An Introduction to Higher Mathematics

Patrick Keef
David Guichard

with modifications by
Russ Gordon

Whitman College

Contents

3

Number Theory 63

4

Functions 103

Bibliography 133

Index 135

1

Logic

Although mathematical ability and opinions about mathematics vary widely, even among educated people, there is certainly widespread agreement that mathematics is *logical*. Indeed, properly conceived, this may be one of the most important defining properties of mathematics.

Logical thought and logical arguments are not easy to come by (ponder some of the discussions you encounter on current topics such as abortion, climate change, evolution, gun control, or same sex marriage to appreciate this statement), nor is it always clear whether a given argument is logical (that is, logically correct). Logic itself deserves study; the right tools and concepts can make logical arguments easier to discover and to discern. In fact, logic is a major and active area of mathematics; for our purposes, a brief introduction will give us the means to investigate more traditional mathematics with confidence.

1.1 Logical Operations

Mathematics typically involves combining true (or hypothetically true) statements in various ways to produce (or prove) new true statements. We begin by clarifying some of these fundamental ideas.

By a **sentence**, we mean a statement that has a definite **truth value** of either true (T) or false (F). For example,

"In terms of area, Pennsylvania is larger than Iowa." (F)

"The integer 289 is a perfect square." (T)

Because we insist that our sentences have a truth value, we are not allowing sentences such as

"Chocolate ice cream is the best."

"This statement is false."

since the first is a matter of opinion and the second leads to a logical dilemma. More generally, by a **formula** we mean a statement, possibly involving some variables, which is either true or false whenever we assign particular values to each of the variables. (Formulas are sometimes referred to as **open sentences**.) We typically use capital letters such as P, Q, and R to designate formulas. If the truth of a formula P depends on the values of, say, x, y, and z, we use notation like $P(x, y, z)$ to denote the formula.

EXAMPLE 1.1 If $P(x, y)$ is "$x^2 + y = 12$", then $P(2, 8)$ and $P(3, 3)$ are true, while $P(1, 4)$ and $P(0, 6)$ are false. If $Q(x, y, z)$ is "$x + y < z$", then $Q(1, 2, 4)$ is true and $Q(2, 3, 4)$ is false. If $R(f(x))$ is "$f(x)$ is differentiable at 0", then $R(x^2 + 2x)$ is true and $R(|x|)$ is false.

Whether a sentence is true or false usually depends on what we are talking about—exactly the same sentence may be true or false depending on the context. As an example, consider the statement "the equation $x^2 + 1 = 0$ has no solutions." In the context of the real numbers, this statement is true; there is no real number x with the property that $x^2 + 1 = 0$. However, if we allow complex numbers, then both i and $-i$ are solutions to the equation. In this case, the statement "the equation $x^2 + 1 = 0$ has no solutions" is false. Examples such as this one emphasize how important it is to be perfectly clear about the context in which a statement is made.

The **universe of discourse** for a particular branch of mathematics is a set that contains all of the elements that are of interest for that subject. When we are studying mathematical formulas such as 'x divides y' or 'f is differentiable at each point', the variables are assumed to take values in whatever universe of discourse is appropriate for the particular subject (the set of integers for the first example and the set of continuous functions for the second). The universe of discourse is frequently clear from the discussion, but occasionally we need to identify it explicitly for clarity. For general purposes, the universe of discourse is usually denoted by U.

Complicated sentences and formulas are put together from simpler ones using a small number of **logical operations**. Just a handful of these operations allow us to represent everything we need to say in mathematics. These operations and their notation are presented below.

The **denial** (or **negation**) of a formula P is the formula "not P", which is written symbolically as $\neg P$. The statement $\neg P$ is false if P is true and vice versa. (This fact follows from the types of statements we are willing to accept as sentences.) For example, the denial of the false sentence "6 is a prime number" is the true sentence "6 is not a prime number" and the denial of the true sentence "343 is a perfect cube" is the false sentence "343 is not a perfect cube."

The **conjunction** of the formulas P and Q is the formula "P and Q", which is written symbolically as $P \wedge Q$. For $P \wedge Q$ to be true both P and Q must be true, otherwise it is false. For example (the reader can easily identify P and Q),

"$5 > 6$ and $7 = 8$." (F)

"17 is prime and 324 is a perfect square." (T)

"$\left\{\dfrac{1}{\sqrt{k}}\right\}$ converges to 0 and $\left\{\left(1 + \dfrac{1}{k}\right)^k\right\}$ converges to 1." (F)

The **disjunction** of the formulas P and Q is the formula "P or Q", which is written symbolically as $P \vee Q$. It is important to note that this is an *inclusive* or, that is, "either or both". In other

words, if P, Q, or *both* P and Q are true, then so is $P \vee Q$. The only way $P \vee Q$ can be false is if both P and Q are false. For example (once again, the reader can easily identify P and Q),

"$5 < 7$ or $8 < 10$." (T)

"19 is prime or 4 divides 15." (T)

"$\sum_{k=1}^{\infty} k^{-1/2}$ converges or $\sum_{k=1}^{\infty} \sqrt[k]{2}$ converges." (F)

Suppose that P and Q are formulas. The sentence "if P, then Q" or "P implies Q" is written $P \Rightarrow Q$, using the **conditional** symbol, $\Rightarrow$. It is not obvious (at least not to most people) under what circumstances $P \Rightarrow Q$ should be true. In part this is because "if ..., then ..." is used in more than one way in ordinary English, yet we need to fix a rule that will let us know precisely when $P \Rightarrow Q$ is true. Certainly, if P is true and Q is false, P cannot imply Q, so $P \Rightarrow Q$ is false in this case. To help us with the other cases, consider the following statement:

"If x is less than 2, then x is less than 4."

This statement should be true regardless of the value of x (assuming that the universe of discourse is something familiar, like the integers). If x is 1, it evaluates to T $\Rightarrow$ T, if x is 3, it becomes F $\Rightarrow$ T, and if x is 5, it becomes F $\Rightarrow$ F. So it appears that $P \Rightarrow Q$ is true unless P is true and Q is false. This is the rule that we adopt.

Finally, the **biconditional** involving the formulas P and Q is the sentence "P if and only if Q", written as $P \Leftrightarrow Q$. Sometimes the phrase "if and only if" is abbreviated as "iff", but we will not use this shorthand here. It should be clear that $P \Leftrightarrow Q$ is true when P and Q have the same truth value, otherwise it is false.

EXAMPLE 1.2 Suppose $P(x, y)$ is "$x + y = 2$" and $Q(x, y)$ is "$xy > 1$." Then when $x = 1$ and $y = 1$, the sentences

$$\neg P(x, y), \quad P(x, y) \wedge Q(x, y), \quad P(x, y) \vee Q(x, y), \quad P(x, y) \Rightarrow Q(x, y), \quad P(x, y) \Leftrightarrow Q(x, y)$$

have truth values F, F, T, F, F, respectively, and when $x = 2$ and $y = 3$, they have truth values T, F, T, T, F, respectively.

Using the operations $\neg$, $\wedge$, $\vee$, $\Rightarrow$, and $\Leftrightarrow$, we can construct **compound** expressions such as

$$(P \wedge (\neg Q)) \Rightarrow ((\neg R) \vee ((\neg P) \wedge Q)).$$

As this example illustrates, it is sometimes necessary to include many parentheses to make the grouping of terms in a formula clear. Just as in algebra, where multiplication takes precedence over addition, we can eliminate some parentheses by agreeing on a particular order in which logical operations are performed. We will apply the operations in this order, from first to last: $\neg$, $\wedge$, $\vee$, $\Rightarrow$ and $\Leftrightarrow$. Thus

$$A \Rightarrow B \vee C \wedge \neg D \qquad \text{is short for} \qquad A \Rightarrow (B \vee (C \wedge (\neg D))).$$

It is generally a good idea to include some extra parentheses to make certain the intended meaning is clear.

Much of the information we have discussed can be summarized in **truth tables**. For example, the truth table for $\neg P$ is:

P	$\neg P$
T	F
F	T

This table has two rows because there are only two possibilities for the truth value of P. The other logical operations involve two formulas, so they require four rows in their truth tables.

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

P	Q	$P \Leftrightarrow Q$
T	T	T
T	F	F
F	T	F
F	F	T

Any compound expression has a truth table. If there are n simple (that is, not compound) formulas in the expression, then there will be 2^n rows in the table because there are this many different ways to assign T's and F's to the n simple formulas in the compound expression. The truth table for $(P \wedge Q) \vee \neg R$ is

P	Q	R	$P \wedge Q$	$\neg R$	$(P \wedge Q) \vee \neg R$
T	T	T	T	F	T
T	T	F	T	T	T
T	F	T	F	F	F
T	F	F	F	T	T
F	T	T	F	F	F
F	T	F	F	T	T
F	F	T	F	F	F
F	F	F	F	T	T

Observe how the inclusion of intermediate steps makes the table easier to calculate and read.

A **tautology** is a logical expression that always evaluates to T, that is, the last column of its truth table consists of nothing but T's. A tautology is sometimes said to be **valid**. (Although "valid" is used in other contexts as well, this should cause no confusion.) For example, the statement $(P \wedge Q) \vee P \Leftrightarrow P$ is a tautology, since its truth table is:

P	Q	$P \wedge Q$	$(P \wedge Q) \vee P$	$(P \wedge Q) \vee P \Leftrightarrow P$
T	T	T	T	T
T	F	F	T	T
F	T	F	F	T
F	F	F	F	T

We list a few important tautologies in the following theorem, including the names by which some of the tautologies are referred to in the literature.

THEOREM 1.3 The following logical statements are tautologies:

a) $P \vee \neg P$ (excluded middle)

b) $P \Leftrightarrow \neg(\neg P)$ (double negation)

c) $P \vee Q \Leftrightarrow Q \vee P$

d) $P \wedge Q \Leftrightarrow Q \wedge P$

e) $(P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R)$

f) $(P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R)$

g) $P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$

h) $P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$

i) $(P \Rightarrow Q) \Leftrightarrow (\neg P \vee Q)$ (conditional disjunction)

j) $(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)$ (contraposition)

k) $(P \wedge (P \Rightarrow Q)) \Rightarrow Q$ (modus ponens)

l) $P \Rightarrow (P \vee Q)$

m) $(P \wedge Q) \Rightarrow P$

n) $((P \vee Q) \wedge \neg P) \Rightarrow Q$ (disjunctive syllogism)

o) $(P \Leftrightarrow Q) \Leftrightarrow ((P \Rightarrow Q) \wedge (Q \Rightarrow P))$ (logical biconditional)

Proof. The proofs are left as exercises. However, we note in passing that it is not always necessary to use a truth table to verify a tautology. For example, a proof of (j) can be written as

$$\begin{aligned}
(P \Rightarrow Q) &\Leftrightarrow (\neg P \vee Q) && \text{by part (i)} \\
&\Leftrightarrow (Q \vee \neg P) && \text{by part (c)} \\
&\Leftrightarrow (\neg(\neg Q) \vee \neg P) && \text{by part (b)} \\
&\Leftrightarrow (\neg Q \Rightarrow \neg P) && \text{by part (i)}
\end{aligned}$$

In other words, previous results can sometimes be used to prove other results. ■

In reading through Theorem 1.3, you may have noticed that $\wedge$ and $\vee$ satisfy many similar properties. These are called "dual" notions—for any property of one, there is a nearly identical property that the other satisfies, with the instances of the two operations interchanged. This often means that when we prove a result involving one notion, we get the corresponding result for its dual with no additional work.

Observe that (c) and (d) are commutative laws, (e) and (f) are associative laws, and (g) and (h) show that $\wedge$ and $\vee$ distribute over each other. This suggests that there is a form of algebra for logical expressions similar to the algebra for numerical expressions. This subject is called **Boolean Algebra** and has many uses, particularly in computer science.

If two formulas always take on the same truth value no matter what elements from the universe of discourse we substitute for the various variables, then we say they are **equivalent**. The advantage of equivalent formulas is that they say the same thing but in a different way. For example, algebraic manipulations such as replacing $x^2 - 2x = 12$ with $(x-1)^2 = 13$ fit into this category. It is always

a valid step in a proof to replace some formula by an equivalent one. In addition, many tautologies contain important ideas for constructing proofs. For example, (o) says that if you wish to show that $P \Leftrightarrow Q$, it is possible (and often advisable) to break the proof into two parts, one proving the implication $P \Rightarrow Q$ and the second proving the converse, $Q \Rightarrow P$.

Since we just mentioned the term "converse," this is probably a good place to refresh your memory of some familiar terminology. In the conditional sentence $P \Rightarrow Q$, the sentence P is usually referred to as the **hypothesis** and the sentence Q is called the **conclusion**. By rearranging and/or negating P and Q, we can form various other conditionals related to $P \Rightarrow Q$; you may remember doing this in a high school geometry class. Beginning with the conditional $P \Rightarrow Q$, the **converse** is $Q \Rightarrow P$, the **contrapositive** is $\neg Q \Rightarrow \neg P$, and the **inverse** is $\neg P \Rightarrow \neg Q$. As an illustration, consider the following important theorem from differential calculus.

conditional:	If f is differentiable at c, then f is continuous at c.
converse:	If f is continuous at c, then f is differentiable at c.
contrapositive:	If f is not continuous at c, then f is not differentiable at c.
inverse:	If f is not differentiable at c, then f is not continuous at c.

As indicated in part (j) of Theorem 1.3, a conditional and its contrapositive always have the same truth value. It is very important to note that the converse may or may not have the same truth value as the given conditional; the previous illustration provides one example where the truth values of a statement and its converse are not the same. (Be certain that you can give an example to show that the converse in this case is false.) It is a common mistake for students to turn theorems around without thinking much about it. Be aware of this potential pitfall and think carefully before drawing conclusions. The inverse, which is the contrapositive of the converse, is not referred to very often in mathematics.

George Boole. Boole (1815–1864) had only a common school education, though he learned Greek and Latin on his own. He began his career as an elementary school teacher, but decided that he needed to know more about mathematics, so he began studying mathematics, as well as the languages he needed to read contemporary literature in mathematics. In 1847, he published a short book, *The Mathematical Analysis of Logic*, which may fairly be said to have founded the study of mathematical logic. The key contribution of the work was in redefining 'mathematics' to mean not simply the 'study of number and magnitude,' but the study of symbols and their manipulation according to certain rules. The importance of this level of abstraction for the future of mathematics would be difficult to overstate. Probably on the strength of this work, he moved into a position at Queens College in Cork.

In *Investigation of the Laws of Thought*, published in 1854, Boole established a real formal logic, developing what today is called Boolean Algebra, or sometimes the **algebra of sets**. He used the symbols for addition and multiplication as operators, but in a wholly abstract sense. Today these symbols are still sometimes used in Boolean algebra, though the symbols '$\wedge$' and '$\vee$',

and '$\cap$' and '$\cup$', are also used. Boole applied algebraic manipulation to the process of reasoning. Here's a simple example of the sort of manipulation he did. The equation $xy = x$ (which today might be written $x \wedge y = x$ or $x \cap y = x$) means that 'all things that satisfy x satisfy y,' or in our terms, $x \Rightarrow y$. If also $yz = y$ (that is, $y \Rightarrow z$), then substituting $y = yz$ into $xy = x$ gives $x(yz) = x$ or $(xy)z = x$. Replacing xy by x, we get $xz = x$, or $x \Rightarrow z$. This simple example of logical reasoning (essentially the transitive property) is used over and over in mathematics.

In 1859, Boole wrote *Treatise on Differential Equations*, in which he introduced the algebra of differential operators. Using D to stand for 'the derivative of,' the second order differential equation $ay'' + by' + cy = 0$ may be written as $aD^2(y) + bD(y) + cy = 0$, or in the more compact form $(aD^2 + bD + c)y = 0$. Remarkably, the solutions to $aD^2 + bD + c = 0$, treating D as a *number*, provide information about the solutions to the differential equation. (If you have taken differential equations, you should be familiar with this approach to solving linear differential equations.)

The information here is taken from *A History of Mathematics,* by Carl B. Boyer, New York: John Wiley and Sons, 1968. For more information, see *Lectures on Ten British Mathematicians*, by Alexander Macfarlane, New York: John Wiley & Sons, 1916.

Exercises 1.1.

1. Determine the truth value of each of the following statements.

a) 51 is a prime or 128 is a square.

b) 211 is a prime and 441 is a square.

c) $\left\{\left(1 - \frac{1}{k}\right)^k\right\}$ converges to 1 or $\displaystyle\sum_{k=1}^{\infty} \frac{1}{2k-1}$ converges.

d) $e = \displaystyle\sum_{k=0}^{\infty} \frac{1}{k!}$ and $\frac{1}{2} = \displaystyle\sum_{k=1}^{\infty} \frac{1}{3^k}$.

e) $\displaystyle\sum_{k=1}^{\infty} \frac{1}{k^2}$ converges or $\displaystyle\sum_{k=1}^{\infty} \frac{1}{2^k}$ converges.

f) The graph of $y = \dfrac{1}{1+x^2}$ is concave down on $\mathbb{R}$ and $\displaystyle\int_{-\infty}^{\infty} \frac{1}{1+x^2}\,dx = \pi$.

g) If $f(x) = \arctan x$, then $f'(x) = 1/(1+x^2)$.

h) $f''(x) = -f(x)$ if and only if $f(x) = \sin x$.

2. Construct truth tables for the following logical expressions.

a) $(P \wedge Q) \vee \neg P$

b) $P \Rightarrow (Q \wedge P)$

c) $(P \wedge Q) \Leftrightarrow (P \vee \neg R)$

d) $\neg P \Rightarrow \neg(Q \vee R)$

3. Verify the tautologies in Theorem 1.3.

4. Suppose $P(x, y)$ is the formula "$x + y = 4$" and $Q(x, y)$ is the formula "$x < y$". Find the truth values for the formulas

$$P(x,y) \wedge Q(x,y), \quad \neg P(x,y) \vee Q(x,y), \quad P(x,y) \Rightarrow \neg Q(x,y), \quad \neg(P(x,y) \Leftrightarrow Q(x,y)),$$

using the values:

a) $x = 1, y = 3$

b) $x = 1, y = 2$

c) $x = 3, y = 1$

d) $x = 2, y = 1$

5. Write the converse and contrapositive of each of the following conditionals. Use your knowledge of mathematics to determine if the statements are true or false. (Note that there are three statements to consider for each part; the original statement and the two new ones derived from it.) For parts (a) and (e), consider different universes and see if the truth values of the statements change.

a) If $x = y$, then $x^3 = y^3$.

b) If f and g are differentiable on $\mathbb{R}$, then $f + g$ is differentiable on $\mathbb{R}$.

c) If $\sum_{n=1}^{\infty} a_n$ converges, then $\lim_{n\to\infty} a_n = 0$.

d) A convergent sequence is bounded. (Begin by writing this as a conditional involving a variable.)

e) If $a < b$, then $a^2 < b^2$.

1.2 Quantifiers

Recall that a formula (or open sentence) is a statement whose truth value may depend on the values of some variables. For example, the formula "$(x \leq 5) \wedge (x > 3)$" is true for $x = 4$ and false for $x = 6$. Compare this with the statement "For every x, $(x \leq 5) \wedge (x > 3)$," which is false and the statement "There exists an x such that $(x \leq 5) \wedge (x > 3)$," which is true. The phrase "for every x" (sometimes "for all x") is called a **universal quantifier** and is denoted by $\forall x$. The phrase "there exists an x such that" is called an **existential quantifier** and is denoted by $\exists x$. A formula that contains variables is not simply true or false unless each of the variables is **bound** by a quantifier. If a variable is not bound, the truth of the formula is contingent on the value assigned to the variable from the universe of discourse.

We were careful in Section 1.1 to define the truth values of compound statements precisely. We do the same for $\forall x\, P(x)$ and $\exists x\, P(x)$, though the intended meanings of these are clear.

The Universal Quantifier

A sentence $\forall x\, P(x)$ is true if and only if $P(x)$ is true no matter what value (from the universe of discourse) is substituted for x. To illustrate this notation, let $\mathbb{R}$ (the set of all real numbers) be the universe of discourse. Then

- $\forall x\ (x^2 \geq 0)$ states that "the square of any real number is nonnegative";
- $\forall x \forall y\ (x + y = y + x)$ represents the commutative law of addition;
- $\forall x \forall y \forall z\ ((xy)z = x(yz))$ represents the associative law of multiplication.

The "all" form. The universal quantifier is frequently encountered in the form $\forall x\ (P(x) \Rightarrow Q(x))$, which may be read, "All x satisfying $P(x)$ also satisfy $Q(x)$." The parentheses are crucial here so be sure to include them. For example (note how the universe changes in these examples),

- $\forall x$ (x is differentiable $\Rightarrow$ x is continuous) represents "all differentiable functions are continuous";
- $\forall x$ (x is a square $\Rightarrow$ x is a rectangle) represents "all squares are rectangles";
- $\forall x$ (x is a perfect square $\Rightarrow$ x is not prime) represents "every perfect square is not a prime."

This construction sometimes is used to express a mathematical sentence of the form "if this, then that," with an "understood" quantifier. (The last exercise in the previous section illustrates how quantifiers appear implicitly.)

EXAMPLE 1.4 Let $\mathbb{R}$ be the universe of discourse.

- If we say, "if x is negative, so is its cube," we usually mean "every negative x has a negative cube." This should be written symbolically as $\forall x\ ((x < 0) \Rightarrow (x^3 < 0))$.
- "If two numbers have the same square, then they have the same absolute value" should be written as $\forall x\, \forall y\ ((x^2 = y^2) \Rightarrow (|x| = |y|))$.
- "If $x = y$, then $x + z = y + z$" should be written as $\forall x\, \forall y\, \forall z\ ((x = y) \Rightarrow (x + z = y + z))$.

If S is a set, the sentence "every x in S satisfies $P(x)$" is written formally as

$$\forall x\ ((x \in S) \Rightarrow P(x)).$$

(We assume that the reader has some familiarity with sets; a set is a collection of objects and the notation $x \in S$ means that the element x belongs to the set S. Sets will be discussed in Section 1.5.) For clarity and brevity, this is usually written $\forall x \in S\,(P(x))$ or $(\forall x \in S)(P(x))$ if there is any chance of confusion. To understand and manipulate the formula $\forall x \in S\,(P(x))$ properly, you will sometimes need to "unabbreviate" it, rewriting it as $\forall x\ ((x \in S) \Rightarrow P(x))$. With $\mathbb{R}$ as the universe of discourse, we use

- $\forall x \in [0, 1]\ (\sqrt{x} \geq x)$ to represent $\forall x\ (x \in [0, 1] \Rightarrow \sqrt{x} \geq x)$;
- $\forall x < 0\ (|x| = -x)$ to represent $\forall x\ (x < 0 \Rightarrow |x| = -x)$.

The Existential Quantifier

A sentence $\exists x\, P(x)$ is true if and only if there is at least one value of x (from the universe of discourse) that makes $P(x)$ true. To illustrate this notation, let $\mathbb{R}$ be the universe of discourse. Then

- $\exists x\ (x > x^2)$ is true since $x = 0.5$ is one of many solutions;
- $\exists x\, \exists y\ (x^2 + y^2 = 2xy)$ is true since $x = y = 1$ is one of many solutions.

For the record, what happens to the truth value for the first of these statements if the universe of discourse is assumed to be the set of positive integers?

The "some" form. The existential quantifier is frequently encountered in the following context:

$$\exists x\ (P(x) \wedge Q(x)),$$

which may be read, "Some x satisfying $P(x)$ also satisfies $Q(x)$." For example (note how the assumed universe changes in these examples),

- $\exists x\,(x$ is a perfect square $\wedge$ x is a perfect cube, that is, "some perfect squares are perfect cubes";
- $\exists x\,(x$ is a prime number $\wedge$ x is even), that is, "some prime number is even";
- $\exists x\,(x$ is bounded $\wedge$ x is not integrable), that is, "some bounded function is not integrable".

It may, at first glance, seem that "Some x satisfying $P(x)$ satisfies $Q(x)$" should be translated as

$$\exists x\ (P(x) \Rightarrow Q(x)),$$

just like the universal quantifier. To see why this does not work, consider the two sentences $P(x)$ = "x is a positive integer" and $Q(x)$ = "x is a rational number between -10 and 0." The

sentence "some positive integers are rational numbers between -10 and 0" is certainly false, but

$$\exists x\ (P(x) \Rightarrow Q(x))$$

is true. To see this, suppose $x_0 = -7$. Then the implication $P(x_0) \Rightarrow Q(x_0)$ is true (since the hypothesis is false) and the existential quantifier is satisfied.

We use abbreviations of the "some" form much like those for the "all" form.

EXAMPLE 1.5 Let $\mathbb{R}$ be the universe of discourse.

- $\exists x < 0\ (x^2 = 1)$ stands for $\exists x\ ((x < 0) \wedge (x^2 = 1))$.
- $\exists x \in [0, 1]\ (2x^2 + x = 1)$ stands for $\exists x\ ((x \in [0, 1]) \wedge (2x^2 + x = 1))$.

If $\forall$ corresponds to "all" and $\exists$ corresponds to "some", do we need a third quantifier to correspond to "none"? As the following examples show, this is not necessary:

- "No perfect squares are prime," can be written $\forall x$ (x is a perfect square $\Rightarrow$ x is not prime);
- "No triangles are rectangles," can be written $\forall x$ (x is a triangle $\Rightarrow$ x is not a rectangle);
- "No unbounded sequences are convergent," can be written $\forall x$ (x is an unbounded sequence $\Rightarrow$ x is not convergent).

In general, the statement "no x satisfying $P(x)$ satisfies $Q(x)$" can be written as

$$\forall x\ (P(x) \Rightarrow \neg Q(x)) \qquad \text{or, equivalently, as} \qquad \forall x\ (Q(x) \Rightarrow \neg P(x)).$$

(You may wonder why we do not use $\neg\exists x\,(P(x) \wedge Q(x))$. In fact, we could—it is equivalent to $\forall x\ (P(x) \Rightarrow \neg Q(x))$; such statements will be considered in the next section.)

Exercises 1.2.

Except for problems 2 and 3, assume that the universe of discourse is the set of real numbers.

1. Express the following as formulas involving quantifiers.

a) Any number raised to the fourth power is nonnegative.

b) Some number raised to the third power is negative.

c) The sine of a number is always between -1 and 1, inclusive.

d) 10 raised to any negative power is strictly between 0 and 1.

2. Let U represent the set of all living people, let $T(x)$ be the statement "x is tall", and let $B(x)$ be the statement "x plays basketball". Express the following as formulas involving quantifiers.

a) All basketball players are tall.

b) Some tall people play basketball.

c) Not all basketball players are tall.

d) No tall person plays basketball.

3. Suppose X and Y are sets. Express the following as formulas involving quantifiers.

a) Every element of X is an element of Y.

b) Some element of X is an element of Y.

c) Some element of X is not an element of Y.

d) No element of X is an element of Y.

