeros of Polynomials

Let's look at the construction of the complex numbers from another viewpoint. We started with a field (the real numbers) and a polynomial with real coefficients which did not factor (x^2+1). We "invented" a root of this polynomial (i) which we "adjoined" to the field (i. e., we formed all expressions like $a+bi$). Then we did arithmetic using forms like $a+bi$ as polynomials in i, except we replaced i^2 with -1 (or, equivalently, i^2+1 with 0).

This same construction can be done for any field and for any polynomial with coefficients in the field and which does not factor over the field!

To do this construction, we start with a polynomial which does not have any polynomial factors with coefficients in our field. Such a polynomial is called *irreducible over the field.* For example, $x^2 - 2$ is irreducible over the rationals (but not over the reals, since $x^2-2 = (x-\sqrt{2})(x+\sqrt{2})$). The polynomial x^2-1 is not irreducible over the rationals or the reals (since $x^2-1 = (x-1)(x+1)$). We summarize in Table 10.1.

Exercise 10.6.1. Fill in a table similar to Table 10.1 for each of the following polynomials: x^2+1, x^2+3x+2, x^2+4x+1, x^4+2x^2+1, x^3+x+1.

Let's continue with our example, using the polynomial $x^2 - 2$. Let's look at all expressions of the form $a + b\sqrt{2}$ where a and b are rational. We will call this set of numbers F. Two examples of elements of F are $\sqrt{2}$ and $3 - 5\sqrt{2}$.

Exercise 10.6.2. Give three more examples of elements of F.

We will now do arithmetic in F. For instance, to add two elements of F, $a + b\sqrt{2}$ and $c + d\sqrt{2}$, we compute $(a + c) + (b + d)\sqrt{2}$. Since a and c are both rational, then $a + c$ is rational. Similarly, $b + d$ is rational, so $(a + c) + (b + d)\sqrt{2}$ is in F.

Subtraction is done in a similar manner.

Exercise 10.6.3. Perform the arithmetic:

i. $(4 - 6\sqrt{2}) + (7 + 3\sqrt{2})$.

ii. $(1.3 - \frac{4}{3}\sqrt{2}) + (-\frac{2}{7} + 3.3\sqrt{2})$.

iii. $(2.2 - \frac{5}{3}\sqrt{2}) - (-\frac{2}{7} + 3\sqrt{2})$.

To multiply, just use the fact that $\sqrt{2} \cdot \sqrt{2} = 2$ (just as we used the fact that $i \cdot i = -1$ for complex numbers). For instance, $(2 - \sqrt{2}) \cdot (-1 - 3\sqrt{2}) = 4 - 5\sqrt{2}$.

Exercise 10.6.4. Perform the arithmetic:

i. $(4 - 6\sqrt{2}) \cdot (7 + 3\sqrt{2})$.

ii. $(1.3 - \frac{4}{3}\sqrt{2}) \cdot (-\frac{2}{7} + 3.3\sqrt{2})$.

iii. $(2.2 - \frac{5}{3}\sqrt{2}) \cdot (-\frac{2}{7} + 3\sqrt{2})$.

The additive identity 0 and the multiplicative identity 1 are both in F ($0 = 0 + 0\sqrt{2}$ and $1 = 1 + 0\sqrt{2}$).

To divide, we perform a step much like finding the complex conjugate. For instance,

$$\begin{aligned}\frac{2 - \sqrt{2}}{-1 - 3\sqrt{2}} &= \frac{2 - \sqrt{2}}{-1 - 3\sqrt{2}} \cdot \frac{-1 + 3\sqrt{2}}{-1 + 3\sqrt{2}} \\ &= \frac{-8 + 7\sqrt{2}}{-17} \\ &= \frac{8}{17} - \frac{7}{17} \cdot \sqrt{2}.\end{aligned}$$

This process is sometimes called *rationalizing the denominator.*

Exercise 10.6.5. Perform the arithmetic:

i.
$$\frac{1}{2\sqrt{2}}.$$

ii.
$$\frac{2-3\sqrt{2}}{-7+\sqrt{2}}.$$

iii.
$$\frac{1-\frac{5}{3}\sqrt{2}}{-\frac{2}{5}+2\sqrt{2}}.$$

Exercise 10.6.6. Find the multiplicative inverse of $1-\sqrt{2}$ in F. Find the multiplicative inverse of $2+3\sqrt{2}$ in F. More generally, find the multiplicative inverse of $a+b\sqrt{2}$ in F, where a and b are rational.

Fields which contain a smaller subfield are called *extensions*. The complex numbers are an extension of the reals; the field F described above is an extension of the rationals.

The fields we described above are special kinds of extensions, called *simple algebraic extensions*. That simply means they are constructed according to the recipe described above. The notation used to name them is $\mathbb{F}(a)$, where $\mathbb{F}$ is the name of the starting field and a is the root adjoined. For example, the complex numbers are $\mathbb{R}(i)$ and the field F above is $\mathbb{Q}(\sqrt{2})$.

Exercise 10.6.7. Find rationals a and b such that
$$a(\sqrt{2}+\sqrt{3})^3-b(\sqrt{2}+\sqrt{3})=\sqrt{2}.$$
Conclude that $\sqrt{2}$ is an element of $\mathbb{Q}(\sqrt{2}+\sqrt{3})$.

Exercise 10.6.8. Find rationals a and b such that
$$a(\sqrt{2}+\sqrt{3})^3-b(\sqrt{2}+\sqrt{3})=\sqrt{3}.$$
Conclude that $\sqrt{3}$ is an element of $\mathbb{Q}(\sqrt{2}+\sqrt{3})$.

Suppose we start with the rationals, then "throw in" $\sqrt{2}$, forming $\mathbb{Q}(\sqrt{2})$. The polynomial x^2-3 is irreducible over $\mathbb{Q}(\sqrt{2})$, so we can "throw in" $\sqrt{3}$. The new field, in our notation, is $\mathbb{Q}(\sqrt{2})(\sqrt{3})$. Certainly $\sqrt{2}+\sqrt{3}$ is an element of $\mathbb{Q}(\sqrt{2})(\sqrt{3})$. This means $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ is a subfield of $\mathbb{Q}(\sqrt{2})(\sqrt{3})$. But Exercise 10.6.7 and Exercise 10.6.8 show that $\mathbb{Q}(\sqrt{2})(\sqrt{3})$ is a subfield of $\mathbb{Q}(\sqrt{2}+\sqrt{3})$, so these two fields must be the same:
$$\mathbb{Q}(\sqrt{2})(\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3}).$$
This is a special case of a remarkable theorem which states that every finite sequence of simple algebraic extensions over the rationals is a simple algebraic extension.

Field extensions have an integer associated with them, called the *degree* of the extension. In the case of simple algebraic extensions, the degree is the degree of the corresponding irreducible polynomial. For example, the complex numbers are an extension of the reals of degree 2, since they introduce i, a root of a second degree polynomial x^2+1. The field $\mathbb{Q}(\sqrt{2})$ is an extension of the rationals of degree 2, because it introduces $\sqrt{2}$, a root of the second degree polynomial x^2-2.

Let's do another example of a field extension. We use as our polynomial x^3-2, which is irreducible over the rationals. As before, we extend the rational field by adjoining a root of this polynomial. In fact, we will adjoin $\sqrt[3]{2}$.

Exercise 10.6.9. What is the degree of $\mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$?

We now do some arithmetic in $\mathbb{Q}(\sqrt[3]{2})$. For example,

$$\begin{aligned}((\sqrt[3]{2})^2+1)\cdot((\sqrt[3]{2})^2+\sqrt[3]{2}-1) &= (\sqrt[3]{2})^4+(\sqrt[3]{2})^3+\sqrt[3]{2}-1\\ &= 2\sqrt[3]{2}+2+\sqrt[3]{2}-1\\ &= 3\sqrt[3]{2}+1\,.\end{aligned}$$

Notice the substitution of 2 for $(\sqrt[3]{2})^3$ in the above calculation.

Exercise 10.6.10. Find rational numbers (a,b,c) such that

$$((\sqrt[3]{2})^2-\sqrt[3]{2}-3)\cdot((\sqrt[3]{2})^2+\sqrt[3]{2}) = a(\sqrt[3]{2})^2+b\sqrt[3]{2}+c\,.$$

Now let's try to find the multiplicative inverse of a number in $\mathbb{Q}(\sqrt[3]{2})$. For example, what is the multiplicative inverse of $\sqrt[3]{2}+1$? That is, we want to "rationalize the denominator" of

$$\frac{1}{\sqrt[3]{2}+1}\,.$$

We don't know what this number is yet, but we do know it must be of the form $a(\sqrt[3]{2})^2+b\sqrt[3]{2}+c$. That is, we want to find rational numbers (a,b,c) such that

$$\frac{1}{\sqrt[3]{2}+1} = a(\sqrt[3]{2})^2+b\sqrt[3]{2}+c\,.$$

Multiplying left and right by $\sqrt[3]{2}+1$, we have

$$\begin{aligned}1 &= (\sqrt[3]{2}+1)\cdot(a(\sqrt[3]{2})^2+b\sqrt[3]{2}+c)\\ &= a(\sqrt[3]{2})^3+b(\sqrt[3]{2})^2+c\sqrt[3]{2}+a(\sqrt[3]{2})^2+b\sqrt[3]{2}+c\\ &= (a+b)(\sqrt[3]{2})^2+(b+c)\sqrt[3]{2}+(2a+c)\end{aligned}$$

The last expression is a quadratic polynomial in $\sqrt[3]{2}$. In order for this polynomial to be exactly 1, the coefficients of $\sqrt[3]{2}$ and $(\sqrt[3]{2})^2$ must be zero and the constant term must be 1. Therefore,

$$\begin{aligned}a+b\qquad &= 0\\ b+c &= 0\\ 2a\qquad+c &= 1\,.\end{aligned}$$

Solving this system of three equations and three unknowns yields

$$a = 1/3$$
$$b = -1/3$$
$$c = 1/3\,.$$

Therefore,

$$\frac{1}{\sqrt[3]{2}+1} = \frac{1}{3}(\sqrt[3]{2})^2 - \frac{1}{3}\sqrt[3]{2} + \frac{1}{3}\,. \tag{10.3}$$

Exercise 10.6.11. Use your calculator to check Equation (10.3).

Exercise 10.6.12. Find the multiplicative inverse in $\mathbb{Q}(\sqrt[3]{2})$ of $(\sqrt[3]{2})^2 - 1$.

Exercise 10.6.13. Rationalize the denominator:

$$\frac{(\sqrt[3]{2})^2 + 2}{(\sqrt[3]{2})^2 - 1}\,.$$

Let's do a final example of a field extension. The last polynomial in Exercise 10.6.1 was irreducible over the rationals. Let α be the number such that $\alpha^3 + \alpha + 1 = 0$. We now do arithmetic in $\mathbb{Q}(\alpha)$. For example,

$$\begin{aligned}(\alpha^2 - 1)\cdot(\alpha + 1) &= \alpha^3 + \alpha^2 - \alpha - 1\\ &= -\alpha - 1 + \alpha^2 - \alpha - 1\\ &= \alpha^2 - 2\alpha - 2.\end{aligned}$$

We will use this α for the next four exercises.

Exercise 10.6.14. What is the degree of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$?

Exercise 10.6.15. Find rational numbers (a, b, c) such that

$$(3\alpha^2 - 2\alpha + 1)\cdot(\alpha^2 + 3) = a\alpha^2 + b\alpha + c\,.$$

Exercise 10.6.16. Find the multiplicative inverse in $\mathbb{Q}(\alpha)$ of α^2.

Exercise 10.6.17. Rationalize the denominator of

$$\frac{\alpha - 1}{\alpha^2}$$

We can now see one way that some real numbers are "better" than others: some real numbers are roots of polynomials with rational coefficients. Such numbers are called *algebraic numbers*. For instance, $\sqrt{2}$ is algebraic because it is a root of $x^2 - 2$. Every rational a is algebraic because it is a root of $x - a$.

Exercise 10.6.18. Show that $1/2$, $3^{1/4}$ and $5^{1/3}$ are all algebraic.

The next exercises show that $\sqrt{2}+\sqrt{3}$ is algebraic of degree 4 over $\mathbb{Q}$.

Exercise 10.6.19. Write $(\sqrt{2}+\sqrt{3})^2$ as $A+B\sqrt{6}$ where A and B are rationals.

Exercise 10.6.20. Write $(\sqrt{2}+\sqrt{3})^4$ as $A+B\sqrt{6}$ where A and B are rationals.

Exercise 10.6.21. Use the previous two exercises to find rationals R and S such that

$$R(\sqrt{2}+\sqrt{3})^4 + S(\sqrt{2}+\sqrt{3})^2 = 1.$$

The last exercise produces a polynomial $Rx^4 + Sx^2 - 1$ which has a zero at $(\sqrt{2}+\sqrt{3})$.

Exercise 10.6.22. Check that $Rx^4 + Sx^2 - 1$ is irreducible over the rationals.

Real numbers which are not algebraic are called *transcendental*. The two most famous transcendental numbers are π and e. The proofs that they are transcendental are not generally given in even undergraduate math classes!

10.7 Infinities

Recall that in Chapter 5, we discussed a kind of infinity called countable. There, we saw that the integers, the rationals, and many other infinite sets were countable.

A beautiful argument due to Cantor shows that the reals are not countable. In fact, it shows that the reals between 0 and 1 are not countable. This will be our first example of an uncountable set.

Suppose we start with some sequence of real numbers between 0 and 1, say $\{r_1, r_2, r_3, r_4, \ldots\}$. Let's write them in their decimal form. For example, suppose our sequence begins:

$$\begin{aligned}
r_1 &= 0.12321012\ldots \\
r_2 &= 0.33223344\ldots \\
r_3 &= 0.66666666\ldots \\
r_4 &= 0.20000000\ldots \\
r_5 &= 0.31313131\ldots \\
r_6 &= 0.12345112\ldots \\
r_7 &= 0.99888777\ldots \\
r_8 &= 0.46646466\ldots \\
&\vdots
\end{aligned}$$

Now let's "construct" a special real s between 0 and 1. The first digit of s after the decimal point will be 3 unless the first digit of r_1 is 3, in which case it is 5. The second digit of s will be 3 unless the second digit of r_2 is 3, in which case it is 5. And so on. The nth digit of s will be 3 unless the nth digit of r_n is 3, in which case it is 5. In our example, $s = 0.35335333\cdots$.

Exercise 10.7.1. Show that s is not in the sequence $\{r_1, r_2, r_3, r_4, \dots\}$, and so conclude that no list of real numbers can contain all the reals.

Exercise 10.7.2. What roles did 3 and 5 play in this construction? Did we have to use 3 and 5?

This argument shows that the reals are not countable (that is, *uncountable*). An extension of this argument can be used to show that there are an infinite number of sizes of infinity.

It is not too hard to show that algebraic numbers are countable. Thus the transcendental numbers must be uncountable. One of the many paradoxes surrounding sizes of sets is the fact that while the algebraic numbers are countable and the transcendental numbers are uncountable, it is very hard to show specific numbers are transcendental.

One of the questions which puzzled Cantor was this: could there be a level of infinity between the countable rationals and the uncountable reals? Cantor conjectured that no such set existed, but was not able to prove it. This conjecture was call the "Continuum Hypothesis" and was a celebrated problem in mathematics until Cohen provided the surprising answer. What Cohen showed was that neither the existence nor the nonexistence of such a set was inconsistent with the axioms of set theory!

10.8 Constructible Numbers

The early Greek mathematicians felt that every number must be "constructible." That is, starting with a line segment of length one, and using only a straightedge and a compass, one could construct a line segment of that length. For instance, $\sqrt{2}$ is constructible by constructing a right triangle with sides of length one, as shown in Figure 10.3. Then the hypotenuse will have length $\sqrt{2}$.

In this figure, two perpendicular lines, m and l, are constructed intersecting at the point P. Then construct the arc r of radius one and center P, intersecting m at A and intersecting l at B. The triangle PAB will have right angle at P and two sides of unit length. Therefore, its hypotenuse, AB, will have length $\sqrt{2}$.

Exercise 10.8.1. Describe the straightedge and compass construction of $\sqrt{5}$, $\sqrt{3}$, $\sqrt{7}$, and $2^{1/4}$.

One of the great achievements of modern algebra was the resolution of the Greeks' constructibility problems. Some of these problems were unsolved for almost 2000 years. One of these problems was to "square a circle," i. e., given a circle, construct a square having the same area.

Exercise 10.8.2. Show that this problem amounts to constructing $\sqrt{\pi}$.

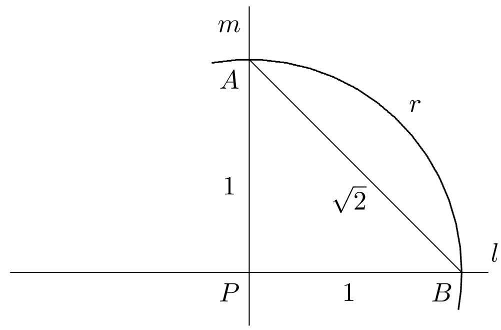


Figure 10.3: Construction of $\sqrt{2}$

Exercise 10.8.3. Show that if you could construct π, then you could construct $\sqrt{\pi}$.

It is not too hard to show that the Greeks' straightedge and compass constructions create numbers in an extension field of degree 2. This comes from the fact that circles are described by the quadratic equation $(x-a)^2+(y-b)^2 = r^2$.

When an extension of an extension is created, the degree of the second extension over the original field is the product of the degrees of the two extensions. Therefore, if a number is constructible, it must live in an extension of the rationals of a degree which is a power of 2.

Exercise 10.8.4. Is the number α such that $\alpha^3 + \alpha + 1 = 0$ discussed in Section 10.6 constructible?

Therefore, each constructible number is certainly algebraic. Furthermore, if it satisfies some irreducible polynomial over the rationals, that polynomial must have degree equal to some power of 2.

In particular, π is not algebraic and therefore not constructible. The proof that π is transcendental thus settled the 2000 year old problem of squaring a circle.

Another of the Greeks' construction problems was trisecting an angle. Was it possible, with straightedge and compass, to trisect every angle?

In fact, we will show it's impossible to trisect $60°$.

A $60°$ angle is easily constructible. Simply construct an equilateral triangle. Such a triangle has three $60°$ angles.

If it is possible to trisect an angle, it should be possible to construct an angle of $20°$.

The cosine of an angle α can be defined in the following way. Draw a right triangle with one of its angles equal to α. The cosine of α is the ratio of the length of the side adjacent to α to the length of the hypotenuse. In Figure 10.4, $\cos \alpha = a/b$.

It is easy to see that if an angle is constructible, so is its cosine. This process is sketched in Figure 10.5.

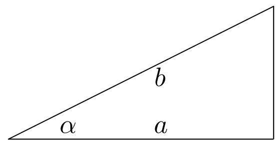


Figure 10.4: Cosine of $\alpha = a/b$

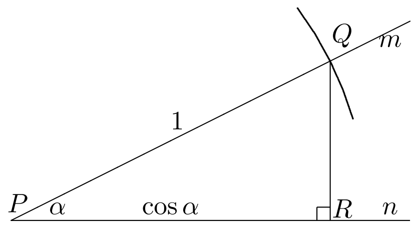


Figure 10.5: Construction of the Cosine

Start with the angle α at P. One side is ray m and the other side is ray n. Using P as center and radius one, draw an arc intersecting m at Q. Now drop a perpendicular from Q down to n, intersecting n at R. The right triangle PQR has hypotenuse length one. Therefore, the side PR will have length $\cos\alpha$.

Let's let $\alpha = 20°$ and $a = \cos\alpha$. A trigonometric identity can then be used to show $8a^3 - 6a - 1 = 0$.

Exercise 10.8.5. Show that the polynomial $8x^3 - 6x - 1$ is irreducible over the rationals. By the discussion above, a is not constructible. Since a is not constructible, α is not constructible, and so it is impossible to trisect $60°$.

Chapter 11

Probability and Statistics, II

In this chapter we conclude our study of the interrelated topics, probability and statistics. In particular, we concentrate on measuring the center and the spread of a body of information. This chapter is highly dependent upon the material in Chapter 7 and in Chapter 2. It is suggested that this material be reviewed at this time.