4. Recall (from calculus) that a function f is increasing on $\mathbb{R}$ if

$$\forall a\ \forall b\ (a < b \Rightarrow f(a) < f(b))$$

Express the following related definitions as formulas involving quantifiers.

a) f is decreasing on $\mathbb{R}$ **b)** f is constant on $\mathbb{R}$ **c)** f has a zero ($f(x) = 0$ has a solution)

5. Express the following algebraic laws symbolically:

a) the commutative law of multiplication

b) the associative law of addition

c) the distributive law

6. Are the following sentences true or false? Explain your answers.

a) $\forall x\ \forall y\ (x < y \Rightarrow x^2 < y^2)$

b) $\forall x\ \forall y\ \forall z \neq 0\ (xz = yz \Rightarrow x = y)$

c) $\exists x < 0\ \exists y < 0\ (x^2 + xy + y^2 = 3)$

d) $\exists x\ \exists y\ \exists z\ (x^2 + y^2 + z^2 = 2xy - 2 + 2z)$

1.3 De Morgan's Laws

If P is some sentence or formula, then (as we have seen) $\neg P$ is called the denial or negation of P. The ability to manipulate the denial of a formula accurately is critical to understanding mathematical arguments. The following tautologies are referred to as **De Morgan's Laws**:

$$\neg(P \vee Q) \Leftrightarrow (\neg P \wedge \neg Q) \qquad \text{and} \qquad \neg(P \wedge Q) \Leftrightarrow (\neg P \vee \neg Q).$$

These are easy to verify using truth tables, but with a little thought, they are not hard to understand directly. The first says that the only way that $P \vee Q$ can fail to be true is if both P and Q fail to be true. For example, the statements "x is neither positive nor negative" and "x is not positive and x is not negative" clearly express the same thought. For an example of the second tautology, consider "x is not between 2 and 3." This can be written symbolically as $\neg((2 < x) \wedge (x < 3))$, and clearly is equivalent to $\neg(2 < x) \vee \neg(x < 3)$, that is, $(x \leq 2) \vee (x \geq 3)$.

We can also use De Morgan's Laws to simplify the denial of $P \Rightarrow Q$:

$$\begin{aligned} \neg(P \Rightarrow Q) &\Leftrightarrow \neg(\neg P \vee Q) \\ &\Leftrightarrow (\neg\neg P) \wedge (\neg Q) \\ &\Leftrightarrow P \wedge \neg Q \end{aligned}$$

so the denial of $P \Rightarrow Q$ is $P \wedge \neg Q$. (What is the justification for the first step?) In other words, it is not the case that P implies Q if and only if P is true and Q is false. Of course, this agrees with the truth table for $P \Rightarrow Q$ that we have already seen.

There are versions of De Morgan's Laws for quantifiers:

$$\begin{aligned} \neg\forall x\, P(x) &\Leftrightarrow \exists x\, \neg P(x); \\ \neg\exists x\, P(x) &\Leftrightarrow \forall x\, \neg P(x). \end{aligned}$$

You may be able to see that these are true immediately. If not, here is an explanation for the statement $\neg\forall x\, P(x) \Rightarrow \exists x\, \neg P(x)$ that should be convincing. If $\neg\forall x\, P(x)$ is true, then $P(x)$ is not true for every value of x, which is to say that for some value a, $P(a)$ is not true. This means that $\neg P(a)$ is true. Since $\neg P(a)$ is true, it is certainly the case that there is some value of x that makes $\neg P(x)$ true and hence $\exists x\, \neg P(x)$ is true. The other three implications may be explained similarly.

Here is another way to think of the quantifier versions of De Morgan's Laws. The statement $\forall x\, P(x)$ is very much like a conjunction of many statements. If the universe of discourse is the set of positive integers, for example, then

$$\forall x\, P(x) \;\Leftrightarrow\; P(1) \wedge P(2) \wedge P(3) \wedge \cdots$$

and its negation would be

$$\begin{aligned} \neg\forall x\, P(x) &\;\Leftrightarrow\; \neg\big(P(1) \wedge P(2) \wedge P(3) \wedge \cdots\big) \\ &\;\Leftrightarrow\; \neg P(1) \vee \neg P(2) \vee \neg P(3) \vee \cdots \\ &\;\Leftrightarrow\; \exists x\, \neg P(x). \end{aligned}$$

Similar reasoning shows that the second quantifier law can also be interpreted this way.

Finally, general understanding is usually aided by specific examples. Suppose the universe is the set of cars. If $P(x)$ is "x has four wheel drive," then the denial of "every car has four wheel drive" is "there exists a car which does not have four wheel drive." This is an example of the first law. If $P(x)$ is "x has three wheels," then the denial of "there is a car with three wheels" is "every car does not have three wheels." This fits the pattern of the second law. In a more mathematical vein, a denial of the sentence "for every x, x^2 is positive" is "there is an x such that x^2 fails to be positive." A denial of "there is an x such that $x^2 = -1$" is "for every x, $x^2 \neq -1$."

It is easy to confuse the denial of a sentence with something stronger. If the universe is the set of all people, the denial of the sentence "All people are tall" is not the sentence "No people are tall." This might be called the **opposite** of the original sentence—it says more than simply "'All people are tall' is untrue." The correct denial of this sentence is "there is someone who is not tall," which is a considerably weaker statement. In symbols, the denial of $\forall x\ P(x)$ is $\exists x\ \neg P(x)$, whereas the opposite is $\forall x\ \neg P(x)$. ("Denial" is an "official" term in wide use; "opposite," as used here, is not widely used.)

De Morgan's Laws can be used to simplify negations of the "some" form and the "all" form; the negations themselves turn out to have the same forms, but "reversed," that is, the negation of an "all" form is a "some" form, and vice versa. Suppose $P(x)$ and $Q(x)$ are formulas. We then have

$$\begin{aligned} \neg\forall x\ (P(x) \Rightarrow Q(x)) &\;\Leftrightarrow\; \exists x\ (P(x) \wedge \neg Q(x)); \\ \neg\exists x\ (P(x) \wedge Q(x)) &\;\Leftrightarrow\; \forall x\ (P(x) \Rightarrow \neg Q(x)). \end{aligned}$$

To illustrate the first form, the denial of the sentence "all lawn mowers run on gasoline" is the sentence "some lawn mower does not run on gasoline" (not "no lawn mowers run on gasoline," the opposite). We will verify the first statement and leave a verification of the second as an exercise. We begin by noting that a formula is usually easier to understand when $\neg$ does not appear in front of any compound expression, that is, it appears only in front of simple statements such as $P(x)$. Using this idea, we find that

$$\neg\forall x\ (P(x) \Rightarrow Q(x)) \;\Leftrightarrow\; \exists x\ \neg(P(x) \Rightarrow Q(x)) \;\Leftrightarrow\; \exists x\ (P(x) \wedge \neg Q(x)),$$

where the last step uses a tautology presented earlier in this section.

Denials of formulas are extremely useful. In a later section we will see that the techniques called proof by contradiction and proof by contraposition use them extensively. Denials can also be a helpful study device. When you read a theorem or a definition in mathematics, it is frequently helpful to form the denial of that sentence to see what it means for the condition to fail. The more ways you think about a concept in mathematics, the clearer it should become. To illustrate this point, we note that definitions in mathematics are biconditional in nature even though they are not always written in this form. In other words, definitions fit into the form $P \Leftrightarrow Q$. To negate a definition means to write out $\neg P \Leftrightarrow \neg Q$. (This is not the same as forming the denial of a biconditional!) Since definitions often involve quantifiers, some care must be taken when doing this. Consider the following definition:

A function f defined on $\mathbb{R}$ is even if $f(-x) = f(x)$ for all $x \in \mathbb{R}$.

As just mentioned, this definition is actually a biconditional even though it is not written explicitly in that form. In symbols, we can express this definition as

$$f \text{ is even } \Leftrightarrow \forall x \in \mathbb{R}(f(x) = f(-x)),$$

which is equivalent to

$$f \text{ is not even } \Leftrightarrow \exists x \in \mathbb{R}(f(x) \neq f(-x)).$$

In words, the negation of the definition is the following:

A function f defined on $\mathbb{R}$ is not even if there exists an $x \in \mathbb{R}$ such that $f(-x) \neq f(x)$.

To illlustrate these ideas, note that the functions $f(x) = x^2$ and $g(x) = \cos x$ are even. To show that the function h defined by $h(x) = 2x^4 - 3x$ is not even, it is sufficient to note that $h(-1) = 5 \neq -1 = h(1)$.

It takes some practice to learn how to express negated definitions in clear words; read your definitions several times to ensure that they represent the correct mathematical idea in a way that others will understand. For the record, it is not always necessary to run through all of the symbols to negate a definition, but it can be helpful in many cases.

Augustus De Morgan. (y–1871; De Morgan himself noted that he turned x years old in the year x^2.) De Morgan's father died when he was ten, after which he was raised by his mother, a devout member of the Church of England, who wanted him to be a minister. Far from becoming a minister, De Morgan developed a pronounced antipathy toward the Church, which would profoundly influence the course of his career.

De Morgan's interest in and talent for mathematics did not become evident until he was fourteen, but already at sixteen he entered Trinity College at Cambridge, where he studied algebra under George Peacock and logic under William Whewell. He was also an excellent flute player, and became prominent in musical clubs at Cambridge.

On graduation, De Morgan was unable to secure a position at Oxford or Cambridge, as he refused to sign the required religious test (a test not abolished until 1875). Instead, at the age of

22, he became Professor of Mathematics at London University, a new institution founded on the principle of religious neutrality.

De Morgan wrote prolifically on the subjects of algebra and logic. Peacock and Gregory had already focused attention on the fundamental importance to algebra of symbol manipulation—that is, they established that the fundamental operations of algebra need not depend on the interpretation of the variables. De Morgan went one (big) step further: he recognized that the operations ($+$, $-$, etc.) also need have no fixed meaning (though he made an exception for equality). Despite this view, De Morgan does seem to have thought that the only appropriate interpretations for algebra were familiar numerical domains, primarily the real and complex numbers. Indeed, he thought that the complex numbers formed the most general possible algebra, because he could not bring himself to abandon the familiar algebraic properties of the real and complex numbers, like commutativity.

One of De Morgan's most widely known books was *A Budget of Paradoxes*. He used the word 'paradox' to mean anything outside the accepted wisdom of a subject. Though this need not be interpreted pejoratively, his examples were in fact of the 'mathematical crank' variety—mathematically näive people who insisted that they could trisect the angle or square the circle, for example.

De Morgan's son George was himself a distinguished mathematician. With a friend, George founded the London Mathematical Society and served as its first secretary; De Morgan was the first president.

In 1866, De Morgan resigned his position to protest an appointment that was made on religious grounds, which De Morgan thought abused the principle of religious neutrality on which London University was founded. Two years later his son George died, and shortly thereafter a daughter died. His own death perhaps hastened by these events, De Morgan died in 1871 of 'nervous prostration.'

The information for this biography is taken from *Lectures on Ten British Mathematicians*, by Alexander Macfarlane, New York: John Wiley & Sons, 1916.

Exercises 1.3.

1. Use truth tables to verify De Morgan's Laws.

2. Let U be the collection of all quadrilaterals. Suppose $R(x)$ is the statement "x is a rectangle," and $S(x)$ is the statement "x is a square." Write the following symbolically and decide which pairs of statements are denials of each other:

a) All rectangles are squares.
b) Some rectangles are squares.
c) Some squares are not rectangles.
d) No squares are rectangles.
e) No rectangles are squares.
f) All squares are rectangles.
g) Some squares are rectangles.
h) Some rectangles are not squares.

3. Find and simplify the denial of each of the following expressions:

a) $\forall x > 0\ (x^2 > x)$
b) $\exists x \in [0,1]\ (x^2 + x < 0)$
c) $\forall x\ \forall y\ (xy = y^2 \Rightarrow x = y)$
d) $\exists x\ \exists y\ (x > y \wedge y > x)$

4. Verify $\neg\exists x\ (P(x) \wedge Q(x)) \Leftrightarrow \forall x\ (P(x) \Rightarrow \neg Q(x))$. Be certain to include all of the steps.

5. Observe that

$$P \vee Q \Leftrightarrow \neg\neg(P \vee Q) \Leftrightarrow \neg(\neg P \wedge \neg Q),$$

which shows that $\vee$ can be expressed in terms of $\wedge$ and $\neg$.

a) Show how to express $\Rightarrow$ in terms of $\wedge$ and $\neg$.

b) Show how to express $\wedge$ in terms of $\neg$ and $\vee$.

c) Show how to express $\vee$ in terms of $\neg$ and $\Rightarrow$.

6. Express the universal quantifier $\forall$ in terms of $\exists$ and $\neg$. Express $\exists$ in terms of $\forall$ and $\neg$.

7. Write (in words) negations for each definition; be careful with your wording. With the exception of part (c), give examples to illustrate both the definition and the negated definition.

a) A function f has a zero if and only if there exists a real number r such that $f(r) = 0$.

b) A positive integer $n > 1$ is square-free if and only if it is not divisible by any perfect square greater than 1.

c) A metric space X is complete if and only if every Cauchy sequence in X converges.

d) Let A be a set of real numbers and let $z \in R$. The point z is a limit point of A if and only if for each positive number r the interval $(z - r, z + r)$ contains a point of A other than z.

e) A function f is increasing on $\mathbb{R}$ if and only if $f(x) < f(y)$ for all real numbers x and y that satisfy $x < y$.

1.4 Mixed Quantifiers

In many of the more interesting mathematical formulas, some variables are universally quantified and others are existentially quantified. You should be very careful when this is the case; in particular, the order of the quantifiers is extremely important. Except as noted, the universe in the following examples is the set of real numbers.

EXAMPLE 1.6 Compare these two valid sentences:

$$\exists x\, \forall y\, (x + y = y), \qquad \forall y\, \exists x\, (x + y = 0).$$

In the first we require that x be a *fixed* value that satisfies the equation regardless of the value of y; clearly $x = 0$ will do. In the second formula, however, x *depends on* y; if $y = 3$, $x = -3$, if $y = 0$, $x = 0$. Note that for any given value of y, we must choose x to be $-y$; this shows the explicit dependence of x on y.

EXAMPLE 1.7 Compare these two sentences:

$$\forall x\, \exists y\, (y^3 = x), \qquad \exists y\, \forall x\ (xy^3 = -x).$$

The first is valid because given any x we can set y equal to the cube root of x. (That is, every real number has a cube root.) So as x varies, y also varies, that is, y depends upon x. The second is valid because there is a single fixed value $y = -1$ which makes the equation $xy^3 = -x$ valid, regardless of the value of x.

EXAMPLE 1.8 Compare these two sentences:

$$\forall x\, \exists y\, (x < y), \qquad \exists y\, \forall x\, (x < y).$$

The first sentence is true and states that given any number there is a strictly larger number, that is, there is no largest number. (A simple choice is $y = x + 1$.) The second sentence is false; it says that there is a single number that is strictly larger than all real numbers.

In general, if you compare $\exists y\, \forall x\, P(x, y)$ with $\forall x\, \exists y\, P(x, y)$, it is clear that the first statement implies the second. If there is a fixed value y_0 which makes $P(x, y)$ true for all x, then no matter what x we are given, we can find a y (the fixed value y_0) which makes $P(x, y)$ true. So the first is a **stronger** statement because one value of y will work for all values of x rather than needing a different value of y for each x. As in Example 1.8, it is usually the case that this implication cannot be reversed.

We now consider some examples that use more than two variables. The sentence "between any two distinct real numbers is another real number" can be written as

$$\forall x\, \forall y\, \exists z\, ((x < y) \Rightarrow (x < z < y)).$$

Observe that z depends in an essential way on both variables "to its left," namely, x and y. (The most common choice is to use $z = (x + y)/2$.) Neither of the following is true:

$$\forall x\, \exists z\, \forall y\, ((x < y) \Rightarrow (x < z < y)), \qquad \exists z\, \forall x\, \forall y\, ((x < y) \Rightarrow (x < z < y)).$$

Be certain that you can explain why these statements are false.

Now suppose that the universe of discourse is the set of integers. The following two sentences are valid:

$$\forall x\, \exists y\, \exists z\, (x = 7y + 5z), \qquad \forall x\, \exists y\, \forall z\, (z > x \Leftrightarrow z \geq y).$$

Consider the first sentence. In words, this sentence says "for each integer x, there exist integers y and z such that $x = 7y + 5z$." If we know the value of x, we can choose $y = -2x$ and $z = 3x$, so $7y + 5z = -14x + 15x = x$. Notice that y and z depend on x in an essential way. Turning to the second, if we know x, we can choose y to be the next integer, $x + 1$. Any z is strictly larger than x if and only if it is at least as large as y.

We often need to form denials of sentences with mixed quantifiers. These are handled with De Morgan's Laws, just as in Section 1.3. For example, using the set of real numbers as the universe, the sentence $\exists x\, \forall y\, (x + y \neq \pi)$ is false because its denial, the sentence $\forall x\, \exists y\, (x + y = \pi)$, is valid. (For any number x, let $y = \pi - x$.) Similarly, with the universe being the set of integers, the sentence $\forall x\, \exists y\, \exists z\, (x = 4y + 6z)$ is false because its denial $\exists x\, \forall y\, \forall z\, (x \neq 4y + 6z)$ is valid. To see this, note that $4y + 6z$ is even for any values of y and z so this expression cannot give any odd integer x.

Exercises 1.4.

1. Using the set of real numbers as the universe of discourse, describe why the following are valid:

a) $\exists x \forall y\,(xy = x^2)$ **b)** $\forall x \exists y\,(x^2 + 6xy + 9y^2 = 0)$

c) $\exists y \forall x\,(x + y > xy)$ **d)** $\forall y \exists x\,(y - x = xy^2 + 1)$

e) $\forall x \exists y\,(y^2 - x = xy + 2)$ **f)** $\exists x \forall y\,(2\sin^2 y + \cos(2y) = x)$

2. Using the integers as the universe of discourse, describe why the following are valid:

a) $\forall x \exists y \forall z\,(z < x \Leftrightarrow z \leq y)$ **b)** $\forall x \exists y \exists z\,(x = 8y + 3z)$

c) $\exists x \forall y \forall z\,(x = yz \Rightarrow y = -z)$ **d)** $\exists x > 1 \forall y \exists z\,((y = xz) \vee (y = xz + 1))$

3. Form the denials of the following statements and simplify using De Morgan's Laws. Which of the statements are true?

a) $\forall x \exists y\,((x+y = 1) \wedge (xy \neq 0))$ **b)** $\exists y \forall x\,((x^2 = y) \Rightarrow (x = y + 1))$

4. Write (in words) negations for each definition; do pay attention to your wording. Except for part (a), try to find examples to illustrate the definitions.

a) A group G is abelian if and only if $x * y = y * x$ for all x and y in G.

b) A sequence $\{x_n\}$ is bounded if and only if there is a number M such that $|x_n| \leq M$ for all n.

c) The sequence $\{x_n\}$ converges to the number L if and only if for each $\epsilon > 0$ there exists a positive integer N such that $|x_n - L| < \epsilon$ for all $n \geq N$.

d) A sequence $\{x_n\}$ is a Cauchy sequence if and only if for each $\epsilon > 0$ there exists a positive integer N such that $|x_m - x_n| < \epsilon$ for all $m, n \geq N$.

e) A function $f\colon \mathbb{R} \to \mathbb{R}$ is continuous at c if and only if for each $\epsilon > 0$ there exists $\delta > 0$ such that $|f(x) - f(c)| < \epsilon$ for all x that satisfy $|x - c| < \delta$.

f) A function f is Lipschitz on $\mathbb{R}$ if and only if there exists a positive constant K such that the inequality $|f(x) - f(y)| \leq K|x - y|$ is valid for all x and y in $\mathbb{R}$.

g) A set A of real numbers is bounded if and only if there exists a positive number M such that $|x| \leq M$ for all $x \in A$.

h) A set A of real numbers is open if and only if for each $x \in A$ there exists a positive number r such that $(x - r, x + r) \subseteq A$.

5. Using quantifiers, define what it means for a function f defined on $\mathbb{R}$ to be **periodic** (for example, recall that $\sin(x)$ is periodic). What does it mean for f to fail to be periodic?

1.5 Logic and Sets

Like logic, the subject of **sets** is rich and interesting for its own sake. However, we will be content to list a few facts about sets and discuss some techniques for dealing with them. Further properties of sets are considered in Chapter 4.

It is necessary for some terms in mathematics to be left undefined; the concept of "set" is one such term. When a term is left undefined, some attempt must be made to explain what is meant by the term. Since everyone has some experience with sets (a set of dishes, a collection of stamps, a herd of buffalo, a pocket full of change), it is not difficult to get across the basic idea of a set. Hence, we say that a **set** is a collection of objects. The objects in a set usually have some features in common, such as the set of real numbers or a set of continuous functions, but a set can also be any random collection of objects. (Actually, there are some restrictions on the types of objects that can be considered, but this restriction will not be important here.) Any one of the objects in

a set is called a **member** or an **element** of the set. If a is an element of a set A, we write $a \in A$; if b does not belong to the set A, we write $b \notin A$.

Some sets occur so frequently that there are standard names and symbols for them. We denote the set of real numbers by $\mathbb{R}$, the set of rational numbers (numbers that can be expressed as the quotient of two integers) by $\mathbb{Q}$, the set of integers by $\mathbb{Z}$, and the set of natural numbers (that is, the set of positive integers) by $\mathbb{N}$ or $\mathbb{Z}^+$. Although we make little or no mention of them in this text, the set of complex numbers is denoted by $\mathbb{C}$.

There is a natural relationship between sets and logic. If A is a set, then the sentence $P(x) =$"$x \in A$" is a formula. It is true for elements of A and false for elements outside of A. Conversely, if we are given a formula $Q(x)$, we can form the **truth set** consisting of all x that make $Q(x)$ true. This is usually written $\{x : Q(x)\}$ or $\{x \mid Q(x)\}$. For example, if the universe is $\mathbb{Z}$, then $\{x : x > 0\}$ represents the set of positive integers and $\{x : \exists n\,(x = 2n)\}$ represents the set of even integers. Another common way to denote this last set is $\{2n : n \in \mathbb{Z}\}$.

If there are a finite number of elements in a set, or if the elements can be arranged in a sequence, we often indicate the set simply by listing its elements. Each of the sets $\{1, 2, 3\}$ and $\{1, 3, 5, 7, 9, \ldots\}$ is a set of integers. The second is presumably the set of all positive odd numbers, but of course there are an infinite number of other possibilities. In all but the most obvious cases, it is usually wise to describe the set ("the set of positive odd numbers, $\{1, 3, 5, 7, 9, \ldots\}$"), to give a formula for the terms ("$\{1, 3, 5, 7, 9, \ldots, 2i + 1, \ldots\}$"), or to write an explicit formula within set notation ($\{2n - 1 : n \in \mathbb{N}\}$).

We indicate the **empty set** by $\emptyset$, that is, $\emptyset = \{\}$ is the set without any elements. Note well that $\emptyset \neq \{\emptyset\}$: the first set contains no elements while the second set contains a single element, namely the empty set. (This may seem a bit crazy at first, but it is an important distinction. You may find it helpful to think about an empty box versus a box that contains an empty box.)

The logical operations $\neg$, $\wedge$, and $\vee$ translate into the theory of sets in a natural way using truth sets. Let U be the universe of discourse. If A is some set comprised of elements from U, then we define the **complement** of A by $A^c = \{x : x \notin A\}$. This set represents all of the elements in the universe U that do not belong to A. If B is a second set, define

$$A \cap B = \{x : x \in A \wedge x \in B\} \qquad \text{and} \qquad A \cup B = \{x : x \in A \vee x \in B\},$$

which are called the **intersection** of A and B and the **union** of A and B, respectively. It is sometimes useful to consider the complement of B relative to A. This set, which is denoted by $A \setminus B$, is the set of all elements that belong to A but do not belong to B. This operation is referred to as **set difference** since the elements of B are removed from A.

EXAMPLE 1.9 Suppose the universe U of discourse consists of the set $\{1, 2, 3, \ldots, 10\}$ and consider the sets $A = \{1, 3, 4, 5, 7\}$ and $B = \{1, 2, 4, 7, 8, 9\}$. Then

$$A^c = \{2, 6, 8, 9, 10\}, \qquad A \cap B = \{1, 4, 7\},$$
$$A \setminus B = \{3, 5\}, \qquad A \cup B = \{1, 2, 3, 4, 5, 7, 8, 9\}.$$

Note that the complement of a set depends on the universe U, while the union, intersection, and set difference of two sets do not.

We often wish to compare two sets. We say that A is a **subset** of B if

$$\forall x\ (x \in A \Rightarrow x \in B),$$

and write $A \subseteq B$. This is not only a definition but a technique of proof. If we wish to show $A \subseteq B$ we may start with an arbitrary element x of A and prove that it must be in B. A proof that uses this approach is sometimes referred to as "chasing points" since we follow a point from A to B. We say the sets A and B are **equal** (and write $A = B$) if and only if $A \subseteq B$ and $B \subseteq A$, that is,

$$\forall x\ (x \in A \Leftrightarrow x \in B).$$

Thus to show two sets are equal one must verify that a biconditional is satisfied, and this often needs to be done in two parts. In other words, a common way to show that $A = B$ is to show that $A \subseteq B$ and $B \subseteq A$. If $A \subseteq B$ and $A \neq B$, we say A is a **proper** subset of B and write $A \subset B$. To illustrate this notation, note that $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$. The first two inclusions are obvious; a proof of the third one will be given in Section 2.8. Finally, we say that A and B are **disjoint** if $A \cap B = \emptyset$. For example, the set of odd integers and the set of even integers are disjoint.

In Section 1.1, we learned that logical operations are related by many tautologies, the study of which is called Boolean Algebra. These tautologies can be interpreted as statements about sets; here are some particularly useful examples.

THEOREM 1.10 Suppose A, B, and C are sets. Then

a) $(A^c)^c = A$

b) $A \cap B \subseteq A$

c) $A \subseteq A \cup B$

d) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

e) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

f) $(A \cap B)^c = A^c \cup B^c$

g) $(A \cup B)^c = A^c \cap B^c$

Proof. We first give a set theoretic proof (or a "chasing points" proof) of part (d). Suppose that $x \in A \cap (B \cup C)$. This means that x belongs to A and to either B or C. It follows that x belongs to either A and B or to A and C, that is, $x \in (A \cap B) \cup (A \cap C)$. We have thus shown that $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$. Now suppose that $x \in (A \cap B) \cup (A \cap C)$. This means that x belongs to either $A \cap B$ or to $A \cap C$, which in turn implies that x belongs to A and to either B or C, that is, $x \in A \cap (B \cup C)$. Therefore, $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$. We conclude that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. The other parts of the theorem can be proved in a similar way.

However, it is important to also realize that all of these facts are consequences of logical statements considered earlier. To illustrate this, define statements $P(x) =$"$x \in A$", $Q(x) =$"$x \in B$", and $R(x) =$"$x \in C$". Then part (d) is simply the tautology (part (g) of Theorem 1.3)

$$P(x) \wedge (Q(x) \vee R(x)) \Leftrightarrow (P(x) \wedge Q(x)) \vee (P(x) \wedge R(x)).$$

The other statements in the theorem are also related to tautologies. ■

As in the case of logic, parts (f) and (g) of Theorem 1.10 are called De Morgan's Laws. Theorem 1.10 certainly is not an exhaustive list of set identities—note that obvious facts such as commutative and associative properties are not included—it merely illustrates a few of the more important ones.

Suppose that A and B are nonempty sets. If $a \in A$ and $b \in B$, then we can form the **ordered pair** (a, b); the pair is said to be ordered since the first element must come from the set A and the second from the set B. The fundamental property of ordered pairs is that $(a_1, b_1) = (a_2, b_2)$ if and only if $a_1 = a_2$ and $b_1 = b_2$, that is, two ordered pairs are the same when both the first elements and the second elements are the same. If A and B are sets, the set

$$A \times B = \{(a, b) : a \in A \wedge b \in B\}$$

is called the **Cartesian product** of A and B. (Note carefully that a Cartesian product does not involve the multiplication of elements.) For example, if $A = \{r, s, t\}$ and $B = \{\$, \%\}$, then

$$A \times B = \{(r, \$), (r, \%), (s, \$), (s, \%), (t, \$), (t, \%)\}.$$

The sets $\mathbb{R} \times \mathbb{R}$ and $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$ are usually abbreviated as $\mathbb{R}^2$ and $\mathbb{R}^3$, respectively, and represent the plane and 3-dimensional space. It is in this latter context that you are most familiar with ordered pairs. As a reminder (via a particular example), the graph of the equation $y = x^2 + 2x + 2$ is the subset of $\mathbb{R}^2$ defined by $\{(x, y) : x \in \mathbb{R} \text{ and } y = x^2 + 2x + 2\}$.

René Descartes. Descartes (1596–1650) was perhaps the most able mathematician of his time (though he may have to share top billing with Pierre de Fermat, a busy lawyer who did mathematics on the side for fun). Despite his ability and his impact on mathematics, Descartes was really a scientist and philosopher at heart. He made one great contribution to mathematics, *La géométrie*, and then concentrated his energies elsewhere.

La géométrie did not even appear on its own, but as an appendix to his most famous work, *Discours de la méthode pour bien conduire sa raison et chercher la vérité dans les sciences* ("Discourse on the method of reasoning well and seeking truth in the sciences"). Descartes is remembered as the father of coordinate or analytic geometry, but his uses of the method were much closer in spirit to the great Greek geometers of antiquity than to modern usage. That is, his interest really lay in geometry; he viewed the introduction of algebra as a powerful tool for solving geometrical problems. Confirming his view that geometry is central, he went to some lengths to show how algebraic operations (for example, finding roots of quadratic equations) could be interpreted geometrically.

In contrast to modern practice, Descartes had no interest in graphing an arbitrary relation in two variables—in the whole of *La géométrie*, he did not plot any new curve from its equation. Further, ordered pairs do not play any role in the work; rectangular coordinates play no special role (Descartes used oblique coordinates freely—that is, his axes were not constrained to meet at a right angle); familiar formulas for distance, slope, angle between lines, and so on, make no

appearance; and negative coordinates, especially negative abscissas, are little used and poorly understood. Ironically, then, there is little about the modern notion of Cartesian coordinates that Descartes would recognize.

Despite all these differences in emphasis and approach, Descartes' work ultimately made a great contribution to the theory of functions. The Cartesian product may be misnamed, but Descartes surely deserves the tribute.

Exercises 1.5.

1. For the given universe U and the given sets A and B, find A^c, $A \cap B$, and $A \cup B$.
- **a)** $U = \{1, 2, 3, 4, 5, 6, 7, 8\}$, $A = \{1, 3, 5, 8\}$, $B = \{2, 3, 5, 6\}$
- **b)** $U = \mathbb{R}$, $A = (-\infty, 2]$, $B = (-1, \infty)$
- **c)** $U = \mathbb{Z}$, $A = \{n : n \text{ is even}\}$, $B = \{n : n \text{ is odd}\}$
- **d)** $U = \mathbb{Q}$, $A = \emptyset$, $B = \{q : q > 0\}$
- **e)** $U = \mathbb{N}$, $A = \mathbb{N}$, $B = \{n : n \text{ is even}\}$
- **f)** $U = \mathbb{R}$, $A = (-\infty, 0]$, $B = [-2, 3)$
- **g)** $U = \mathbb{N}$, $A = \{n : n \leq 6\}$, $B = \{1, 2, 4, 5, 7, 8\}$
- **h)** $U = \mathbb{R} \times \mathbb{R}$, $A = \{(x, y) : x^2 + y^2 \leq 1\}$, $B = \{(x, y) : x \geq 0, y \geq 0\}$.

2. For the sets in Exercise 1a, 1b, and 1e, find $A \setminus B$ and $B \setminus A$.

3. Prove that $A \setminus B = A \cap B^c$.

4. Prove the parts of Theorem 1.10 not proved in the text. Be certain you understand both approaches to these proofs.

5. Use Exercise 3 and Theorem 1.10 to prove that $(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$.

6. Suppose U is some universe of discourse. Find $\{x : x = x\}$ and $\{x : x \neq x\}$.

7. Prove carefully from the definition of "$\subseteq$" that for any set A, $\emptyset \subseteq A$.

8.
- **a)** For $A = \{1, 2, 3, 4\}$ and $B = \{x, y\}$, write out $A \times B$, $A \times A$, and $B \times B$.
- **b)** If A has m elements and B has n elements, how many elements are in $A \times B$?
- **c)** Describe $A \times \emptyset$. Justify your answer.
- **d)** What name do we give the set $(0, \infty) \times (0, \infty)$ in the universe $\mathbb{R}^2$?
- **e)** What kind of geometric figure is $[1, 2] \times [1, 2] \times [1, 2]$ in the universe $\mathbb{R}^3$?

9. If A and B are sets, show that $A \subseteq B$, $A \cap B^c = \emptyset$, and $A^c \cup B = U$ are equivalent statements, that is, each pair is related by the biconditional. What are the corresponding logical statements?

10. Suppose A, B, C, and D are sets.
- **a)** Prove that $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$.
- **b)** Does (a) hold with $\cap$ replaced by $\cup$? Prove any set inclusion that is true and give an example of any result that fails.
- **c)** Illustrate the results in parts (a) and (b) graphically in $\mathbb{R}^2$.

11. Suppose we say a set S is **normal** if $S \notin S$. (You probably have encountered only normal sets. For example, the *set* of real numbers is not a real number. However, consider the set of all abstract ideas. Most people would agree that this set is not normal.) Consider $N = \{S : S \text{ is a normal set}\}$. Is N a normal set? (This is called Russell's Paradox. Examples like this helped make set theory a mathematical subject in its own right. Although the concept of a set at first seems straightforward, even trivial, it emphatically is not.)

1.6 Families of Sets

Suppose I is a set and with each $i \in I$, associate a set A_i. The set I is referred to as the **index set** and we call $\{A_i : i \in I\}$ an **indexed family of sets**. Sometimes this is denoted by $\{A_i\}_{i\in I}$. Consider the following examples of this concept.

- Suppose I is the days of the year, and for each $i \in I$, let B_i be the set of people whose birthday is i. So, for example, Beethoven $\in B_{(\text{December } 16)}$.
- Suppose I is the set of integers and for each $i \in I$, let C_i be the set of multiples of i, that is, $C_i = \{ni : n \in \mathbb{Z}\}$. For example, $C_7 = \{\ldots, -21, -14, -7, 0, 7, 14, 21, \ldots\}$.
- For each real number x, let $D_x = \{x - 1, x, x + 1\}$. In this case, the index set I is the set of real numbers. For example, $D_\pi = \{\pi - 1, \pi, \pi + 1\}$.

Given an indexed family $\{A_i : i \in I\}$, we can define the intersection and union of the sets A_i using the universal and existential quantifiers:

$$\bigcap_{i\in I} A_i = \{x : \forall i \in I\,(x \in A_i)\} \quad \text{and} \quad \bigcup_{i\in I} A_i = \{x : \exists i \in I\,(x \in A_i)\}.$$

Referring to the examples given above,

- $\bigcap_{i\in I} B_i$ is the empty set and $\bigcup_{i\in I} B_i$ is the set of all people;
- $\bigcap_{i\in I} C_i$ is $\{0\}$ and $\bigcup_{i\in I} C_i$ is the set of all integers;
- $\bigcap_{x\in\mathbb{R}} D_x = \emptyset$ and $\bigcup_{x\in\mathbb{R}} D_x = \mathbb{R}$.

Since the intersection and union of an indexed family are essentially "translations" of the universal and existential quantifiers, it should not be too surprising that there are De Morgan's Laws that apply to these unions and intersections.

THEOREM 1.11 If $\{A_i : i \in I\}$ is an indexed family of sets then

a) $\left(\bigcap_{i\in I} A_i\right)^c = \bigcup_{i\in I} A_i^c$,

b) $\left(\bigcup_{i\in I} A_i\right)^c = \bigcap_{i\in I} A_i^c$.

Proof. We prove (a) and leave a proof of (b) as an exercise. In words, part (a) states that the complement of the intersection is the union of the complements and the equivalences

$$\begin{aligned} x \in \left(\bigcap_{i\in I} A_i\right)^c &\Leftrightarrow x \notin \bigcap_{i\in I} A_i \\ &\Leftrightarrow \exists i \in I\,(x \notin A_i) \\ &\Leftrightarrow \exists i \in I\,(x \in A_i^c) \\ &\Leftrightarrow x \in \bigcup_{i\in I} A_i^c. \end{aligned}$$

show that the sets are equal. The reader should make certain each step is clear. ∎

You may be puzzled by the inclusion of this theorem as it seems to be a simple consequence of the latter part of Theorem 1.10. However, parts (f) and (g) of Theorem 1.10 concern the

intersection or union of two sets only. This can be extended easily to the intersection or union of a finite number of sets, though even this modest extension does require separate proof (see Section 2.6). The real problem is with intersections or unions of an infinite number of sets. Though in this case the extension to infinite operations has an easy proof, it is not always the case that what is true for a finite number of operations is true for an infinite number of operations, and even when true, the proof in the infinite case may be more difficult. (For example, a finite sum of differentiable functions is differentiable, but an infinite sum of differentiable functions may not be differentiable.)

The relationships in the following theorem are simple but useful; they illustrate the dual nature of the union and intersection of families of sets.

THEOREM 1.12 If $\{A_i : i \in I\}$ is an indexed family of sets and B is any set, then

a) $\bigcap_{i\in I} A_i \subseteq A_j$ for each $j \in I$;

b) $A_j \subseteq \bigcup_{i\in I} A_i$ for each $j \in I$;

c) if $B \subseteq A_i$ for all $i \in I$, then $B \subseteq \bigcap_{i\in I} A_i$;

d) if $A_i \subseteq B$ for all $i \in I$, then $\bigcup_{i\in I} A_i \subseteq B$.

Proof. Part (a) is a case of **specialization**. Suppose that $x \in \bigcap_{i\in I} A_i$. This means that $x \in A_i$ for all $i \in I$. In particular, $x \in A_j$ for any choice of $j \in I$. We have thus shown that $\bigcap_{i\in I} A_i \subseteq A_j$ for each $j \in I$. Part (d) follows in much the same way. Suppose that $x \in \bigcup_{i\in I} A_i$. It follows that $x \in A_i$ for some $i \in I$. Since $A_i \subseteq B$, we see that $x \in B$. We have thus shown that $\bigcup_{i\in I} A_i \subseteq B$. Proofs for parts (b) and (c) are left as exercises. ■

An indexed family $\{A_i : i \in I\}$ is **pairwise disjoint** if $A_i \cap A_j = \emptyset$ whenever i and j are distinct elements of I. For example, the indexed family $\{B_i\}$ involving birthdays is pairwise disjoint, but the family $\{C_i\}$ involving multiples is not. If S is a set, then an indexed family $\{A_i : i \in I\}$ of nonempty subsets of S is a **partition** of S if it is pairwise disjoint and $S = \bigcup_{i\in I} A_i$. Partitions appear frequently in mathematics; one important way to generate partitions appears in the next section. Two simple examples are the following.

- Let $I = \{e, o\}$, let A_e be the set of even integers, and let A_o be the set of odd integers. Then $\{A_i : i \in I\}$ is a partition of $S = \mathbb{Z}$. (Technically, this fact requires proof; see the next chapter.)
- Let $I = \mathbb{R}$, let $S = \mathbb{R}^2$, and for each $i \in I$, let $A_i = \{(x, i) : x \in \mathbb{R}\}$. Each A_i is the graph of a horizontal line and the indexed family partitions the plane S.

Sometimes we want to discuss a collection of sets (that is, a set of sets) even though there is no natural index present. In this case we can use the collection itself as the index. For example, if $\mathcal{S}$ is $\{\{1, 3, 4\}, \{2, 3, 4, 6\}, \{3, 4, 5, 7\}\}$, then we have $\bigcap_{A\in\mathcal{S}} A = \{3, 4\}$ and $\bigcup_{A\in\mathcal{S}} A = \{1, 2, 3, 4, 5, 6, 7\}$.

An especially useful collection of sets is the **power set** of a set. If X is any set, the power set $\mathcal{P}(X)$ of X is the set that contains all of the subsets of X, that is, $\mathcal{P}(X) = \{A : A \subseteq X\}$. Note that each element of a power set is itself a set. If $X = \{1, 2\}$, then $\mathcal{P}(X) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$. For the record, $\mathcal{P}(\emptyset) = \{\emptyset\}$, that is, the power set of the empty set is nonempty.

Exercises 1.6.

1. Let $I = \{1, 2, 3\}$, $A_1 = \{1, 3, 4, 6, 7\}$, $A_2 = \{1, 4, 5, 7, 8, 9\}$, and $A_3 = \{2, 4, 7, 10\}$. Find $\bigcap_{i\in I} A_i$ and $\bigcup_{i\in I} A_i$.
2. Let $I = \mathbb{N}$ and for each positive integer i, define the intervals $A_i = [0, 1/i]$, $B_i = (i, i + 1)$, and $C_i = [i, \infty)$. Find each of the following.
   a) $\bigcap_{i\in I} A_i$ and $\bigcup_{i\in I} A_i$ **b)** $\bigcap_{i\in I} B_i$ and $\bigcup_{i\in I} B_i$ **c)** $\bigcap_{i\in I} C_i$ and $\bigcup_{i\in I} C_i$
3. For each $x \in [0, 1]$, let A_x be the interval $(x - 1, x + 1)$. Find $\bigcap_{x\in[0,1]} A_x$ and $\bigcup_{x\in[0,1]} A_x$.
4. Use part (a) of Theorem 1.11 (and some logic or set properties) to prove part (b) of the theorem.
5. Prove parts (b) and (c) of Theorem 1.12.
6. Let P be the set of prime numbers that are less than 20. Give an example of a partition of P that consists of four sets.
7. Let $I = [0, \infty)$ and for each $i \in I$, let $A_i = \{(x, y) : x^2 + y^2 = i^2\}$. Show that $\{A_i : i \in I\}$ is a partition of $\mathbb{R}^2$.
8. Let $\{A_i\}_{i\in I}$ be a partition of a set S and let $T \subseteq S$. Prove that the nonempty sets in the collection $\{A_i \cap T\}_{i\in I}$ form a partition of T.
9. Suppose $\mathcal{S}$ is a collection of sets and B is some other set. Show that if B is disjoint from every $A \in \mathcal{S}$ then B is disjoint from $\bigcup_{A\in\mathcal{S}} A$.
10. Write out the power set for the set $\{a, b, c\}$.

1.7 Equivalence Relations

We might arguably say that mathematics is the study of how various entities are related; in any case, the relationships between mathematical objects are a large part of what we study. You are already familiar with many such relationships: If $f(x) = y$, then x and y are related in a special way by the function f; if we say $x < y$ or $x = y$ or $x \geq y$, we are highlighting a particular relationship between the numbers x and y; the symbols $A \subseteq B$ also indicate a relationship, this time involving the sets A and B.

Certain kinds of relationships appear over and over in mathematics, and therefore deserve careful treatment and study. We use the notation $x \sim y$ to mean that x and y are related in some special way; "$\sim$" is called a **relation**. The meaning of $\sim$ changes with context—it is not a fixed relation. In some cases, of course, we can use other symbols that have come to be associated with particular relations, like "$<$", "$\subseteq$", or "$=$". A very important type of relation is given in the next definition.

DEFINITION 1.13 A relation $\sim$ on a nonempty set A is an **equivalence relation** on A if it satisfies the following three properties:

a) reflexivity: for all $a \in A$, $a \sim a$.

b) symmetry: for all $a \in A$ and all $b \in A$, if $a \sim b$, then $b \sim a$.

c) transitivity: for all $a \in A$, all $b \in A$, and all $c \in A$, if $a \sim b$ and $b \sim c$, then $a \sim c$.

Equality ($=$) is certainly an equivalence relation. It is, of course, enormously important, but it is not a very interesting example of an equivalence relation since no two distinct objects are related by equality. Less than or equal to ($\leq$) is not an equivalence relation since if fails to be symmetric.

The following examples indicate that equivalence relations can be more interesting than equality. For the first example, recall that a is a multiple of n if there exists an integer j such that $a = jn$.

EXAMPLE 1.14 Suppose $A = \mathbb{Z}$ and let n be a fixed positive integer. Let $a \sim b$ mean that $a - b$ is a multiple of n. For each integer a, it is clear that $a - a = 0$ is a multiple of n. This shows that $\sim$ is reflexive. If a and b are any integers for which $a - b$ is a multiple of n, it follows easily that $b - a$ is also a multiple of n. In other words, $a \sim b$ implies $b \sim a$ for all a and b in the set $\mathbb{Z}$, and we conclude that $\sim$ is symmetric. Finally, suppose that a, b, and c are any integers for which $a \sim b$ and $b \sim c$. This means that there exist integers j and k such that $a - b = jn$ and $b - c = kn$. Since

$$a - c = (a - b) + (b - c) = jn + kn = (j + k)n,$$

we see that $a - c$ is a multiple of n. It follows that $a \sim c$, revealing that $\sim$ is transitive. Since the relation $\sim$ is reflexive, symmetric, and transitive, it is an equivalence relation on $\mathbb{Z}$.

EXAMPLE 1.15 Let A be the set of all words. If $a \in A$ and $b \in A$, define $a \sim b$ to mean that a and b have the same number of letters. It is easy to verify that $\sim$ is an equivalence relation on A.

EXAMPLE 1.16 Let A be the set $\mathbb{R}^2$. If $a \in A$ and $b \in A$, with $a = (x_1, y_1)$ and $b = (x_2, y_2)$, define $a \sim b$ to mean that $x_1^2 + y_1^2 = x_2^2 + y_2^2$. We leave as an exercise a proof that $\sim$ is an equivalence relation on $\mathbb{R}^2$.

If $\sim$ is an equivalence relation defined on a set A and $a \in A$, let $[a] = \{x \in A : x \sim a\}$. This set is called the **equivalence class** corresponding to a. Observe that reflexivity implies that $a \in [a]$. Referring to our earlier examples, we obtain the following:

- Letting $n = 6$ in Example 1.14, we find that

$$[2] = \{6n + 2 : n \in \mathbb{Z}\} = \{\ldots, -10, -4, 2, 8, \ldots\};$$
$$[5] = \{6n + 5 : n \in \mathbb{Z}\} = \{\ldots, -7, -1, 5, 11, \ldots\}.$$

  Note that [2] and [5] are disjoint, that [2] = [8], and that [5] = [29].
- Using the relation of Example 1.15, [math] is the set consisting of all four letter words.
- Using the relation of Example 1.16, $[(1, 0)]$ is the boundary of the unit circle.

The words "the following are equivalent" followed by a list of statements such as P, Q, and R mean that each of the biconditionals $P \Leftrightarrow Q$, $P \Leftrightarrow R$, and $Q \Leftrightarrow R$ are valid. Although there are six conditional statements here, the reader should verify that it is sufficient to prove the three conditionals $P \Rightarrow Q$, $Q \Rightarrow R$, and $R \Rightarrow P$. This is the plan of action for the following proof.

THEOREM 1.17 Suppose $\sim$ is an equivalence relation on a set A. Then for any two elements a and b in A, the following are equivalent:

1) $a \sim b$;

2) $[a] \cap [b] \neq \emptyset$;

3) $[a] = [b]$.

Proof. We first prove that (1) $\Rightarrow$ (2). Suppose $a \sim b$. By definition, we find that a is an element of $[b]$. Since a is also in $[a]$, we know that $a \in [a] \cap [b]$. This shows that $[a] \cap [b] \neq \emptyset$.

We next prove that (2) $\Rightarrow$ (3). Suppose that $[a] \cap [b] \neq \emptyset$. Since $[a] \cap [b]$ is not empty, we can choose $y \in A$ such that y is in both $[a]$ and $[b]$. This means that $y \sim a$ and $y \sim b$. Using both the symmetric and transitive properties of $\sim$, it follows that $a \sim b$. We need to show that the two sets $[a]$ and $[b]$ are equal. To do so, note that (be certain you can verify each step)

$$x \in [a] \;\Rightarrow\; x \sim a \;\Rightarrow\; x \sim b \;\Rightarrow\; x \in [b];$$
$$x \in [b] \;\Rightarrow\; x \sim b \;\Rightarrow\; x \sim a \;\Rightarrow\; x \in [a].$$

The first line shows that $[a] \subseteq [b]$ and the second line shows that $[b] \subseteq [a]$. We conclude that $[a] = [b]$.

To prove that (3) $\Rightarrow$ (1), assume that $[a] = [b]$. Since $a \in [a]$ and $[a] = [b]$, we find that $a \in [b]$. It follows that $a \sim b$. This completes the proof. ∎

Suppose that $\sim$ is an equivalence relation on a set A and let $A/\sim$ denote the collection of all the corresponding equivalence classes. By the previous theorem, we see that $A/\sim$ is a partition of A. The expression "$A/\sim$" is usually pronounced "A mod twiddle."

EXAMPLE 1.18 Using the relation of Example 1.14 with $n = 6$,

$$\mathbb{Z}/\sim = \{[0], [1], [2], [3], [4], [5]\}.$$

We could also write this as

$$\mathbb{Z}/\sim = \{[12], [-5], [8], [15], [64], [29]\},$$

but most people find the first form much easier to understand. Note that these nonempty sets are pairwise disjoint and that

$$\mathbb{Z} = [0] \cup [1] \cup [2] \cup [3] \cup [4] \cup [5],$$

that is, we have a partition of $\mathbb{Z}$.

EXAMPLE 1.19 Using the relation of Example 1.15,

$$A/\sim = \{\{\text{one letter words}\}, \{\text{two letter words}\}, \{\text{three letter words}\}, \ldots\}.$$

It is easy to see that the nonempty sets in this collection form a partition of the set of all words.

EXAMPLE 1.20 Using the relation of Example 1.16, $A/\sim = \{C_r : r \geq 0\}$, where for each positive real number r, C_r is the circle of radius r centered at the origin (just the circumference) and $C_0 = \{(0, 0)\}$. Note that the resulting partition of $\mathbb{R}^2$ has a simple geometric description.

Exercises 1.7.

1. Let $A = \mathbb{R}^3$. Let $a \sim b$ mean that a and b have the same z coordinate. Show $\sim$ is an equivalence relation and describe $[a]$ geometrically.

2. Show that the relation defined in Example 1.16 is an equivalence relation.

3. Find examples (more than one if possible) of relations with the given property; indicate the set and the relation clearly.

a) The relation is reflexive and symmetric but not transitive.

b) The relation is symmetric and transitive but not reflexive.

c) The relation is reflexive and transitive but not symmetric.

4. Suppose $\sim$ is a relation on A. The following purports to prove that the reflexivity condition is unnecessary, that is, it can be derived from symmetry and transitivity:

> Suppose $a \sim b$. By symmetry, $b \sim a$. Since $a \sim b$ and $b \sim a$, by transitivity, $a \sim a$. Therefore, $\sim$ is reflexive.

What is wrong with this argument?

5. Suppose $\sim$ is a relation on A that is reflexive and has the property that for all elements a, b, and c in A, if $a \sim b$ and $a \sim c$, then $b \sim c$. Prove that $\sim$ is an equivalence relation on A.

6. Let $f\colon \mathbb{R} \to \mathbb{R}$ be a function and define a relation $\sim$ on $\mathbb{R}$ by $a \sim b$ if $f(a) = f(b)$.

a) Prove that $\sim$ is an equivalence relation on $\mathbb{R}$.

b) For $f(x) = x^2 + 2x$, find $[5]$.

c) For $f(x) = \sin x$, find $[\pi/2]$ and $[\pi/6]$.

7. Define a relation $\sim$ on $\mathbb{R}$ by $x \sim y$ if there exist integers a, b, c, and d with $|ad - bc| = 1$ such that

$$y = \frac{ax + b}{cx + d}.$$

Prove that $\sim$ is an equivalence relation on $\mathbb{R}$. Can you identify the equivalence class $[0]$?

8. Let $\mathbb{Z}^*$ be the set of all nonzero integers. Define a relation on $\mathbb{Z} \times \mathbb{Z}^*$ by $(a, b) \sim (c, d)$ if and only if $ad = bc$. Prove that $\sim$ is an equivalence relation on $\mathbb{Z} \times \mathbb{Z}^*$. (Remember to use only integers in your proof; fractions should not appear.)

9. Let S be the collection of all sequences of real numbers and define a relation on S by $\{x_n\} \sim \{y_n\}$ if and only if $\{x_n - y_n\}$ converges to 0.

a) Prove that $\sim$ is an equivalence relation on S.

b) What happens if $\sim$ is defined by $\{x_n\} \sim \{y_n\}$ if and only if $\{x_n + y_n\}$ converges to 0?

10. Let C be the collection of all continuous functions defined on $\mathbb{R}$ and define a relation on C by $f \sim g$ if and only if $f - g$ is differentiable on $\mathbb{R}$. Prove that $\sim$ is an equivalence relation on C.

2

Proofs

Proof may be what best distinguishes mathematics from other disciplines. The notion of proof even distinguishes mathematics from the sciences, which (according to most people) are logical, rigorous, and to a greater or lesser degree (depending on the discipline) based on mathematics. By using rigorous, logically correct reasoning, we aim to prove mathematical theorems—that is, to demonstrate that something is true beyond all doubt (assuming, of course, that the axioms we choose to accept are valid).

It is impossible to give a formula or algorithm for proving any and all mathematical statements, yet certain approaches or strategies appear over and over in successful proofs, so studying proof itself is worthwhile. Of course, even if the subject is proof itself, we need to prove *something*, so in this chapter we begin our study of **number theory**, that is, the properties of the integers (often, but not always, the non-negative integers). A mathematical theory such as number theory or geometry is a collection of related statements that are known or accepted to be true. The theory consists of definitions, axioms, and derived results. The derived results are usually called theorems, but other names (such as propositions) are sometimes used as well. Before proceeding with our study of some aspects of elementary number theory, we present a general discussion of definitions, axioms, and theorems.

Definitions represent a mathematical shorthand. A word or short phrase is used to represent some concept. For example, a prime number is a positive integer p such that $p > 1$ and the only positive divisors of p are p and 1. The term 'prime number' replaces the longer phrase. It is much easier to write or say 'prime number' than it is to write or say "a positive integer greater than 1 whose only positive divisors are itself and 1". The tradeoff, of course, is that you must learn what is meant by the term 'prime number'. Although the longer version is not written, it must be known. Notice that the definition of a prime number requires knowledge of positive integers and the notion of divisibility of integers. New terms are defined using previously defined terms and concepts. This process cannot go on indefinitely. In order to avoid circular definitions, some terms must remain

undefined. In geometry, points and lines are undefined terms. Other objects, such as triangles and squares, are defined in terms of points and lines. Although most people are comfortable with the concepts of points and lines, it is not possible to give them a definition in terms of simpler concepts. As we have seen, another undefined term in mathematics is the term 'set'. Attempts to define a set result in a list of synonyms (such as collection, group, or aggregate) that do not define the term. In summary, certain terms in a mathematical theory must remain undefined. New terms may be defined using the undefined terms or previously defined terms.