11.1 Expectation

If a pair of fair dice is rolled 60 times, you would expect seven to come up about ten times. However, that does not mean that seven will come up ten times every time you roll the dice 60 times. Furthermore, if you roll the dice 50 times, seven certainly will not come up $\frac{50}{6}$ times!

If a fair coin is tossed 20 times, you would expect heads to turn up about ten times. However, that does not mean that in every 20 tosses, you will get exactly ten heads. And you certainly will not toss one and one-half heads in three tosses!

In many probabilistic settings, the sample space is partitioned into disjoint events, and a value is assigned to each event. This value is called a *random variable*. The "weighted" average of this value is called the *expectation*. By "weighted" average, we mean that the values of the various events are weighted by their probabilities.

More precisely, suppose there are n outcomes, with probabilities $p_1, \ldots, p_n$. A random variable is a value assigned to each of the n outcomes. If the random variable is X, then $X_1, \ldots, X_n$ are the values assigned to the n outcomes.

The expectation of X, written $E(X)$, is defined by

$$E(X) = p_1X_1 + p_2X_2 + \cdots + p_nX_n\,. \tag{11.1}$$

Outcome	0 Heads	1 Head	2 Heads
Value of Random Variable	0	1	2
Probability	$\frac{1}{4}$	$\frac{1}{2}$	$\frac{1}{4}$

Table 11.1: A random variable distribution

The expectation is a kind of average, if an experiment is run many times with the same probability distribution. In any particular experiment you should not expect to achieve the expectation.

For instance, if a fair coin is tossed twice, heads appears twice with probability 1/4, heads appears exactly once with probability 1/2, and heads appears not at all with probability 1/4. So the expected number of heads in two tosses of a fair coin is

$$0 \cdot \frac{1}{4} + 1 \cdot \frac{1}{2} + 2 \cdot \frac{1}{4} = 1\,.$$

When computing expectations, it is sometimes useful to write down a table listing the outcomes, the value of the random variable, and the probabilities. In the above example, the table would look something like Table 11.1.

Exercise 11.1.1. What is the expected number of heads you would toss in three tosses of a fair coin? Do the calculation described in the example above.

Exercise 11.1.2. What do you think is the expected number of heads you would toss in ten tosses of a fair coin? In n tosses?

Exercise 11.1.3. Do the calculation to compute the expected number of times you would roll seven in two rolls of a pair of fair dice.

Exercise 11.1.4. What do you think is the expected number of times you would roll seven in 60 rolls of a pair of fair dice? In 50 rolls? In n rolls?

Expectation is used to describe potential winnings and losings from games. But it is also a tool to determine public policy regarding the use of scarce resources and as a method for making business decisions.

Here is an example. In the game of roulette, a wheel has 37 equally spaced slots, numbered 0 to 36. A player bets \$1 on one of the numbers. This bet is collected by the croupier (a person working for the casino). The wheel is spun and a ball comes to rest in one of the slots. If the ball comes to rest in the player's slot, she wins 36 times her bet (\$36). Otherwise, she loses her \$1.

If we assume that each slot is equally likely, the probability that the ball comes to rest in her slot is $\frac{1}{37}$. Her winnings will be \$35, since she has paid \$1 to play the game. Thus the weighted average is $\frac{1}{37} \cdot 35 + \frac{36}{37} \cdot (-1)$ or approximately -0.027. Table 11.2 shows the outcomes and probabilities. The value of the random variable is called the "payoff" in this table.

Alternatively, she will win $\frac{1}{37} \cdot 36$ which is approximately 0.973 in an "average game." Since it costs her \$1 to play, she loses approximately $1.00 - 0.973 = 0.027$.

Outcome	Player's slot	Another slot
Payoff	35	-1
Probability	$\frac{1}{37}$	$\frac{36}{37}$

Table 11.2: Another random variable distribution

Outcome	2	3	4, then 7	4, then 4	$\cdots$
Payoff	-1	-1	-1	$+1$	$\cdots$
Probability	$\frac{1}{36}$	$\frac{2}{36}$	$\frac{1}{18}$	$\frac{1}{36}$	$\cdots$

Table 11.3: Craps payoff distribution

Exercise 11.1.5. Our player may also bet on "red" or "black." The numbers 1 to 36 are divided evenly between these two colors. Suppose our player bets on "red." If a "red" number turns up, she wins twice her bet. If a "black" number or 0 turns up, she wins nothing. If she bets \$1, what are her expected winnings?

Exercise 11.1.6. In an alternate version of the game in Exercise 11.1.5, "red" and "black" payoff as before, but if 0 turns up, the wheel is spun until a "red" or "black" number appears. If it is "black," the player loses; if it is "red," she wins only her original bet back. Now what are her expected winnings?

In the game of craps, a pair of dice is tossed. If the shooter rolls 7 or 11, she wins. If she rolls 2, 3 or 12, she loses. Otherwise, she continues to roll until she rolls either 7 or she repeats her first roll. If it is a 7, she loses; if she repeats, she wins. Let's assume that if she wins, she wins \$1, and if she loses, she loses \$1. The next three exercises refer to this game.

Let's start by making up the distribution table, Table 11.3. This table is not complete. We have not put all the possible outcomes in, nor have we computed all the probabilities.

Exercise 11.1.7. List all the possible outcomes in the game of craps. That is, complete the first row of Table 11.3.

How were the probabilities $1/18$ and $1/36$ under the outcomes "first 4, eventually 7" and "first 4, eventually 4" computed? The probability of rolling 4 is $3/36 = 1/12$. Now the shooter continues to roll until either a 4 or a 7 comes up. There are 3 ways a 4 can come up and there are 6 ways a 7 can come up. (See Table 7.1 in Chapter 7.) Therefore there are 9 ways that will stop the shooter from rolling. Since 3 of these 9 ways ends with rolling 4, the probability that she eventually will roll 4 is $3/9 = 1/3$. Since 6 of these 9 ways ends with rolling 7, the probability that she will eventually roll 7 is $6/9 = 2/3$.

Of course, all this is conditioned on the event that the shooter first rolled 4, so using the conditional probability formula (see Equation (7.6) in Chapter 7), the

Matches	Powerball	Payoff
5	Yes	Jackpot
5	No	\$100,000
4	Yes	\$5,000
4	No	\$100
3	Yes	\$100
3	No	\$7
2	Yes	\$7
1	Yes	\$4
0	Yes	\$3

Table 11.4: Powerball Payoff

probability that she rolls 4, then eventually rolls 4 again, is $(1/12)(1/3) = 1/36$, while the probability that she rolls 4, then eventually rolls 7, is $(1/12)(2/3) = 1/18$.

Exercise 11.1.8. Complete Table 11.3 by filling in all outcomes, probabilities and payoffs.

Exercise 11.1.9. Compute the expected winnings.

Powerball is a Minnesota State Lottery game. In this game, the player picks five numbers from 1 to 49. Then she picks another number, called the *Powerball Number*, from 1 to 42. It costs \$1 to play the game. Winners are determined when five numbers from 1 to 49 are selected at random and one Powerball Number, from 1 to 42, is selected at random. Prizes are determined by Table 11.4. The Jackpot is divided among the winning tickets.

So, for example, the probability that a player gets 3 balls correct and also gets the powerball correct is

$$\frac{\binom{5}{3}\binom{44}{2}}{\binom{49}{5}} \cdot \frac{1}{42}.$$

This is because there are $\binom{5}{3}$ ways that 3 of the players 5 balls can be selected and $\binom{44}{2}$ ways that 2 of the 44 balls the player did not select can be picked. In all there are $\binom{49}{5}$ ways that 5 balls can be selected. Finally, the probability of getting the powerball correct is $1/42$.

The following three exercises ask you to analyze this game.

Exercise 11.1.10. Compute the probability of each prize.

Exercise 11.1.11. Compute the expected winnings, assuming the Jackpot is \$10,000,000 and assuming it is not divided among winning tickets.

Exercise 11.1.12. The Jackpot prize is paid out in yearly equal installments over 20 years. The Jackpot builds up each week if there are no winners and is divided if there are several winners. Comment on how these considerations affect the expected winnings.

Exercise 11.1.13. Suppose Congress must choose between spending \$2,000,000 on enforcing certain airline safety regulations which would reduce airline fatalities by 10%, or spending \$50,000 on enforcing certain automobile safety regulations which would reduce traffic fatalities by 0.1%. Suppose the number of airline fatalities per year is 200 and the number of automobile fatalities per year is 43,500. What do you think they should do?

Suppose an experiment is repeated independently n times. Suppose each experiment has probability of success p (and probability of failure $q = 1 - p$). From expression 7.4 in Chapter 7, the probability of exactly k successes in the n trials, $p_{n,k}$, is

$$p_{n,k} = \binom{n}{k} p^k q^{n-k} . \tag{11.2}$$

Now we will find the expected number of successes for such an experiment. First, let's set up an appropriate random variable. Let X be the random variable which gives the number of successes of the experiment. So the probability that X is k is given by Equation (11.2). Therefore, by Equation (11.1), the expectation of X is given by

$$\begin{aligned} E(X) &= 0 \cdot \binom{n}{0} p^0 q^n + 1 \cdot \binom{n}{1} p^1 q^{n-1} + 2 \cdot \binom{n}{2} p^2 q^{n-2} + \cdots + n \cdot \binom{n}{n} p^n q^0 \\ &= 1 \cdot \binom{n}{1} p^1 q^{n-1} + 2 \cdot \binom{n}{2} p^2 q^{n-2} + \cdots + n \cdot \binom{n}{n} p^n q^0 . \end{aligned}$$

Exercise 11.1.14. What happened to the first term in this sum?

Exercise 11.1.15. Show the following three identities:

$$\begin{aligned} 1 \cdot \binom{n}{1} &= n \cdot \binom{n-1}{0} \\ 2 \cdot \binom{n}{2} &= n \cdot \binom{n-1}{1} \\ 3 \cdot \binom{n}{3} &= n \cdot \binom{n-1}{2} . \end{aligned}$$

Exercise 11.1.16. More generally, show:

$$k \cdot \binom{n}{k} = n \cdot \binom{n-1}{k-1} .$$

(This exercise is the same as Exercise 2.3.35 from Chapter 2.)

Exercise 11.1.17. Now use Exercise 11.1.16 to show

$$E(X) = n \cdot \binom{n-1}{0} p^1 q^{n-1} + n \cdot \binom{n-1}{1} p^2 q^{n-2} + \cdots + n \cdot \binom{n-1}{n-1} p^n q^0 .$$

Exercise 11.1.18. Explain each of the steps in the following sequence of equalities:

$$\begin{aligned} E(X) &= np\left(\binom{n-1}{0} p^0 q^{n-1} + \binom{n-1}{1} p^1 q^{n-2} + \binom{n-1}{2} p^2 q^{n-3} \right. \\ &\qquad \left. + \cdots + \binom{n-1}{n-1} p^{n-1} q^0 \right) \\ &= np(q+p)^{n-1} \\ &= np \cdot 1 = np . \end{aligned}$$

Hint: use the binomial theorem (Theorem 1).

Therefore, from Exercise 11.1.18 we have the following.

If X is the number of successes in n independent trials, where p is the probability of success in any given trial, then

$$E(X) = np . \tag{11.3}$$

11.2 Central Measures

The expectation measures the "center" of a predetermined probability distribution. However, it is also important to find some measure of the "center" of numerical data. One common measure is the average of the values. This measure is called the *mean.*

Table 11.5 gives the test scores for two tests from a group of 30 students who took a math course for elementary education students.

Exercise 11.2.1. Find the mean for each of the two test scores in Table 11.5.

Exercise 11.2.2. A simple calculation device for computing the mean is to add up the product of the value and the frequency of that value, then divide by the number of values. Did you use this method in Exercise 11.2.1? If not, do so now.

We must be very careful when computing averages of averages. Here is an example. Suppose the governors of two upper midwestern states M and W peruse the average salaries of professors at their respective state universities. Here is what they find:

	State M	State W
Full Professor	\$80,000	\$72,000
Associate Professor	\$60,000	\$54,000

Student	Test 1	Test 2	Student	Test 1	Test 2
1	18	48	16	54	63
2	98	65	17	82	82
3	89	40	18	83	55
4	84	85	19	77	94
5	92	88	20	80	59
6	86	51	21	91	43
7	82	75	22	95	83
8	93	78	23	84	64
9	61	61	24	83	21
10	98	94	25	98	86
11	91	81	26	100	88
12	97	83	27	98	81
13	98	93	28	94	40
14	91	74	29	98	100
15	90	75	30	100	96

Table 11.5: Test Scores

The governor of state M says "State W pays 10% less than my state, we should cut salaries."

The governor of state W notes that his state's average salary of all tenured professors (full and associate) is $4,000 more than state M, He says "we need to cut salaries."

Exercise 11.2.3. Construct data which support both positions.

At this point, let's introduce a very useful notation to express complicated sums. This notation is

$$\sum_{i=k}^{n} a_i \,.$$

This is shorthand for

$$a_k + a_{k+1} + a_{k+2} + \cdots + a_{n-1} + a_n \,.$$

The $\sum$ means "sum." The letter i, called the *summation index*, takes on all the integer values from k (indicated in the $i = k$ part below the sum symbol) to n (indicated by the n on top of the sum symbol). The values k and n are called the *summation limits* or the *lower summation limit* and *upper summation limit.* In the example above, we used i as the summation index, but any letter could be used. The expression following the sum symbol is evaluated for each of the values of the summation index and then the values are added.

Here are a few examples of the summation notation, with some practice exercises. A simple example:

$$\sum_{i=1}^{4} 2i^2 = 2\cdot 1 + 2\cdot 4 + 2\cdot 9 + 2\cdot 16 = 60\,.$$

If $F(t)$ is given by

$$F(t) = \sum_{k=3}^{5} t^{k/2}\,,$$

then

$$F(2) = 2^{3/2} + 2^{4/2} + 2^{5/2} = 4 + 6\sqrt{2}$$

and

$$F(x^2) = x^3 + x^4 + x^5\,.$$

Finally, if

$$G(k) = \sum_{j=2}^{k^2} j\binom{j}{2}\,,$$

then

$$G(2) = 2\binom{2}{2} + 3\binom{3}{2} + 4\binom{4}{2} = 35\,.$$

Exercise 11.2.4. Compute

$$\sum_{l=2}^{5} \binom{2l-1}{l}\,.$$

Exercise 11.2.5. Compute

$$\sum_{r=1}^{5} (-1)^r \frac{2r-1}{r+1}\,.$$

Exercise 11.2.6. Let

$$f(t) = \sum_{j=0}^{t} \binom{2j}{j}^2\,.$$

Find $f(3)$.

Exercise 11.2.7. Let

$$g(y) = \sum_{t=1}^{4} (-1)^t \frac{y-t}{y^2+t}\,.$$

Find $g(4)$ and $g(x^2)$.

Exercise 11.2.8. Let

$$F(s) = \sum_{r=1}^{s} \frac{r(s-r+1)}{r+1}\,.$$

Find $F(4)$.

Here is a collection of examples of the use of this notation from equations and expressions from earlier chapters. From Chapter 1, the formula for the triangular numbers can be written

$$\sum_{j=1}^{n} j = n(n+1)/2 = \binom{n+1}{2},$$

since the symbol

$$\sum_{j=1}^{n} j$$

is shorthand for $1+2+3+\cdots+n$. Also from Chapter 1, recall the formula for the sum of the first n terms of a geometric sequence:

$$r^0 + r^1 + \cdots + r^{n-1} = \frac{r^n - 1}{r - 1}, \qquad r \neq 1\,. \tag{11.4}$$

Exercise 11.2.9. Express the left-hand side of Equation (11.4) using the summation notation.

From this same chapter, the infinite sum of the geometric sequence of powers of 1/2 is expressed by

$$\sum_{i=0}^{\infty} (1/2)^i = 2\,.$$

Notice that the upper summation limit is ∞. This means we take the finite sum with upper summation limit N, then let N get big.

From Chapter 2, the binomial theorem can be written

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}\,.$$

Exercise 11.2.10. Use the summation notation for the left-hand side of the equation which expresses the fact that the alternating sum of binomial coefficients is 0:

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots \pm \binom{n}{n} = 0\,.$$

From Chapter 3, the Catalan recursion is

$$C_n = C_0C_{n-1} + C_1C_{n-2} + \cdots + C_{n-2}C_1 + C_{n-1}C_0\,. \tag{11.5}$$

Exercise 11.2.11. Use the summation notation to express the right-hand side of Equation (11.5).

From Chapter 5, the base 10 representation of N is written

$$N = \sum_{i=0}^{n} d_i 10^i \,.$$

The base b representation is

$$N = \sum_{i=0}^{n} d_i b^i \,.$$

In this chapter, the computation of the mean of a binomially distributed random variable, which was done in Section 11.1, can be done as follows:

$$\begin{aligned}
E(X) &= \sum_{k=0}^{n} k \binom{n}{k} p^k q^{n-k} \\
&= \sum_{k=1}^{n} k \binom{n}{k} p^k q^{n-k} \\
&= \sum_{k=1}^{n} n \binom{n-1}{k-1} p^k q^{n-k} \\
&= \sum_{k=1}^{n} np \binom{n-1}{k-1} p^{k-1} q^{n-k} \\
&= np \sum_{k=1}^{n} \binom{n-1}{k-1} p^{k-1} q^{n-k} \\
&= np \sum_{k=0}^{n-1} \binom{n-1}{k} p^k q^{n-1-k} \\
&= np(q+p)^{n-1} \\
&= np \cdot 1 = np \,.
\end{aligned}$$

Exercise 11.2.12. Explain each step in this calculation.

The summation notation is quite general. For instance, the "handshake theorem" from Chapter 4 can be written

$$\sum_{v \in G} d(v) = 2E \,.$$

In this example, the sum is "over" vertices in the graph G; the number being summed is $d(v)$, the degree of the vertex; and the result is twice the number of edges.

The summation notation gives an easy way of writing the mean. If

$$x_1, x_2, \ldots, x_n$$

are the values of the data and $\bar{x}$ is their mean, then we could write

$$\bar{x} = \frac{x_1 + x_2 + \cdots + x_n}{n} .$$

Instead, we use the summation notation.

The mean of the set of numbers $x_1, x_2, \ldots, x_n$ is given by

$$\bar{x} = \frac{1}{n} \sum_{i=1}^{n} x_i , \tag{11.6}$$

Exercise 11.2.13. Work through Exercise 11.2.1 again, using Equation (11.6) for $\bar{x}$, explaining what n and x_i are.

Returning to our discussion of the mean, a disadvantage of the mean as a central measure is that a small number of exceptionally large or exceptionally small values can skew the mean so that it does not convey the true notion of centrality. Some examples of the type of data for which this happens are salaries and test scores.

Another central measure which compensates for this effect is the *median*. The median is the "middle" value of the list of numbers. That is, first order the list of number. If the list has odd length, the median is the middle number. If the list has even length, the median is the mean of the two middle numbers.

Exercise 11.2.14. Find the medians for the two test scores above.

Exercise 11.2.15. If there are a few exceptionally large values and many small values, will the median be larger than, equal to or less than the mean? Explain.

11.3 Measures of the Spread

Here are two sets of data: $(4, 4, 4, 3, 5, 4)$ and $(0, 8, 10, 4, 1, 1)$.

Exercise 11.3.1. Verify that the means of these two sets are equal.

The mean reduces a collection of numbers to a single number. In doing so, much information is lost. In the above example, the first group of numbers are bunched together. The second group is spread out.

Exercise 11.3.2. One thousand engineering students took a standard test. The average score was 71.3 out of 100. One thousand left-handed engineering students took the same test and scored 74.5 out of 100. Comment on the assertion: "Left-handed engineering students will usually score higher on this test than right-handed engineering students."

To recover some of the information lost when we computed the mean, we try to find a number to measure the "spread," i.e., how far from the mean the numbers are. One such measure might be to average the absolute value of the differences between the mean and the numbers.

Exercise 11.3.3. Do this for the two sets of data above. Why do we average the absolute values and not the differences themselves?

While this is a simple and natural measure of the spread, it is not what is typically used. Instead we use a slightly more complicated number. Why we use this number instead will be explained in the next section.

Instead of averaging the absolute values of the differences, we average the square of the differences between the mean and the numbers. Then we take the square root. The resulting number is called the *standard deviation*. As we shall see, it is an important number, almost as important as the mean or the median.

Exercise 11.3.4. Calculate the standard deviation for the two sets of data above.