A mathematical theory cannot get off the ground with definitions only. It is necessary to know something about the terms and/or how they are related to each other. Basic information about the terms and their relationships is provided by axioms. An **axiom** is a statement that is assumed to be true. Most axioms are statements that are easy to believe. Turning to geometry once again, one axiom states that two distinct points determine exactly one line. This statement certainly makes sense. The important point, however, is that this statement cannot be proved. It is simply a statement that is assumed to be true. Although the axioms are generally chosen by intuition, the only real requirement for a list of axioms is that they be consistent. This means that the axioms do not lead to contradictions.

For clarity, for aesthetics, and for ease of checking for consistency, the number of undefined terms and axioms is kept to a bare minimum. A short list of undefined terms and axioms lies at the foundation of every branch of mathematics. In fact, most branches of mathematics share a common foundation. This common base involves properties of sets and properties of positive integers. However, most mathematics courses do not start at this level. A typical mathematics course generally assumes knowledge of other aspects of mathematics. For instance, the set of positive integers can be used to define the set of real numbers. However, for a course in real analysis, it is assumed that the reader already has a working knowledge of the set of real numbers, that is, it is taken for granted that a rigorous definition of the set of real numbers using more basic concepts exists. At a different level, a graduate course in number theory would assume a working knowledge of the ideas presented in Chapter 3 of this book.

A **theorem** is a true statement that follows from the axioms, definitions, and previously derived results. An example from calculus is the following theorem:

> If f is differentiable at c, then f is continuous at c.

This result follows from the definitions of continuity and differentiability, and from previous results on limits. The bulk of a mathematical theory is made up of theorems. Most of this book is made up of theorems and their corresponding proofs. Some authors refer to derived results as propositions, but the use of the word 'theorem' is much more common.

One other comment on terminology is worth mentioning. A common sequence of derived results is lemma, theorem, corollary. A **lemma** is a derived result whose primary purpose is as an aid in the proof of a theorem. The lemma is usually only referred to in the proof of the associated theorem—it is not of interest in and of itself. A lemma is often used to shorten a proof or to make a proof read more easily. If part of the proof of a theorem involves some technical details that divert the reader's attention from the main points, then this result is pulled out and called a lemma. The technical details in the proof of the theorem are replaced by a phrase such as "by the lemma."

A proof that requires a number of fairly long steps is sometimes split into parts, each of which becomes a lemma. A **corollary** is a result that follows almost immediately from a theorem. It is a simple consequence of the result recorded in the theorem. None of these labels (lemma, theorem, proposition, corollary) has an exact meaning and their use may vary from author to author. The common theme is that each represents a derived result.

Another important aspect of a mathematical theory are examples. **Examples** are objects that illustrate definitions and other concepts. Examples give the mind some specific content to ponder when thinking about a definition or a concept. For instance, after defining a prime number, it is helpful to note that 7 is prime and $6 = 2 \cdot 3$ is not. Abstract mathematics is brought to life by examples. It is possible to create all kinds of definitions, but unless there are some examples that satisfy a given definition, the definition is not very useful. Consider the following "artificial" definition:

> A positive integer n is called a **century prime** if both n and $n + 100$ are prime numbers and there are no prime numbers between n and $n + 100$.

Before proving theorems about century primes, an example of a century prime should be found. If there are no century primes, there is no need to study the concept. For the calculus theorem stated earlier in this chapter introduction, an example of a function f and a point c such that f is continuous at c but f is not differentiable at c would be interesting and enlightening. The study of and search for examples can lead to conjectures about possible theorems and/or indicate that proposed theorems are false. With every new definition and concept, you should always generate a number of specific examples.

After the axioms and definitions have been recorded, how are derived results generated? The discovery of a derived result involves hard work, intuition, and, on occasion, creative insight. The new result must then be proved. The validity of the axioms and previous results must be used to establish the validity of the new result. This is where logic enters the picture. The rules of logic make it possible to move from one true statement to another. To understand a mathematical theory, it is necessary to understand the logic that establishes the validity of derived results; this was the purpose of Chapter 1.

In this textbook, we will primarily focus on proofs involving the integers (number theory) for two reasons. First, it is a very good subject in which to learn to write proofs. The proofs in number theory are typically very clean and clear; there is little in the way of abstraction to cloud one's understanding of the essential points of an argument. Secondly, the integers have a central position in mathematics and are used extensively in other fields such as computer science. Although the great twentieth century mathematician G. H. Hardy boasted that he did number theory because there was no chance that it could be construed as applied mathematics, it has in fact become enormously useful and important in the study of computation and particularly in cryptography. Many people also find number theory intrinsically interesting, one of the most beautiful subjects in modern mathematics, and all the more interesting because of its roots in antiquity. Unless otherwise specified, then, the universe of discourse is the set of integers, $\mathbb{Z}$.

2.1 Direct Proofs

A **proof** is a sequence of statements. These statements come in two forms: **givens** and **deductions**. The following are the most important types of "givens."

Hypotheses: Usually the theorem we are trying to prove is of the form $P_1 \wedge \cdots \wedge P_n \Rightarrow Q$. The P_i's are the hypotheses of the theorem. We can *assume* that the hypotheses are true, because if one of the P_i's is false, then the implication is automatically true.

Known results: In addition to any stated hypotheses, it is always valid in a proof to write down a theorem that has already been established, or an unstated hypothesis (which is usually understood from context). In an introductory course such as this, it is sometimes difficult to decide what you can assume and what you must prove. This should become clearer as we go.

Definitions: If a term is defined by some formula, it is always legitimate in a proof to replace the term by the formula or the formula by the term.

We turn now to the most important ways a statement can appear as a consequence of (or deduction from) other statements:

Tautology: If P is a statement in a proof and Q is logically equivalent to P, we can then write down Q.

Modus Ponens: If P has occurred in a proof and $P \Rightarrow Q$ is a theorem or an earlier statement in the proof, we can write down Q. Modus ponens is used frequently, though sometimes in a disguised form; for example, most algebraic manipulations are examples of modus ponens.

Specialization: If we know "$\forall x\, P(x)$," then we can write down "$P(x_0)$" whenever x_0 is a particular value. Similarly, if "$P(x_0)$" has appeared in a proof, it is valid to continue with "$\exists x\, P(x)$". Frequently, choosing a useful special case of a general proposition is the key step in an argument.

When you read or write a proof you should always be very clear *exactly* why each statement is valid. You should always be able to identify how it follows from earlier statements.

A **direct proof** is a sequence of statements which are either givens or deductions from previous statements, and whose last statement is the conclusion to be proved. The statements generally come in three forms: premises, added assumptions, and deductions. The deductions follow from the rules of logic, primarily the tautologies discussed in the first chapter. We introduce the notion of proof with two-column logic proofs (a statement in the left column and its corresponding justification in the right column) of purely symbolic statements. The point of these proofs is to focus on the logic rather than on any particular content.

EXAMPLE 2.1 Prove $\neg S$, given $T \Rightarrow \neg Q$, R, $S \Rightarrow Q$, and $R \Leftrightarrow T$.

(1)	R	premise
(2)	$R \Leftrightarrow T$	premise
(3)	T	biconditional replacement (1) (2)
(4)	$T \Rightarrow \neg Q$	premise
(5)	$\neg Q$	modus ponens (3) (4)
(6)	$S \Rightarrow Q$	premise
(7)	$\neg Q \Rightarrow \neg S$	contraposition (6)
(8)	$\neg S$	modus ponens (5) (7)

Each step requires justification. Here the steps are either premises or known tautologies. As in this example, it is helpful to give line numbers to indicate precisely which information is being used. This format should be followed in the exercises.

Why are we doing proofs of this type? In principle, every mathematical proof can be reduced to steps like this. For better or worse (depending upon your perspective), this is seldom done in practice. However, when one is trying to sort out a difficult proof it is sometimes necessary to do a partial breakdown of the proof to see what is going on. Although proofs found in the literature are most often in words, these words reflect the sort of steps written out above. The order, logic, and transitions should all be apparent in the proof. There is room within the framework of written proofs to develop a style of your own, but certain conventions must be followed and the logic must be valid.

The next example shows how to give a direct proof of a conditional statement of the form $P \Rightarrow Q$. Since $P \Rightarrow Q$ is automatically true in the case in which P is false, all we need to prove is that Q is true when P is true. In a proof of this type, we can use P as an added premise. (You may find it helpful to look again at the list of tautologies given in Theorem 1.3.)

EXAMPLE 2.2 Prove $A \Rightarrow \neg D$, given $A \Rightarrow (B \vee C)$, $B \Rightarrow \neg A$, and $D \Rightarrow \neg C$.

(1)	A	added premise
(2)	$B \Rightarrow \neg A$	premise
(3)	$A \Rightarrow \neg B$	contraposition (2)
(4)	$\neg B$	modus ponens (1) (3)
(5)	$A \Rightarrow (B \vee C)$	premise
(6)	$B \vee C$	modus ponens (1) (5)
(7)	C	disjunctive syllogism (4) (6)
(8)	$D \Rightarrow \neg C$	premise
(9)	$C \Rightarrow \neg D$	contraposition (8)
(10)	$\neg D$	modus ponens (7) (9)
(11)	$A \Rightarrow \neg D$	conditional proof (1) (10)

Although the previous examples strip a proof to its bare essentials, they are misleading in one important regard. When given a statement to prove, you are seldom given all of the information that you need to write the proof. Determining what other premises are known and useful can be difficult and may require some creative leaps. It is this aspect of mathematics that is both exciting and frustrating.

We continue now with our list of givens that appear (or need to be determined) in proofs. Many theorems in mathematics involve variables. For example, the familiar calculus theorem that says 'If f is differentiable at c, then f is continuous at c' involves two variables, a function f and a point c.

Variables: The proper use of variables in an argument is critical. Their improper use results in unclear and even incorrect arguments. Every variable in a proof has a quantifier associated with it, so there are two types of variables: those that are universally quantified and those that are

existentially quantified. We may fail to mention explicitly how a variable is quantified when this information is clear from the context, but every variable has an associated quantifier.

A universally quantified variable is introduced when trying to prove a statement of the form $\forall x(P(x) \Rightarrow Q(x))$. The language typically employed is "Suppose x satisfies $P(x)$", "Assume $P(x)$", or "Let $P(x)$". The variable x represents a fixed but arbitrary element chosen from some universe. It is important to be certain to not use any special properties of x that do not apply to the entire universe. For example, if x represents a positive real number, you cannot assume that $x^2 \geq x$ in the proof because this statement is not true for all positive real numbers.

When we introduce an existentially quantified variable, it is usually defined in terms of other things that have been introduced earlier in the argument. In other words, it depends on previously mentioned quantities. Note how the integer k appears in the following familiar definition; it depends on the integer n.

DEFINITION 2.3 An integer n is **even** if and only if there is an integer k such that $n = 2k$. An integer n is **odd** if and only if there is an integer k such that $n = 2k + 1$.

We assume that every integer is either even or odd. Although this seems like an obvious statement, it does require proof. We postpone the proof to a later section (see, for instance, the Division Algorithm in Section 2.7).

EXAMPLE 2.4 If n is an even integer, then n^2 is an even integer.

Proof. Suppose that n is an even integer (n is a universally quantified variable which appears in the statement we are trying to prove). By definition, there exists an integer k such that $n = 2k$ (k is existentially quantified, defined in terms of n, which appears previously). It follows easily that $n^2 = 4k^2 = 2(2k^2)$. Letting $j = 2k^2$ (j is existentially quantified, defined in terms of k), we find that j is an integer and that $n^2 = 2j$. Therefore, the integer n^2 is even (by definition). ■

The parenthetical remarks are not part of the actual proof; they are included at this stage to help explain what is going on. We will soon be omitting such remarks. Note how both directions of the biconditional definition have been used in the proof; one direction to obtain the integer k given a value for n and the other to verify that n^2 is even. By the way, what is the contrapositive of the statement proved in this example? (You might find this fact useful in the exercises.)

The next example is not presented in the standard "if ..., then ..." form; the reader should write the theorem in this form before proceeding to read the proof.

EXAMPLE 2.5 The sum of two odd integers is even.

Proof. Suppose that m and n are odd integers (introducing two universally quantified variables to stand for the quantities implicitly mentioned in the statement). By definition, there exist integers j and k such that $m = 2j + 1$ and $n = 2k + 1$ (introducing existentially quantified variables, defined in terms of quantities already mentioned). We then have $m + n = (2j + 1) + (2k + 1) = 2(j + k + 1)$. Letting $i = j + k + 1$ (existentially quantified), we find that i is an integer and that $m + n = 2i$. It follows that $m + n$ is even (by definition). ■

Exercises 2.1.

For problems 1–5, give a two-column logic proof. Use the style of Examples 2.1 and 2.2.

1. Prove $\neg T$, given $R \Rightarrow \neg T$, S, and $S \Rightarrow R$.

2. Prove Q, given T, R, and $R \Rightarrow (\neg T \vee Q)$.

3. Prove $\neg N$, given $R \Leftrightarrow \neg S$, R, $\neg S \Rightarrow Q$, and $N \Rightarrow \neg Q$.

4. Prove $R \Rightarrow \neg P$, given $P \Rightarrow Q$, and $R \Rightarrow \neg Q$.

5. Prove $D \Rightarrow C$, given $A \Rightarrow (B \Rightarrow C)$, $\neg D \vee A$, and B.

For problems 6–9, write proofs for the given statements, inserting parenthetic remarks to explain the rationale behind each step (as in Examples 2.4 and 2.5).

6. The sum of two even numbers is even.

7. The sum of an even number and an odd number is odd.

8. The product of two odd numbers is odd (and thus the square of an odd number is odd).

9. The product of an even number and any other number is even.

There are several options for proofs of the statements in problems 10–11. Try to find proofs that take advantage of results already proved in this section.

10. Prove that x is odd if and only if $|x|$ is odd.

11. Suppose that x and y are integers and that $x^2 + y^2$ is even. Prove that $x + y$ is even.

2.2 Divisibility

We begin this section with a simple definition.

DEFINITION 2.6 Let a and n be integers with $n \neq 0$. Then n **divides** a, denoted $n|a$, if and only if there exists an integer m such that $a = nm$. When $n|a$, we say n is a **divisor** of a and a is a **multiple** of n. (Whenever the notation $n|a$ appears, it is implicitly assumed that $n \neq 0$.)

The concept of an integer dividing another integer (that is, going in evenly) is familiar to elementary school children. For example, the multiplication fact $7 \cdot 12 = 84$ shows that 7 divides 84, that is, $7|84$. The same equation shows that $12|84$. We can also say that 84 is a multiple of both 7 and 12. A word of caution: The symbol $n|a$ is *not* a fraction, but a formula. It means that there is a relationship between the two numbers which is either true or false (5 and 20 have this relationship, 5 and 21 do not). While we are studying number theory we will have little occasion to mention rational numbers—in fact, we avoid them except for a few exercises. There are several reasons for this. One is practical: a given fraction has more than one representation (for example $4/12 = 5/15$). It is also possible that a number that doesn't look like an integer is, in fact, an integer (for example $51/17$). These ambiguities can be a real source of confusion. A second reason is theoretical: the integers can be used to define other number systems (such as the rational numbers), so the integers should be studied as a self-contained subject before dealing with these other systems. A third reason is aesthetic: number theory is the study of the *integers*; it is somehow more elegant and satisfying to provide proofs that use only number theoretic results and techniques. (We do not mean to overstate this. Mathematics is a single discipline, and some of the most beautiful and elegant proofs bring apparently unrelated parts of mathematics together to

solve a problem. These surprising connections between different parts of mathematics enhance the whole mathematical enterprise.)

In spite of their simplicity, the following results will be very useful.

THEOREM 2.7

a) If $n \neq 0$, then $n|0$ and $n|n$.

b) $1|n$ for any integer n.

c) If $n|a$, then $n|ab$ for any integer b.

d) If $n|a$ and $a|b$, then $n|b$.

e) If $m|a$ and $n|b$, then $mn|ab$.

f) If $n|a$ and $n|b$, then $n|(ax + by)$ for any $x, y \in \mathbb{Z}$.

Proof. The equations $0 = n \cdot 0$ and $n = n \cdot 1$ prove part (a), while the equation $n = 1 \cdot n$ establishes part (b). To prove part (c), suppose that $n|a$ and let b be any integer. By definition, there exists an integer k such that $a = nk$. It follows that $ab = n(bk)$, revealing that $n|ab$. Turning to part (f), suppose that n, a, and b are integers such that $n|a$ and $n|b$. By definition, there exist integers i and j such that $a = ni$ and $b = nj$. If x and y are any integers, then

$$ax + by = (ni)x + (nj)y = n(ix + jy).$$

Since $ix + jy$ is an integer, this equation shows that $n|(ax + by)$. This proves part (f). Proofs for parts (d) and (e) will be left as exercises. ∎

THEOREM 2.8 If $a|b$ and $b \neq 0$, then $|a| \leq |b|$.

Proof. Suppose that a and b are integers such that $a|b$ and $b \neq 0$. Since $a|b$, there exists an integer c such that $b = ac$. Note that $c \neq 0$ since $b \neq 0$. Since $c \neq 0$ and c is an integer, we know that $|c| \geq 1$. It follows that $|b| = |ac| = |a| \cdot |c| \geq |a|$. ∎

COROLLARY 2.9 If a and b are positive integers such that $a|b$ and $b|a$, then $a = b$.

Proof. The proof will be left as an exercise. ∎

DEFINITION 2.10 An integer $p > 0$ is called **prime** if it has exactly two positive divisors, namely, 1 and p. If $a > 0$ has more than two positive divisors, we say it is **composite**.

It is important to remember that 1 is neither prime nor composite. A prime has exactly two positive divisors, but 1 has only one (1 itself). Observe that if $a > 1$ is composite, then there exist integers n and m such that $a = nm$, $1 < n < a$, and $1 < m < a$ (just let n be any positive divisor of a other than 1 or a).

There are many theorems about primes that are truly amazing and some of these are amazingly difficult to prove. There are also many questions involving primes which, though they are easy to state, have resisted all attempts at proof. A simple question of this type concerns so-called **twin primes**, pairs of primes of the form p and $p + 2$. For example, 5 and 7 are twin primes as are 59

and 61. No one knows whether there are an infinite number of such pairs, though they occur as far out as anyone has checked (by computer). There also are some arguments that make it appear likely that the number of twin primes is infinite. But the twin primes conjecture (as well as several other related questions) remains an unsolved mystery.

Exercises 2.2.

1. For the given integers n and a, show $n|a$ by finding an integer m with $a = nm$.

a) $7|119$ **b)** $5|-65$ **c)** $-3|51$

d) $-9|-252$ **e)** $-1|12$ **f)** $6|0$

2. Find, with proof, all integers n such that $n|(2n+3)$.

3. Prove parts (d) and (e) of Theorem 2.7.

4. Let $n > 1$ be an integer. Suppose that there exists an integer a such that $n|(5a+3)$ and $n|(8a+11)$. Prove that $n = 31$. Try to find a suitable value for a.

5. Suppose that $m \neq 0$. Prove $nm|am$ if and only if $n|a$. Give careful details for each part.

6. Prove that if $a|b$, then $|a| \Big| |b|$. Is the converse true?

7. Prove Corollary 2.9.

8. For each positive integer n, let (n) denote the set of all multiples of n, that is, $(n) = \{an : a \in \mathbb{Z}\}$.

a) List several of the elements of (3), (5), and (10).

b) Prove that $(n) = \{a \in \mathbb{Z} : n|a\}$.

c) Suppose that a and b are elements of (n) and that x and y are any integers. Prove that $ax + by$ belongs to the set (n).

d) Suppose that m and n are positive integers. Prove that $(n) \subseteq (m)$ if and only if $m|n$.

9. Suppose that a and b are positive integers such that ab divides $a + b$. Prove that $a = b$, then prove that a is either 1 or 2.

10. Define a relation on $\mathbb{Z}$ by $a \sim b$ if $a|b$. What properties of an equivalence relation does $\sim$ satisfy? Does the list of valid properties change if $\mathbb{Z}$ is replaced with $\mathbb{Z}^+$?

11. Suppose we call primes of the form p, $p+2$, $p+4$ triplet primes. Present a convincing argument to show that 3, 5, 7 is the only set of triplet primes. What can be said about primes of the form p, $p+2$, $p+6$?

2.3 Existence proofs

Many interesting and important theorems have the form $\exists x\, P(x)$, that is, that there exists an object x satisfying some formula P. In such **existence proofs**, try to be as specific as possible. The most satisfying and useful existence proofs often give a concrete example or describe explicitly how to produce the object x.

- To prove the statement, *there is a prime number p such that $p+2$ and $p+6$ are also prime numbers*, note that $p = 5$ works because $5+2 = 7$ and $5+6 = 11$ are also primes.
- Suppose that U is the collection of all differentiable functions defined on $\mathbb{R}$. To prove the statement, *there is a function f such that $f' = 2f$*, note that $f(x) = e^{2x}$ works (as does any constant multiple of e^{2x}).

In the first example, 5 is not the only number that works (for example, 11 works as well). In fact, it is a famous unsolved problem whether there are infinitely many primes that work. Proving that there are infinitely many primes with this property would be a more interesting result (and would give the author of the proof some notoriety), but the point remains: when doing an existence proof, be as concrete as possible. In each of the above examples, an explicit object satisfying the desired properties is produced.

A slight variation on the existence proof is the *counterexample*. Suppose you look at a sentence of the form $\forall x P(x)$ and you come to the conclusion that it is false. To demonstrate this, you need to prove $\neg\forall x P(x)$, which by one of De Morgan's Laws is equivalent to $\exists x \neg P(x)$. A specific x satisfying $\neg P(x)$ is called a counterexample to the assertion $\forall x P(x)$.

- To disprove the sentence *for every integer n, the integer $5n^2+1$ is not a perfect square*, we need to find an integer n such that $5n^2+1$ is a perfect square. Note that 4 provides a counterexample to the sentence, that is, 4 is an integer but $5(4)^2 + 1 = 81$ is a perfect square.
- Suppose U is the collection of all continuous functions defined on $\mathbb{R}$. To disprove the sentence *for every function f, if f is continuous at 0 then it is differentiable at 0*, note that $f(x) = |x|$ is a counterexample.

Once again, the most satisfying way to prove something false is to come up with a specific counterexample. Note well that it is never sufficient simply to find an error in the proof of some sentence to conclude that it is false—it is easy to come up with erroneous proofs of correct facts. If you have trouble proving a statement of the form $\forall x\, P(x)$, try looking at some particular cases of the result. You may find a counterexample, or you may get a hint about why the statement really is true.

There are occasions when it is impossible, or very difficult, to find a specific example. An existence proof sometimes can be constructed by indirect means, or by using other existence results.

EXAMPLE 2.11 To show *there is a real number x such that $x^7 + 3x - 2 = 0$*, let f be the function defined by $f(x) = x^7 + 3x - 2$. Then f is a continuous function (since it is a polynomial) such that $f(0) = -2$ and $f(1) = 2$. By the Intermediate Value Theorem, there is a number c in the interval $(0, 1)$ for which $f(c) = 0$.

In this example, notice that a formula or method to actually determine the point c is not given. There are various ways to approximate the point c, but the actual existence of this point depends on an axiom concerning the set of real numbers. However, even though we do not have a method for determining the exact value of c, we are guaranteed that such a point exists.

All calculus books include a proof of the Mean Value Theorem. However, if you trace the proof, you will find that the Mean Value Theorem (which is an existence result), is proved by referring to Rolle's Theorem (another existence result), which is proved by referring to the Extreme Value Theorem (yet a third existence result, sometimes called the Maximum Value Theorem), which is proved "indirectly," (if it is proved at all; you may need to consult a text in real analysis) without ever exhibiting the object that is claimed to exist. At no point are we given a formula for the quantity we seek, and the result is perhaps not as satisfying as we would like. In general, then, try

to be specific when doing an existence proof, but if you cannot, it may still be possible to show that an example exists using some other existence result or another technique of proof.

Trying to prove a statement of the form $\forall x \exists y P(x, y)$ is rather like trying to do many existence arguments at the same time. For any given value of x, we would like to construct or describe a value for y that makes $P(x, y)$ true.

- Suppose we want to prove that there is no largest integer. This statement can be expressed as $\forall n \exists m(n < m)$. To prove this well-known fact, suppose $n \in \mathbb{Z}$ is given and let $m = n + 1$. Then m is an integer and $n < n + 1 = m$.
- We claim that there are arbitrarily long gaps in the sequence of prime numbers. In other words, we are asserting that for every positive integer n there is a positive integer m such that $m + 1$, $m + 2$, ..., $m + n$ are all composite. Given a positive integer n, let

$$m = (n + 1)! + 1 = (n + 1)n(n - 1) \cdots 3 \cdot 2 \cdot 1 + 1.$$

  We note in passing that $m \geq 3$. If $1 \leq k \leq n$, then $m + k = (n + 1)! + (k + 1)$. Since both $(n + 1)!$ and $k + 1$ are divisible by $k + 1$, it follows that $m + k$ is divisible by $k + 1$. Since $1 < k + 1 < k + m$, the number $m + k$ is composite. We have thus constructed n consecutive composite numbers. The size of the numbers that appear here is rather difficult to imagine. For instance, this result shows that there exist 10 billion consecutive composite numbers. However, the universe itself is not a large enough canvas on which to actually write out all of the digits in the number 10 billion factorial.

Exercises 2.3.

As you work through these exercises, don't simply find one example and move on to the next problem; try to find other examples, look for patterns, and make note of your thought process.

1. Show that there is a prime number p such that $p + 4$ and $p + 6$ are also prime numbers.

2. Show that there is a two-digit prime number p such that $p + 8$ is a prime number and there are no prime numbers between p and $p + 8$.

3. Show that there are prime numbers p and q such that $p + q = 128$. (This is a case of the famous **Goldbach Conjecture**, which says that every even integer $n \geq 6$ can be written as the sum of two odd primes. It seems highly probable from work with computers that the Goldbach Conjecture is true, but no one has discovered a proof.)

4. Show that there is a nonzero differentiable function f such that $xf'(x) = 5f(x)$.

5. Show that there is a positive real number x such that $x = 2 \sin x$.

6. Show that every odd integer is the sum of two consecutive integers.

7. Show that every odd integer is the difference between two consecutive perfect squares.

8. Show that for each positive integer $n > 1$ there exists a positive integer q such that $n^2 < 4q < (n+1)^2$.

9. Find counterexamples for each of the following statements; use $\mathbb{N}$ as the universe of discourse.

a) If $12|n^2$, then $12|n$.

b) If $n|ab$, then $n|a$ or $n|b$.

c) If $n^2|m^3$, then $n|m$.

d) $n^2 - n + 11$ is a prime number for every n. (Find the smallest counterexample.)

e) $7n^2 + 4$ is not a perfect square for every n.

10. Suppose U is the collection of all continuous functions defined on $\mathbb{R}$. Disprove the following sentence: for every $f \in U$, either f is differentiable at 4 or f is differentiable at 7.