Again, the summation notation gives a shorthand way of writing the standard deviation. Using the notation in Section 11.2 and letting the Greek letter σ be the standard deviation, we have the following.

The standard deviation of the set of data $x_1, x_2, \ldots, x_n$ with mean $\bar{x}$ is

$$\sigma = \sqrt{\frac{\sum_{i=1}^{n}(x_i - \bar{x})^2}{n}}\,. \tag{11.7}$$

Exercise 11.3.5. Demonstrate the use of Equation (11.7) on the two sets of data at the start of this section.

Suppose we square the data from the second set at the start of this section. We get $(0, 64, 100, 16, 1, 1)$. Now let's average this group of numbers. We get $30.33\cdots$. This is the mean of the squares. Now let's compute the square of the mean. That is 16. The difference is $14.33\cdots$, which is σ^2.

Exercise 11.3.6. Repeat this calculation for the other set of data at the start of this section.

Exercise 11.3.7. Explain why this method of calculating σ works. That is, use Equation (11.7) to show

$$\sigma^2 = \frac{1}{n}\sum_{i=1}^{n} x_i^2 - \bar{x}^2\,.$$

The method of calculating σ just described can be written in an especially elegant way.

If $\overline{x^2}$ is the mean of the squares, then

$$\sigma^2 = \overline{x^2} - \bar{x}^2\,. \tag{11.8}$$

That is, the square of the standard deviation is the difference of the mean of the squares and the square of the mean.

Exercise 11.3.8. Use Equation (11.8) to calculate the standard deviation for the two sets of test scores in Table 11.5.

11.4 The Central Limit Theorem

The central limit theorem (actually, it's a collection of theorems) simply says that in a wide variety of common situations, numerical data tend to be distributed in a bell-shaped curve called a *normal distribution*. Such random variables are said to be *normally distributed*. For example, suppose we graph the probability of rolling some number of 7's in fifty rolls of a pair of fair dice. The x-axis will be the number of 7's rolled in 50 rolls; the y-axis the probability of that many 7's. This graph is drawn in Figure 11.1.

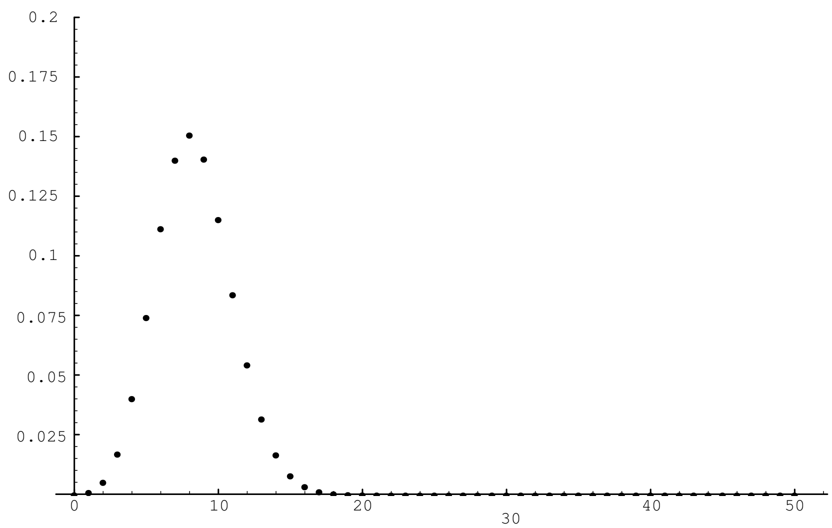


Figure 11.1: Fifty Dice Rolls

Exercise 11.4.1. What is the sum of the probabilities of the 51 different outcomes?

The normal distribution curve is the function

$$f(x) = \frac{1}{\sqrt{2\pi}} e^{-x^2/2} .$$

Notice that this amazing function contains both of the famous mathematical constants e and π! Even before trying to draw this function, we can say a lot about it.

Exercise 11.4.2. What is $f(0)$? Can $f(x)$ ever be negative? What happens to $f(x)$ when x grows very large? Show that $f(x) = f(-x)$.

Also, the total area between this curve and the x-axis is one.

Exercise 11.4.3. If you have a graphing calculator, graph this function.

The graph of f(x) is shown in Figure 11.2. Except for some rescaling and coordinate shifting, it is roughly the same curve as the probability distribution of rolling 7's.

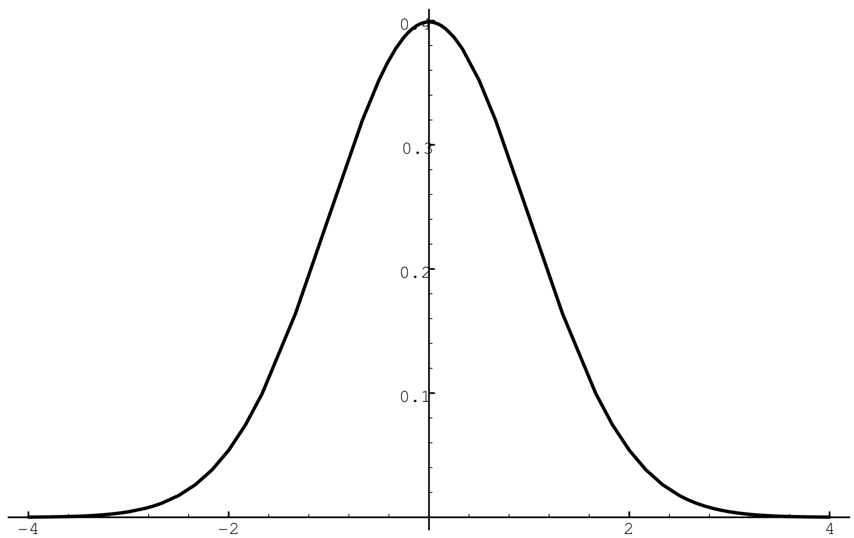


Figure 11.2: Normal Distribution

In fact, a distribution that is normally distributed has the property that one standard deviation becomes one unit of the normal curve in the following sense: the proportion of the area below the distribution curve, above the x-axis, and between the mean and one standard deviation away from the mean is approximately the same as the area between $x = 0$ and $x = 1$ in the normal curve. We thus say that the normal curve has mean 0 and standard deviation 1.

This relationship is important because the normal curve is very well understood. The total area between the normal curve and the x-axis is 1. Since this curve is symmetric about the y-axis, the area between the normal curve and the x-axis and to the right (or to the left) of the y-axis is $1/2$. Suppose we draw a vertical line some distance z along the x-axis. Let $A(z)$ be the area under the curve between the y-axis (the mean) and the line $x = z$. This is shown in Figure 11.3.

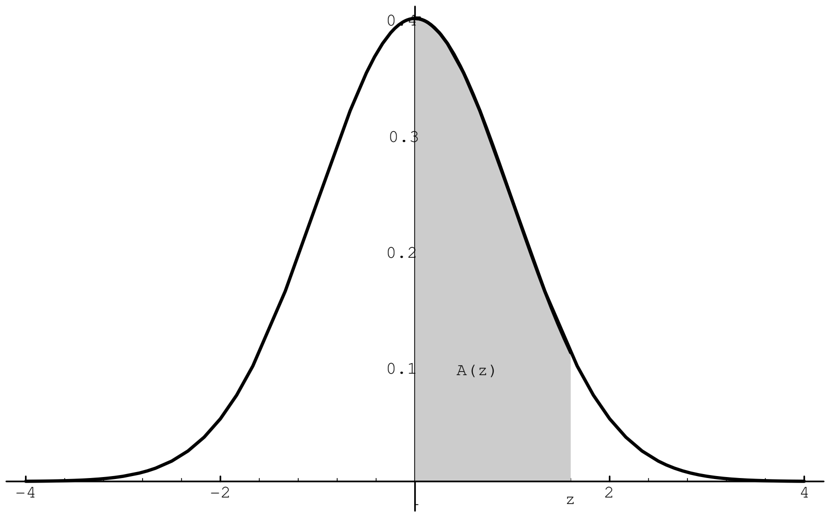


Figure 11.3: Area Under Normal Curve

Table 11.6 gives $A(z)$ for different values of z. Notice that $A(z)$ represents the area under the normal curve to the right of the y-axis. Then the symmetry of the normal curve implies that $2A(z)$ would represent the area under the curve and within z standard deviation units of the mean. Furthermore, for z above the mean, $1/2 + A(z)$ would represent the area under the curve and below z standard deviation units. The following three exercises illustrate these points.

Exercise 11.4.4. Suppose 25% of the area under the curve lies between the mean and z standard deviation units above the mean. What is z?

Exercise 11.4.5. Now suppose 95% of the area under the normal curve lies within z standard deviation units of the mean. What is z? What is z for 90%?

Exercise 11.4.6. Suppose 95% of the area under the normal curve lies below z standard deviation units above the mean. What is z? What is z for 90%?

Translating a normal distribution to the normal curve is similar to converting from Fahrenheit to Celsius. First compute how far from the mean a particular value is. Then determine how many standard deviations this is by dividing this distance by the standard deviation.

For example, suppose the mean for a particular test is 76 and the standard deviation is 7 and suppose we assume the scores are normally distributed. Let's try to approximate the number of scores 90 and above.

First, take $89.5 - 76 = 13.5$ and divide by 7 to get about 1.9. This is the number of standard deviation units that 89.5 is away from the mean. From

z	$A(z)$	z	$A(z)$	z	$A(z)$	z	$A(z)$	z	$A(z)$	z	$A(z)$	z	$A(z)$
0.00	0.0000												
0.01	0.0040	0.31	0.1217	0.61	0.2291	0.91	0.3186	1.21	0.3869	1.51	0.4345	1.81	0.4649
0.02	0.0080	0.32	0.1255	0.62	0.2324	0.92	0.3212	1.22	0.3888	1.52	0.4357	1.82	0.4656
0.03	0.0120	0.33	0.1293	0.63	0.2357	0.93	0.3238	1.23	0.3907	1.53	0.4370	1.83	0.4664
0.04	0.0160	0.34	0.1331	0.64	0.2389	0.94	0.3264	1.24	0.3925	1.54	0.4382	1.84	0.4671
0.05	0.0199	0.35	0.1368	0.65	0.2422	0.95	0.3289	1.25	0.3943	1.55	0.4394	1.85	0.4678
0.06	0.0239	0.36	0.1406	0.66	0.2454	0.96	0.3315	1.26	0.3962	1.56	0.4406	1.86	0.4686
0.07	0.0279	0.37	0.1443	0.67	0.2486	0.97	0.3340	1.27	0.3980	1.57	0.4418	1.87	0.4693
0.08	0.0319	0.38	0.1480	0.68	0.2517	0.98	0.3365	1.28	0.3997	1.58	0.4429	1.88	0.4699
0.09	0.0359	0.39	0.1517	0.69	0.2549	0.99	0.3389	1.29	0.4015	1.59	0.4441	1.89	0.4706
0.10	0.0398	0.40	0.1554	0.70	0.2580	1.00	0.3413	1.30	0.4032	1.60	0.4452	1.90	0.4713
0.11	0.0438	0.41	0.1591	0.71	0.2611	1.01	0.3438	1.31	0.4049	1.61	0.4463	1.91	0.4719
0.12	0.0478	0.42	0.1628	0.72	0.2642	1.02	0.3461	1.32	0.4066	1.62	0.4474	1.92	0.4726
0.13	0.0517	0.43	0.1664	0.73	0.2673	1.03	0.3485	1.33	0.4082	1.63	0.4484	1.93	0.4732
0.14	0.0557	0.44	0.1700	0.74	0.2703	1.04	0.3508	1.34	0.4099	1.64	0.4495	1.94	0.4738
0.15	0.0596	0.45	0.1736	0.75	0.2734	1.05	0.3531	1.35	0.4115	1.65	0.4505	1.95	0.4744
0.16	0.0636	0.46	0.1772	0.76	0.2764	1.06	0.3554	1.36	0.4131	1.66	0.4515	1.96	0.4750
0.17	0.0675	0.47	0.1808	0.77	0.2793	1.07	0.3577	1.37	0.4147	1.67	0.4525	1.97	0.4756
0.18	0.0714	0.48	0.1844	0.78	0.2823	1.08	0.3599	1.38	0.4162	1.68	0.4535	1.98	0.4761
0.19	0.0753	0.49	0.1879	0.79	0.2852	1.09	0.3621	1.39	0.4177	1.69	0.4545	1.99	0.4767
0.20	0.0793	0.50	0.1915	0.80	0.2881	1.10	0.3643	1.40	0.4192	1.70	0.4554	2.00	0.4773
0.21	0.0832	0.51	0.1950	0.81	0.2910	1.11	0.3665	1.41	0.4207	1.71	0.4564	2.01	0.4778
0.22	0.0871	0.52	0.1985	0.82	0.2939	1.12	0.3686	1.42	0.4222	1.72	0.4573	2.02	0.4783
0.23	0.0910	0.53	0.2019	0.83	0.2967	1.13	0.3708	1.43	0.4236	1.73	0.4582	2.03	0.4788
0.24	0.0948	0.54	0.2054	0.84	0.2995	1.14	0.3729	1.44	0.4251	1.74	0.4591	2.04	0.4793
0.25	0.0987	0.55	0.2088	0.85	0.3023	1.15	0.3749	1.45	0.4265	1.75	0.4599	2.05	0.4798
0.26	0.1026	0.56	0.2123	0.86	0.3051	1.16	0.3770	1.46	0.4279	1.76	0.4608	2.06	0.4803
0.27	0.1064	0.57	0.2157	0.87	0.3079	1.17	0.3790	1.47	0.4292	1.77	0.4616	2.07	0.4808
0.28	0.1103	0.58	0.2190	0.88	0.3106	1.18	0.3810	1.48	0.4306	1.78	0.4625	2.08	0.4812
0.29	0.1141	0.59	0.2224	0.89	0.3133	1.19	0.3830	1.49	0.4319	1.79	0.4633	2.09	0.4817
0.30	0.1179	0.60	0.2257	0.90	0.3159	1.20	0.3849	1.50	0.4332	1.80	0.4641	2.10	0.4821

z	$A(z)$	z	$A(z)$	z	$A(z)$	z	$A(z)$	z	$A(z)$	z	$A(z)$	z	$A(z)$
2.11	0.4826	2.41	0.4920	2.71	0.49664	3.01	0.49869	3.31	0.499534	3.61	0.499847	3.91	0.499954
2.12	0.4830	2.42	0.4922	2.72	0.49674	3.02	0.49874	3.32	0.499550	3.62	0.499853	3.92	0.499956
2.13	0.4834	2.43	0.4925	2.73	0.49683	3.03	0.49878	3.33	0.499566	3.63	0.499858	3.93	0.499958
2.14	0.4838	2.44	0.4927	2.74	0.49693	3.04	0.49882	3.34	0.499581	3.64	0.499864	3.94	0.499959
2.15	0.4842	2.45	0.4929	2.75	0.49702	3.05	0.49886	3.35	0.499596	3.65	0.499869	3.95	0.499961
2.16	0.4846	2.46	0.4931	2.76	0.49711	3.06	0.49889	3.36	0.499610	3.66	0.499874	3.96	0.499963
2.17	0.4850	2.47	0.4932	2.77	0.49720	3.07	0.49893	3.37	0.499624	3.67	0.499879	3.97	0.499964
2.18	0.4854	2.48	0.4934	2.78	0.49728	3.08	0.49896	3.38	0.499638	3.68	0.499883	3.98	0.499966
2.19	0.4857	2.49	0.4936	2.79	0.49737	3.09	0.49900	3.39	0.499651	3.69	0.499888	3.99	0.499967
2.20	0.4861	2.50	0.4938	2.80	0.49745	3.10	0.49903	3.40	0.499663	3.70	0.499892	4.00	0.499968
2.21	0.4864	2.51	0.4940	2.81	0.49752	3.11	0.49906	3.41	0.499675	3.71	0.499896		
2.22	0.4868	2.52	0.4941	2.82	0.49760	3.12	0.49910	3.42	0.499687	3.72	0.499900		
2.23	0.4871	2.53	0.4943	2.83	0.49767	3.13	0.49913	3.43	0.499698	3.73	0.499904		
2.24	0.4875	2.54	0.4945	2.84	0.49774	3.14	0.49916	3.44	0.499709	3.74	0.499908		
2.25	0.4878	2.55	0.4946	2.85	0.49781	3.15	0.49918	3.45	0.499720	3.75	0.499912		
2.26	0.4881	2.56	0.4948	2.86	0.49788	3.16	0.49921	3.46	0.499730	3.76	0.499915		
2.27	0.4884	2.57	0.4949	2.87	0.49795	3.17	0.49924	3.47	0.499740	3.77	0.499918		
2.28	0.4887	2.58	0.4951	2.88	0.49801	3.18	0.49926	3.48	0.499749	3.78	0.499922		
2.29	0.4890	2.59	0.4952	2.89	0.49807	3.19	0.49929	3.49	0.499758	3.79	0.499925		
2.30	0.4893	2.60	0.49534	2.90	0.49813	3.20	0.49931	3.50	0.499767	3.80	0.499928		
2.31	0.4896	2.61	0.49547	2.91	0.49819	3.21	0.49934	3.51	0.499776	3.81	0.499931		
2.32	0.4898	2.62	0.49560	2.92	0.49825	3.22	0.49936	3.52	0.499784	3.82	0.499933		
2.33	0.4901	2.63	0.49573	2.93	0.49830	3.23	0.49938	3.53	0.499792	3.83	0.499936		
2.34	0.4904	2.64	0.49585	2.94	0.49836	3.24	0.49940	3.54	0.499800	3.84	0.499938		
2.35	0.4906	2.65	0.49597	2.95	0.49841	3.25	0.49942	3.55	0.499807	3.85	0.499941		
2.36	0.4909	2.66	0.49609	2.96	0.49846	3.26	0.49944	3.56	0.499815	3.86	0.499943		
2.37	0.4911	2.67	0.49621	2.97	0.49851	3.27	0.49946	3.57	0.499822	3.87	0.499946		
2.38	0.4913	2.68	0.49632	2.98	0.49856	3.28	0.49948	3.58	0.499828	3.88	0.499948		
2.39	0.4916	2.69	0.49643	2.99	0.49861	3.29	0.49950	3.59	0.499835	3.89	0.499950		
2.40	0.4918	2.70	0.49653	3.00	0.49865	3.30	0.499517	3.60	0.499841	3.90	0.499952		

Table 11.6: Values of $A(z)$

Table 11.6 note that if $z = 1.9$, then $A(z) = 0.4713$. Thus, approximately 3% of the area under the normal curve is greater than $z = 1.9$, and so approximately 3% of the scores will be 90 or above.

Exercise 11.4.7. Why do you think 89.5 was used in the above calculation instead of 90?

Exercise 11.4.8. For the same test, about what percentage of the scores will be 80 or above?

Exercise 11.4.9. The average height of a U. S. female is 66 inches and the standard deviation is 4 inches. Assuming height is normally distributed, find the height which 95% of the females exceed.

Exercise 11.4.10. Using the information from the previous exercise, estimate the percentage of the females who are shorter than 6 feet tall.

Exercise 11.4.11. Again using the height statistics for U. S. females, estimate the percentage of females between 5 feet and 6 feet tall.

Math and statistics books use various notations for the number of standard deviation units away from the mean which corresponds to a particular outcome in a normally distributed experiment. We will simply say "standard deviations."

11.5 Applying the Central Limit Theorem

Let's work through the calculations involved in three applications of the central limit theorem. However, before we can do these examples, we need to know what the standard deviation is for the binomial distribution of Section 7.3. Fortunately, there is a well-known formula for this standard deviation. While the derivation of this formula takes us somewhat far afield, we can outline the steps. First, compute the mean. This will be the expected number of successes, and this calculation was done in Exercise 11.1.18. This mean is np, where n is the number of trials and p is the probability of success in each trial.

Next compute the mean of the squares. This requires more work. It is $p^2n(n-1) + np$.

Exercise 11.5.1. Use Equation (11.8) to show the following.

The standard deviation for a sequence of n independent trials with probability of success p is

$$\sigma = \sqrt{npq}\,, \tag{11.9}$$

where $q = 1 - p$.

For our first example, let's estimate the probability that if a pair of fair dice are tossed 180 times, 30 of the tosses will be sevens. If p denotes the probability of tossing seven, then $p = \frac{1}{6}$, $q = \frac{5}{6}$ and $n = 180$.

Exercise 11.5.2. Find the mean $\bar{x}$ and the standard deviation σ for this experiment.

The area under the normal curve that approximates the probability of rolling 30 sevens is the area between the values which correspond to 29.5 and 30.5.

To compute this area, we convert 30.5 to standard deviations.

Exercise 11.5.3. Show that 30.5 is 0.1 standard deviations above the mean. Similarly, show that 29.5 is 0.1 standard deviations below the mean.

Exercise 11.5.4. Use Table 11.6 to find the area under the normal curve between $x = -0.1$ and $x = +0.1$.

Exercise 11.5.5. Use a calculator to compute the probability of rolling 30 sevens exactly. Use the formula in Exercise 7.3.7.

Exercise 11.5.6. Use Table 11.6 to estimate the probability of rolling 40 or more sevens in the 180 tosses.

We all know that airlines regularly overbook flights. The reason they give is that they can fill empty seats left by "no-shows." Let's see what kind of calculation an airline might use to determine how many reservations to take.

Suppose a particular flight can carry 250 passengers. Suppose the airline has historical data which show that any one passenger who has booked that flight will actually take the flight with probability 0.9. How many seats can the airline book and not have to "bump" passengers 80% of the time? Figure 11.4 describes the situation

Before we can solve this, we first find the mean and the standard deviation as a function of the number of bookings. We assume that each passenger is an "independent trial" in an experiment, where success means the passenger takes the flight, and failure means the passenger is a no-show. We assume the binomial model applies.

Exercise 11.5.7. Use Exercise 11.1.18 to find the mean, $\bar{x}$, as a function of n, the number of passengers booked.

Exercise 11.5.8. Use Equation (11.9) to find the standard deviation, σ, as a function of n, the number of passengers booked.

Now that we know the mean and the standard deviation, we next find out the number of standard deviations above the mean such that 80% of the outcomes are smaller.

Exercise 11.5.9. Use Table 11.6 to find z so that 80% of the outcomes are smaller than z.

Exercise 11.5.10. Using the solutions above for $\bar{x}$, z and σ, find n by solving the equation $\bar{x} + z\sigma = 250$. Explain why the solution to this equation is the n we seek.

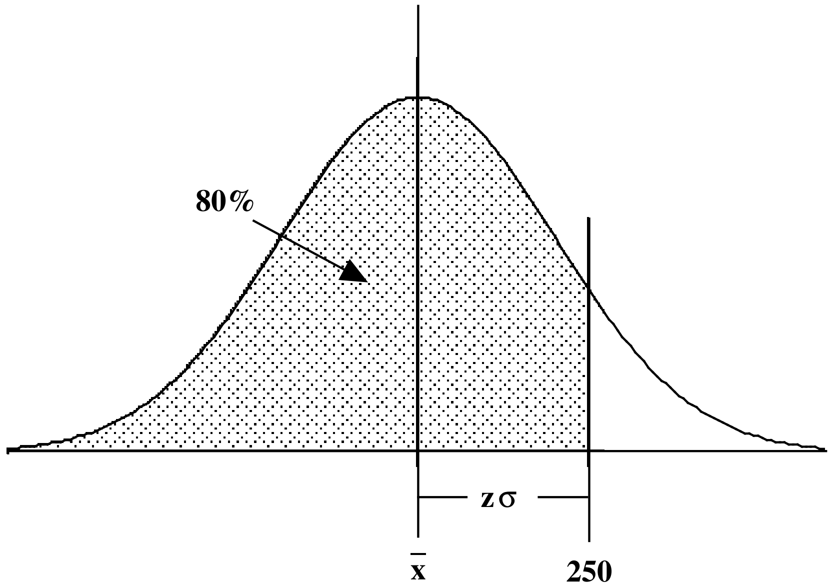


Figure 11.4: Airline Booking

Exercise 11.5.11. Suppose a flight carries 150 passengers. Suppose the probability that someone who buys a ticket actually takes the flight is 0.95. How many seats must be sold in order to avoid "bumping" 75% of the time?

Suppose that in a certain Minnesota lake, there are N walleyes. Suppose that 500 of these have been marked and returned to the lake. Later, a sample of 400 walleyes is collected and it is noted that 35 of these are marked.

Exercise 11.5.12. If the number of marked fish in the sample is in the same proportion as the number of marked fish in the lake, how many fish would be in the lake?

Let's call the number you obtained in Exercise 11.5.12 the *standard estimate*. It is very unlikely that the number of fish in the lake is exactly the standard estimate. We would like to "bracket" the standard estimate with upper and lower bounds, so that we know with some certainty that the number of fish in the lake is between our two bounds.

Once again, we need to know the mean and the standard deviation. First, we assume that our sample of 400 walleyes is 400 independent trials. This is not precisely correct, since this is probably sampling without replacement. But if the total number of fish is large, it is approximately correct. Second, we know that the probability of choosing a marked fish is $\frac{500}{N}$. Thus, the mean is $400 \cdot \frac{500}{N}$.

For the standard deviation, we can simplify calculations quite a bit by approximating the probability. If $p = q = \frac{1}{2}$, then $\sigma = \sqrt{npq} = \sqrt{400 \cdot \frac{1}{2} \cdot \frac{1}{2}} = 10$.

All other values of p and q give smaller σ, so if we approximate σ with 10, we will get a more conservative estimate of the number of fish.

Now that we have the mean and the standard deviation, we find out how many standard deviations on either side of the mean we must take to have a large percentage of the outcomes occur within that range. Let's make that large percentage equal to 95%. Figure 11.5 describes the situation.

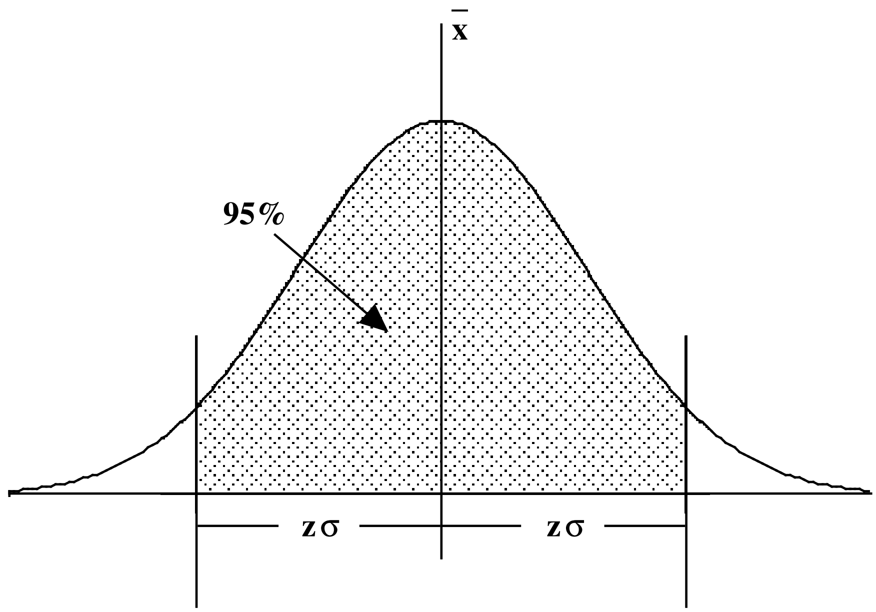


Figure 11.5: Fish in Lake

Exercise 11.5.13. Use Table 11.6 to find z such that 95% of the outcomes are between $-z$ and $+z$.

Since the mean is $400 \cdot \frac{500}{N}$, it is 95% certain that the number N will be such that

$$400 \cdot \frac{500}{N} - z\sigma \leq 35 \leq 400 \cdot \frac{500}{N} + z\sigma\,. \tag{11.10}$$

Exercise 11.5.14. Use Inequalities (11.10) and the approximation $\sigma = 10$ to find upper and lower bounds on the number of walleyes in the lake.

Exercise 11.5.15. Our estimate used the approximation of $p = q = \frac{1}{2}$ in the calculation of σ. Improve the estimate by using $p = \frac{500}{N}$ and $q = \frac{N-500}{N}$. Solving Inequalities (11.10) will now require solving quadratic equations.

You should note that the standard estimate lies between the two bounds obtained in either of the previous two exercises.

Exercise 11.5.16. Suppose only 100 fish have been marked, then a sample of 64 is taken and 10 in the sample are marked. Now estimate the number of fish in the lake with 95% confidence, assuming the sampling is done with replacement and approximating σ by letting $p = q = \frac{1}{2}$.

11.6 Odds

Probabilities are often stated in popular media as *odds*. The odds in favor of an event is the ratio of the probability of the event to the probability of the complement of the event. For instance, the probability of rolling seven with a pair of dice is 1/6. The odds in favor of rolling a seven would be the ratio 1/6 to 5/6 or

$$\frac{1/6}{5/6} = \frac{1}{5}\,.$$

Sometimes we write this as 1 : 5 or 1 to 5.

The odds against an event turns the ratio around: it is the ratio of the probability of the complement to the probability of the event. In the dice example above, the odds against rolling seven are 5 to 1.

To convert odds to probabilities is quite easy. If the odds against the Twins winning the World Series this year are 150 to 1, that means the probability of the Twins winning the World Series is $\frac{1}{150+1}$. If the odds against were 3 to 2, then the probability would be $\frac{2}{3+2}$.

Gambling odds are usually written as odds against (even though they are described, confusingly, as odds for). For example, at a racetrack, the odds listed on the tote board are the odds against each horse. These odds, of course, are not true probabilities. In fact, the sum of the corresponding probabilities will not even be one. Instead, these odds are a description of the payoff. A horse listed at 3 to 2 will pay \$5 back on a \$2 ticket if it wins.

Exercise 11.6.1. Suppose three horses are in a race, with odds listed as even (1 to 1), 3 to 1 and 2 to 1. Find the probability associated with each of these odds. What is the sum of these probabilities.

Exercise 11.6.2. Explain why the sum of the probabilities associated with the odds for a sporting event must add to a number greater than one.

Table 11.7 lists the "odds" that a newspaper assigned to possible Oscar winners.

Exercise 11.6.3. Compute the probabilities for each Oscar candidate.

Exercise 11.6.4. Suppose the newspaper accepted bets based on the odds in Table 11.7. In which categories is it possible to formulate a series of bets which will guarantee that you will win money? Pick one of these categories and formulate such a series of bets.

Picture	Director	Actor	Actress	Supp. Actor	Supp. Actress
FG 7 to 5	RZ 7 to 5	TH 3 to 1	JL 2 to 1	ML 2 to 1	DW 3 to 1
PF 3 to 1	QT 3 to 1	PN 4 to 1	JF 3 to 1	SLJ 3 to 1	UT 4 to 1
QS 6 to 1	RR 6 to 1	JT 5 to 1	WR 4 to 1	PS 5 to 1	HM 8 to 1
TSR 8 to 1	WA 10 to 1	MF 8 to 1	SS 5 to 1	CP 6 to 1	RH 8 to 1
FWAAF 12 to 1	KK 15 to 1	NH 15 to 1	MR 8 to 1	GS 8 to 1	JT 9 to 1

Table 11.7: Oscar Handicapping

Chapter 12

Finite Fields

In this chapter we describe one of the applications of finite fields. We will also learn how to construct finite fields.

12.1 A Review of Modular Arithmetic

In Chapter 6 we learned about finite number systems called modular arithmetic. Let's review a few of the ideas from that chapter. We start with the definition: for integers A and B and integer $m \geq 2$,

$$A \equiv B \mod m$$

means m divides $B - A$. For example, $23 \equiv 8 \mod 5$, $-4 \equiv 26 \mod 6$, etc.

Exercise 12.1.1. Is $19 \equiv 5 \mod 7$? Is $19 \equiv 5 \mod 5$?

Exercise 12.1.2. Describe all the integers which are $\equiv 1 \mod 2$.

We can then do arithmetic mod m by doing usual integer arithmetic and "reducing" mod m at various stages. It usually doesn't matter when we do the reduction. We can wait until after all our calculations are completed, or we can reduce after each calculation. "Reduction" amounts to dividing by m and taking the remainder.

For example, to compute $9 \cdot (13 \cdot (7 + 19) - 26 \cdot (4 - 13))$ in mod 5, we can first reduce mod 5 to $4 \cdot (3 \cdot (2 + 4) - 1 \cdot (4 - 3))$, then simplify to

$$4 \cdot (3 \cdot 1 - 1 \cdot 1) = 4 \cdot (3 - 1) = 4 \cdot 2 = 8,$$

which reduces to 3 in mod 5. Or we could compute

$$9 \cdot (13 \cdot (7 + 19) - 26 \cdot (4 - 13)) = 5148,$$

and then reduce to 3.

Exercise 12.1.3. Find an integer x such that

$$12 \cdot (19 - 5) + 36^2 \equiv x \mod 7.$$

Exercise 12.1.4. Find an integer x such that

$$18 \cdot 27^4 - 31^5 \equiv x \mod 6.$$

Sometimes we use the fact that $m - 1 \equiv -1 \mod m$.

Exercise 12.1.5. Compute $(42 - 17)^{50}$ in mod 13.

Notice that in the above examples, we avoided division. We saw in Chapter 6 that division in modular arithmetic is problematic. For instance, what is 2/4 in mod 6? Is it 2 (since $2 \cdot 4 \equiv 2 \mod 6$)? Or is it 5 (since $5 \cdot 4 \equiv 2 \mod 6$)? Or what is 1/4 in mod 6? No integer when multiplied by 4, then divided by 6, gives a remainder of 1.

We found in Chapter 6 that modular arithmetic was a field (that is, had a well-defined division) if and only if the modulus was prime (see Exercise 6.3.12). For this reason, we will stick to prime modulus for much of the remainder of this chapter.

Also in Chapter 6 we introduced solving linear equations and linear systems. These solutions usually involved finding multiplicative inverses. For small modulus, this can be done by trial and error (although a general method was described in Chapter 6).

Exercise 12.1.6. Find the multiplicative inverse of 3 in mod 11. Find the multiplicative inverse of 4 in mod 7.

Exercise 12.1.7. Solve: $3x + 5 \equiv 4 \mod 11$.

Exercise 12.1.8. Solve the system

$$3x + 5y \equiv 4 \mod 11$$
$$2x + 8y \equiv 6 \mod 11.$$

Finally, we related planar Cartesian geometry with a kind of finite geometry based on modular arithmetic. For instance, a "point" is just a pair (a, b) where a and b are numbers in our arithmetic system. For example, for mod 7 there are $7 \cdot 7$ points since there are 7 choices for a and 7 choices for b.

Exercise 12.1.9. How many points are there in mod p arithmetic?

To count lines, note that there are two kinds of lines: lines of the form

$$y = mx + b,$$

where m and b are chosen from the number system, and lines of the form

$$x = a,$$

where a is chosen from the number system. The second kind correspond to vertical lines in our usual Cartesian system.

For example, for mod 7, there are $7 \cdot 7$ lines of the first kind (7 choices for m and 7 choices for b) and there are 7 lines of the second kind (7 choices for a).

Exercise 12.1.10. How many lines are there in arithmetic mod p?

Exercise 12.1.11. How many points lie on the line $y \equiv 4x + 7 \mod 11$?

Exercise 12.1.12. If m and b are fixed, how many points lie on the line $y \equiv mx + b \mod p$?

Exercise 12.1.13. If a is fixed, how many points lie on the line $x \equiv a \mod p$?

Exercise 12.1.14. How many lines pass through the point $(6, 3)$ in mod 7 arithmetic?

Exercise 12.1.15. How many lines pass through the point (r, s) in mod p arithmetic?

Exercise 12.1.16. Find all the lines which pass through the points $(6, 3)$ and $(5, 5)$ in mod 7 arithmetic.

Exercise 12.1.17. If p is prime, how many lines pass through two points in mod p arithmetic?

12.2 A Tournament

Nine students are finalists in a school's spelling contest. These nine students are:

Allison	Bernard	Christine
Debbie	Edward	Frank
Georgia	Heather	Isaac

You have been given the job of organizing a tournament among these nine students. You have decided to choose them three at a time and have a small contest among those three. If you arrange them in three groups of three, each finalist would participate in one such contest. For instance, the three contests might be given in Table 12.1.

Notice that while Allison competes against Bernie and Chris, she does not compete against Deb or Ed or any of the other six students.

On the other hand, if you ran contests among every group of three students, you would have to run $\binom{9}{3} = 84$ separate contests.

You decide to find some middle ground—some set of contests in which the following three conditions are satisfied:

Contest 1	Contest 2	Contest 3
Allison	Deb	Georgia
Bernie	Ed	Heather
Chris	Frank	Isaac

Table 12.1: Three Contests

i. Every student participates the same number of times;

ii. Every contest is among three students;

iii. Every pair of students is in the same number of contests.

In the example of three groups of three above, condition (i) condition (ii) are satisfied, but not condition (iii). If every group of three students is used, all three conditions are satisfied.

Exercise 12.2.1. If every group of three students is used, find the number of contests each student is in.

Each contest contains $\binom{3}{2} = 3$ pairs of students and there are 84 contests, so there are $3 \cdot 84 = 252$ student-pairs appearing in the contests. On the other hand, there are $\binom{9}{2} = 36$ pairs of students. Therefore, each pair of students must appear in $252/36 = 7$ contests. Variations of this argument will be used several times below.

More generally, let C stand for the number of contests. Since each contest has 3 participants, there will be $3C$ names written down in the table of contests and participants. On the other hand there are 9 different names.

Exercise 12.2.2. Show that the number of contests that each student participates in is $C/3$. Use this to explain why you shouldn't run ten contests.

Exercise 12.2.3. Show that every pair of students will be in $C/12$ contests.

Therefore, you decide to arrange twelve contests, each among three students, so that each student is in four contests and every pair of students is in one contest together. These contests are described in Table 12.2.

Exercise 12.2.4. Verify that in these contests, every student is in four contests and every pair of students is in one contest.

Is there a more "mathematical" construction of these contests, one that does not rely on trial and error? You may have noticed already the similarity between the preceding exercises and our enumeration of points, lines, points on a line and lines through a point in Section 12.1.

Contest 1	Contest 2	Contest 3	Contest 4
Allison Bernie Chris	Deb Ed Frank	Georgia Heather Isaac	Allison Deb Georgia
Contest 5	**Contest 6**	**Contest 7**	**Contest 8**
Bernie Ed Heather	Chris Frank Isaac	Allison Ed Isaac	Bernie Frank Georgia
Contest 9	**Contest 10**	**Contest 11**	**Contest 12**
Chris Deb Heather	Allison Frank Heather	Bernie Deb Isaac	Chris Ed Georgia

Table 12.2: Twelve Contests

Student	corresponds to point
Allison	$(0,0)$
Bernie	$(0,1)$
Chris	$(0,2)$
Deb	$(1,0)$
Ed	$(1,1)$
Frank	$(1,2)$
Georgia	$(2,0)$
Heather	$(2,1)$
Isaac	$(2,2)$

Table 12.3: Points-to-Students

If we use mod 3 arithmetic, then we know that the plane has nine points and each line on the plane contains three points. There are a total of twelve lines. Furthermore, every pair of points determines one line.

Therefore, the finite geometry of mod 3 arithmetic provides the precise mechanism for constructing our tournament! The nine points correspond to the nine students; the twelve lines correspond to the twelve contests. Since each line contains three points, each contest will have three students. Each point is on four different lines, so each student will be in four contests. Two points are on exactly one line, so every pair of students will be in exactly one contest.

Here is the precise translation. The points are given in Table 12.3.

And the lines are are given in Table 12.4.

Exercise 12.2.5. Construct a tournament with 25 participants and 30 "contests" among five players, so that each player is in 6 contests and each pair of players is in one contest. Base your construction on mod 5 arithmetic.