11. Find a positive integer $n > 25$ such that $(n+1)^2 - n^2$ is a perfect square.

12. Find distinct positive integers a, b, and c such that $a^2 - ac + c^2 = b^2$.

2.4 Mathematical Induction

The set $\mathbb{Z}$ of integers and its properties are at the root of all mathematical disciplines. The algebraic and order properties of the integers, whether used formally or informally, are the properties that are most relevant when doing mathematics. However, the set of integers has another property that is independent of its algebraic and order properties. This additional property of the integers is quite important and is the topic of discussion for the next few sections.

Statements of the form, "for each positive integer n, something is true," occur in all branches of mathematics. Three simple examples are

1. For each positive integer n, the number $92n^2 + 1$ is not a perfect square.

2. For each positive integer n, $1^2 + 2^2 + 3^2 + \cdots + n^2 = \dfrac{n(n+1)(2n+1)}{6}$.

3. For each positive integer n, $\big(\cos x + i \sin x\big)^n = \cos(nx) + i \sin(nx)$.

To prove that statements such as these are false, it is only necessary to find one positive integer n for which the statement is false. For instance, statement (1) is false; it is possible (but requires some patience) to find a positive integer n for which $92n^2 + 1$ is a perfect square. However, it is not possible to prove such statements are true by showing that they are true for several values of n (or even a whole lot of values of n); the formulas or statements must somehow be verified for every positive integer n. Since it is not possible to actually prove individually an infinite number of statements, some other method of proof is needed. The Principle of Mathematical Induction is a useful tool for proving some statements of this type. This important property, which we accept as an axiom, is stated below.

Principle of Mathematical Induction: If S is a set of positive integers that contains 1 and satisfies the condition "if $k \in S$, then $k + 1 \in S$," then $S = \mathbb{Z}^+$.

The Principle of Mathematical Induction can be compared to a chain reaction. If we know that each event (the quantifier $\forall$ is implicitly used here) will set off the next (the condition in quotes) and if the first event occurs ($1 \in S$), then the entire chain reaction will occur. Perhaps you have seen one of those amazing domino exhibits where thousands of dominoes fall over in interesting patterns. The dominoes must be set up in such a way that each domino knocks over the next, and someone must begin the process by pushing over the first domino.

Given a statement of the form "for each positive integer n, something is true," let S be the set of all positive integers n for which the statement is true. In order to prove that the statement is true for all positive integers, we must show that $S = \mathbb{Z}^+$. By the Principle of Mathematical Induction, it is sufficient to prove that S contains 1 and satisfies the condition "if $k \in S$, then $k + 1 \in S$." In almost every situation of this type, it is easy to prove that $1 \in S$. However, a proof that $k + 1 \in S$ under the assumption that $k \in S$ requires more effort. (Make careful note of what

is assumed and what is to be proved. We assume that the statement is true for some fixed value k and then try to use this fact to prove that it is true for the next value $k+1$.) Two examples of such proofs are given below. We provide two proofs of the first result; one in the formal style indicated by the statement of the Principle of Mathematical Induction and a second in the more common informal style. You may use whichever style of proof you prefer, but it may be a good idea to use the longer form until you become proficient with this type of proof.

THEOREM 2.12 The formula

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

is valid for each positive integer n.

Proof. (first version) We will use the Principle of Mathematical Induction. Let S be the set of all positive integers n such that

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

When $n = 1$, the formula reduces to $1^2 = (1 \cdot 2 \cdot 3)/6$. Since this statement is true, it follows that $1 \in S$. Suppose that $k \in S$ for some positive integer k. This means that

$$1^2 + 2^2 + 3^2 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{6}.$$

We want to show that this assumption implies that $k+1 \in S$, that is,

$$1^2 + 2^2 + 3^2 + \cdots + (k+1)^2 = \frac{(k+1)(k+2)(2(k+1)+1)}{6}.$$

To show that the two expressions are equal, we begin with one side of the equation and manipulate it using algebra and known results to obtain the other side. In this case, we have

$$\begin{aligned} 1^2 + 2^2 + 3^2 + \cdots + k^2 + (k+1)^2 &= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \\ &= \frac{k+1}{6}\left(2k^2 + k + 6k + 6\right) \\ &= \frac{(k+1)(k+2)(2k+3)}{6}, \end{aligned}$$

which indicates that $k+1 \in S$. We have thus shown that "if $k \in S$, then $k+1 \in S$." By the Principle of Mathematical Induction, $S = \mathbb{Z}^+$. Hence,

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

for all positive integers n. This completes the proof.

(second version) The formula is easily verified for $n = 1$. Suppose that the formula is valid for some positive integer k. Then

$$\begin{aligned} 1^2 + 2^2 + 3^2 + \cdots + k^2 + (k+1)^2 &= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \\ &= \frac{k+1}{6}\big(2k^2 + k + 6k + 6\big) \\ &= \frac{(k+1)(k+2)(2k+3)}{6}, \end{aligned}$$

showing that the formula is valid for $k + 1$ as well. The result now follows by the Principle of Mathematical Induction. ■

THEOREM 2.13 For each positive integer n, the integer $9^n - 8n - 1$ is divisible by 64.

Proof. We will use the Principle of Mathematical Induction. Since 0 is divisible by 64, the statement is valid when $n = 1$. Suppose that $9^k - 8k - 1$ is divisible by 64 for some positive integer k. By definition, there exists an integer j such that $64j = 9^k - 8k - 1$. We then have

$$\begin{aligned} 9^{k+1} - 8(k+1) - 1 &= 9(9^k - 1) - 8k \\ &= 9(64j + 8k) - 8k \\ &= 64(9j + k). \end{aligned}$$

Since $9j + k$ is an integer, we find that $9^{k+1} - 8(k + 1) - 1$ is divisible by 64. By the Principle of Mathematical Induction, for each positive integer n, the integer $9^n - 8n - 1$ is divisible by 64. ■

It is not necessary that 1 be the starting point in the Principle of Mathematical Induction; any integer a will do. If S is a set of integers that contains a and satisfies the condition "if $k \geq a$ and $k \in S$, then $k + 1 \in S$," then $S = \{n \in \mathbb{Z} : n \geq a\}$. The fact that this statement is equivalent to the Principle of Mathematical Induction follows by making a simple change of variables; the details will be left to the reader. There are situations for which this slight modification to the Principle of Mathematical Induction is helpful. An example appears below.

THEOREM 2.14 For each positive integer $n \geq 8$, the inequality $n < (1.3)^n$ is valid.

Proof. Using a calculator, it is easy to verify that $8 < (1.3)^8$. Suppose that $k < (1.3)^k$ for some positive integer $k \geq 8$. Then

$$k + 1 < k + 0.3k = 1.3k < 1.3(1.3)^k = (1.3)^{k+1},$$

so the inequality is valid for $k+1$ as well. By the Principle of Mathematical Induction, the inequality $n < (1.3)^n$ is valid for all $n \geq 8$. ■

It will be helpful to make several comments concerning terminology. The hypothesis "if $k \in S$" or "suppose the result is valid when $n = k$" is known as the **induction hypothesis**. The part of the argument that uses this assumption (remember it is an assumption that something is true for this one particular value of k) to prove that $k + 1 \in S$ or that the result holds for $n = k + 1$ is

called the **inductive step**. A proof that uses the Principle of Mathematical Induction is called a **proof by induction**. In those cases in which the inductive step is easy, the proof is usually left out. A phrase such as "the result follows by induction" means that the induction argument is easy and is left to the reader.

The Principle of Mathematical Induction requires the validation of two hypotheses. The first involves checking that the result is valid for some starting value of n. Even though this step is usually very easy, it is still necessary. Suppose that someone claims that $n^2 + 7n - 3$ is an even number for each positive integer n. If $k^2 + 7k - 3$ is even for some positive integer k, then

$$(k+1)^2 + 7(k+1) - 3 = (k^2 + 7k - 3) + 2(k+4)$$

is the sum of two even numbers and thus an even number. This establishes the condition "if $k \in S$, then $k+1 \in S$," where S is the set of all positive integers n for which n^2+7n-3 is even. However, the result is false for $n = 1$ (and also false for every other positive integer n). It is generally a good idea to check a formula for several values of n before trying to find a general proof. Not only does this give you more evidence of the validity of the statement, it can sometimes give you a good idea of the steps that are needed for a proof of the induction hypothesis.

As a final comment, it is important to realize that not every statement that involves positive integers requires the Principle of Mathematical Induction in its proof. There may be better or easier methods to prove the result; the following result provides one simple example.

EXAMPLE 2.15 For each positive integer $n > 1$, the inequality $n^3 + 1 > n^2 + 2n$ is valid.

Proof. Since $n > 1$, we know that

$$n^2 > 3 \geq 1 + \frac{n}{n-1}.$$

Multiplying this inequality by the positive number $n - 1$ yields

$$n^2(n-1) > (n-1) + n \quad \text{or} \quad n^3 - n^2 > 2n - 1.$$

Adding $n^2 + 1$ to both sides gives the desired result. ■

Exercises 2.4.

1. Prove that $1 + 3 + 5 + \cdots + (2n-1) = n^2$ for each positive integer n.

2. Prove that $1^3 + 2^3 + 3^3 + \cdots + n^3 = \dfrac{n^2(n+1)^2}{4}$ for each positive integer n.

3. Prove that $\dfrac{1}{1\cdot 2} + \dfrac{1}{2\cdot 3} + \dfrac{1}{3\cdot 4} + \cdots + \dfrac{1}{n\cdot(n+1)} = \dfrac{n}{n+1}$ for each positive integer n.

4. Find and prove a formula for $1^3 + 3^3 + 5^3 + \cdots + (2n-1)^3$.

5. Prove that for each positive integer n, the integer $3^{2n+1} + 2^{n+2}$ is divisible by 7.

6. Prove that for each positive integer n, the inequality $\dfrac{1}{1!} + \dfrac{1}{2!} + \dfrac{1}{3!} + \cdots + \dfrac{1}{n!} \leq 2 - \dfrac{1}{n}$ is valid.

7. Let $a_1 = 1$ and $a_{n+1} = 3 - (1/a_n)$ for each integer $n \geq 1$. Prove that $1 \leq a_n \leq 3$ for each positive integer n.

8. Prove that the product of any four consecutive positive integers is one less than a perfect square.

9. Prove that $n + 1 < 2^{n-1}$ for all integers $n > 3$.

10. Let a and b be real numbers. Prove that

$$a^n - b^n = (a - b)\Big(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + b^{n-1}\Big)$$

for each positive integer $n > 1$.

11. Suppose that $a_1 = -1/3$ and let $a_{n+1} = (1 + 2a_n)/3$ for each $n > 1$. Find and prove a simple formula for a_n.

12. Suppose that $x > -1$ and that $x \neq 0$. Prove that $(1 + x)^n > 1 + nx$ for each positive integer $n \geq 2$. This result is known as **Bernoulli's Inequality**.

13. Let A be a set with n elements, where n is a positive integer. Prove that $\mathcal{P}(A)$ has 2^n elements.

14. A polygon in the plane is convex if the segment connecting any two vertices of the polygon is contained entirely inside the polygon. (Since you are most familiar with convex polygons, you might find it helpful to draw a polygon that is not convex.) Prove that the sum of the n angles of a convex polygon with n vertices is $(n - 2)\pi$.

2.5 Two Important Results

In this section, we present two well-known and useful results. Although the results extend beyond the realm of the integers, the proofs of each of them involve mathematical induction. The results are included here because they provide practice in reading more elaborate induction proofs and they present some important mathematical ideas.

The first goal is to state and prove the Binomial Theorem, the familiar theorem that gives a formula for expanding $(a + b)^n$. We begin with some notation. For each positive integer n, define $n!$ (read "n factorial") by $n! = n(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1$. Even for small values of n, factorials can be very large; for example, $70! > 10^{100}$. For sound mathematical reasons (see Exercise 12 below), $0!$ is defined to be 1. For a positive integer n and a nonnegative integer k such that $0 \leq k \leq n$, define the **binomial coefficient** $\binom{n}{k}$ by

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

It is easy to verify that $\binom{n}{k} = \binom{n}{n-k}$. To illustrate binomial coefficients, note that

$$\binom{3}{0} = \frac{3!}{0!\,3!} = 1; \qquad \binom{3}{1} = \frac{3!}{1!\,2!} = 3; \qquad \binom{3}{2} = \frac{3!}{2!\,1!} = 3; \qquad \binom{3}{3} = \frac{3!}{3!\,0!} = 1.$$

The reader should recognize these numbers as the coefficients that appear in the expansion of $(a + b)^3$:

$$(a + b)^3 = a^3 + 3a^2b + 3ab^2 + b^3.$$

This is no coincidence and provides one example of a general formula for $(a + b)^n$, where n is a positive integer. Our next goal is to derive this formula, which is known as the Binomial Theorem. We begin with a simple lemma.

LEMMA 2.16 If n and k are positive integers with $1 \le k \le n$, then

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

Proof. Using the definition of binomial coefficients,

$$\begin{aligned}\binom{n}{k} + \binom{n}{k-1} &= \frac{n!}{k!\,(n-k)!} + \frac{n!}{(k-1)!\,(n-k+1)!} \\ &= \frac{(n-k+1)n!}{k!\,(n-k+1)!} + \frac{kn!}{k!\,(n-k+1)!} \\ &= \frac{(n+1)!}{k!\,(n+1-k)!} = \binom{n+1}{k}.\end{aligned}$$

This completes the proof. ■

The symbol $\binom{n}{k}$ is often read as "n choose k." It can be interpreted as the number of ways to choose k objects from a group of n objects. For example, suppose there are ten kids in a classroom and the teacher needs to pick four of them to take an extra exam. There are

$$\binom{10}{4} = \frac{10!}{4!\,6!} = \frac{10 \cdot 9 \cdot 8 \cdot 7}{4 \cdot 3 \cdot 2 \cdot 1} = 10 \cdot 3 \cdot 7 = 210$$

ways for the teacher to make the selection. Note that there are the same number of ways for her to choose six kids to not take the exam: $\binom{10}{6} = \binom{10}{4}$. The reader should be able to interpret the equation given in the lemma using this idea of n choose k.

THEOREM 2.17 Binomial Theorem If a and b are real numbers, then

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

for each positive integer n.

Proof. We first use mathematical induction to prove the following special case of the binomial theorem: if x is a real number, then

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k$$

for each positive integer n. When $n = 1$, the formula reads

$$1 + x = \binom{1}{0} x^0 + \binom{1}{1} x^1 = 1 + x,$$

which is clearly a true statement. Suppose that the formula holds for some positive integer n. Using the previous lemma, we find that

$$\begin{aligned}(1+x)^{n+1} &= (1+x)(1+x)^n \\ &= (1+x)\sum_{k=0}^{n}\binom{n}{k}x^k \\ &= \sum_{k=0}^{n}\binom{n}{k}x^k + \sum_{k=0}^{n}\binom{n}{k}x^{k+1} \\ &= 1 + \sum_{k=1}^{n}\binom{n}{k}x^k + \sum_{k=1}^{n}\binom{n}{k-1}x^k + x^{n+1} \\ &= \binom{n+1}{0} + \sum_{k=1}^{n}\binom{n+1}{k}x^k + \binom{n+1}{n+1}x^{n+1} \\ &= \sum_{k=0}^{n+1}\binom{n+1}{k}x^k.\end{aligned}$$

Hence, the formula is valid for $n+1$ as well. The result now follows by the Principle of Mathematical Induction.

We now consider the general case. If $b = 0$, then the only nonzero term in the sum occurs when $k = n$; this yields the equation $a^n = a^n$. Assume that $b \neq 0$. Using the special case proved above, we obtain

$$(a+b)^n = b^n\left(1+\frac{a}{b}\right)^n = b^n\sum_{k=0}^{n}\binom{n}{k}\left(\frac{a}{b}\right)^k = \sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k}.$$

This completes the proof. ∎

COROLLARY 2.18 For each positive integer n, $\displaystyle\sum_{k=0}^{n}\binom{n}{k} = 2^n$ and $\displaystyle\sum_{k=0}^{n}(-1)^k\binom{n}{k} = 0$.

Proof. The proof will be left as an exercise. ∎

As in the proof of the Binomial Theorem, it is common in mathematics to prove a special case of a theorem first, then to show how the general case reduces to the special case. The reader familiar with Pascal's Triangle should recognize that the numbers that appear in the rows of this triangle are binomial coefficients and that the "rule" for generating one row from the previous row is simply Lemma 2.16. By looking at the rows of Pascal's Triangle, it is easy to verify Corollary 2.18 for small values of n.

We next consider an important and useful inequality that concerns the relationship between the arithmetic mean and the geometric mean of a set of real numbers. Let n be a positive integer and let $a_1, a_2, \ldots, a_n$ be nonnegative real numbers. Then the **arithmetic mean** and the **geometric mean** of this set of numbers are defined by

$$\frac{a_1 + a_2 + \cdots + a_n}{n} \quad \text{and} \quad (a_1 a_2 \cdots a_n)^{1/n},$$

respectively. For the record, the arithmetic mean of a set of numbers, which is sometimes called the average of the numbers, can be defined even if the numbers are not nonnegative. The arithmetic

mean of two numbers represents the number that is halfway between the two numbers. For two positive real numbers x and y, their geometric mean $\sqrt{xy}$ represents the length of the side of a square whose area is the same as the area of a rectangle with sides of lengths x and y. It is easy to verify that the geometric mean of two positive numbers is less than or equal to the arithmetic mean of the numbers. It turns out that this result is true for every set of n nonnegative numbers, but a proof for values of $n > 2$ is more difficult. As with the previous result, the proof presented here begins with a lemma.

LEMMA 2.19 Let $n \geq 2$ be an integer. Suppose that $b_1, b_2, \ldots, b_n$ are positive real numbers that are not all equal. If $b_1 b_2 \cdots b_n = 1$, then $b_1 + b_2 + \cdots + b_n > n$.

Proof. We will use the Principle of Mathematical Induction. For the case $n = 2$, we know that $b_1 \neq b_2$ and $b_1 b_2 = 1$. It follows that

$$0 < \left(\sqrt{b_1} - \sqrt{b_2}\right)^2 = b_1 - 2\sqrt{b_1 b_2} + b_2 = b_1 - 2 + b_2 \quad \text{and thus} \quad b_1 + b_2 > 2,$$

showing that the result is true when $n = 2$. Now suppose the result is valid for some positive integer $p \geq 2$. Let $b_1, b_2, \ldots, b_p, b_{p+1}$ be positive real numbers that are not all equal and satisfy $b_1 b_2 \cdots b_p b_{p+1} = 1$. Without loss of generality, we may assume that the numbers are in increasing order, that is, $b_1 \leq b_2 \leq \cdots \leq b_p \leq b_{p+1}$. By the assumptions on these numbers, we must have $b_1 < 1 < b_{p+1}$. Since the conclusion of the lemma is assumed to be true when $n = p$, we consider the product $(b_1 b_{p+1}) b_2 \cdots b_p = 1$, which is a product of p numbers. If all of these numbers are equal (and thus all equal 1), then

$$b_2 + b_3 + \cdots + b_p = p - 1 \qquad \text{and} \qquad b_1 + b_{p+1} > 2$$

(the inequality follows from the first part of the proof) and it follows that

$$b_1 + b_2 + \cdots + b_p + b_{p+1} > p + 1.$$

If the numbers $b_1 b_{p+1}, b_2, \ldots, b_p$ are not all equal, then

$$b_1 b_{p+1} + b_2 + \cdots + b_p > p$$

by the induction hypothesis. Since the quantity $(b_{p+1} - 1)(1 - b_1)$ is positive, we find that

$$\begin{aligned} b_1 + b_2 + \cdots + b_{p+1} &= (b_1 b_{p+1} + b_2 + \cdots + b_p) + 1 + (b_{p+1} - 1)(1 - b_1) \\ &> p + 1 + (b_{p+1} - 1)(1 - b_1) \\ &> p + 1. \end{aligned}$$

This shows that the result holds when $n = p + 1$. By the Principle of Mathematical Induction, the conditional statement given in the lemma is valid for all integers $n \geq 2$. ■

THEOREM 2.20 Arithmetic Mean/Geometric Mean Inequality Let n be a positive integer. If $a_1, a_2, \ldots, a_n$ are nonnegative real numbers, then

$$\left(a_1 a_2 \cdots a_n\right)^{1/n} \leq \frac{a_1 + a_2 + \cdots + a_n}{n}.$$

Equality occurs if and only if $a_1 = a_2 = \cdots = a_n$.

Proof. Equality certainly occurs if $a_1 = a_2 = \cdots = a_n$. In addition, the result is trivial if $n = 1$ or if one of the a_k's is 0. Suppose that $n \geq 2$, that all of the a_k's are positive, and that the a_k's are not all equal. Let $r = \left(a_1 a_2 \cdots a_n\right)^{1/n}$ and note that $r \neq 0$. Since

$$\frac{a_1}{r} \cdot \frac{a_2}{r} \cdot \ \cdots \ \cdot \frac{a_n}{r} = \frac{a_1 a_2 \cdots a_n}{r^n} = 1,$$

the previous lemma yields

$$\frac{a_1}{r} + \frac{a_2}{r} + \cdots + \frac{a_n}{r} > n,$$

which is equivalent to

$$\frac{a_1 + a_2 + \cdots + a_n}{n} > r = \left(a_1 a_2 \cdots a_n\right)^{1/n}.$$

(Note the reduction of the general case to a special case.) This completes the proof. ∎

To see one application of this inequality, consider the following fairly traditional optimization problem from calculus: find the minimum surface area of an open top rectangular box having a square base and a fixed volume of 4000 cubic feet. To solve this problem, let x be the length and width (in feet) of the base of the box and let h be the height (in feet) of the box. Then the volume V and surface area S of the box are given by $V = x^2 h$ and $S = x^2 + 4xh$. The Arithmetic Mean/Geometric Mean Inequality, along with some simple algebra, yields

$$\begin{aligned} S &= x^2 + 4xh \\ &= x^2 + 2xh + 2xh \\ &\geq 3\sqrt[3]{x^2 \cdot 2xh \cdot 2xh} \\ &= 3\sqrt[3]{4V^2} = 1200. \end{aligned}$$

Hence, the surface area of the box is always at least as large as 1200 square feet. We know that this minimum is attainable when equality occurs in the AM/GM inequality, that is, when $x^2 = 2xh = 2xh$. Since the sum of these equal numbers must be 1200, we find that each of them must be 400. It follows that $x = 20$ and $h = 10$. Note that the minimum surface area occurs when the area of the base of the box is the same as the area of two opposite sides of the box. The crucial step in this particular solution to the problem is writing the expression for S in such a way that the product of all the terms gives an expression for V. In practice, it may take some trial and error to find the right combination. By the way, make sure you see why writing $S = x^2 + xh + 3xh$, which does provide a lower bound for the surface area, is not useful for finding the minimum value of S.

Exercises 2.5.

1. Use the Binomial Theorem to expand each of the following.

a) $(1 + x)^6$ **b)** $(a + b)^5$ **c)** $(2x + y)^7$

2. What is the coefficient of x^{13} in $(1 + x)^{17}$?

3. A coach has 11 runners on his cross country team. For a given race, he must designate 6 runners whose times will count for the team scoring. How many different ways can he make the selection?

4. Prove Corollary 2.18.

5. Prove that $\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$.

6. Let A be a set with n elements, where n is a positive integer. Use the Binomial Theorem to prove that $\mathcal{P}(A)$ has 2^n elements.

7. Use the Binomial Theorem to give an alternate proof of Theorem 2.13.

8. Let n be a positive integer and let $a_1, a_2, \ldots, a_n$ be nonnegative real numbers. Prove that the arithmetic mean and the geometric mean of this set of numbers lie in the closed interval $[m, M]$, where m and M are defined by $m = \min\{a_1, a_2, \ldots, a_n\}$ and $M = \max\{a_1, a_2, \ldots, a_n\}$.

9. Let x and y be positive numbers. For each of the following conditions on x and y, find the maximum value for the product xy and the values of x and y that generate this product.

a) $4x + 9y = 36$ **b)** $4x^2 + 9y^2 = 36$ **c)** $4x^2 + 9y = 36$

10. Find the minimum value for $4x + 9y$, subject to the conditions $x > 0$, $y > 0$, and $x^2y^3 = 100$.

11. Let n be a positive integer and let $a_1, a_2, \ldots, a_n$ be positive numbers. The **harmonic mean** of these numbers is the reciprocal of the arithmetic mean of the reciprocals of the numbers. Prove that the harmonic mean of a set of positive numbers is less than or equal to the geometric mean. When does equality occur?

12. The following set of results provides a different way to think of factorials.

a) Use mathematical induction and L'Hôpital's Rule to prove that $\lim_{x\to\infty} x^n e^{-x} = 0$ for all $n \in \mathbb{Z}^+$.

b) Use part (a) and mathematical induction to prove that $\int_0^\infty x^n e^{-x}\,dx = n!$ for all $n \in \mathbb{Z}^+$.

c) Use the result from part (b) to explain why 0! is defined to be 1.

2.6 Strong Induction

The Principle of Mathematical Induction is equivalent to the following statement; a proof of this fact will be given in the next section.

Principle of Strong Induction: If S is a set of positive integers that contains 1 and satisfies the condition "if $1, 2, \ldots, k \in S$, then $k + 1 \in S$," then $S = \mathbb{Z}^+$.

This stronger form of induction (the statement is assumed to be true for all of the positive integers up to k, not just for k) is needed in some cases. (Strong induction is sometimes referred to as complete induction.) An example of a proof that uses this stronger form of induction follows.

EXAMPLE 2.21 Suppose that $a_1 = 1$, $a_2 = -1/2$, and $a_{n+1} = (a_n + a_{n-1})/2$ for each positive integer $n > 1$. Then $a_n = (-1/2)^{n-1}$ for each positive integer n.

Proof. We will use the Principle of Strong Induction. Let S be the set of all positive integers n such that $a_n = (-1/2)^{n-1}$. It is easy to see both 1 and 2 belong to S. (We need to check both of these cases since these numbers do not fit the general pattern for the generation of terms.) Suppose that all the integers $1, 2, \ldots, k$ belong to S for some positive integer $k \geq 2$. To prove that $k+1 \in S$, we must show that $a_{k+1} = (-1/2)^k$. Using the assumption that all of the a_i terms for i from 1 to k satisfy the pattern (all we really need to know is that the pattern is valid for the terms k and $k - 1$, but the crucial point is that we need more than just k),

$$a_{k+1} = \frac{a_k + a_{k-1}}{2} = \frac{\left(-\frac{1}{2}\right)^{k-1} + \left(-\frac{1}{2}\right)^{k-2}}{2} = \frac{\left(-\frac{1}{2}\right)^{k}\left(-2 + 4\right)}{2} = \left(-\frac{1}{2}\right)^{k}.$$

This shows that $k+1 \in S$. By the Principle of Strong Induction, it follows that $S = \mathbb{Z}^+$. Therefore, the formula $a_n = (-1/2)^{n-1}$ is valid for all positive integers n. ■

What is the main difference between the Principle of Mathematical Induction and the Principle of Strong Induction? The condition "if $k \in S$, then $k+1 \in S$" is replaced by the condition "if $1, 2, \ldots, k \in S$, then $k+1 \in S$"; the hypothesis of the condition is stronger (more results are assumed to be true) for the Principle of Strong Induction. The assumption that all of the integers $1, 2, \ldots, k$ belong to S gives more information to use in the proof that $k+1 \in S$. Here is another way to compare the two forms of induction. Suppose we want to prove that the formula $Q(n)$ is true for every positive integer n. For the Principle of Mathematical Induction, the key step is proving the conditional

$$Q(k) \Rightarrow Q(k+1),$$

whereas for the Principle of Strong Induction, the key step is proving the conditional

$$\big(Q(1) \wedge Q(2) \wedge \cdots \wedge Q(k)\big) \Rightarrow Q(k+1).$$

In some cases (as in the above example), the stronger hypothesis is needed to prove that $Q(k+1)$ is true. In the preceding proof, all we really needed was for the formula to be valid for both k and $k-1$ to prove that the formula was valid for $k+1$; the other hypotheses were simply ignored. The important point is that knowing the formula is valid only for k is not sufficient to prove that the formula is valid for $k+1$; thus we need the stronger form of induction.