Line	equation:	which contains			corresponding to		
Line 1	$x = 0$	$(0,0)$	$(0,1)$	$(0,2)$	A	B	C
Line 2	$x = 1$	$(1,0)$	$(1,1)$	$(1,2)$	D	E	F
Line 3	$x = 2$	$(2,0)$	$(2,1)$	$(2,2)$	G	H	I
Line 4	$y = 0$	$(0,0)$	$(1,0)$	$(2,0)$	A	D	G
Line 5	$y = 1$	$(0,1)$	$(1,1)$	$(2,1)$	B	E	H
Line 6	$y = 2$	$(0,2)$	$(1,2)$	$(2,2)$	C	F	I
Line 7	$y = x$	$(0,0)$	$(1,1)$	$(2,2)$	A	E	I
Line 8	$y = x + 1$	$(0,1)$	$(1,2)$	$(2,0)$	B	F	G
Line 9	$y = x + 2$	$(0,2)$	$(1,0)$	$(2,1)$	C	D	H
Line 10	$y = 2x$	$(0,0)$	$(1,2)$	$(2,1)$	A	F	H
Line 11	$y = 2x + 1$	$(0,1)$	$(1,0)$	$(2,2)$	B	D	I
Line 12	$y = 2x + 2$	$(0,2)$	$(1,1)$	$(2,0)$	C	E	G

Table 12.4: Lines-to-Contests

Exercise 12.2.6. Try constructing a tournament with 16 participants and 20 "contests" among four players, so that each player is in five contests and each pair of players is in one contest, basing your construction on mod 4 arithmetic. What goes wrong?

12.3 A Field with Four Elements

In this section we will construct a finite field with four elements. This field cannot be arithmetic mod 4 because the number 2 in mod 4 does not have a multiplicative inverse.

This missing multiplicative inverse was the defect you found in Exercise 12.2.6 above. Therefore, if we wish to construct the tournament described in Exercise 12.2.6, we will have to go about it in a different way.

Let's start by giving names to the four elements in this field. Let's call them 0, 1, a and b. We know the field must have additive and multiplicative identities. Those are 0 and 1 respectively. We must now describe how to do arithmetic in this field. We do this by constructing addition and multiplication tables.

The partial construction of the addition table is given in Table 12.5. The entries that have been filled in are the values we know from the additive identity axiom.

The partial construction of the multiplication table is given in Table 12.6. The entries that have been filled in are the values we know from the multiplicative identity axiom and from the fact that $0 \cdot x = 0$ in every field.

Uniqueness of the additive inverse tells us that each row and each column of the addition table is some permutation of all the elements of the field. Uniqueness of the multiplicative inverse tells us that each row and each column (except for the first row and first column) is some permutation of all the elements of the field.

+	0	1	a	b
0	0	1	a	b
1	1	?	?	?
a	a	?	?	?
b	b	?	?	?

Table 12.5: Addition Table

$\times$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	?	?
b	0	b	?	?

Table 12.6: Multiplication Table

Exercise 12.3.1. Fill in the remaining values of the table. Use the facts above plus the other field axioms (especially the distributive axiom) to help you.

Exercise 12.3.2. Construct a tournament with 16 participants and 20 "contests" among four players, so that each player is in five contests and each pair of players is in one contest, basing your construction on the field you constructed in Exercise 12.3.1.

12.4 Constructing Finite Fields

The construction you performed in Exercise 12.3.1 is obviously too hard in general. How are we to construct a field with, say, 64 elements by just fiddling with the field axioms and making up multiplication and addition tables?

Fortunately there is a general method for constructing such fields, a method that you have, in fact, already learned!

In Chapter 10, you learned that by finding an irreducible polynomial over the rational numbers, you could build a larger field by incorporating a root of that polynomial into the field. Thus we constructed fields such as in Section 10.6, or the complex numbers themselves.

The same construction works if we start with a finite field instead of the rationals or reals. For example, let's start with the simplest of all fields, the field with two elements. Let's call this field F_2.

Exercise 12.4.1. Show that $x^2 + x + 1$ has no roots in F_2. Conclude that $x^2 + x + 1$ is irreducible over F_2.

Now we invent a root of this polynomial. Let's call it r. Since r is a root of $x^2 + x + 1$, $r^2 + r + 1 = 0$.

Exercise 12.4.2. Show that $r^2 = r + 1$ (remember, do your coefficient arithmetic in mod 2).

Now incorporate r into F_2 (just as we incorporated i into the reals to form the complex numbers). We construct all expressions of the form $ar + b$ where a and b are in F_2. This gives us our four elements: 0, 1, r and $r + 1$. Using the notation from Chapter 10, this is $F_2(r)$.

Exercise 12.4.3. Build the multiplication and addition tables for these four elements. Be sure to use the fact that $r^2 = r + 1$ in the multiplication table and that $r + r = 2r \equiv 0 \mod 2$ in the addition table.

Exercise 12.4.4. Show that the field you constructed in Exercise 12.4.3 is the same (except for a relabeling) as the field you constructed in Exercise 12.3.1.

Exercise 12.4.5. Find a cubic irreducible polynomial over F_2. Use a root of this polynomial to construct a field with eight elements. Build the addition and multiplication tables.

Exercise 12.4.6. Find a quadratic irreducible polynomial over F_3, mod 3 arithmetic. Use a root of this polynomial to construct a field with nine elements. Build the addition and multiplication tables.

It is not too hard to show that there are irreducible polynomials of every degree over every finite field. The number of elements in the corresponding extension field will be p^n where p is the number of elements in the original field and n is the degree of the polynomial.

Therefore, there are finite fields with q elements whenever q is a power of a prime number.

But even more is known. If q is a power of a prime number, say $q = p^n$, and F is a field with q elements, then, except for a relabeling, F is the same as the field we get by incorporating a root of some irreducible polynomial of degree n over F_p, the mod p field.

Furthermore, if q is not a power of a prime number, then there is no finite field with q elements.

In summary, the only finite fields are modular arithmetic with prime modulus, or simple algebraic extensions thereof. The number of elements in such fields is the prime modulus raised to a power equal to the degree of the extension.

Exercise 12.4.7. Find all q from 2 to 50 for which there is a finite field with q elements.

Exercise 12.4.8. Describe in words how to go about constructing a field with 243 elements.

Contest 1	Contest 2	Contest 3	Contest 4	Contest 5
A	A	A	B	B
B	C	B	C	C
D	E	F	D	E
Contest 6	Contest 7	Contest 8	Contest 9	Contest 10
C	A	D	B	A
D	D	E	E	C
F	E	F	F	F

Table 12.7: Another Tournament

12.5 Tournaments Revisited

Finite fields are not the only way to construct the kind of tournaments described in Section 12.2. For instance, a tournament for six players (A, B, C, D, E, F) with 10 contests, each contest involving three players, each player in five contests, and each pair of players in two contests is given in Table 12.7

Exercise 12.5.1. Verify that these ten contests satisfy the conditions stated above.

As we saw in the first section, certain divisibility conditions must be satisfied before we can attempt to construct such a tournament.

Let N be the number of players, C be the number of contests, R be the number of players per contest and D be the number of contests that each player is in.

Exercise 12.5.2. Show that $ND = CR$.

Finally, let P be the number of contests each pair of players is in.

Exercise 12.5.3. Show that $P(N-1) = D(R-1)$.

Exercise 12.5.4. Find N, D, R, C, and P for each of the tournaments in this Chapter.

The conditions in Exercises 12.5.2 and 12.5.3 are not enough to define when we can construct such tournaments. In fact, there is no known general rule.

Exercise 12.5.5. Arithmetically verify that $N = 36$, $D = 7$, $C = 42$, $R = 6$ and $P = 1$ satisfy the conditions in Exercises 12.5.2 and 12.5.3.

The parameters in Exercise 12.5.5 would be exactly what we would get if we could construct a tournament using lines in a field with six elements. But no such field exists and no such tournament exists!

Finally, we have been discussing tournaments, but these objects arise in other contexts. For example, suppose we are responsible for taste-testing granolas.

We want to test sixteen different brands and we have 20 different people to test them.

Exercise 12.5.6. Describe how the 20 people can test the 16 brands so that each person tests four brands, each brand is tested five times, and each pair of brands is tested by the same person exactly once.

Chapter 13

Areas and Triangles

In this chapter we will learn how to compute areas of various geometric objects. We will learn some things about triangles and circles, and about the Pythagorean Theorem.

13.1 Areas of Some Simple Figures

Let's start with the simplest geometric figure we know: a rectangle. A *rectangle* is a four-sided polygon (four-sided polygons are called *quadrilaterals*) such that all the angles are right angles. It follows from theorems in plane geometry that opposite sides have equal length. You no doubt learned the formula for the area of a rectangle as "length times width."

Exercise 13.1.1. Suppose a rectangle has length 6 units and width 4 units. Give an argument why its area is 24 square units.

Exercise 13.1.2. Suppose a rectangle has length 8/3 units and width 5/8 units. Give an argument why its area is 5/3 square units. Hint: describe the length as 8 "units" of size 1/3 and the width as 5 "units" of size 1/8. Now argue that the rectangle contains 40 "rectangular units" all the same size. Then explain why each of these "rectangular units" has size 1/24 square unit.

Exercise 13.1.3. Suppose a rectangle has length π and width $\pi/3$. Why do you think the area of this rectangle is $\pi^2/3$?

Now let's move to some other polygons. A *parallelogram* is a quadrilateral with opposite sides parallel. A theorem from plane geometry states that opposite sides of a parallelogram are equal.

Exercise 13.1.4. Suppose A and B are two parallelograms, each with two sides of length 6 and two sides of length 9. Do A and B have the same area?

Exercise 13.1.5. Suppose A is a parallelogram and has one side length a and the other side length b. Is the area of A equal to ab? Why or why not?

Let's pick one side of the parallelogram to call its *base*. Its *height* is then the perpendicular distance between the base and the opposite side.

Exercise 13.1.6. Using Figure 13.1, show that the area of a parallelogram of height h and base b is bh.

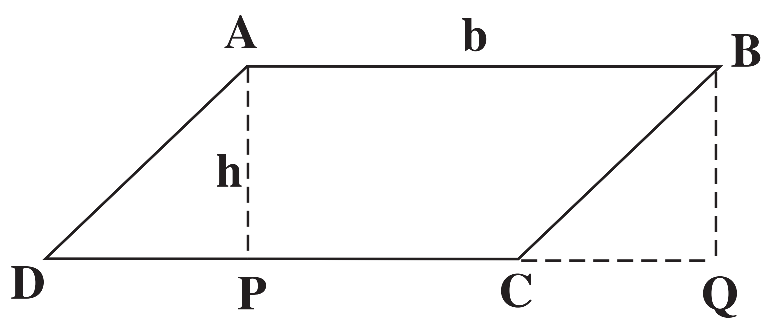


Figure 13.1: Area of parallelogram

A *triangle* is a three-sided polygon. If one side is called its *base*, then its *height* is the perpendicular distance from the opposite vertex to the base (or an extension of the base). Any triangle has three possible bases and three corresponding heights.

Exercise 13.1.7. Using Figure 13.2, show that the area of a triangle of height h and base b is $bh/2$.

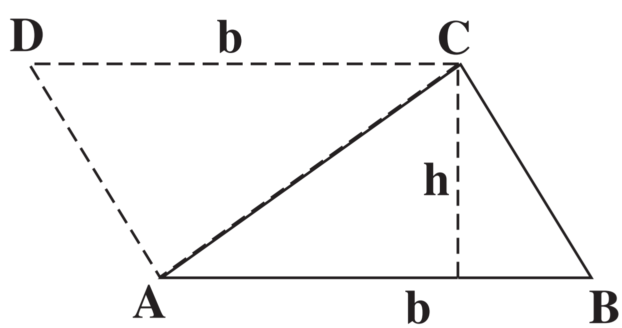


Figure 13.2: Area of triangle

Exercise 13.1.8. Triangle ABC in Figure 13.2 is an *acute* triangle, that is, all the angles are less than 90°. Does the argument in the figure still work if the triangle is *obtuse*, that is, has an angle of greater than 90°?

A *trapezoid* is a quadrilateral with one pair of opposite parallel sides. These two parallel sides are called the two *bases*, and the perpendicular distance between them is the *height*.

Exercise 13.1.9. Using Figure 13.3, show that the area of a trapezoid of height h and bases a and b is $(a + b)h/2$.

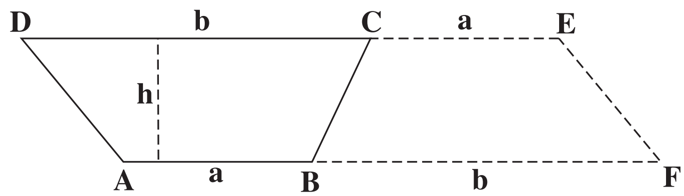


Figure 13.3: Area of trapezoid

Exercise 13.1.10. Suppose a line is drawn connecting the two points 2/3 of the way up two sides of a triangle (see Figure 13.4). That is, the length of segment AC is 2/3 the length of segment AP, while the length of segment BD is 2/3 the length of segment BP. It can be shown using theorems from plane geometry that lines CD and AB are parallel, so that quadrilateral $ABDC$ is a trapezoid. Suppose the area of triangle ABP is 1 square unit. Find the area of $ABDC$.

Exercise 13.1.11. If the perimeter of a triangle increases, does the area necessarily increase? Either construct an example where this doesn't happen or give a reason why it does. Now repeat this question, replacing the word "triangle" with "parallelogram," "rectangle," and "square," respectively.

13.2 Areas of Similar Figures

Suppose X and X' are two polygons with the same number of sides. An *angle-side correspondence* is a one-to-one correspondence between the vertices of X and the vertices of X', in such a way that if AB is a side of X and A corresponds to A' in X' and B corresponds to B' in X', then $A'B'$ is a side in X'. See Figure 13.5.

Two polygons are *congruent* if there is an angle-side correspondence between them such that corresponding angles are equal and corresponding sides are equal.

Another name for congruent polygons is *isometric* polygons. Isometric means equal lengths; an isometry is a transformation from one geometric object into another which preserves all distances. Figure 13.6 illustrates this idea. All the quadrilaterals in this figure are congruent.

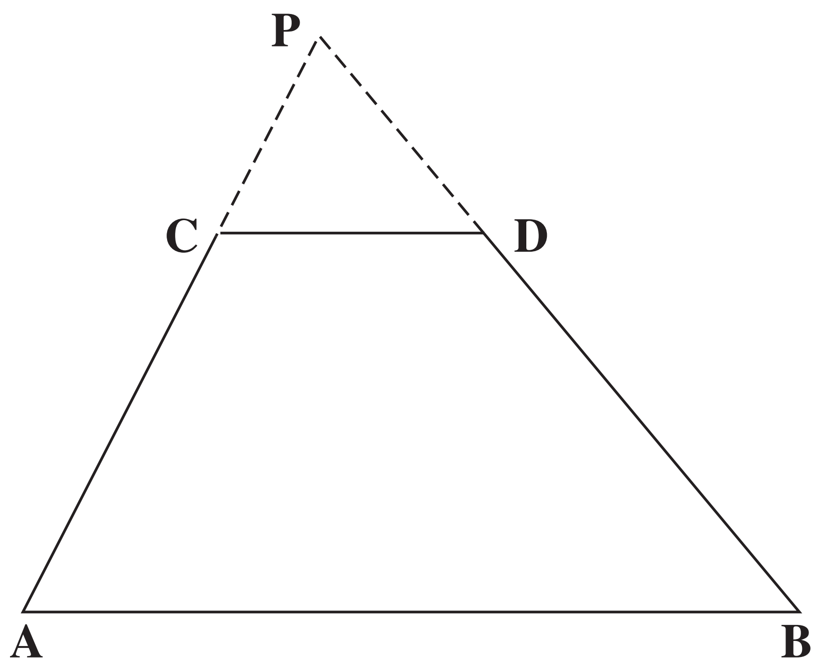


Figure 13.4: Triangle with top removed

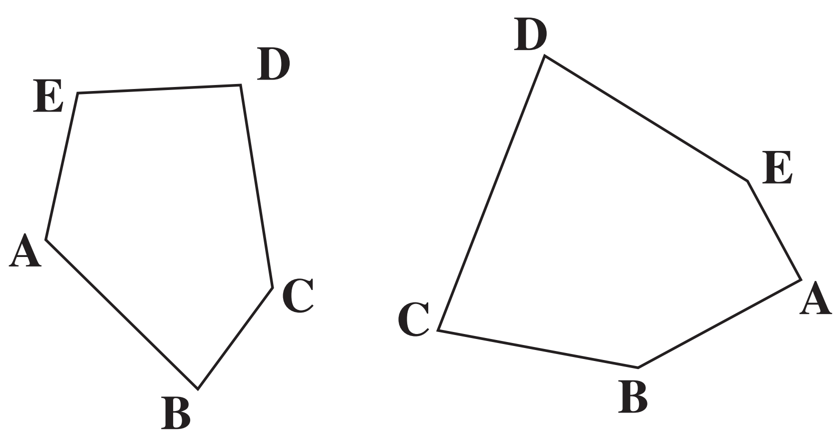


Figure 13.5: An angle-side correspondence

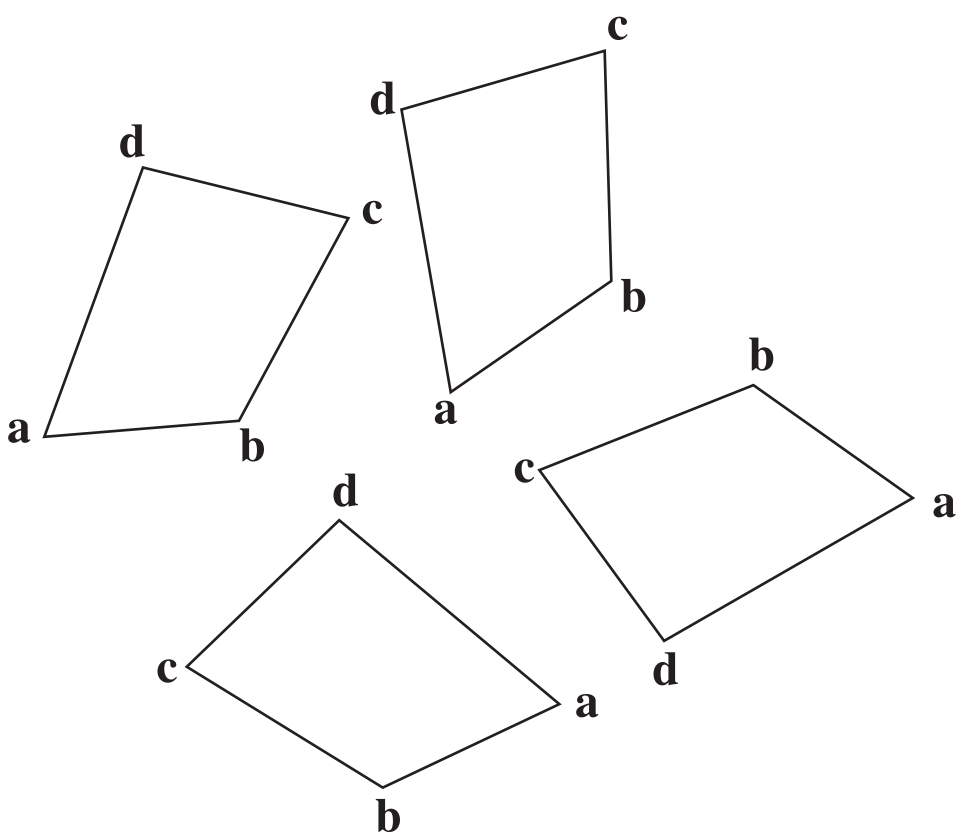


Figure 13.6: Congruent quadrilaterals

The fact that the angles must be preserved is quite important. For example, Figure 13.7 shows two parallelograms whose sides are equal but which are not congruent.

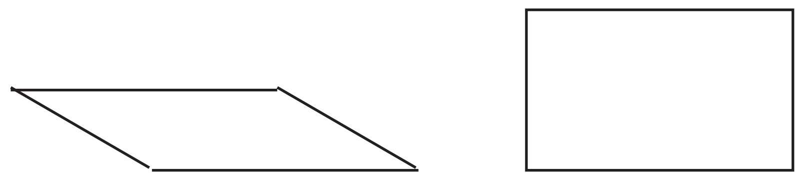


Figure 13.7: Not congruent parallelograms

Three important theorems from plane geometry, called SAS, ASA and SSS, respectively, tell when triangles are congruent. We will gather these three theorems into a single statement.

Theorem 22.

SAS: *If the lengths of the two sides and the included angle of one triangle equal the lengths of the two sides and the included angle of another triangle, the two triangles are congruent.*

ASA: *If the two angles and the length of the included side of one triangle equal the two angles and the length of the included side of another triangle, the two triangles are congruent.*

SSS: *If the lengths of the three sides of one triangle equal the lengths of the three sides of another triangle, the two triangles are congruent.*

Exercise 13.2.1. Do you think the triangles in Figure 13.8 are congruent? Why or why not?