By the way, the sequence $\{a_n\}$ defined in the statement of Example 2.21 is known as a recursively defined sequence; the sequence is generated by the first few terms and a rule to determine successive terms from previous ones. The fact that a_n is defined for every positive integer n is a simple consequence of the Principle of Strong Induction. In this case, the numbers a_1 and a_2 are defined. Assuming that the numbers $a_1, a_2, \ldots, a_k$ are defined, the formula shows how to define a_{k+1}. It follows that a_n is defined for every positive integer n. The Principle of Strong Induction is generally not mentioned in such cases; instead, a comment such as "continue this process" is made. As long as the first couple of terms are defined and it is evident how to determine the next term from previous terms, the Principle of Strong Induction guarantees that there is a term defined for each positive integer.

As a second illustration of the Principle of Strong Induction, we prove the existence portion of the Fundamental Theorem of Arithmetic. This is an important result in number theory, and it will be used many times in this book, often without special recognition.

THEOREM 2.22 Fundamental Theorem of Arithmetic Every positive integer $n > 1$ is either a prime number or can be factored into a product of prime numbers.

Proof. It is clear that 2 is a prime number. Suppose that for some positive integer k, each of the integers $2, 3, \ldots, k$ is either a prime number or can be factored into a product of prime numbers. Consider the integer $k+1$. If $k+1$ is a prime number, there is nothing further to prove. If $k+1$ is not a prime number, then $k+1 = ab$, where a and b are integers between 2 and k, inclusively. By the induction hypothesis, each of the integers a and b is either a prime number or can be factored into a product of prime numbers. It follows that $k+1 = ab$ can be factored into a product of prime numbers. By the Principle of Strong Induction, every integer $n \geq 2$ is either a prime number or can be factored into a product of prime numbers. ■

The rest of the Fundamental Theorem of Arithmetic states that the factorization of positive integers into products of primes is unique except for the order in which the factors are written. The proof of the uniqueness part of this theorem is not difficult, but it does involve some simple facts about prime numbers that we have not yet discussed. The proof will therefore be postponed until the next chapter (see Theorem 3.30 in Section 3.6).

The first part of the Fundamental Theorem of Arithmetic is often written as

Every integer $n > 1$ can be factored into a product of primes.

This statement is shorter and more concise than the one stated above and the proof requires fewer words. However, the reader must make a mental adjustment by considering a single prime number, such as 2 or 13, as a product. A number by itself is not normally considered to be a product—a product requires two or more numbers. Writing $2 = 2 \cdot 1$ does not solve the problem here since 1 is not a prime number. In this instance, the single number 2 must be thought of as a product. Simplifications and generalizations such as this occur frequently in mathematics; it is therefore necessary to learn how to make the appropriate mental adjustments.

COROLLARY 2.23 Every positive integer $n > 1$ is divisible by some prime.

Proof. Suppose that $n > 1$ is an integer. If n is a prime, then n is certainly divisible by a prime, namely itself. If n is not a prime, then it can be written as a product of two or more (not necessarily distinct) primes. Any one of the primes in this product divides n. ■

There is a common situation in which the Principle of Mathematical Induction occurs in disguised form (typically in the regular form, not the strong form) or is only mentioned as an aside. One such example from calculus is the following. After a proof of the familiar fact $(f+g)' = f'+g'$, an example such as

$$\frac{d}{dx}\left(x^3 + 2x^2 + 3x + 2\right) = \frac{d}{dx}x^3 + \frac{d}{dx}2x^2 + \frac{d}{dx}3x + \frac{d}{dx}2 = 3x^2 + 4x + 3$$

is given. What is the problem? The theorem is stated for the sum of two functions and has been applied to a sum of four functions. Some calculus texts make no mention of this; others say that it is possible to extend the result to n functions using induction. However, the proof is seldom given because it is so boring. Since it is important to see such proofs at least once, we will prove this property of derivatives. (It is assumed that the reader has some familiarity with limits and derivatives.)

THEOREM 2.24 For each positive integer n, the derivative of the sum of n differentiable functions is the sum of the derivatives of the functions.

Proof. There is nothing to prove if $n = 1$, so we first establish the result for the sum of two differentiable functions. Let f_1 and f_2 be differentiable functions and use the definition of the

derivative to compute

$$\begin{aligned}(f_1 + f_2)'(x) &= \lim_{h\to 0} \frac{\big(f_1(x+h) + f_2(x+h)\big) - \big(f_1(x) + f_2(x)\big)}{h} \\ &= \lim_{h\to 0} \Big(\frac{f_1(x+h) - f_1(x)}{h} + \frac{f_2(x+h) - f_2(x)}{h}\Big) \\ &= f_1'(x) + f_2'(x).\end{aligned}$$

Hence, the derivative of $f_1 + f_2$ is $f_1' + f_2'$. Now suppose that for some $k \geq 2$, the derivative of the sum of k differentiable functions is the sum of the derivatives of the functions and let $f_1, \ldots, f_{k+1}$ be differentiable functions. Using the induction hypothesis and the fact that the result has already been proved for two functions, we obtain

$$\begin{aligned}\big(f_1 + \cdots + f_k + f_{k+1}\big)' &= \big(\big(f_1 + \cdots + f_k\big) + f_{k+1}\big)' \\ &= \big(f_1 + \cdots + f_k\big)' + f_{k+1}' \\ &= \big(f_1' + \cdots + f_k'\big) + f_{k+1}' \\ &= f_1' + \cdots + f_k' + f_{k+1}',\end{aligned}$$

the desired result. By the Principle of Mathematical Induction, for each positive integer n, the derivative of the sum of n differentiable functions is the sum of the derivatives of the functions. ■

Note that the first step in the preceding proof requires the definition, but that the inductive step uses only previous results and assumptions. Since the latter part of the proof is rather routine and requires more words than thinking, it is often left out. However, it is important to know what goes on in such situations. As you read through the main body of this textbook, look for situations such as this where a result for two is extended to a result for more than two.

A cautionary word is appropriate at this point. Theorem 2.24 states that

$$\Big(\sum_{k=1}^{n} f_k(x)\Big)' = \sum_{k=1}^{n} f_k'(x),$$

where n is any positive integer. It is not possible to conclude from this that

$$\Big(\sum_{k=1}^{\infty} f_k(x)\Big)' = \sum_{k=1}^{\infty} f_k'(x).$$

In fact, this result is not true in general. An induction argument only shows that a result is valid for finite sums of any size; it does not say anything about infinite sums.

Exercises 2.6.

1. Let $b_1 = 1$, $b_2 = 2$, and $b_n = 3b_{n-1} - 2b_{n-2}$ for each positive integer $n > 2$. Find and prove a formula for b_n. You should begin by finding a few more terms of the sequence.
2. Prove that any nonnegative integer n can be expressed as $n = 3q + r$, where $0 \leq r < 3$.
3. Prove that any integer $n \geq 8$ can be expressed as $n = 3x + 5y$, where $x \geq 0$ and $0 \leq y < 3$.

4. Write each integer as a product of primes. (Do this without technology.)

a) 119 **b)** 561 **c)** 825 **d)** 3042

e) 1938 **f)** 1955 **g)** 2079 **h)** 111111

5. This exercise refers to the Fibonacci numbers $1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots$. These numbers are defined by $f_1 = 1$, $f_2 = 1$, and $f_{n+1} = f_n + f_{n-1}$ for each $n \geq 2$. (You may find it helpful to first write the formulas in (a) through (d) using summation notation.)

a) Prove that $f_1 + f_2 + \cdots + f_n = f_{n+2} - 1$ for each positive integer n.

b) Prove that $f_1^2 + f_2^2 + \cdots + f_n^2 = f_n f_{n+1}$ for each positive integer n.

c) Prove that $f_1 + f_3 + f_5 + \cdots + f_{2n-1} = f_{2n}$ for each positive integer n.

d) Prove that $f_1 f_2 + f_2 f_3 + f_3 f_4 + \cdots + f_{2n-1} f_{2n} = f_{2n}^2$ for each positive integer n.

e) Prove that $f_{n+1} f_{n-1} = f_n^2 + (-1)^n$ for each positive integer $n > 1$.

f) Find and prove a formula for $f_1 + f_4 + f_7 + \cdots + f_{3n-2}$.

g) Find and prove a formula for $\sum_{k=1}^{n} (-1)^{k+1} f_k$.

h) Let α and $\beta < \alpha$ be the two solutions to the equation $x^2 = x + 1$. Note that $\alpha + \beta = 1$, $\alpha - \beta = \sqrt{5}$, and $\alpha\beta = -1$. Prove that $\sqrt{5}\, f_n = \alpha^n - \beta^n$ for each positive integer n.

i) Find and prove a formula (it should be a simple and interesting one) for $f_n^2 + f_{n+1}^2$.

6. Suppose that n distinct lines are drawn in the plane in such a way that no two lines are parallel and no three lines share a common point. Into how many regions do these n lines divide the plane? Of course, you must provide a proof of your conjecture.

7. Assume that it has been proved that $\det(AB) = \det A \det B$ for square matrices of a given size. Use this fact and induction to prove that

$$\det(A_1 A_2 \cdots A_n) = \det A_1 \det A_2 \cdots \det A_n$$

for each positive integer n.

2.7 Well-Ordering Property

A set $A \subseteq \mathbb{Z}$ contains a least element if there exists an integer $q \in A$ such that $q \leq a$ for all $a \in A$. For example, the set of prime numbers contains a least element—namely, the integer 2. The set of all even integers does not contain a least element. Now consider the following statement about sets of positive integers.

Well-Ordering Property: Every nonempty set of positive integers contains a least element.

The Well-Ordering Property should make intuitive sense. Given a list of positive integers, it is always possible to find the smallest number in the list. This is not true for sets of positive real numbers. In particular, there is a smallest positive integer, but there is no smallest positive real number.

Although the Well-Ordering Property and the two forms of the Principle of Mathematical Induction are plausible, none of them can be proved from the algebraic or order properties of the integers. In fact, these statements must be accepted as axioms. This may come as a surprise since they seem so obvious, but it is sometimes the case that what seems obvious cannot be proved. In such situations, it is necessary to introduce an axiom. It is an interesting fact that all three of these statements effectively say the same thing, that is, that they are logically equivalent. Consequently,

any one of these three statements can be taken as an axiom and the other two can be derived from it as theorems. A proof of the equivalence of these statements is given below.

THEOREM 2.25 The following are equivalent:

1. Well-Ordering Property;
2. Principle of Mathematical Induction;
3. Principle of Strong Induction.

Proof. We prove (1) $\Rightarrow$ (2) and (3) $\Rightarrow$ (1), leaving a proof of (2) $\Rightarrow$ (3) as an exercise. It then follows that all three statements are equivalent.

Suppose first that the Well-Ordering Property is true. Let S be a set of positive integers that contains 1 and satisfies the condition "if $k \in S$, then $k + 1 \in S$", and let $A = \mathbb{Z}^+ \setminus S$. To prove (2), it is sufficient to show that $A = \emptyset$. We give a proof by contradiction (see the next section for further details on this proof technique). Suppose that $A \neq \emptyset$. Since A is a nonempty set of positive integers, the Well-Ordering Property guarantees the existence of an integer $q \in A$ such that $q \leq a$ for all $a \in A$. Since $q \in A$, we know that $q \notin S$. It follows that $q \neq 1$, so $q - 1$ is a positive integer. Note that $q - 1 \in S$ since q is the smallest integer in A. By the properties of the set S, the integer $q = (q - 1) + 1$ belongs to the set S. This is a contradiction to the fact that $q \notin S$. Hence, the set A is empty. Therefore, the Principle of Mathematical Induction follows from the Well-Ordering Property.

Now suppose that the Principle of Strong Induction is true. Let S be the set of all positive integers n with the following property:

> Any set of positive integers that contains an integer less than or equal to n has a least element.

It is clear that $1 \in S$. Suppose that $1, 2, \ldots, k \in S$ for some positive integer k. Let A be a set of positive integers that contains an integer less than or equal to $k + 1$. If A contains no integer less than $k + 1$, then $k + 1$ is the least element in A. If A contains an integer $a < k + 1$, then A is a set of positive integers that contains an integer less than or equal to a. Since $a \in S$, the set A has a least element. This shows that every set of positive integers that contains an integer less than or equal to $k + 1$ has a least element. It follows that $k + 1 \in S$. By the Principle of Strong Induction, $S = \mathbb{Z}^+$. Therefore, every nonempty set of positive integers has a least element, that is, the Well-Ordering Property holds. ■

As mentioned prior to the theorem, one of these statements is accepted as an axiom. Hence, all three statements are valid. We have yet to mention a proof that uses the Well-Ordering Property. Since it is equivalent to the Principle of Mathematical Induction, any proof that uses the Principle of Mathematical Induction could also be done using the Well-Ordering Property. The only change is the format of the proof.

THEOREM 2.26 For each positive integer n, the formula

$$1^3 + 2^3 + 3^3 + \cdots + n^3 = \left(\frac{n(n+1)}{2}\right)^2$$

is valid.

Proof. Let B be the set of all positive integers n for which the formula is false. We need to show that B is the empty set. Suppose (to give a proof by contradiction) that B is nonempty. By the Well-Ordering Property, the set B contains a least element, call it q. It is clear that $q \neq 1$ since the formula is easily seen to be true for $n = 1$. Since $q - 1$ is a positive integer that is not in B, the formula is valid for $q - 1$. That is,

$$1^3 + 2^3 + 3^3 + \cdots + (q-1)^3 = \left(\frac{(q-1)q}{2}\right)^2.$$

It follows that

$$\begin{aligned} 1^3 + 2^3 + 3^3 + \cdots + (q-1)^3 + q^3 &= \left(\frac{(q-1)q}{2}\right)^2 + q^3 \\ &= \frac{q^2}{4}\left((q-1)^2 + 4q\right) \\ &= \left(\frac{q(q+1)}{2}\right)^2, \end{aligned}$$

which indicates that q is not in B, a contradiction. We conclude that B is empty. Hence, the formula is valid for all positive integers. ■

It is probably more natural to use the Principle of Mathematical Induction rather than the Well-Ordering Property to prove the formula in Theorem 2.26, but the proof does indicate how this property can be used. However, there are some situations in which it is easier to use the Well-Ordering Property. The proof of the next result, known as the *Division Algorithm*, is such a case. Its conclusion includes the rather obvious statement that when one positive integer is divided by another the result is a quotient and a remainder that is smaller than the divisor; this simple statement is the basis for many results in number theory. The proof also provides a good example of an **existence/uniqueness proof**; a proof that establishes the existence of some "object" and shows that there is only one object with the given property.

THEOREM 2.27 Division Algorithm If a and b are integers with $b \geq 1$, then there exist unique integers q and r such that $a = bq + r$ and $0 \leq r < b$.

Proof. For the existence part, we restrict ourselves to the case in which $a \geq 0$; the case in which $a < 0$ is left as an exercise. Suppose that $a \geq 0$. There are two easy situations that can be handled quickly.

i) If $a < b$, then $a = b \cdot 0 + a$ has the desired form.

ii) If $b = 1$, then $a = 1 \cdot a + 0$ has the desired form.

Suppose that $a \geq b > 1$. The set $C = \{k \in \mathbb{Z}^+ : bk \geq a\}$ is a nonempty set of positive integers. By the Well-Ordering Property, the set C contains a least element p. This means that $b(p-1) < a \leq bp$. We now consider two options:

if $a = bp$, then let $q = p$ and $r = 0$;

if $a \neq bp$, then let $q = p - 1$ and let $r = a - b(p - 1)$.

In both cases, the integers q and r have the desired properties.

To establish uniqueness (this is for the general case where a is any integer), suppose that there are two representations for a:

$$a = bq_1 + r_1 \quad \text{and} \quad a = bq_2 + r_2,$$

where r_1 and r_2 are nonnegative integers less than b. By relabeling the integers if necessary, we may assume that $r_1 \geq r_2$. It follows that $0 \leq r_1 - r_2 < b$ and thus $0 \leq b(q_2 - q_1) < b$. Since $0 \leq q_2 - q_1 < 1$ and $q_2 - q_1$ is an integer, we find that $q_1 = q_2$ and thus $r_1 = r_2$. Therefore, there is only one representation of the desired form for a. This completes the proof. ■

You may find some of the steps in the above proof less than obvious. (Why is the set C nonempty?) You may find some sentences require you to take out a piece of paper and do some writing. (Why do q and r have the desired properties?) You may have to think a while and/or ask for some help. The important point here is the emphasis on "you." It is important that you understand each and every step in a proof; do not be a passive reader.

You may object that this is an awful lot of work for such an "obvious" result. But this result almost certainly seems obvious because it is so familiar—you know by experience that you can always get a quotient and remainder. Yet pressed to explain how you know that no matter how you do it, you always get the *same* remainder, you would probably find yourself at something of a loss. As we set out to establish a body of true mathematical facts, it is important to have complete confidence that the foundation is solid. Many a convincing proof has turned out to be wrong; the first place to look for a mistake is *always* the line that says "now, it is obvious that . . . "

COROLLARY 2.28 Using the notation in the Division Algorithm, $b|a$ if and only if $r = 0$. ■

As we have just seen, some of the more useful and interesting existence theorems are "existence and uniqueness statements"—they say that there is one and only one object with a specified property. The symbol $\exists! x\ P(x)$ stands for "there exists a unique x satisfying $P(x)$," or "there is exactly one x such that $P(x)$," or any equivalent formulation. The following examples illustrate this notation and show that the $\exists!$ quantifier can be combined with other quantifiers.

- If the universe is $\mathbb{R}$, then the statement $\exists! x\,(x^2 + 1 = 2x)$ is true since $x = 1$ is not only a solution, but the *only* solution. (Can you prove this?)
- If the universe is $\mathbb{Z}$, then $\forall x\,\exists! y\,(x < y < x + 2)$ is true since only $y = x + 1$ satisfies the inequalities.

The quantifier $\exists!$ can be broken down into the "existence" part and the "uniqueness" part. In other words, $\exists x!\, P(x)$ says the same thing as

$$\big(\exists x\, P(x)\big) \wedge \big(\forall x\, \forall y\, (P(x) \wedge P(y) \Rightarrow x = y)\big).$$

The second part of this formula is the "uniqueness" part; it says that any two elements that satisfy $P(x)$ must, in fact, be the same. More often than not, we must prove existence and uniqueness

separately; often one of the proofs is easier than the other. (Quite frequently, the uniqueness part is the easier of the two.)

EXAMPLE 2.29 The equation $x^3 + 6x^2 + 13x - 100 = 0$ has a unique solution.

Proof. Let f be the function defined by $f(x) = x^3 + 6x^2 + 13x - 100$. Since f is a polynomial, it is both continuous and differentiable. Note that

$$f(0) = -100 < 0 < 20 = f(3).$$

By the Intermediate Value Theorem, there exists a point $c \in (0, 3)$ such that $f(c) = 0$. This shows that the equation has at least one solution. Now suppose that both a and b are solutions to the equation and assume that $a < b$. The function f is differentiable on the interval $[a, b]$ and $f(a) = 0 = f(b)$. By Rolle's Theorem, there exists a point $z \in (a, b)$ such that $f'(z) = 0$. However,

$$f'(x) = 3x^2 + 12x + 13 = 3(x + 2)^2 + 1$$

is easily seen to be positive for every value of x. This is a contradiction so a and b must be equal. It follows that the equation $x^3 + 6x^2 + 13x - 100 = 0$ has a unique solution. ■

EXAMPLE 2.30 There is a unique function f such that $f'(x) = 2x$ for all x and $f(0) = 3$.

Proof. The function f defined by $f(x) = x^2 + 3$ clearly works. If $f_0(x)$ and $f_1(x)$ both satisfy these conditions, then $f_0'(x) = 2x = f_1'(x)$, so (by the Mean Value Theorem) the two functions differ by a constant, that is, there is a constant C such that $f_0(x) = f_1(x) + C$ for all $x \in \mathbb{R}$. Letting $x = 0$ yields $3 = f_0(0) = f_1(0) + C = 3 + C$, which shows that $C = 0$. It follows that $f_0 = f_1$. ■

Exercises 2.7.

1. Finish the proof of Theorem 2.25 by proving that (2) implies (3). Begin by letting S be a set that satisfies the hypotheses of the Principle of Strong Induction, then define a new set T by

$$T = \{n \in \mathbb{Z}^+ : 1, 2, \ldots, n \in S\}.$$

Show that T satisfies the hypotheses of the Principle of Mathematical Induction.

2. Use the Well-Ordering Property to prove $1 + 3 + 5 + \cdots + (2n - 1) = n^2$ for each positive integer n.

3. Finish the proof of Theorem 2.27 by establishing the existence portion for $a < 0$. You should use the result already proved for $a > 0$ rather than adapting the given proof.

4. For the following values of a and b, find q and r such that $0 \leq r < b$ and $a = qb + r$.

a) $a = 81$, $b = 6$ **b)** $a = 728$, $b = 7$ **c)** $a = -11$, $b = 8$

d) $a = -57$, $b = 9$ **e)** $a = 375$, $b = 1$ **f)** $a = 7$, $b = 11$

For the next two exercises, identify the existence part and the uniqueness part of your proof clearly.

5. There is a unique solution to $2x - 3 = 7$.

6. For every x there is a unique y such that $(x + 1)^3 - x^3 = 3y + 1$.

For Exercises 7–8, assume the universe of discourse is the collection of differentiable functions on $\mathbb{R}$.

7. Prove that there is a unique function f such that $f'(x) = \sin x$ for all values of x and $f(\pi/2) = 0$.

8. Prove that there is a unique function f such that $f'(x) = f(x)$ for all values of x and $f(0) = 1$. (To show uniqueness, let f_0 be the "obvious" solution and let f_1 be any other solution. What is the derivative of f_1/f_0?)
9. Find a positive integer a and integers c and d so that $a = 5c + 1 = 7d + 3$. Is a unique?
10. Prove the following modification of the Division Algorithm: If a and b are positive integers, then there exist integers q and r such that $a = bq + r$ and $|r| \leq b/2$. Can you conclude that the integers q and r are unique?
11. Let f be a differentiable function on $\mathbb{R}$ and suppose that $|f'(x)| < 1$ for all $x \in \mathbb{R}$. Prove that there exists at most one real number c such that $f(c) = c$.

2.8 Indirect Proof

There are times when it is difficult (or impossible) to prove something directly, but easier (at least possible) to prove it *indirectly.* The essence of the idea is simple: for example, suppose you are inside your house and want to know whether it is overcast or sunny, but you can't see the sky through your window. You usually can tell, indirectly, by the quality of light that you *can* see. Without formalizing the process, you make use of something like the following: If it is sunny I will be able to see areas of bright light and areas of shadow in the garden; I don't, so it must be (at least partially) overcast. What logical fact (that is, which tautology) is being used here?

There are two methods of indirect proof; proof of the contrapositive and proof by contradiction. They are closely related, even interchangeable in some circumstances, though proof by contradiction is more powerful. What unites them is that they both start by *assuming the denial of the conclusion.*

Proof of the Contrapositive

Recall that the contrapositive of the statement $P \Rightarrow Q$ is $\neg Q \Rightarrow \neg P$. Since a conditional and its contrapositive are logically equivalent, a proof of $\neg Q \Rightarrow \neg P$ yields a proof of $P \Rightarrow Q$. As indicated by the following example, it is sometimes easier or more natural to prove the contrapositive than it is to prove the given conditional.

EXAMPLE 2.31 Let $n \geq 1$ be a positive integer. If $2^n - 1$ is prime, then n is prime.

Proof. We will prove the contrapositive: if $n \geq 1$ is not prime, then $2^n - 1$ is not prime. The case in which $n = 1$ is trivial so suppose that $n > 1$ is composite. This means that there exist integers a and b such that $1 < a < n$, $1 < b < n$, and $n = ab$. The equation

$$x^b - 1 = (x - 1)\,(x^{b-1} + x^{b-2} + \cdots + 1)$$

is valid for all real numbers x (see Exercise 10 in Section 2.4). Applying this formula, we find that

$$2^n - 1 = (2^a)^b - 1 = (2^a - 1)\left((2^a)^{b-1} + (2^a)^{b-2} + \cdots + 1\right).$$

This shows that $2^a - 1$ is a divisor of $2^n - 1$. Since $1 < 2^a - 1 < 2^n - 1$, it follows that $2^n - 1$ is composite. ∎

Proof by Contradiction

To prove a sentence P by contradiction, we assume $\neg P$ and derive a statement that is known to be false. Since mathematics is consistent (at least we hope so), this means P must be true. Several examples of such proofs can be found in the previous section.

In the case that the sentence we are trying to prove is of the form $P \Rightarrow Q$, we assume that P is true and Q is false (because $P \wedge \neg Q$ is the negation of $P \Rightarrow Q$), and try to derive a statement known to be false. Note that this statement need not be $\neg P$—this is the principal difference between proof by contradiction and proof of the contrapositive. In logical symbols, a proof by contradiction of $P \Rightarrow Q$ can often be expressed as

$$((P \wedge \neg Q) \Rightarrow (R \wedge \neg R)) \Rightarrow (P \Rightarrow Q).$$

In a proof of the contrapositive, we assume that Q is false and try to prove that P is false.

EXAMPLE 2.32 The number $\log_2 5$ is irrational.

Proof. Suppose that the number $\log_2 5$ is not irrational, that is, suppose that $\log_2 5$ is rational. It follows that $\log_2 5 = a/b$, where a and b are positive integers. We then have $2^{a/b} = 5$ or $2^a = 5^b$. However, the integer 2^a is even and the integer 5^b (a product of odd numbers) is odd. Since an integer cannot be both even and odd, we have a contradiction. We conclude that $\log_2 5$ is an irrational number. ■

When should a proof by contraposition or a proof by contradiction be attempted? There is no foolproof method for deciding when such a proof will be helpful; this is the sort of knowledge that comes with practice. However, when the hypothesis provides very little useful information, a proof by contraposition or a proof by contradiction may be helpful or necessary. The hypothesis in Example 2.31 involves a prime number. The definition of a prime number is essentially a negative definition: a prime number does not have any positive divisors except itself and 1. By starting with the negation of the conclusion, we can work with a composite number—a number that can be factored. This factorization provides the key to the proof. The statement to be proved in Example 2.32 is a negative statement; we want to prove that a given number is not rational. By assuming that the number is rational, we can express it as a ratio of two integers; our assumption that the conclusion is false gave us some information that we could use.

These two types of proofs, which are sometimes referred to as **indirect proofs**, should be kept in mind as possible options when presented with a theorem or result to prove. However, it is important to think carefully about the logic behind your proof. Students sometimes write a proof in the style of proof by contradiction when the logic they have used is actually proof by contraposition. In addition, although there are plenty of exceptions, a direct proof or at least a proof by contraposition, is generally preferred over a proof by contradiction. A direct proof often provides a better indication as to why a theorem or result is valid.