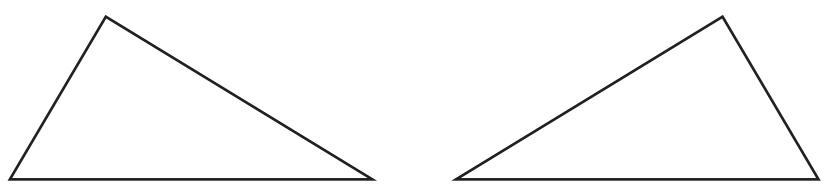


Figure 13.8: Congruent triangles?

Exercise 13.2.2. If the three sides and the two included angles of one quadrilateral equal the three sides and the two included angles of another quadrilateral, are they congruent? Why or why not?

Exercise 13.2.3. If the three angles and the two included sides of one quadrilateral equal the three angles and the two included sides of another quadrilateral, are they congruent? Why or why not?

Exercise 13.2.4. If the four sides of one quadrilateral equal the four sides of another quadrilateral (in the same order), are they congruent? Why or why not?

An important property of congruent polygons is that they have equal areas.

Exercise 13.2.5. Suppose two triangles have sides with lengths 12, 14 and 7. Must their areas be the same? Why or why not? Hint: use SSS.

Suppose a is a line segment. We will denote the length of a by $\mathcal{L}(a)$. Also, if P is a polygon, we will denote its area by $\mathcal{A}(P)$.

Two polygons are *similar* if there is an angle-side correspondence such that the angles are all equal and the sides are in equal ratio. That is, if a corresponds to a' and b to b', then

$$\frac{\mathcal{L}(a)}{\mathcal{L}(a')} = \frac{\mathcal{L}(b)}{\mathcal{L}(b')} .$$

We call this common ratio the *similarity ratio*.

Another theorem from plane geometry tells us when two triangles are similar.

Theorem 23. *Two triangles are similar if two of the angles of one equal two of the angles of the other.*

Exercise 13.2.6. Are two quadrilaterals similar if the angles of one equal the corresponding angles of the other? Why or why not?

Suppose T and T' are two triangles and suppose there is an angle-side correspondence between T and T' such that the sides lengths are in equal ratio. Construct a third triangle T'' as follows. Let two angles of T'' be two of the angles of T, and let the side between these two angles have the same length as the corresponding side in T'. By ASA, this determines T''.

Exercise 13.2.7. Why is T'' similar to T?

Since T'' is similar to T, the ratio of its side lengths to the corresponding side lengths of T is constant, so the side lengths of T'' are the same as the side lengths of T'.

Exercise 13.2.8. Why is T' congruent to T''?

Exercise 13.2.9. Why is T similar to T'?

Summarizing these last three exercises, if T and T' are two triangles whose side lengths are in equal ratio, then T and T' similar.

Let T be a right triangle and D be the triangle obtained by doubling all the sides of T.

Exercise 13.2.10. Is D a right triangle? Why or why not?

Exercise 13.2.11. Prove D is similar to T.

Exercise 13.2.12. Suppose h is any altitude in T and let k be the corresponding altitude in D. Show $k = 2h$.

Exercise 13.2.13. Prove that $\mathcal{A}(D) = 4\mathcal{A}(T)$.

Exercise 13.2.14. Let R be formed from T by tripling all the sides of T. Prove R is similar to T. Show that if h is any altitude of T and m is the corresponding altitude of R, then $m = 3h$. Finally, show that $\mathcal{A}(R) = 9\mathcal{A}(T)$.

Exercise 13.2.15. Let S be formed from T by multiplying all the sides of T by s. Prove S is similar to T. Show that if h is any altitude of T and p is the corresponding altitude of S, then $p = sh$. Finally, show that $\frac{\mathcal{A}(S)}{\mathcal{A}(T)} = s^2$.

Exercise 13.2.15 illustrates a fundamental principal of similar geometric objects: linear dimensions grow linearly with the similarity ratio, while area dimensions grow quadratically.

Exercise 13.2.16. Let T and S be two similar triangles (not necessarily right) with similarity ratio r. Show that the ratio of the altitudes of T to the corresponding altitudes of S is also r. Show that the ratio of the perimeter of T to the perimeter of S is r. Show that the ratio of $\mathcal{A}(T)$ to $\mathcal{A}(S)$ is r^2.

Exercise 13.2.17. Let T and S be two similar polygons with similarity ratio r. Show that the ratio of the perimeter of T to the perimeter of S is r. Show that the ratio of $\mathcal{A}(T)$ to $\mathcal{A}(S)$ is r^2.

13.3 The Pythagorean theorem

The Pythagorean Theorem is perhaps the most famous theorem in mathematics.

> **Theorem 24.** *If T is a right triangle with leg lengths a and b and hypotenuse length c, then $a^2 + b^2 = c^2$. That is, the sum of the squares of the two leg lengths equals the square of the hypotenuse length.*

There are literally hundreds of proofs of the Pythagorean Theorem, some dating back over 2000 years, and one due to President James Garfield. We will give a couple of these proofs. Both are based on some simple geometry. First, look at Figure 13.9.

Exercise 13.3.1. Prove that the angle α is a right angle.

Now look at Figure 13.10.

Exercise 13.3.2. Use Figure 13.10 to prove that $a^2 + b^2 = c^2$. Hint: Why is the quadrilateral $PQRS$ a square? Why is $\mathcal{A}(PQRS)$ the same as the sum of $\mathcal{A}(ABCD)$ and $\mathcal{A}(DEFG)$?

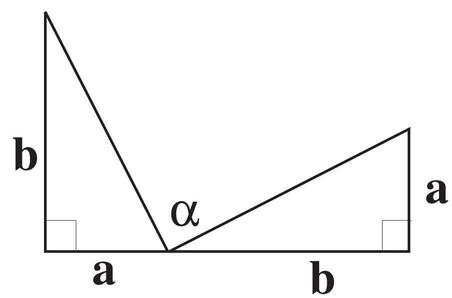


Figure 13.9: Two congruent right triangles

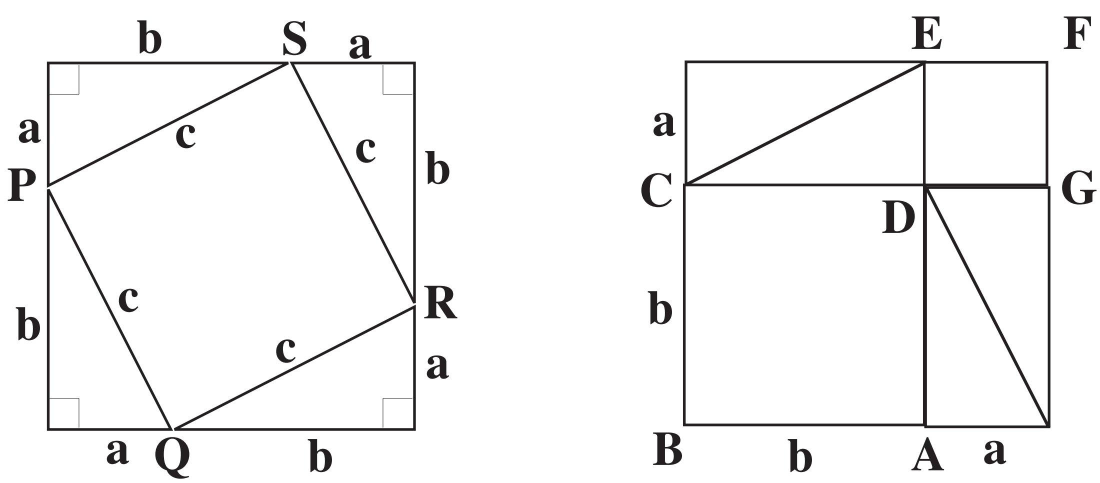


Figure 13.10: First proof of the Pythagorean Theorem

Another proof is based on Figures 13.11 and 13.12. In Figure 13.11, triangles APB and PCD are congruent right triangles with sides a and b and hypotenuse c.

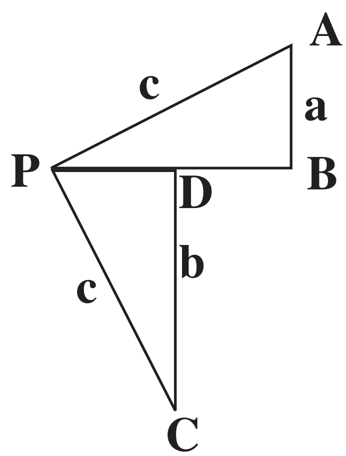


Figure 13.11: Two congruent right triangles

Exercise 13.3.3. Show the angle APC is a right angle.

Now draw four congruent right triangles, as shown in Figure 13.12. From the previous exercise, $PQRS$ is a square.

Exercise 13.3.4. Prove that $a^2 + b^2 = c^2$ by computing the total area of the square in two ways.

Exercise 13.3.5. Prove the "converse" of the Pythagorean Theorem. That is, suppose T is a triangle whose side lengths are a, b and c, and suppose $a^2 + b^2 = c^2$. Prove that T is a right triangle. Hint: Use SSS.

SSS tells us that any two triangles with the same side lengths must be congruent, and therefore have the same area. We should then be able to compute this area just using the lengths of the three sides. In fact, there is a beautiful formula, called Heron's formula, for the area of a triangle as a function of the three side lengths.

Theorem 25. *If a triangle T has side lengths a, b and c, then the area of T is given by*

$$\mathcal{A}(T) = \sqrt{s(s-a)(s-b)(s-c)}\,,$$

where

$$s = \frac{a+b+c}{2}\,.$$

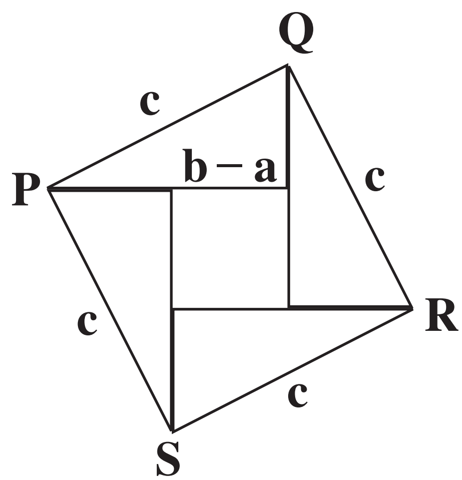


Figure 13.12: Second proof of the Pythagorean Theorem

The factors $s-a$, $s-b$ and $s-c$ have a simple form.

Exercise 13.3.6. Show the following:

$$\begin{aligned} s-a &= \frac{-a+b+c}{2} \\ s-b &= \frac{a-b+c}{2} \\ s-c &= \frac{a+b-c}{2}\,. \end{aligned}$$

There are a number of proofs of Heron's formula. We will give the most direct, which uses the Pythagorean theorem twice. We will use Figure 13.13.

In this figure, we wish to compute the area of triangle ABC, where $a = \mathcal{L}(BC)$, $b = \mathcal{L}(AC)$, and $c = \mathcal{L}(AB)$. We draw a height h from vertex A to side BC, intersecting BC at D. (We can assume this altitude intersects the opposite side, since every triangle has at least one altitude which intersects the opposite side.)

From Section 13.1 we know that the area of triangle ABC is $ah/2$.

Let $x = \mathcal{L}(DB)$, so that $a - x = \mathcal{L}(DC)$. We now have two right triangles, ADC and ADB. We use the Pythagorean theorem twice to get

$$h^2 + x^2 = c^2 \tag{13.1}$$

and

$$h^2 + (a-x)^2 = b^2\,.$$

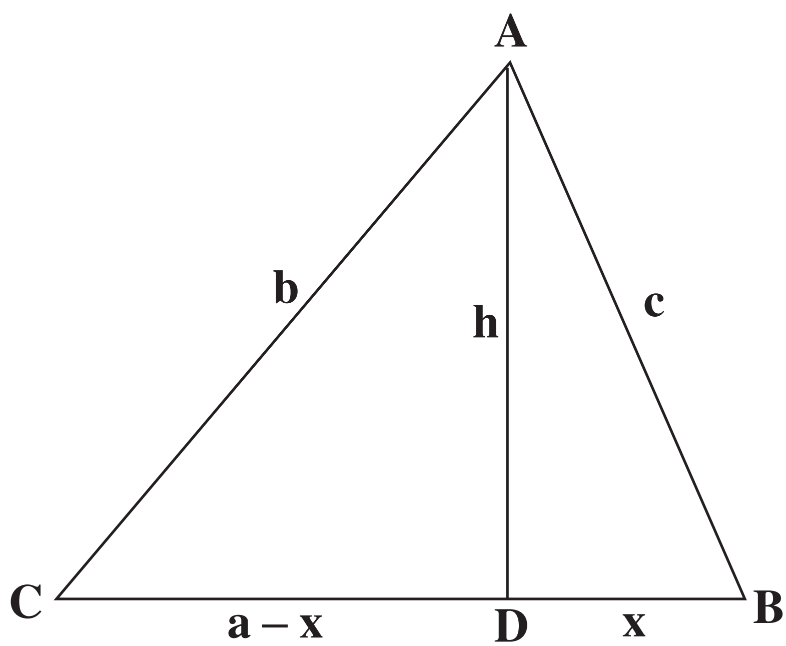


Figure 13.13: Heron's formula

Exercise 13.3.7. Subtract these two equations to obtain the following formula for x:

$$x = \frac{a^2 + c^2 - b^2}{2a} .$$

From Equation 13.1 we have

$$h^2 = c^2 - x^2 = (c - x)(c + x) .$$

Let's eliminate x from one of these factors:

$$\begin{aligned} c - x &= c - \frac{a^2 + c^2 - b^2)}{2a} \\ &= \frac{2ac - a^2 - c^2 + b^2}{2a} \\ &= \frac{b^2 - (a - c)^2}{2a} . \end{aligned}$$

Exercise 13.3.8. Performing a similar calculation, show

$$c + x = \frac{(a + c)^2 - b^2}{2a} .$$

Then put the results for $c + x$ and $c - x$ together to obtain

$$h^2 = \frac{((a + c)^2 - b^2)(b^2 - (a - c)^2)}{4a^2} . \tag{13.2}$$

Since Heron's formula involves a square root, let's get rid of the root by squaring the area.

Exercise 13.3.9. Using Equation 13.2 and the fact that $\mathcal{A}(T) = ah/2$, show

$$\mathcal{A}(T)^2 = \frac{((a + c)^2 - b^2)(b^2 - (a - c)^2)}{16} . \tag{13.3}$$

To complete the proof of Heron's formula, we must show that the right hand side of Equation 13.3 is the same as

$$s(s - a)(s - b)(s - c).$$

First, we write

$$s = \frac{(a + c) + b}{2} . \tag{13.4}$$

Exercise 13.3.10. Show that

$$s - b = \frac{(a + c) - b}{2} . \tag{13.5}$$

Exercise 13.3.11. From Equation 13.4 and Equation 13.5, show

$$s(s - b) = \frac{(a + c)^2 - b^2}{4} . \tag{13.6}$$

Exercise 13.3.12. Now show

$$s - a = \frac{b - (a - c)}{2} \tag{13.7}$$

and

$$s - c = \frac{b + (a - c)}{2} \,. \tag{13.8}$$

Exercise 13.3.13. From Equation 13.7 and Equation 13.8, show

$$(s - a)(s - c) = \frac{b^2 - (a - c)^2}{4} \,. \tag{13.9}$$

Exercise 13.3.14. Multiply Equation 13.6 and Equation 13.9 together to obtain

$$s(s - a)(s - b)(s - c) = \frac{((a + c)^2 - b^2)(b^2 - (a - c)^2)}{16} \,.$$

Since this last expression is the same as the right hand side of Equation 13.3, it follows that

$$\mathcal{A}(T)^2 = s(s - a)(s - b)(s - c) \,.$$

Exercise 13.3.15. What goes wrong with Heron's formula if $a + b < c$? If $a + b = c$?

Exercise 13.3.16. Find the area of the triangle whose sides are 6, 9 and 13.

13.4 Pythagorean triples

You are probably already familiar with the famous "3-4-5 right triangle." That is, if the two sides of a right triangle are 3 and 4, respectively, then, by the Pythagorean Theorem, the hypotenuse is 5. This right triangle has *integral* sides. Three positive integers, (a, b, c), which satisfy $a^2 + b^2 = c^2$ are called *Pythagorean triples.* Such triples will correspond to right triangles with integral sides.

Are there other Pythagorean triples? Certainly one way to construct them is simply to multiply the numbers 3, 4 and 5 by the same number. For instance, $(6, 8, 10)$ is another Pythagorean triple.

Exercise 13.4.1. Suppose (a, b, c) is a Pythagorean triple. Prove that for any positive integer k, (ka, kb, kc) is another Pythagorean triple.

Triples such as $(6, 8, 10)$ are not interesting, since they are derived from other triples. We call a Pythagorean triple (a, b, c) *primitive* if a, b and c do not have a common factor. Thus, $(3, 4, 5)$ is a primitive Pythagorean triple, while $(6, 8, 10)$ is not primitive.

Exercise 13.4.2. Suppose (a, b, c) is a Pythagorean triple. Show that if k divides any two of a, b or c, then it divides the third.

It follows from Exercise 13.4.2 that if (a, b, c) is any Pythagorean triple, then $\text{GCD}(a, b) = \text{GCD}(a, c) = \text{GCD}(b, c) = \text{GCD}(a, b, c)$. Therefore, primitive Pythagorean triples are those Pythagorean triples for which all these GCD's are 1.

Are there other primitive Pythagorean triples? You may be familiar with the triple $(5, 12, 13)$. In fact, there are an infinite number of primitive Pythagorean triples. We will describe how to generate them in the rest of this section.

Exercise 13.4.3. Which of the following triples are Pythagorean triples and which of these are primitive?

i. $(40, 42, 58)$

ii. $(35, 12, 36)$

iii. $(7, 24, 25)$

iv. $(40, 9, 41)$.

Let's first look at the primitive Pythagorean triples from Exercise 13.4.3 (and the triples $(3, 4, 5)$ and $(5, 12, 13)$). Notice that in each case, exactly one of the first two numbers in the triple is even, and the other two numbers are odd. Let's try to prove that.

Exercise 13.4.4. If (a, b, c) is a primitive Pythagorean triple, can a and b both be even? Why or why not?

It might appear that both a and b could be odd. But this cannot happen in any Pythagorean triple. Suppose a is odd. Then $a \equiv 1 \mod 4$ or $a \equiv 3 \mod 4$. In both cases, $a^2 \equiv 1 \mod 4$. Similarly $b^2 \equiv 1 \mod 4$. So $c^2 \equiv 2 \mod 4$.

Exercise 13.4.5. Show $c^2 \not\equiv 2 \mod 4$ by considering the four possible mod 4 congruence classes for c.

We therefore conclude that exactly one of a and b is even and the other is odd.

Exercise 13.4.6. If (a, b, c) is a Pythagorean triple, with one of a and b even and the other odd, is c even or odd and why?

We reduced the set of Pythagorean triples to the primitive triples because the non-primitive triples were "not different" from the primitive ones from which they were derived. In a similar vein, the primitive triples (a, b, c) and (b, a, c) are really the same. By applying the above exercises, we will always assume our primitive triples have a odd and b even (and c odd).

We're now ready to describe how to construct all primitive Pythagorean triples.

Theorem 26. *Suppose $r < s$ are two positive integers such that GCD$(r, s) = 1$ and r and s are not both odd. Then (a, b, c) is a primitive Pythagorean triple, where*

$$a = s^2 - r^2 \qquad (13.10)$$
$$b = 2rs$$
$$c = s^2 + r^2.$$

Conversely, suppose (a, b, c) is a primitive Pythagorean triple with b even. Then there exists a unique r and s with $r < s$, GCD$(r, s) = 1$, and r and s not both odd, such that Equations (13.10) hold. Furthermore, if $b/(c+a)$ is reduced to lowest terms, the resulting fraction is r/s.

For example, if we choose $r = 4$ and $s = 5$, then $a = 9$, $b = 40$ and $c = 41$.

Exercise 13.4.7. Verify that $(9, 40, 41)$ is a primitive Pythagorean triple.

On the other hand, for the triple $(3, 4, 5)$, $r/s = 4/8 = 1/2$, so $r = 1$ and $s = 2$.

Exercise 13.4.8. Find the primitive Pythagorean triple which corresponds to $r = 3$ and $s = 8$. Find the primitive Pythagorean triple which corresponds to $r = 5$ and $s = 6$. Find the primitive Pythagorean triple which corresponds to $r = 2$ and $s = 7$.

Exercise 13.4.9. Find r and s which correspond to the triple $(5, 12, 13)$. Find the r and s which correspond to the triple $(45, 28, 53)$.

Exercise 13.4.10. Find two different primitive Pythagorean triples with the same b.

Exercise 13.4.11. Find two different primitive Pythagorean triples with the same a.

Exercise 13.4.12. Find two different primitive Pythagorean triples with the same c.

We will now work through a few exercises which will prove Theorem 26. First, suppose $r < s$ (with no divisibility conditions). Define a, b and c as in Equations (13.10).

Exercise 13.4.13. Show that $a^2+b^2 = c^2$. That is, show (a, b, c) is a Pythagorean triple.

We now add the divisibility conditions and show this triple is primitive. These divisibility conditions are that GCD$(r, s) = 1$ and r and s are not both odd.

Exercise 13.4.14. Use Equations 13.10 and the fact that one of r and s is even and one is odd to prove that a and c are both odd. Also, why is b even?

Therefore, 2 is not a common factor of a, b and c. Suppose p is some common prime divisor of a, b and c, $p \neq 2$. Then p is a divisor of $c + a$ and $c - a$.

Exercise 13.4.15. Show that p is therefore a divisor of $2r^2$ and $2s^2$. Explain why this means that p is a divisor of r and s.

But p cannot be a divisor of r and s, since $\text{GCD}(r, s) = 1$. Therefore, a, b and c have no common divisor, so (a, b, c) is a primitive Pythagorean triple.

Now suppose (a, b, c) is a primitive Pythagorean triple (b even). Our program is as follows. We will show how to construct r and s such that Equations (13.10) hold and $\text{GCD}(r, s) = 1$ with not both r and s odd. The fact that $r/s = b/(a+c)$ reduced to lowest terms comes from the following exercise:

Exercise 13.4.16. If a, b and c are related to r and s through Equations (13.10), show $b/(a + c) = r/s$.

Since $\text{GCD}(r, s) = 1$, r/s must be reduced to lowest terms.

To construct r and s, we begin by writing $b = 2u$, where u is an integer. We can do this since b is even.

Exercise 13.4.17. Show $4u^2 = (c - a)(c + a)$.

Exercise 13.4.18. Why are $c - a$ and $c + a$ both even?

Since $c - a$ is even and $c + a$ is even, we will write them as follows:

$$\begin{aligned} c - a &= 2x \\ c + a &= 2y \end{aligned}$$

We can solve this system of equations for a and c.

Exercise 13.4.19. Show

$$\begin{aligned} a &= y - x \\ c &= y + x \end{aligned} \tag{13.11}$$

If x and y had a common factor, then it would be a factor of a and c. But a and c have no common factor, so neither do x and y. That is, $\text{GCD}(x, y) = 1$.

We then have

$$4u^2 = 4xy,$$

or $u^2 = xy$. But since $\text{GCD}(x, y) = 1$, the only way their product could be a perfect square is if each of x and y is a perfect square (see Exercise 5.1.13 in Chapter 5). That is, let $x = r^2$ and $y = s^2$. These are the r and s we seek. We must now check all the conditions we wanted.

First,

$$a = y - x = s^2 - r^2$$

and

$$c = y + x = s^2 + r^2.$$

Also,

$$b^2 = 4u^2 = 4xy = 4r^2s^2$$

so that $b = 2rs$. Therefore Equations 13.10 hold.

Since $y - x > 0$, $s^2 > r^2$, so that $s > r$. Now suppose r and s have a common factor. Then x and y would also, but $\text{GCD}(x, y) = 1$ as we noted earlier. Finally, suppose both r and s are odd. Then a and c will both be even, and so (a, b, c) would not be primitive. This completes the proof.

Equations 13.10 allow us to make some observations about divisibility of primitive Pythagorean triples. For example, since one of r and s is even and $b = 2rs$, it follows that b is divisible by 4.

In a similar vein, suppose b is not a multiple of 3. Then neither r nor s is a multiple of 3.

Exercise 13.4.20. If r and s are both not multiples of 3, show $r^2, s^2 \equiv 1 \mod 3$.

Since $a = s^2 - r^2$, it follows that $a \equiv 0 \mod 3$, i.e., a is divisible by 3. Therefore, one of a or b is divisible by 3.

Exercise 13.4.21. Use similar arguments to show that one of a, b or c is divisible by 5.

Summarizing, if (a, b, c) is a Pythagorean triple, then at least one of a and b is a multiple of 3, at least one of a and b is a multiple of 4, and at least one of a, b and c is a multiple of 5. Furthermore, if (a, b, c) is a primitive Pythagorean triple, then exactly one of a and b is a multiple of 3, exactly one of a and b is a multiple of 4, and exactly one of a, b and c is a multiple of 5.

13.5 Circle geometry

Recall from Section 13.2 the general principle: linear dimensions of similar polygons grow linearly with the similarity ratio.

Let's put this principal to work to find the circumference of a circle. Let's start with a regular hexagon (all six angles equal and all six sides equal) P_1. We will call the distance from the center of the regular hexagon to any vertex its *radius*, r_1. Since P_1 is regular, the definition of r_1 is independent of the choice of vertex. Suppose P_2 is another regular hexagon whose radius is r_2. Then according to the above principle, the perimeter of P_2 is r_2/r_1 times the perimeter of P_1. That is, the ratio of the perimeters is the same as the ratio of the radii.

For example, in Figure 13.14, two regular hexagons are drawn. In one, the radius is 1, while in the other, the radius is 3.

Exercise 13.5.1. Compute the perimeters of the two regular hexagons in Figure 13.14 and verify that the perimeter of the second is 3 times the perimeter of the first.

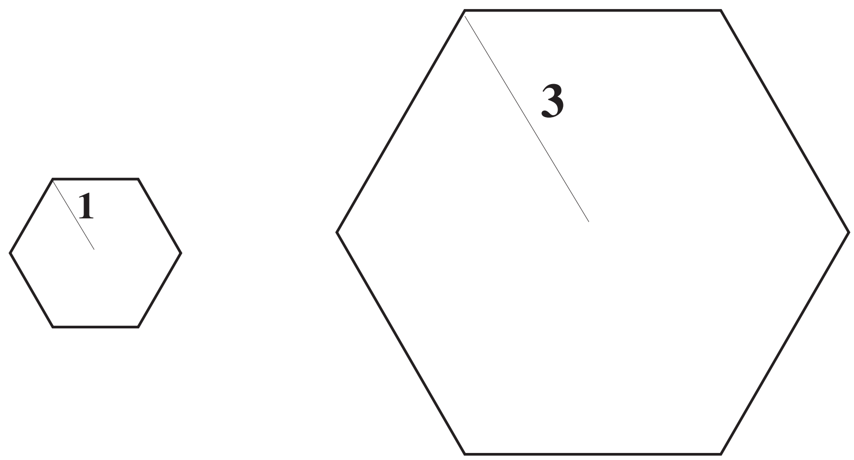


Figure 13.14: Similar regular hexagons

If p_1 and p_2 are the perimeters of P_1 and P_2, respectively, we have

$$\frac{p_1}{p_2} = \frac{r_1}{r_2}$$

or, equivalently,

$$\frac{p_1}{r_1} = \frac{p_2}{r_2}.$$

This last equation says the the ratio of the perimeter to the radius is always the same, i. e., a constant.

Exercise 13.5.2. Compute this ratio for regular hexagons.

If, instead of hexagons, we had chosen 10 or 100 sided regular polygons, the general principle would still hold: the ratio of the perimeter to the radius is a constant (which will depend on the number of sides).

Exercise 13.5.3. Compute this constant for regular triangles (equilateral triangles), for regular quadrilaterals (squares), for regular octagons and for regular 12-sided polygons. (You will have to use the Pythagorean theorem several times.)

As the number of sides of the polygon increases, the polygon looks more and more like a circle (see Figure 13.15), and the ratio of the perimeter to the radius will approach a special number. We call that number 2π. Therefore, the ratio of the circumference of a circle to the radius of a circle is 2π, or

$$c = 2\pi r.$$

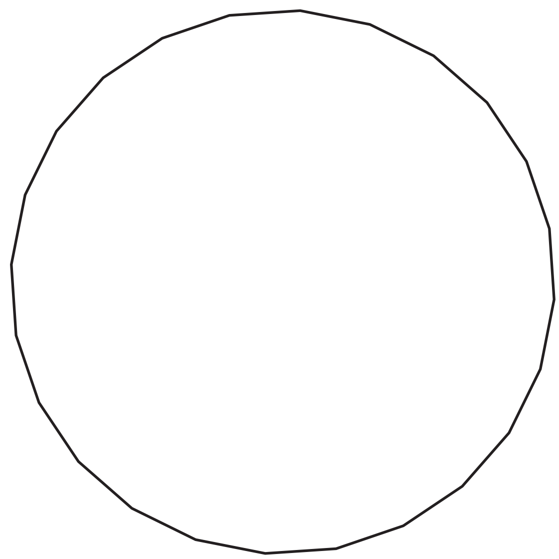


Figure 13.15: A regular 24-gon

A surprising fact about π is that it appears in both the circumference formula and the area formula for a circle. Let's see why.

If we slice the circle up into "pie pieces" and redraw the pieces (see Figure 13.16), we get a region R that is "almost" a rectangle. The more pieces we cut the pie into, the closer we get to a rectangle. The height of the rectangle is r and the width is $c/2$. Therefore, $\mathcal{A}(R) = rc/2$. Since $c = 2\pi r$, $\mathcal{A}(R) = \pi r^2$.

Now let's see if we can find approximate values for π. The calculations in Exercise 13.5.3 have actually produced lower bounds for π in the following way. If a polygon of radius r is inscribed in a circle of radius r, the perimeter of the polygon, p, is less than the circumference of the circle, c. See Figure 13.17 to see an inscribed square.

Let k_n denote the ratio of the perimeter to the radius of a regular n-sided polygon. Then $p = k_n r$ and $c = 2\pi r$, but $p < c$. Therefore,

$$\pi > \frac{k_n}{2}.$$

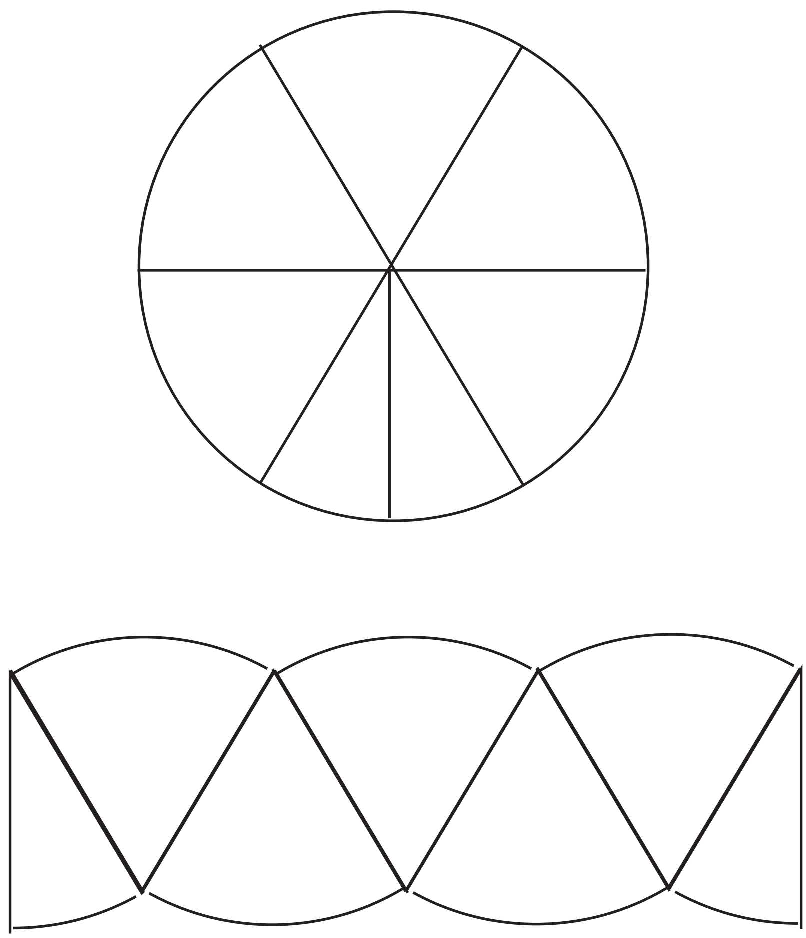


Figure 13.16: The area of a circle

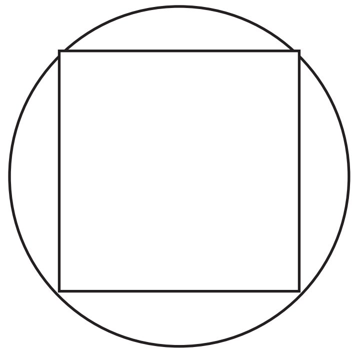


Figure 13.17: A square inscribed in a circle

Exercise 13.5.4. Use Exercise 13.5.3 to give lower bounds for π.

We may use a similar idea to obtain upper bounds for π. Instead of using inscribed polygons, we use circumscribed polygons. However, one technical problem emerges. It is easy to see that the perimeter of an inscribed polygon is smaller than the perimeter of the circle. We simply use the geometry axiom that the shortest line between two points is a straight line.

We have no such axiom to fall back upon in the circumscribed polygon case. Our intuition tells us that the perimeter of the square in Figure 13.18 is greater than the circumference of the circle, but what principle are we using for this intuition?

We can avoid this technical difficulty by relying on areas instead of circumferences. That is, we could compute the area of the circumscribed polygon, which is clearly greater than the area of the circle, since the circle is inside the polygon. This would give us a bound, since we now know that π must also appear in the area formula. This approach actually gives us a weaker bound than the perimeter approach for the same polygon.

We will do examples using both approaches.

Exercise 13.5.5. By computing the perimeter of the square and the circumference of the circle in Figure 13.18, find an upper bound for π. Then find an upper bound by using areas instead of perimeters.

Exercise 13.5.6. Find a better upper bound by using the perimeter of a regular polygon with more sides than a square.

Exercise 13.5.7. Find another upper bound by using the area of a regular polygon with more sides than a square.

The first recorded approximations to π were made by the Babylonians around 2000 B.C. The techniques described in this section were used by Archimedes to

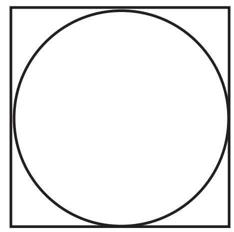


Figure 13.18: A square circumscribed outside a circle

establish $223/71 < \pi < 22/7$. As better computational tools emerged and as better formulas became known, the approximations improved. For example, using the invention of the zero, Tsu Ch'ung-Chi established $3.1415926 < \pi < 3.1415927$ in the 5th century A.D.

In the 17th century, Gregory and Leibniz discovered arctangent series which greatly aided π approximations. By the 18th century, π had been approximated to over 100 decimal places. In 1766, Lambert proved π was irrational, thus dispelling the notion that there might be some undiscovered integers p and q such that $\pi = p/q$. Then in 1882, Lindemann proved π was transcendental, which ended the two thousand year quest to find a straightedge-compass construction which would convert a circle to a square with the same area.

At the dawn of the computer age, π had been computed to nearly 1000 decimal places. Now we can approximate π virtually without limit. As of June, 2000, it had been computed to over 200 billion decimal places.

More than any other mathematical concept, π attracts crackpot "mathematicians." This may be due in part to the Greek problem of squaring a circle, which was resolved by Lindemann. It may also be due to the simplicity of the definition of π as the ratio of the circumference to the diameter of a circle. In any case, in 1897 a bill was introduced into the Indiana State Legislature, which, among other things, presented a purported proof of squaring the circle, and gave a rational value for π. The bill was written by Edwin J. Goodman, M. D., who promised Indiana free use of his invention. This bill passed the Indiana House, and probably would have passed the Senate except for the intervention of C. A. Waldo, a mathematician from Purdue, who happened to be at the capitol lobbying for university funding.

13.6 Finding Volumes

Some of the principles and techniques we learned in Section 13.2 and in Section 13.5 can be expanded to compute volumes of solid geometric objects. We will use the notation $\mathcal{V}(S)$ for the volume of the solid object S.

A *parallelepiped* is a polyhedron consisting of six faces, with three pairs of opposite faces. Each face is a parallelogram. Opposite faces are congruent and parallel. If F is one face, the *height* corresponding to F is the perpendicular distance from F to its opposite face.

A *rectangular parallelepiped* is a parallelepiped all of whose faces are rectangles. Therefore, all the angles in a parallelepiped are right angles. By arguments similar to those in Section 13.1, the volume of a rectangular parallelepiped is length times width times height. That is, it is the area of one rectangular face times the corresponding height.

An important general principle for computing volumes is the "cross-section" principle of Cavalieri. Suppose two solids are placed on a table. Then imagine slicing the two solids with a series of planes parallel to the table. If the cross-section area of one solid is the same as the cross-section area of the other solid for each slice, then their volumes are the same.

Let's apply Cavalieri's principle to give a formula for the volume of a parallelepiped. Suppose a parallelepiped has a base parallelogram with area A and corresponding height h. Construct a rectangular parallelepiped with base rectangle having area A and corresponding height h.

Exercise 13.6.1. Use Cavalieri's principle to show these two parallelepipeds have the same volume. Then use the formula for the volume of a rectangular parallelepiped to give a formula for the volume of a general parallelepiped.

We will use Cavalieri's principle to find the volume of general conical solids. Let's start with a tetrahedron. If we place a tetrahedron on a table, (see Figure 13.19) it has a base triangle (ABC in the figure) and a height equal to the perpendicular distance from the table to the top of the tetrahedron ($l(DP)$ in the figure). Now suppose we slice this tetrahedron with a plane parallel to the plane of the base. The intersection of the slicing plane and the tetrahedron is a triangle (EFG in the figure), which, together with the top of the original tetrahedron, forms a new, smaller tetrahedron ($DEFG$).

We will show that triangles ABC and EFG are similar with similarity ratio equal to $\frac{\mathcal{L}(DQ)}{\mathcal{L}(DP)}$.

Exercise 13.6.2. Show triangle DQE is similar to triangle DPA. Hint: first show they are right triangles.

Since the plane of ABC is parallel to the plane of EFG, it follows that EG is parallel to AC.

Exercise 13.6.3. Show triangle DEG is similar to triangle DAC.

Exercise 13.6.4. Conclude that triangle EFG is similar to triangle ABC with similarity ratio $\frac{\mathcal{L}(DQ)}{\mathcal{L}(DP)}$.

Exercise 13.6.5. Show that

$$\frac{\mathcal{A}(EFG)}{\mathcal{A}(ABC)} = \Big(\frac{\mathcal{L}(DQ)}{\mathcal{L}(DP)}\Big)^2.$$

Hint: use Exercise 13.2.15.

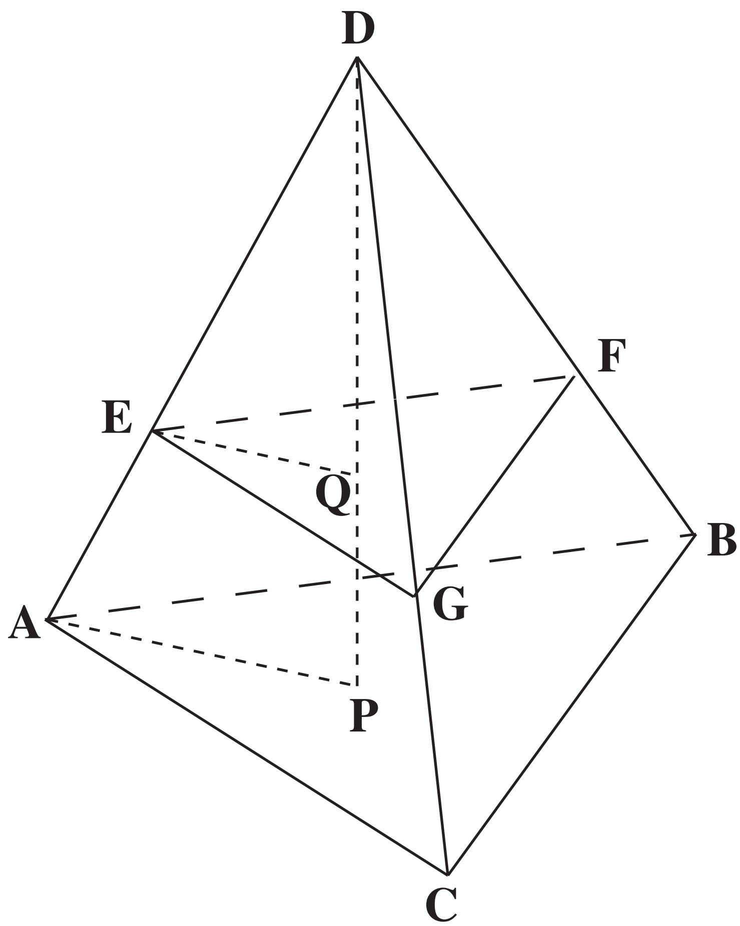


Figure 13.19: Tetrahedron sliced with plane parallel to base

Now suppose two tetrahedra have bases of equal area and equal corresponding heights (see Figure 13.20). In this figure, the two heights h are equal, while the two base triangles ABC and EFG have equal area.