Proof by contradiction makes some people uneasy—it seems a little like magic, perhaps because throughout the proof we appear to be 'proving' false statements. A direct proof, or even a proof of the contrapositive, may seem more satisfying. Still, there seems to be no way to avoid proof by contradiction. (Attempts to do so have led to the strange world of "constructive mathematics.")

We close this section with the following simple but wonderful indirect proof that there are an infinite number of primes. This proof is at least as old as Euclid's book *The Elements*. (This result is Proposition 20 in Book IX. Euclid's proof is very interesting as it illustrates the difficulty of the idea of representing a generic number of things with symbols.)

THEOREM 2.33 There are infinitely many primes.

Proof. Suppose that there are only a finite number of primes. It is then possible to write all of the primes in a list: $p_1, p_2, \ldots, p_n$. Consider the integer $m = p_1 p_2 \cdots p_n + 1$. By Corollary 2.23, the integer m must be divisible by some prime in our list, say p_j. Since p_j clearly divides the product $p_1 p_2 \cdots p_n$, part (f) of Theorem 2.7 guarantees that p_j divides $m - p_1 p_2 \cdots p_n$. Since $m - p_1 p_2 \cdots p_n = 1$, we have reached the contradiction that $p_j > 1$ and p_j divides 1. Hence, there are an infinite number of primes. ■

It is important to realize that the proof of this theorem does not give us a formula or method for constructing an infinite list of prime numbers. In particular, the integer m that appears in the proof is not necessarily prime. Although many people have tried over the centuries, to date no one has devised a prime-generating formula.

Euclid of Alexandria. Euclid, who flourished around 300 BC, is known to most high school students as the father of geometry. Surprisingly little is known of his life, not even his dates or birthplace. Shortly before 300 BC, Ptolemy I founded the great university at Alexandria, the first institution of its kind, and not unlike the universities of today. Euclid was recruited, probably from Athens, to head the mathematics department.

Euclid appears to have been primarily a teacher, not a great originator of new material. His *Elements*, unquestionably the most successful textbook of all time, often is thought to be an encyclopedia of all geometrical knowledge at the time. In fact, it is an elementary textbook covering geometry, arithmetic and algebra; Euclid himself knew and wrote about more advanced topics in mathematics. The perception that the *Elements* is only about geometry presumably is due to two facts: his name is most closely associated with geometry in modern elementary mathematics; and the mathematicians of antiquity, lacking modern algebraic notation, did all arithmetic and algebra in the language of geometry—for example, numbers were not thought of in the abstract, but as the lengths of line segments, or measures of areas or volumes.

The *Elements* consists of thirteen books containing much that is still familiar to students: most of elementary geometry, of course, including the Pythagorean Theorem; the theorem on the number of primes and the *Fundamental Theorem of Arithmetic*; and the *Euclidean Algorithm*, which we will see in Section 3.3.

Two famous stories are told about Euclid. It is said that Ptolemy asked him if geometry could be learned without reading the *Elements,* to which Euclid replied, "There is no royal road to geometry." (This story is also told about Menaechmus and Alexander the Great, which perhaps diminishes its credibility somewhat.) In response to a student who questioned the use of geometry,

Euclid reportedly ordered that the student be given three pence, "since he must needs make gain of what he learns."

For more information, see *A History of Mathematics,* by Carl B. Boyer, New York: John Wiley and Sons, 1968; or *An Introduction to the History of Mathematics,* by Howard Eves, New York: Holt, Rinehart and Winston, 1976.

Exercises 2.8.

1. Suppose that a and b are integers for which $a + b$ is odd. Prove that either a or b is odd. Give an indirect proof.

2. Suppose that a and b are real numbers for which $a + b > 100$. Prove that either $a > 50$ or $b > 50$. Give both a direct proof and an indirect proof.

3. An integer n is said to be **square-free** if it has no divisors that are perfect squares (other than 1). Show that any divisor of a square-free integer is square-free.

4. Prove that $\sqrt{2}$ is not a rational number.

5. Show that the converse of the statement in Example 2.31 is false.

6. Suppose that $2^n + 1$ is a prime. Prove that n is a power of 2.

7. Prove that $\log_2 25$ and $\log_2 \sqrt[3]{5}$ are irrational numbers. Give a direct proof by using previous results.

8. Prove that $\log_2 7$ is irrational.

9. Let x be a real number. Prove that either $\log_2 5 - x$ or $\log_2 5 + x$ is irrational.

10. Let $p_1, p_2, p_3, \ldots$ be a listing of the prime numbers in increasing order. Find a value of n for which $p_1 p_2 \cdots p_n + 1$ is not a prime number.

11. Show that for every integer $n > 2$ there is a prime between n and $n!$.

12. Prove that the sum of a rational number and an irrational number is irrational. You may use the fact that the sum of two rational numbers is rational.

13. Suppose that the function f is differentiable and that the function g is not differentiable. Prove that the function $f - g$ is not differentiable.

14. Fill in the details of the following proof that $\sqrt{2}$ is irrational using the Well-Ordering Property.

> Suppose that $\sqrt{2}$ is rational. Then there exist positive integers a and b such that $(a/b)^2 = 2$. Let $P = \{n \in \mathbb{N} : n(a/b) \text{ is an integer}\}$. By the Well-Ordering Property, the set P contains a least integer p. Then $p(a/b) - p$ is a positive integer that belongs to P and is less than p. This is a contradiction so $\sqrt{2}$ is irrational.

3

Number Theory

In this chapter, we begin our study of number theory in earnest. We discuss and prove a number of well-known and useful theorems in this interesting area of mathematics. The section headings for the chapter should give readers a good indication of the range of topics to be considered. Along the way, we will have occasion to take a brief look at the structure of the abstract spaces $\mathbb{Z}_n$ and $\mathbb{U}_n$. The chapter concludes with a discussion of quadratic residues and a characterization of those positive integers that can be represented as a sum of two squares.

3.1 Congruence

We begin our study of number theory by defining the notion of congruence. As with so many concepts we will see, **congruence** is simple (and perhaps familiar to you) yet enormously useful and powerful in the study of number theory.

DEFINITION 3.1 Let n be a positive integer. The integers a and b are **congruent** modulo n, denoted by $a \equiv b \pmod{n}$, if and only if $n|(a-b)$.

The notation for congruence, as well as much of the elementary theory of congruence, is due to the famous German mathematician, Carl Friedrich Gauss—certainly the outstanding mathematician of his time, and perhaps the greatest mathematician of all time. A short biography of Gauss can be found at the end of this section.

From the definition, it is easy to see that $36 \equiv 1 \pmod{7}$. In fact, any two numbers in the set $\{\ldots, -13, -6, 1, 8, 15, \ldots\}$ are congruent modulo 7 because their differences are multiples of 7. Note that each of these numbers leaves a remainder of 1 when divided by 7. Any two numbers in the set $\{\ldots, -4, 4, 12, 20, \ldots\}$ are congruent modulo 8. What are the remainders of these numbers when divided by 8? Finally, we note that $42 \equiv -2 \pmod{11}$ and $-71 \equiv 6 \pmod{11}$.

The examples in the previous paragraph make the next result plausible. Although it is quite simple, it is a wonderfully useful result. For the record, by the remainder on division by n, we mean the unique number r, guaranteed by the Division Algorithm, for which $0 \leq r < n$.

THEOREM 3.2 Let n be a positive integer. Then $a \equiv b \pmod{n}$ if and only if a and b have the same remainder when divided by n. Consequently, for each integer a, there exists a unique integer r such that $0 \leq r < n$ and $a \equiv r \pmod{n}$.

Proof. Since this is a biconditional statement, we break the proof into two parts. Suppose first that $a \equiv b \pmod{n}$. By definition, there exists an integer x such that $a - b = xn$. By the Division Algorithm, there exist unique integers q and r such that $b = nq + r$ and $0 \leq r < n$. We then have

$$a = b + xn = (nq + r) + xn = n(q + x) + r.$$

It follows that the remainder is r when a is divided by n. Therefore, the integers a and b have the same remainder when divided by n.

Now suppose that a and b have the same remainder when divided by n. By the Division Algorithm, there exist unique integers q_1, q_2, and r such that $a = nq_1 + r$, $b = nq_2 + r$, and $0 \leq r < n$. Since

$$a - b = (nq_1 + r) - (nq_2 + r) = n(q_1 - q_2),$$

we see that n divides $a - b$. It follows that $a \equiv b \pmod{n}$. ∎

Whenever we use the notation $a \equiv b \pmod{n}$, it is assumed that a and b are integers and that n is a positive integer. If the value of n is clear from the context, we often write simply $a \equiv b$. Congruence of integers shares many properties with equality (due to the fact that equal remainders are involved); we list a few of these properties in the next theorem.

THEOREM 3.3 Congruence modulo n has the following properties.

1. $a \equiv a$ for any a.
2. If $a \equiv b$, then $b \equiv a$.
3. If $a \equiv b$ and $b \equiv c$, then $a \equiv c$.
4. $a \equiv 0$ if and only if $n|a$.
5. If $a \equiv b$ and $c \equiv d$, then $a + c \equiv b + d$.
6. If $a \equiv b$ and $c \equiv d$, then $a - c \equiv b - d$.
7. If $a \equiv b$ and $c \equiv d$, then $ac \equiv bd$.
8. If $a \equiv b$ and j is any positive integer, then $a^j \equiv b^j$.

Proof. Parts (1) through (4) follow easily from the definition of congruence and the properties of divisibility. Alternatively, each of these four results is a simple consequence of Theorem 3.2. In what follows, we prove parts (6) and (8); proofs for parts (5) and (7) are left as exercises.

To prove part (6), suppose that $a \equiv b$ and $c \equiv d$. From the definition of congruence, we know that $n|(a-b)$ and that $n|(c-d)$. It follows that n divides the quantity (see Theorem 2.7)

$$(a-b)-(c-d) = (a-c)-(b-d).$$

Using the definition (remember that definitions are biconditional), we see that $a-c \equiv b-d$.

Part (8) follows from part (7) and the simple form of mathematical induction discussed in Section 2.6. However, this result also follows from the equality

$$a^j - b^j = (a-b)(a^{j-1} + a^{j-2}b + \ldots + ab^{j-2} + b^{j-1})$$

(see Exercise 10 in Section 2.4). Suppose that $a \equiv b$ and that j is a positive integer. By definition, we know that $n|(a-b)$. It then follows from the above equation that $n|(a^j - b^j)$. We conclude that $a^j \equiv b^j$. ■

Note that parts (1), (2), and (3) of this theorem show that congruence modulo n defines an equivalence relation on $\mathbb{Z}$. Parts (5) through (8) can be summarized by saying that in any expression involving $+, -, \cdot$, and positive integer exponents (that is, any "polynomial"), if individual terms are replaced by other terms that are congruent to them modulo n, the resulting expression is congruent to the original. (Do you notice anything related to induction in this comment?) To illustrate this, consider the polynomial Q defined by $Q(x) = 3x^3 + 22x^2 - 6x + 73$. Suppose that we want to find the remainder when $Q(17)$ is divided by 5. Using the results from Theorem 3.3, we have (modulo 5)

$$\begin{aligned} Q(17) &\equiv 3 \cdot 17^3 + 22 \cdot 17^2 - 6 \cdot 17 + 73 \\ &\equiv 3 \cdot 2^3 + 2 \cdot 2^2 - 1 \cdot 2 + 3 \\ &\equiv -1 + 3 - 2 + 3 \equiv 3. \end{aligned}$$

This is certainly much easier than evaluating $Q(17)$ and then dividing by 5.

The following simple result will play an important role later in this chapter.

THEOREM 3.4 Any perfect square is of the form $4k$ or $4k+1$.

Proof. Restating the theorem in the language of congruences yields the following: for each positive integer m, either $m^2 \equiv 0 \pmod 4$ or $m^2 \equiv 1 \pmod 4$. To see this, suppose that m is any positive integer and note that m is congruent modulo 4 to exactly one of 0, 1, 2, or 3. It follows that m^2 is congruent to $0^2 \equiv 0$, $1^2 \equiv 1$, $2^2 \equiv 0$, or $3^2 \equiv 1$. ■

It is also possible to solve equations involving congruences. To illustrate this, suppose we want to find all integers x such that $3x-5$ is divisible by 11. Putting this statement into the language of congruence, we are trying to solve the congruence equation $3x \equiv 5 \pmod{11}$ for x. Let's assume $3x \equiv 5$ and see what this tells us about x. Working modulo 11, we find that

$$3x \equiv 5 \;\Rightarrow\; 12x \equiv 20 \;\Rightarrow\; x \equiv 9.$$

We have thus shown that if $3x \equiv 5$, then $x \equiv 9$. We also need to verify the converse, that is, we need to show that if $x \equiv 9$, then $3x \equiv 5$:

$$x \equiv 9 \;\Rightarrow\; 3x \equiv 27 \;\Rightarrow\; 3x \equiv 5.$$

Therefore, the solution set of the equation $3x \equiv 5 \pmod{11}$ is

$$\{11n + 9 : n \in \mathbb{Z}\} = \{\ldots, -13, -2, 9, 20, \ldots\}.$$

In particular, there are an infinite number of solutions to the equation.

For a second example, suppose we want to solve the congruence equation $11x \equiv 1 \pmod{103}$. Working modulo 103 (and leaving some details to the reader), we find that

$$11x \equiv 1 \quad \Rightarrow \quad 99x \equiv 9 \quad \Rightarrow \quad 4x \equiv -9 \quad \Rightarrow \quad 104x \equiv -234 \quad \Rightarrow \quad x \equiv 75$$

and

$$x \equiv 75 \quad \Rightarrow \quad 11x \equiv 825 \quad \Rightarrow \quad 11x \equiv 1.$$

Therefore, the solution set of the equation $11x \equiv 1 \pmod{103}$ is $\{103n + 75 : n \in \mathbb{Z}\}$.

We present one final illustration of the power of simple congruences.

EXAMPLE 3.5 You may be familiar with the old rule, known as "casting out nines," that an integer is divisible by 9 if and only if the sum of its digits is divisible by 9. To prove this fact, suppose that x is a positive integer. When we write x in decimal form, it looks like $d_k d_{k-1} \ldots d_1 d_0$, where each digit d_i is an integer between 0 and 9. This means that

$$x = d_k \cdot 10^k + d_{k-1} \cdot 10^{k-1} + \ldots + d_1 \cdot 10 + d_0.$$

Since $10 \equiv 1 \pmod{9}$, we find that $10^i \equiv 1^i \equiv 1 \pmod{9}$ for every nonnegative integer i and thus

$$x \equiv d_k + d_{k-1} + \ldots + d_1 + d_0 \pmod{9}.$$

Note that we have actually proved that an integer and the sum of its digits are congruent modulo 9, that is, the remainder when a number is divided by 9 is the same as the remainder that is obtained when the sum of its digits is divided by 9. For example, the numbers 4357 and $19 = 4 + 3 + 5 + 7$ both have a remainder of 1 when divided by 9. In particular, a number is divisible by 9 if and only if the sum of its digits is divisible by 9.

Carl Friedrich Gauss. Gauss (1777–1855) was an infant prodigy and arguably the greatest mathematician of all time (if such rankings mean anything; certainly he would be in almost everyone's list of the top five mathematicians, as measured by talent, accomplishment, and influence). Perhaps the most famous story about Gauss relates his triumph over busywork. As Carl Boyer tells the story: "One day, in order to keep the class occupied, the teacher had the students add up all the numbers from one to a hundred, with instructions that each should place his slate on a table as soon as he had completed the task. Almost immediately Carl placed his slate on the table, saying, 'There it is;' the teacher looked at him scornfully while the others worked diligently. When the instructor finally looked at the results, the slate of Gauss was the only one to have the

correct answer, 5050, with no further calculation. The ten-year-old boy evidently had computed mentally the sum of the arithmetic progression $1 + 2 + \cdots + 100$, presumably through the formula $m(m + 1)/2$."

By the time Gauss was about 17, he had devised and justified the method of least squares, but had not decided whether to become a mathematician or a philologist. Just short of his nineteenth birthday, he chose mathematics, when he succeeded in constructing (under the ancient restriction to compass and straightedge) a seventeen-sided regular polygon, the first polygon with a prime number of sides to be constructed in over 2000 years; previously, only the equilateral triangle and the regular pentagon had been constructed. Gauss later proved precisely which regular polygons can be constructed. (The answer is somewhat unsatisfying, however. He proved that the regular polygons that can be constructed have $2^m p_1 p_2 \cdots p_r$ sides, for any $m \geq 0$ and distinct **Fermat primes** p_i, that is, prime numbers having the form $2^{2^n} + 1$ for some n. Unfortunately, it is not known whether there are an infinite number of Fermat primes.)

Gauss published relatively little of his work, but from 1796 to 1814 kept a small diary, just nineteen pages long and containing 146 brief statements. This diary remained unknown until 1898. It establishes in large part the breadth of his genius and his priority in many discoveries. Quoting Boyer again: "The unpublished memoranda of Gauss hung like a sword of Damocles over mathematics of the first half of the nineteenth century. When an important new development was announced by others, it frequently turned out that Gauss had had the idea earlier, but had permitted it to go unpublished."

The range of Gauss's contributions is truly stunning, including some deep and still standard results such as the *Quadratic Reciprocity Theorem* and the *Fundamental Theorem of Algebra*. He devoted much of his later life to astronomy and statistics, and made significant contributions in many other fields as well. His name is attached to many mathematical objects, methods, and theorems; students of physics may know him best as the namesake of the standard unit of magnetic intensity, the **gauss**.

The information here is taken from *A History of Mathematics*, by Carl Boyer, New York: John Wiley & Sons, 1968.

Exercises 3.1.

1. For the given values of n and a, find the number b that belongs to the set $\{0, 1, \ldots, n-1\}$ for which $a \equiv b \pmod{n}$. Do your computations without the aid of a calculator.

a) $n = 7$, $a = 30$ **b)** $n = 9$, $a = 69$ **c)** $n = 2$, $a = 7461$

d) $n = 6$, $a = -60$ **e)** $n = 11$, $a = -63$ **f)** $n = 17$, $a = -38$

2. Prove parts (5) and (7) of Theorem 3.3.

3. Use induction and part (7) to prove part (8) of Theorem 3.3.

4. What digits can appear in the 1's place of a perfect square?

5. Prove that 8 divides the difference of any two odd squares.

6. Use congruences to prove that $n^3 - n$ is divisible by 6 for every integer n.

7. For the polynomial Q discussed in this section, find the remainder when $Q(11)$ is divided by 13 and the remainder when $Q(101)$ is divided by 7. Do your computations without the aid of a calculator.

8. Solve each of the following by finding all values of x that satisfy the congruence. As in the examples in the text, your solution requires two parts. (Try to solve these without a calculator.)

a) $7x \equiv 6 \pmod 9$ **b)** $5x \equiv 7 \pmod{13}$ **c)** $11x + 6 \equiv 5 \pmod{19}$

d) $11x + 7 \equiv 2 \pmod{23}$ **e)** $8x - 1 \equiv 14 \pmod{37}$ **f)** $19x - 9 \equiv 22 \pmod{97}$

9. Solve the following system of congruences: $x \equiv 4 \pmod{17}$ and $x \equiv 7 \pmod{29}$. Note that a solution x must satisfy both equations and that you are seeking all possible solutions.

10. Suppose that $m, n \in \mathbb{N}$. Prove that $ma \equiv mb \pmod{mn}$ if and only if $a \equiv b \pmod n$.

11. State and prove a result similar to Example 3.5 regarding divisibility by 3.

12. State and prove a result similar to Example 3.5 regarding divisibility by 11.

13. Use results in this section to find the remainder when each of the integers is divided by 3, 9, or 11.

a) 573 **b)** 3721 **c)** 11519 **d)** 822237

3.2 The spaces $\mathbb{Z}_n$

One interpretation of Theorem 3.3 is that doing arithmetic modulo a positive integer n can be simplified by replacing some numbers with numbers that are equivalent modulo n. In other words, the result of a computation doesn't depend on which numbers we compute with, only that they are the same modulo n. For example, to compute $38 \cdot 96 \pmod{11}$, we can more easily compute the product $5 \cdot 8 \pmod{11}$, since $38 \equiv 5$ and $96 \equiv 8$. This suggests that we can go further, devising some universe in which there really is no difference between 38 and 5 or between 96 and 8 (assuming that we want to work modulo 11).

Let n be a fixed positive integer. Since congruence modulo n is an equivalence relation on $\mathbb{Z}$, we can consider the equivalence classes associated with each integer. In particular, for every integer a, the symbol $[a]$ denotes the set $\{b \in \mathbb{Z} : b \equiv a \pmod n\}$. Note that $[a]$ represents a set that contains an infinite number of integers. However, we treat $[a]$ as a single entity; we are entering the realm of the abstract. Theorem 1.17 shows that the sets $[a_1]$ and $[a_2]$ are either disjoint (when $a_1 \not\equiv a_2$) or identical (when $a_1 \equiv a_2$). Recall that if r is the remainder on dividing n into a, then $a \equiv r$ or, in our new language, $[a] = [r]$. This means that every $[a]$ is equal to some $[r]$ for $0 \le r < n$. In other words, the sets $[0]$, $[1]$, …, $[n-1]$ are the distinct equivalence classes that partition $\mathbb{Z}$. In particular,

$$\mathbb{Z} = \bigcup_{r=0}^{n-1} [r] \qquad \text{and} \qquad [r_1] \cap [r_2] = \emptyset \quad \text{when } 0 \le r_1 < r_2 < n.$$

We are thus led to make the following definition.

DEFINITION 3.6 For each positive integer n, let $\mathbb{Z}_n = \{[0], [1], [2], \ldots, [n-1]\}$.

For example, $\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$ and $\mathbb{Z}_7 = \{[0], [1], [2], [3], [4], [5], [6]\}$. Note that $[3]$ has a different meaning when interpreted as an element of $\mathbb{Z}_7$ rather than an element of $\mathbb{Z}_4$; the context should make this clear. For the record, we could write $\mathbb{Z}_4 = \{[-80], [25], [102], [-13]\}$, but only to make a point—this is not done in practice.

The set $\mathbb{Z}_n$ thus consists of n elements. Each of its elements is a set that contains an infinite number of integers. This is a new universe in which we can investigate "arithmetic." We begin

by presenting definitions for the familiar operations that are defined on integers, namely, addition, subtraction, and multiplication.

DEFINITION 3.7 For elements $[a]$ and $[b]$ of $\mathbb{Z}_n$, define the operations of addition, subtraction, and multiplication by $[a] + [b] = [a + b]$, $[a] - [b] = [a - b]$, and $[a] \cdot [b] = [ab]$, respectively.

Most mathematicians would agree that these definitions are quite natural. To illustrate these operations, we present the complete addition and multiplication tables for $\mathbb{Z}_4$.

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

$\times$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$
$[2]$	$[0]$	$[2]$	$[0]$	$[2]$
$[3]$	$[0]$	$[3]$	$[2]$	$[1]$

For example, to find $[3] + [2]$, locate $[3]$ in the left column of the $+$ table, then follow across its corresponding row until you are under the $[2]$ located in the top row of the table. This entry ($[1]$) is the desired sum.

Although we have characterized the definitions of addition, subtraction, and multiplication as "natural," the situation is not as straightforward as it may first appear. For example, the definition $[a] + [b] = [a + b]$ depends on the manipulation of specific integers a and b, but we know that there are other integers c and d with $[a] = [c]$ and $[b] = [d]$. What if we compute $[c + d]$? The value of $[c + d]$ must be the same as $[a + b]$ or the definition of addition doesn't make sense. Fortunately, Theorem 3.3 comes to the rescue. Since $[a] = [c]$ and $[b] = [d]$, we know that a and c are congruent modulo n, as are b and d. Thus their sums $a + b$ and $c + d$ are congruent modulo n, which means that $[a + b] = [c + d]$. The operations of subtraction and multiplication can be justified in the same way. What we have shown is that the definitions of addition, subtraction, and multiplication are "well-defined."

Many of the basic algebraic properties of integers carry over to $\mathbb{Z}_n$. The following theorem lists a few of the more familiar properties.

THEOREM 3.8 The following properties are valid in $\mathbb{Z}_n$.

a) $[a] + [b] = [b] + [a]$ for all $[a]$ and $[b]$ in $\mathbb{Z}_n$.

b) $[a] + ([b] + [c]) = ([a] + [b]) + [c]$ for all $[a]$, $[b]$, and $[c]$ in $\mathbb{Z}_n$.

c) $[a] \cdot [b] = [b] \cdot [a]$ for all $[a]$ and $[b]$ in $\mathbb{Z}_n$.

d) $[a] \cdot ([b] \cdot [c]) = ([a] \cdot [b]) \cdot [c]$ for all $[a]$, $[b]$, and $[c]$ in $\mathbb{Z}_n$.

e) $[a] \cdot ([b] + [c]) = [a] \cdot [b] + [a] \cdot [c]$ for all $[a]$, $[b]$, and $[c]$ in $\mathbb{Z}_n$.

f) $[0] + [a] = [a]$ for all $[a]$ $\mathbb{Z}_n$.

g) $[a] + [n - a] = [0]$ for all $[a]$ in $\mathbb{Z}_n$.

h) $[0] \cdot [a] = [0]$ for all $[a]$ in $\mathbb{Z}_n$.

i) $[1] \cdot [a] = [a]$ for all $[a]$ in $\mathbb{Z}_n$.

Proof. We prove two parts and leave the rest as exercises. Although the proofs are quite easy, it is important that you think about the steps that are involved.

To prove part (a), suppose that $[a]$ and $[b]$ are elements of $\mathbb{Z}_n$. We then have

$$[a] + [b] = [a + b] = [b + a] = [b] + [a].$$

Note that the definition of addition in $\mathbb{Z}_n$ involves addition in $\mathbb{Z}$. Since we know the properties of addition in $\mathbb{Z}$, we can apply them to determine the properties of addition in $\mathbb{Z}_n$. Similarly, part (f) follows from the simple equation $[0] + [a] = [0 + a] = [a]$. ∎

Parts (a) and (c) are commutative laws, parts (b) and (d) are associative laws, and part (e) says that multiplication distributes over addition. Parts (f), (g), (h), and (i) show that [0] and [1] act in $\mathbb{Z}_n$ in much the same way that 0 and 1 act in $\mathbb{Z}$.

Though many properties of the integers are shared by $\mathbb{Z}_n$, there are some exceptions. Consider the following statements that are true in $\mathbb{Z}$.

If $ab = 0$, then either $a = 0$ or $b = 0$.
If $a^2 = 1$, then either $a = 1$ or $a = -1$.
If $ab = ac$ and $a \neq 0$, then $b = c$.

(For the record, the second and third statements are consequences of the first statement.) These statements are not necessarily true in $\mathbb{Z}_n$. Working in $\mathbb{Z}_{24}$, we find that

$[3] \cdot [8] = [24] = [0]$, but $[3] \neq [0]$ and $[8] \neq [0]$;
$[5] \cdot [5] = [25] = [1]$, but $[5] \neq [1]$ and $[5] \neq [-1]$;
$[2] \cdot [4] = [8] = [32] = [2] \cdot [16]$, but $[2] \neq [0]$ and $[4] \neq [16]$.