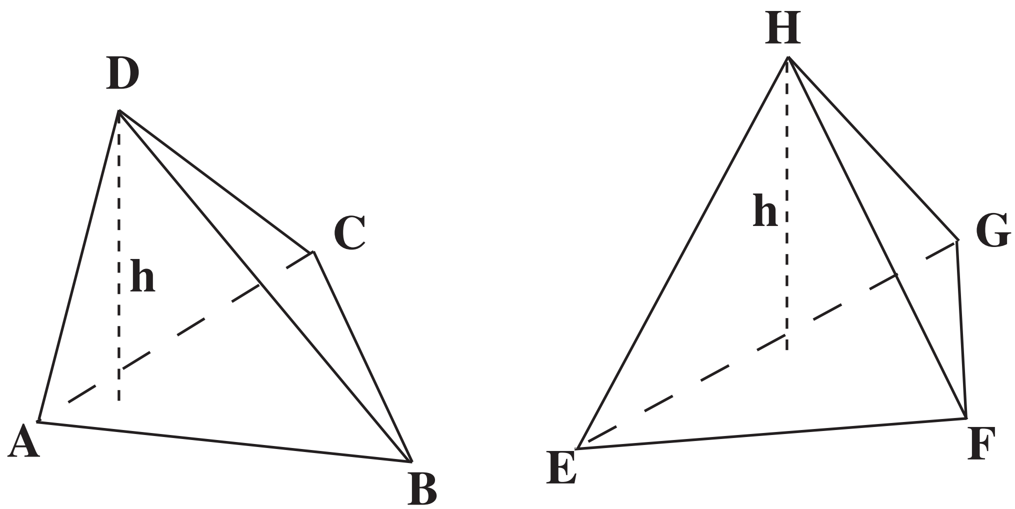


Figure 13.20: Equal volumes

Exercise 13.6.6. Explain why any plane slicing through these two tetrahedra intersects the tetrahedra in triangles of equal area. Hint: Use Exercise 13.6.5. Conclude from Cavalieri's principle that the two tetrahedra have the same volume.

We therefore conclude that all tetrahedra with the same area base and the same corresponding height have the same volume.

To find a formula for this volume, our program is as follows. We cut a rectangular parallelepiped up into six pieces. Each piece will be a tetrahedron. Using the above fact, we show that all six pieces have the same volume, which must be

$$\mathcal{V}(T) = \frac{1}{6}lwh. \tag{13.12}$$

Also, at least one of them has a base triangle S equal to half of one of the rectangular sides of the parallelepiped and height equal to the corresponding height of the parallelepiped. Therefore, for one of the tetrahedra,

$$\mathcal{A}(S) = \frac{1}{2}lw. \tag{13.13}$$

Putting Equation (13.12) and Equation (13.13) together gives

$$\mathcal{V}(T) = \frac{1}{3}\mathcal{A}(S)h. \tag{13.14}$$

Since every tetrahedron with the same area base and same height has the same volume, Equation (13.14) is the formula for the volume of a tetrahedron with base S and height h.

The next series of exercises carries out the details of this program.

Look carefully at Figures 13.21, 13.22, 13.23, and 13.24. In Figures 13.21 and 13.22, a rectangular parallelepiped has been cut diagonally down the middle into two congruent pieces. Figure 13.23 shows one of these pieces.

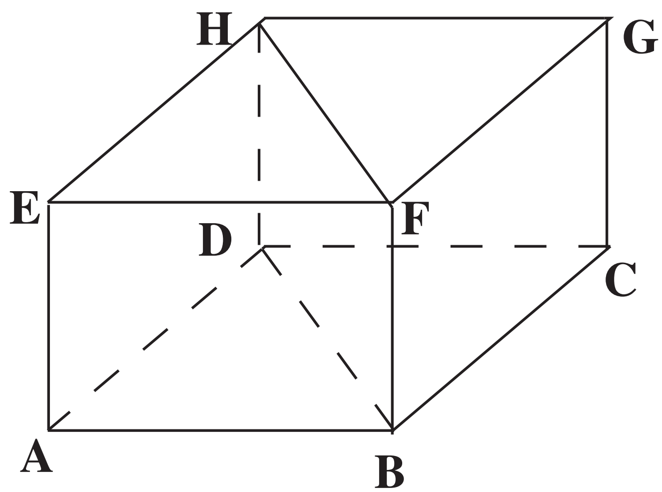


Figure 13.21: A rectangular parallelepiped to be sliced

Figure 13.24 shows how this piece is further cut into three tetrahedra. Two slices have been made. The first is in the plane determined by A, H and F. It slices off E, forming tetrahedron $AFHE$. The second is in the plane determined by A, D and F. It slices off B, forming tetrahedron $ADFB$. What is left is tetrahedron $AFDH$.

Exercise 13.6.7. Show $\mathcal{V}(ADFB) = \mathcal{V}(AFHE)$ by showing they have congruent bases and equal heights. Hint: use base ADB for the first tetrahedron and base EHF for the second.

Exercise 13.6.8. Show $\mathcal{V}(ADFB) = \mathcal{V}(AFDH)$ by showing they have congruent bases and equal corresponding heights. Hint: Use bases DFB and FDH.

Exercise 13.6.9. Conclude that all three tetrahedra $ADFB$, $AFHE$ and $AFDH$ have the same volume.

Exercise 13.6.10. Find the volume of the regular tetrahedron whose side length is 1.

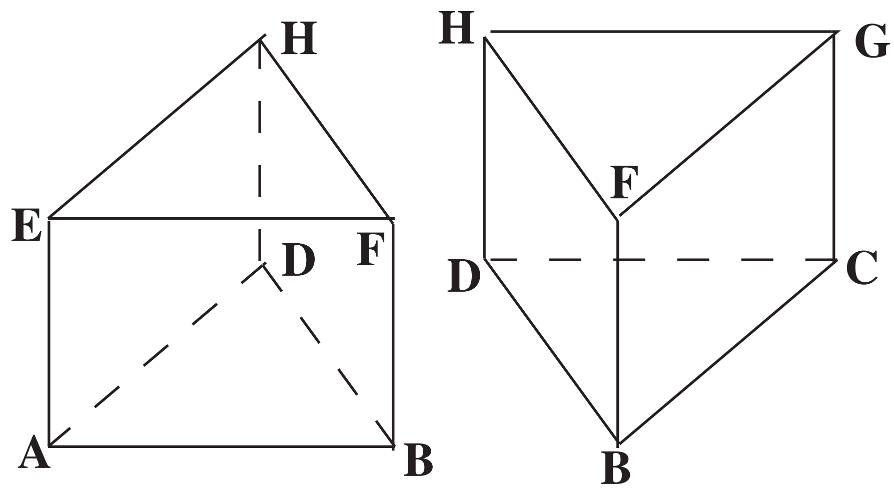


Figure 13.22: Sliced rectangular parallelepiped

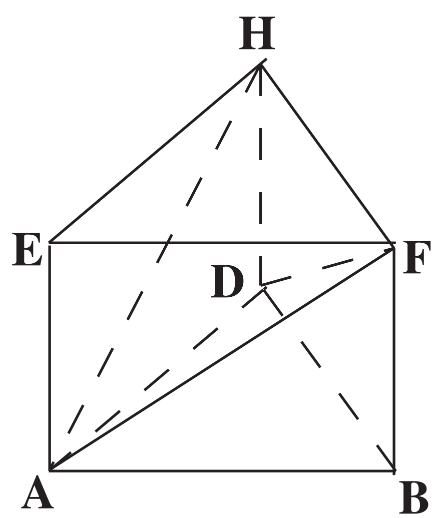


Figure 13.23: A half rectangular parallelepiped to be sliced

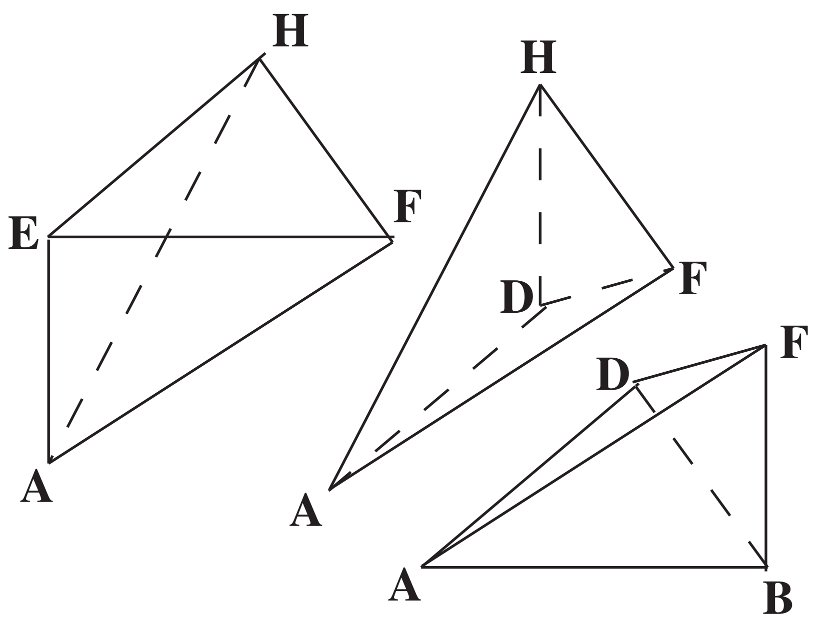


Figure 13.24: Sliced half of a rectangular parallelepiped

By triangulating polygons, we can compute the volume of any "cone" C with base polygon P and height h:

$$\mathcal{V}(C) = \mathcal{A}(P)h/3,$$

See Figure 13.25.

Exercise 13.6.11. Compute the volume of the Great Pyramid of Egypt. It has a square base, 751 feet on a side, and a height of 481 feet.

By approximating curved regions with polygons, we obtain the formula for the volume of a general cone. If a cone C has base given by region R and height h, then

$$\mathcal{V}(C) = \mathcal{A}(R)h/3.$$

For example, if R is a circle of radius r, then the formula for the volume of the cone is $\pi r^2 h/3$.

Exercise 13.6.12. Find the volume of an ice cream cone with radius $3/2$ inches and height 5 inches.

Let's now calculate some formulas for a sphere, S. First, there is a simple relationship between the volume of a sphere, $\mathcal{V}(S)$ and its surface area, $\mathcal{A}(S)$. This relationship is similar to the relationship between the area of a circle and the circumference of the circle.

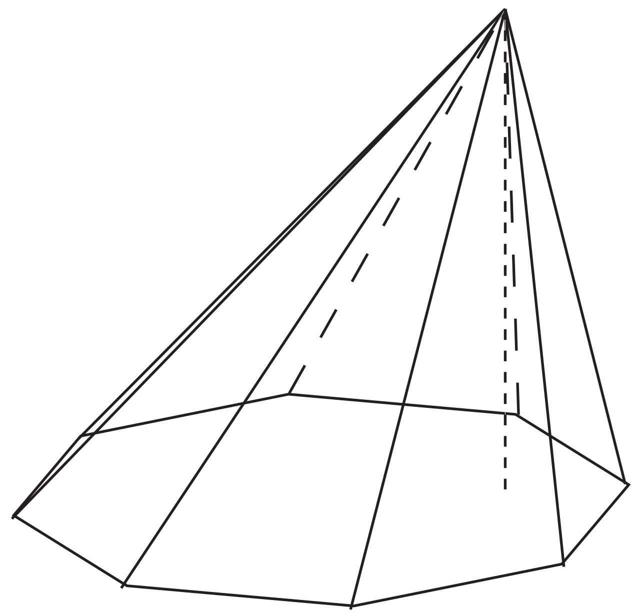


Figure 13.25: A generalized cone

First, we approximate S with a polyhedron with many faces. The solid formed by each face and the center of S is a cone with base equal to the face and height approximately the radius of the S, r. See Figure 13.26, which shows two such cones, one with an octagonal base and the other with a triangular base.

If C is one of these cones, with base B, its volume is given by

$$\mathcal{V}(C) = \mathcal{A}(B)r/3$$

Now sum this equation over all the cones in the polyhedron. The left-hand side sums to the volume of the polyhedron, which is approximately $\mathcal{V}(S)$. The right hand side sums to approximately $\mathcal{A}(S)r/3$. The smaller the base of the cones, the better the approximation. Therefore,

$$\mathcal{V}(S) = \frac{1}{3}\mathcal{A}(S)r \tag{13.15}$$

We now concentrate our attention on the surface area of the sphere. Imagine that the surface area of the sphere is like the surface of the earth. At each latitude (latitudes measure distance from the equator), suppose we mark off a band 1 mile wide (in the north-south direction) at the same latitude, wrapping all the way around the earth. Let's compute the surface area of this band.

Figure 13.27 shows how to do this. This figure shows a great circle cross-section view of the sphere. In our earth-analogy, the north pole is N and the

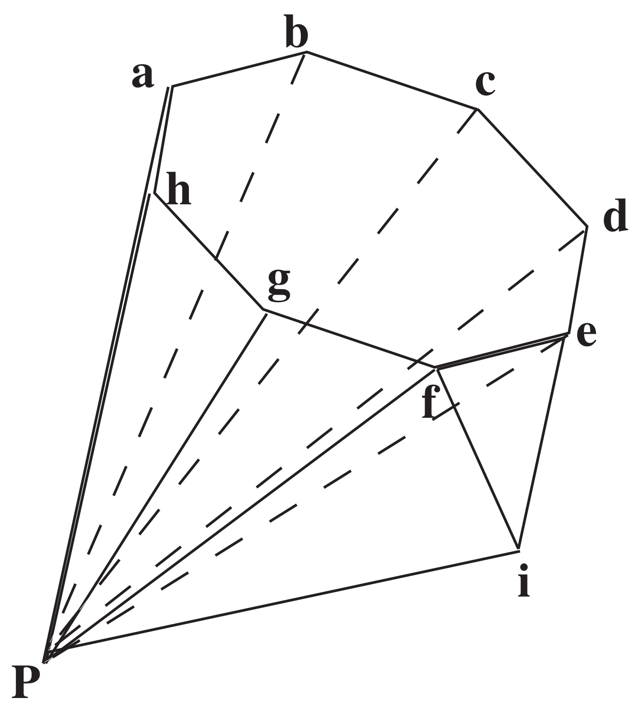


Figure 13.26: Cones in a sphere

center of the earth is P. The radius AP is a line from the center of the earth to the southernmost edge of the band, and the radius CP is a line from the center of the earth to the northernmost edge. The arc AC is a north-south line across the band. If the band is very narrow, i. e., A is close to C, then the length of the arc AC is approximately the length of the line segment AC.

Exercise 13.6.13. Prove that triangle ACD and triangle BPA are similar.

By the proportionality principles of similar objects, we get

$$\frac{\mathcal{L}(AC)}{\mathcal{L}(CD)} = \frac{r}{\mathcal{L}(AB)},$$

or

$$\mathcal{L}(AC) = r\frac{\mathcal{L}(CD)}{\mathcal{L}(AB)} \tag{13.16}$$

We now use Equation (13.16) to approximate the area of the band. Since $\mathcal{L}(AC)$ is approximately the length of the arc AC, the area of the band will be approximately $\mathcal{L}(AC)$ times the circumference of the circle whose radius is $\mathcal{L}(AB)$, i. e., $2\pi\mathcal{L}(AB)\mathcal{L}(AC)$. Substituting Equation (13.16) into this expression, we get

$$2\pi\mathcal{L}(CD)r \tag{13.17}$$

as the formula for the approximate area of that small strip of equal latitude around the sphere. Surprisingly, this formula is independent of the latitude! We now sum this formula over all such thin strips in the upper hemisphere. Each small region contributes an amount given by Equation (13.17). The entire sum will then be

$$2\pi r^2,$$

since the $\mathcal{L}(CD)$'s will all add to r. Now double this to get both hemispheres, and we have

$$\mathcal{A}(S) = 4\pi r^2.$$

Exercise 13.6.14. Use Equation (13.15) to find the formula for $\mathcal{V}(S)$.

Exercise 13.6.15. Suppose the ice cream cone in Exercise 13.6.12 is filled with ice cream and the ice cream mounds up to form a half sphere above the cone. What is the volume of ice cream?

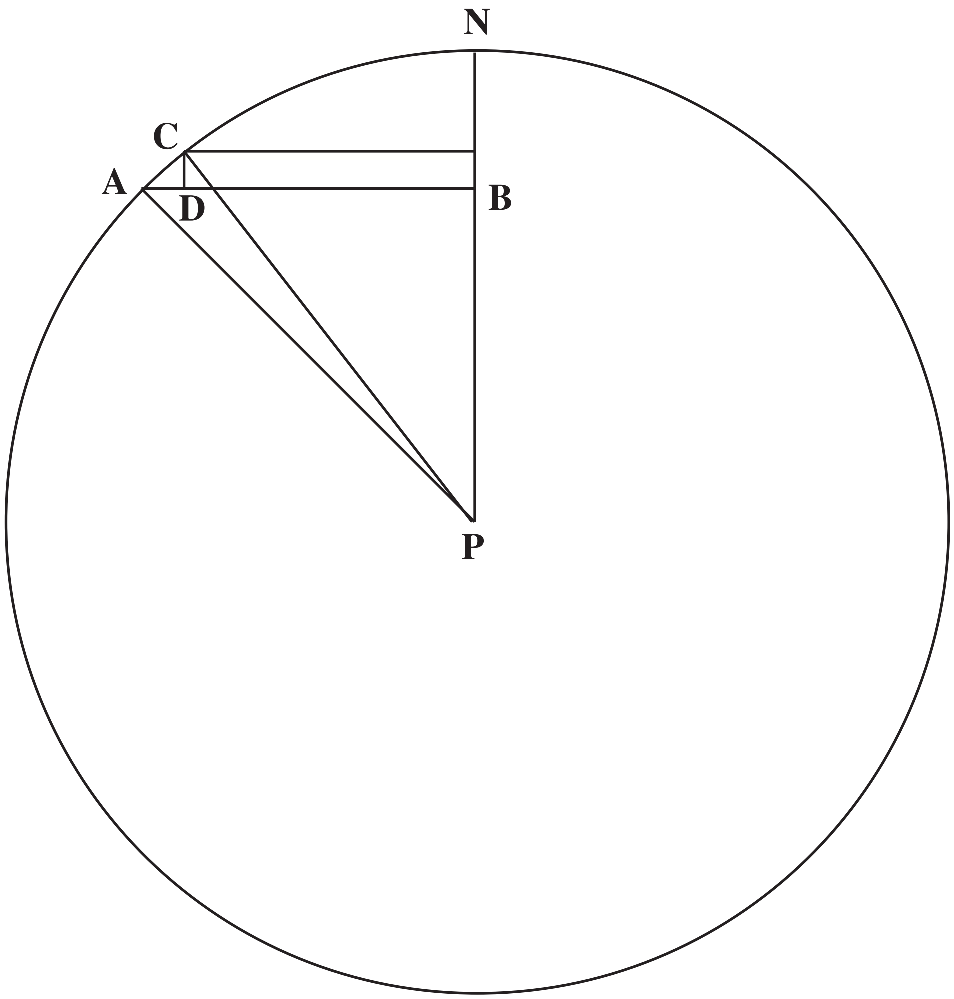


Figure 13.27: Cross-section of a sphere

Index