Examples such as these should serve as a reminder that there are differences between the arithmetic operations in $\mathbb{Z}$ and $\mathbb{Z}_n$.

It is important to remember that $[a]$ is not an integer; it represents an infinite collection of integers. Hence, the set $\mathbb{Z}_n$ is not a subset of $\mathbb{Z}$. It is sometimes tempting to confuse the set $\mathbb{Z}_n = \{[0], [1], [2], \ldots, [n-1]\}$ with the set $\{0, 1, 2, \ldots, n-1\} \subseteq \mathbb{Z}$. The brackets make all the difference in the world: in $\mathbb{Z}_5$, the elements [2] and [7] are the same, but of course 2 and 7 are different integers. The set $\mathbb{Z}_n$, along with the operations of addition and multiplication, is an example of an abstract space. The general properties of such spaces are studied in detail in higher mathematics. As this may be your first exposure to abstract spaces, you will need to spend some time and energy thinking about these objects.

Exercises 3.2.

1. Construct addition and multiplication tables for

a) $\mathbb{Z}_2$ **b)** $\mathbb{Z}_5$ **c)** $\mathbb{Z}_6$

2. In $\mathbb{Z}_{23}$, find each of the following. Give your answer in the form $[r]$, where $0 \leq r < 23$.

a) $[10] + [17]$ **b)** $[8] + [22]$ **c)** $[6] - [16]$
d) $[14] - [20]$ **e)** $[8] \cdot [12]$ **f)** $[13] \cdot [19]$

3. Prove the remaining parts of Theorem 3.8.

4. Suppose that $[a]$ and $[b]$ are in $\mathbb{Z}_n$. Prove that there exists a unique $[x] \in \mathbb{Z}_n$ such that $[a] + [x] = [b]$.

5. Use the table from Exercise 1(c) to verify the following statements.
   a) There is a unique $[x] \in \mathbb{Z}_6$ such that $[5] \cdot [x] = [2]$.
   b) There is no $[x] \in \mathbb{Z}_6$ such that $[3] \cdot [x] = [4]$.
   c) There is an $[x] \in \mathbb{Z}_6$ such that $[4] \cdot [x] = [2]$, but it is not unique.

6. Give examples in $\mathbb{Z}_{14}$ to illustrate each of the following.
   a) $[a] \cdot [b] = [0]$ but $[a] \neq [0]$ and $[b] \neq [0]$.
   b) $[a]$ and $[b]$ so that $[a] \cdot [b] = [1]$ but neither $[a]$ nor $[b]$ are $[1]$ or $[-1]$.
   c) $[a]$, $[b]$, and $[c]$ so that $[a] \cdot [b] = [a] \cdot [c]$ but neither $[a] = [0]$ nor $[b] = [c]$.

7. Find all the elements $[x]$ of $\mathbb{Z}_{15}$ such that $[x] = [p]$ for some prime number p ($p < 15$ is not required).

8. Find (with proof) the sum of all the elements of $\mathbb{Z}_n$. (Consider the even and odd cases separately.)

9. In $\mathbb{Z}_{360}$, find all of the elements $[x]$ such that $[x]^n = [0]$ for some positive integer n. Of course, the symbols $[x]^n$ mean to multiply $[x]$ times itself n times.

10. Let $[a]$ be an element in $\mathbb{Z}_n$.
   a) Suppose that $[a] + [x] = [a] + [y]$. Prove that $[x] = [y]$.
   b) Suppose that $[a] \cdot [x] = [a] \cdot [y]$. Give an example in $\mathbb{Z}_{35}$ to show that $[x]$ may not equal $[y]$.

3.3 The Euclidean Algorithm

Consider the numbers 12 and 18. We know (from elementary school and also our formal Definition 2.6) that the divisors of 12 are ± 1, ± 2, ± 3, ± 4, ± 6, and ± 12 and that the divisors of 18 are ± 1, ± 2, ± 3, ± 6, ± 9, and ± 18. If we want the common divisors of 12 and 18, we take the intersection of these two lists. Thus the divisors of both 12 and 18 are ± 1, ± 2, ± 3, and ± 6. The largest number in this common list, namely 6, is called the greatest common divisor of 12 and 18.

DEFINITION 3.9 Suppose a and b are integers, not both zero. The *greatest common divisor* of a and b, denoted by (a, b) or $\gcd(a, b)$, is the largest positive integer that divides both a and b.

We will be concerned almost exclusively with the case in which a and b are nonnegative, but since $(a, b) = (|a|, |b|)$ the theory goes through with essentially no change in case a or b or both are negative. (Note that $(0, 0)$ is undefined.) The notation (a, b) might be somewhat confusing since it is also used to denote ordered pairs and open intervals. The meaning is usually clear from the context; if there is a chance for confusion, we use $\gcd(a, b)$. In the discussion preceding the definition, we showed that $(18, 12) = 6$. For further examples, it should be clear that $(21, 7) = 7$, $(28, 18) = 2$, and $(31, 13) = 1$.

For the record, whenever the notation (a, b) is used, it is assumed that at least one of a or b is nonzero. The next theorem lists some simple but important observations concerning (a, b).

THEOREM 3.10 The greatest common divisor satisfies the following properties:

a) $(a, 1) = 1$ for every integer a;

b) $(a, 0) = a$ for every positive integer a;

c) $(a, b) = (b, a)$ for any integers a and b, not both zero;

d) $(a, b) \leq \min\{|a|, |b|\}$ for any nonzero integers a and b;

e) If $a > 0$ and $a|b$, then $(a, b) = a$;

f) For any positive integer n, if $a \equiv b \pmod{n}$, then $(a, n) = (b, n)$.

Proof. Parts (a), (b), and (c) follow very easily from the definition of the greatest common divisor. Proofs for parts (d) and (e) are left as exercises. To prove part (f), suppose that $a \equiv b \pmod{n}$. By the definition of congruence modulo n, there exists an integer k such that $a - b = kn$. It follows that

$$a = b + kn \quad \text{and} \quad b = a - kn.$$

Let A be the set of all common divisors of a and n, and let B be the set of all common divisors of b and n. Suppose that $x \in A$. This means that x divides both a and n. Using part (f) of Theorem 2.7, the equation on the right reveals that x divides b. Since x divides both b and n, we see that $x \in B$. We have thus shown that $A \subseteq B$. Similar reasoning shows that $B \subseteq A$ and it follows that $A = B$. Since the sets A and B are equal, it follows that $(a, n) = (b, n)$. ∎

It perhaps is surprising to learn that part (f) of this theorem is all that is necessary to compute the greatest common divisor of two integers and, moreover, to compute it very efficiently. This remarkable fact is known as the *Euclidean Algorithm*. As the name implies, the Euclidean Algorithm was known to Euclid (see the biography in Section 2.8) and appears in *The Elements*. As we will see, the Euclidean Algorithm is an important theoretical tool as well as a practical algorithm. Here is how it works.

Suppose that a and b are positive integers with $a > b$ and, without loss of generality, assume that b does not divide a. Use the Division Algorithm repeatedly to obtain

$$\begin{aligned}
a &= q_1 b + r_1, && 0 < r_1 < b; && (\, a \equiv r_1 \pmod{b}\,)\\
b &= q_2 r_1 + r_2, && 0 < r_2 < r_1; && (\, b \equiv r_2 \pmod{r_1}\,)\\
r_1 &= q_3 r_2 + r_3, && 0 < r_3 < r_2; && (\, r_1 \equiv r_3 \pmod{r_2}\,)\\
r_2 &= q_4 r_3 + r_4, && 0 < r_4 < r_3; && (\, r_2 \equiv r_4 \pmod{r_3}\,)\\
&\vdots && && \vdots
\end{aligned}$$

Since a decreasing list of nonnegative integers cannot continue indefinitely, eventually one of the remainders is 0. It follows that the last two steps in the list would look like

$$\begin{aligned}
r_{k-2} &= q_k r_{k-1} + r_k, && 0 < r_k < r_{k-1}; && (\, r_{k-2} \equiv r_k \pmod{r_{k-1}}\,)\\
r_{k-1} &= q_{k+1} r_k + 0. && && (\, r_{k-1} \equiv 0 \pmod{r_k}\,)
\end{aligned}$$

By part (f) of Theorem 3.10, we know that

$$(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_{k-1}, r_k) = (r_k, 0) = r_k.$$

In other words, the last nonzero remainder in this process is the greatest common divisor of a and b.

If you have done some computer programming, you should see just how easy it is to implement this algorithm in any reasonable programming language. Since it is a very fast algorithm, it plays

an important role in many applications. For example, to find the greatest common divisor of 198 and 168 with this method, we would compute

$$\begin{aligned} 198 &= 1 \cdot 168 + 30 & (198, 168) &= (168, 30) \\ 168 &= 5 \cdot 30 + 18 & &= (30, 18) \\ 30 &= 1 \cdot 18 + 12 & &= (18, 12) \\ 18 &= 1 \cdot 12 + 6 & &= (12, 6) \\ 12 &= 2 \cdot 6 & &= (6, 0) = 6. \end{aligned}$$

Furthermore, with a little extra bookkeeping, we can use the Euclidean Algorithm to show that (a, b) is actually a **linear combination** of a and b. Referring to the previous example with $a = 198$ and $b = 168$, we find that

$$\begin{aligned} 30 &= 198 - 168 = a - b, \\ 18 &= 168 - 5 \cdot 30 = b - 5(a - b) = -5a + 6b, \\ 12 &= 30 - 18 = (a - b) - (-5a + 6b) = 6a - 7b, \\ 6 &= 18 - 12 = (-5a + 6b) - (6a - 7b) = -11a + 13b. \end{aligned}$$

Notice that the numbers in the left column are precisely the remainders computed by the Euclidean Algorithm. This example leads to the following general result, known as the *Extended Euclidean Algorithm*. In spite of its simplicity, this is an extremely important theorem, one of the most crucial results in this book.

THEOREM 3.11 If a and b are integers, not both zero, then there exist integers x and y such that $(a, b) = ax + by$.

Proof. Referring to the steps in the Euclidean Algorithm, we find that

r_1 is a linear combination of a and b;

r_2 is a linear combination of b and r_1 and thus a linear combination of a and b;

r_3 is a linear combination of r_1 and r_2 and thus a linear combination of a and b;

$\vdots$

r_k is a linear combination of r_{k-2} and r_{k-1} and thus a linear combination of a and b.

Assuming that r_k is the last nonzero remainder, we find that $(a, b) = r_k$ is a linear combination of a and b. The result then follows by the Principle of Mathematical Induction (which is implicitly taking place in the ... portion of the proof).

Since this is such an important result and the preceding proof, although easy to believe, is rather short on rigor, we offer a second proof. Let $D = \{ai + bj : i, j \in \mathbb{Z}\} \cap \mathbb{N}$, that is, let D be the set of all positive integers that can be expressed as linear combinations of a and b. Since at least one of the numbers $|a|$ or $|b|$ is positive and thus belongs to the set D, we find that D is nonempty. By the Well-Ordering Property, the set D contains a least element, call it d. Choose integers i and j so that $d = ai + bj$ and let $g = (a, b)$. We want to prove that $d = g$. Since $g|a$ and $g|b$, it is clear

that $g|d$ and thus $g \leq d$. To complete the proof, we need to prove that $d \leq g$ and to do this, it is sufficient to prove that $d|a$ and $d|b$. By the Division Algorithm, there exist integers q and r such that $a = dq + r$ and $0 \leq r < d$. It follows that

$$r = a - dq = a - (ai + bj)q = a(1 - iq) + b(-jq)$$

is a linear combination of a and b. If $r > 0$, then r is an element of D that is smaller than d, a contradiction to the fact that d is the least element of D. We conclude that $r = 0$ and thus that $d|a$. In a similar way, it follows that $d|b$. This completes the proof. ■

It is rather remarkable that the greatest common divisor of a and b can be written as a linear combination of a and b. In fact, the second of the proofs given above reveals that (a, b) is the smallest positive integer with this property.

The following definition introduces an important concept in number theory.

DEFINITION 3.12 The integers a and b are **relatively prime** if and only if $(a, b) = 1$.

It is easy to verify that 6 and 5 are relatively prime as are 21 and 10, but the integers 12 and 20 are not relatively prime. Part (a) of Theorem 3.10 can be rephrased to say that 1 and a are relatively prime for any integer a. Finally, if p is a prime and a is any integer that satisfies $1 \leq a < p$, then a and p are relatively prime. An extremely useful characterization of relatively prime integers is given below; its proof is left as an exercise.

THEOREM 3.13 Suppose that a and b are integers, not both zero. Then a and b are relatively prime if and only if there exist integers x and y such that $ax + by = 1$. ■

Exercises 3.3.

1. For each pair of integers a and b, find (a, b) and integers x and y satisfying $(a, b) = ax + by$. Which pairs of integers are relatively prime?

a) $a = 32$, $b = 13$ **b)** $a = 148$, $b = 40$ **c)** $a = 300$, $b = 55$

d) $a = 58$, $b = 17$ **e)** $a = 147$, $b = 105$ **f)** $a = 338$, $b = 225$

2. Let p be a prime and let a be a positive integer. What are the possible values for (a, p)?

3. Let a and b be integers, not both 0. Prove that $(a, b) = (|a|, |b|)$.

4. Prove parts (d) and (e) of Theorem 3.10.

5. Prove Theorem 3.13.

6. Let a and b be positive integers. Suppose that there exist integers x and y such that $ax + by = 6$. What are the possible values for (a, b)?

7. Suppose that $g = (a, b)$. Prove that $g^2|(ab)$.

8. Suppose that g is a positive integer and let x be a multiple of g^2. Show that there exist integers a and b such that $(a, b) = g$ and $ab = x$.

9. Show that there are an infinite number of ways of expressing (a, b) as a linear combination of a and b.

10. Let a and b be integers, not both zero, and let $g = (a, b)$. Prove that an integer can be expressed as a linear combination of a and b if and only if it is a multiple of g.

11. Prove that a and b are relatively prime if and only if a^2 and b^2 are relatively prime.

12. The Euclidean Algorithm works so well that it is difficult to find pairs of numbers that make it take a long time. Find two numbers whose greatest common divisor is 1 for which the Euclidean Algorithm takes 10 steps.

3.4 The spaces $\mathbb{U}_n$

As the last part of Section 3.2 indicates, some of the arithmetic properties of $\mathbb{Z}_n$ are different from those of $\mathbb{Z}$. In particular, it is possible for two nonzero numbers to have a product of zero ($[3] \cdot [8] = [0]$ in $\mathbb{Z}_{24}$) and for the square of a number other than $[1]$ or $[-1]$ to be $[1]$ ($[5]^2 = [1]$ in $\mathbb{Z}_{24}$). Notice also that $[2] \cdot [3] = [1]$ in $\mathbb{Z}_5$ but that neither $[2]$ nor $[3]$ is $[1]$ or $[-1]$. This last observation shows that there can be multiplicative inverses for elements in $\mathbb{Z}_n$ other than $[1]$ and $[-1]$. We are thus led to consider a notion of division (that is, multiplication by multiplicative inverses) in $\mathbb{Z}_n$, but in order to do so, we must eliminate some of the problem elements, namely those that do not have multiplicative inverses. The next theorem and its three corollaries are quite useful in this regard and for our later work. The proofs of the corollaries are left as exercises.

THEOREM 3.14 If n and a are relatively prime and $n|ab$, then $n|b$.

Proof. Suppose that n, a, and b are integers such that n and a are relatively prime and $n|ab$. By the definition of divisibility, there exists an integer k such that $ab = nk$. Since n and a are relatively prime, Theorem 3.13 shows that there exist integers x and y such that $nx + ay = 1$. It follows that

$$b = b(nx + ay) = nbx + aby = nbx + nky = n(bx + ky),$$

revealing that $n|b$. ■

COROLLARY 3.15 If p is a prime and $p|ab$, then $p|a$ or $p|b$. ■

COROLLARY 3.16 If p is a prime and p divides the product $a_1 a_2 \cdots a_n$, then $p|a_i$ for some index i that satisfies $1 \leq i \leq n$. ■

COROLLARY 3.17 If p, p_1, p_2, ..., p_n are primes and p divides the product $p_1 p_2 \cdots p_n$, then $p = p_i$ for some index i that satisfies $1 \leq i \leq n$. ■

Given a positive integer $n > 1$, the set $\mathbb{Z}_n$ can be best represented as

$$\{[0], [1], [2], \ldots, [n-2], [n-1]\} = \{[i] : 0 \leq i \leq n-1\}.$$

For some elements $[i]$ of $\mathbb{Z}_n$, we find that $(i, n) = 1$, while $(i, n) > 1$ for other values of i. It turns out that the subset $\mathbb{U}_n$ of $\mathbb{Z}_n$ that consists of those elements $[u]$ of $\mathbb{Z}_n$ for which $(u, n) = 1$ has some interesting properties. In particular (see Corollary 3.20 below), each element of $\mathbb{U}_n$ has a multiplicative inverse .

DEFINITION 3.18 Let $n > 1$ be a positive integer. The set $\mathbb{U}_n \subseteq \mathbb{Z}_n$ is defined to be the set of all $[u] \in \mathbb{Z}_n$ such that $(u, n) = 1$.

As indicated by the definition, the set $\mathbb{U}_1$ is not defined. The set $\mathbb{U}_2$ consists of a single element, namely, $\{[1]\}$. It is easy to verify the following examples of sets $\mathbb{U}_n$:

$$\mathbb{U}_6 = \{[1], [5]\};$$
$$\mathbb{U}_7 = \{[1], [2], [3], [4], [5], [6]\};$$
$$\mathbb{U}_8 = \{[1], [3], [5], [7]\};$$
$$\mathbb{U}_{21} = \{[1], [2], [4], [5], [8], [10], [11], [13], [16], [17], [19], [20]\}.$$

Note that $[0]$ is never an element of $\mathbb{U}_n$ while $[1]$ and $[n-1]$ are elements of $\mathbb{U}_n$ for $n > 2$. The most important property of elements of $\mathbb{U}_n$ is given in the following result.

THEOREM 3.19 Suppose that u and n are integers with $n > 1$. Then u and n are relatively prime if and only if there exists an integer v such that $uv \equiv 1 \pmod{n}$.

Proof. Let u and n be integers with $n > 1$. We first suppose that u and n are relatively prime. By Theorem 3.13, there exist integers v and w such that $uv + nw = 1$. Since $uv - 1$ is a multiple of n, it follows that $uv \equiv 1 \pmod{n}$. Now suppose that $uv \equiv 1 \pmod{n}$. By definition, there exists an integer k such that $uv - 1 = kn$. This equation can be written as $uv + n(-k) = 1$. Applying Theorem 3.13 once again, we find that u and n are relatively prime. (For the record, since the integers u and v are interchangeable in the proof, the integers v and n are relatively prime.) ■

COROLLARY 3.20 If $n > 1$ is an integer, then for each $[u] \in \mathbb{U}_n$ there exists a $[v] \in \mathbb{U}_n$ such that $[u] \cdot [v] = [1]$.

Proof. Let $n > 1$ be an integer and suppose that $[u] \in \mathbb{U}_n$. Since u and n are relatively prime by the definition of $\mathbb{U}_n$, the theorem guarantees the existence of an integer v such that $uv \equiv 1 \pmod{n}$. Referring to the theorem once again, we find that v and n are relatively prime and thus $[v] \in \mathbb{U}_n$. The equation $uv \equiv 1 \pmod{n}$ is equivalent to $[u] \cdot [v] = [1]$ in $\mathbb{U}_n$. ■

Therefore, the set $\mathbb{U}_n$ consists of those $[u] \in \mathbb{Z}_n$ such that for some $[v] \in \mathbb{Z}_n$ we have $[u] \cdot [v] = [1]$. In other words, the set $\mathbb{U}_n$ is the set of all elements of $\mathbb{Z}_n$ that have multiplicative inverses. The invertible elements of $\mathbb{Z}_n$ are sometimes called *units*—hence the use of the symbol $\mathbb{U}_n$ for this set. We say $[v]$ is a *multiplicative inverse* (or *reciprocal*) of $[u]$. Note that $[u]$ is an inverse of $[v]$ when $[v]$ is an inverse of $[u]$. For some specific examples, for $\mathbb{U}_5 = \{[1], [2], [3], [4]\}$, we see that $[2]$ and $[3]$ are inverses of each other, while $[1]$ and $[4]$ are their own inverses. In $\mathbb{U}_{14} = \{[1], [3], [5], [9], [11], [13]\}$, we find that $[3]$ and $[5]$ are inverses, as are $[9]$ and $[11]$; and that $[1]$ and $[13]$ are their own inverses.

For these examples it is easy to find an inverse by inspection. In general, this can be done by the Extended Euclidean Algorithm or by solving a congruence equation.

EXAMPLE 3.21 Find an inverse for $[17]$ in the set $\mathbb{U}_{37}$. We apply the Extended Euclidean Algorithm (details omitted) to find that

$$-13 \cdot 17 + 6 \cdot 37 = 1 \;\Leftrightarrow\; -13 \cdot 17 \equiv 1 \pmod{37} \;\Leftrightarrow\; [-13] \cdot [17] = [1].$$

It follows that $[-13] = [24]$ is an inverse for $[17]$. Alternatively, we can solve the following congruence modulo 37:

$$17x \equiv 1 \;\Rightarrow\; 34x \equiv 2 \;\Rightarrow\; -3x \equiv 2 \;\Rightarrow\; -36x \equiv 24 \;\Rightarrow\; x \equiv 24,$$

showing again that [24] is an inverse for [17]. In either case, we can check that when the product $17 \cdot 24$ is divided by 37, the remainder is 1.

Notice that both methods in the above example produced the same inverse for [17]. This is no accident; each element in $\mathbb{U}_n$ has exactly one inverse.

THEOREM 3.22 If $[u] \in \mathbb{U}_n$, then the inverse of $[u]$ is unique and is also an element of $\mathbb{U}_n$.

Proof. By Corollary 3.20, we know that $[u]$ has at least one inverse in $\mathbb{U}_n$. Suppose that $[v_1]$ and $[v_2]$ are both inverses of $[u]$. This means that $[u] \cdot [v_1] = [1] = [u] \cdot [v_2]$ or, in the language of congruence, $uv_1 \equiv uv_2 \pmod{n}$. It follows that n divides the product $u(v_1 - v_2)$. Since u and n are relatively prime, we find that n divides $v_1 - v_2$ (see Theorem 3.14) and thus $[v_1] = [v_2]$. ■

We denote the multiplicative inverse of $[u]$ by $[u]^{-1}$. Note well that this notation only makes sense if $[u] \in \mathbb{U}_n$; an arbitrary element of $\mathbb{Z}_n$ may not have a multiplicative inverse. For elements $[u]$ of $\mathbb{U}_n$ and positive integers k, we define $[u]^{-k}$ to be $\left([u]^{-1}\right)^k$; thus (adopting the usual convention that $[u]^0 = [1]$) for elements $[u]$ of $\mathbb{U}_n$, the expression $[u]^k$ is defined for all integers k

THEOREM 3.23 The product of any two elements of $\mathbb{U}_n$ is an element of $\mathbb{U}_n$. Hence, the product of any number of elements of $\mathbb{U}_n$ is an element of $\mathbb{U}_n$.

Proof. Suppose that $[u_1]$ and $[u_2]$ are in $\mathbb{U}_n$. Since $(u_1, n) = 1 = (u_2, n)$, by Theorem 3.19, there exist integers v_1 and v_2 such that $u_1v_1 \equiv 1$ and $u_2v_2 \equiv 1$. It follows that $(u_1u_2)(v_1v_2) \equiv 1$. This last equation, along with Theorem 3.19 once again, shows that $(u_1u_2, n) = 1$ and thus $[u_1u_2] \in \mathbb{U}_n$. Since $[u_1u_2] = [u_1] \cdot [u_2]$, we find that the product $[u_1] \cdot [u_2]$ belongs to $\mathbb{U}_n$. Since

$$[u_1u_2] \cdot [v_1v_2] = [1] \quad \Rightarrow \quad \big([u_1] \cdot [u_2]\big) \cdot \big([v_1] \cdot [v_2]\big) = [1] \quad \Rightarrow \quad \big([u_1] \cdot [u_2]\big) \cdot \big([u_1]^{-1} \cdot [u_2]^{-1}\big) = [1],$$

it follows that $\big([u_1] \cdot [u_2]\big)^{-1} = [u_1]^{-1} \cdot [u_2]^{-1}$. ■

To illustrate these ideas, here is a complete multiplication table for $\mathbb{U}_9$:

$\times$	[1]	[2]	[4]	[5]	[7]	[8]
[1]	[1]	[2]	[4]	[5]	[7]	[8]
[2]	[2]	[4]	[8]	[1]	[5]	[7]
[4]	[4]	[8]	[7]	[2]	[1]	[5]
[5]	[5]	[1]	[2]	[7]	[8]	[4]
[7]	[7]	[5]	[1]	[8]	[4]	[2]
[8]	[8]	[7]	[5]	[4]	[2]	[1]

Notice that every row in this multiplication table is a list of all of the elements of $\mathbb{U}_9$. In particular, each row contains [1] exactly once, as it must, allowing us to read off inverses: $[1]^{-1} = [1]$, $[2]^{-1} = [5]$, $[4]^{-1} = [7]$, and $[8]^{-1} = [8]$. The fact that $\mathbb{U}_n$ appears in each row is true in general and will be useful to us later. We record it below and leave the proof as an exercise.

THEOREM 3.24 Let $n > 1$ be an integer and let $[a_1], [a_2], \ldots, [a_k]$ be a list of all the elements of $\mathbb{U}_n$. If $[u] \in \mathbb{U}_n$, then $[u] \cdot [a_1], [u] \cdot [a_2], \ldots, [u] \cdot [a_k]$ is also a list of all the elements of $\mathbb{U}_n$. ■

In $\mathbb{Z}_n$ we can add, subtract, and multiply, but, as in $\mathbb{Z}$, we cannot divide. However, since division is defined as multiplication by the multiplicative inverse, we can do division in $\mathbb{U}_n$. Thus, if p is a prime, algebra in $\mathbb{Z}_p$ is much like algebra in $\mathbb{Q}$.

Exercises 3.4.

1. Prove Corollary 3.15.
2. Prove Corollary 3.16.
3. Prove Corollary 3.17.
4. We say that $\mathbb{Z}_n$ has the zero product property if $[x] \cdot [y] = [0]$ implies either $[x] = [0]$ or $[y] = [0]$. Prove that $\mathbb{Z}_n$ for $n \geq 2$ has the zero product property if and only if n is prime.
5. Suppose that $(a, b) = 1$, $a|n$, and $b|n$. Prove that $(ab)|n$.
6. Construct multiplication tables for $\mathbb{U}_5$ and $\mathbb{U}_{14}$.
7. Determine $[u]^{-1}$ in $\mathbb{U}_n$, where
   a) $u = 5$, $n = 13$ **b)** $u = 13$, $n = 19$ **c)** $u = 7$, $n = 15$
   d) $u = 25$, $n = 37$ **e)** $u = 11$, $n = 37$ **f)** $u = 23$, $n = 37$
8. Use the fact that $[4]^{-1} = [10]$ in $\mathbb{U}_{39}$ to find $[16]^{-1}$.
9. Suppose that $n > 2$. Prove that $[1]$ and $[n-1]$ are elements of $\mathbb{U}_n$ and that they are their own inverses.
10. Suppose that $n \geq 7$ is an odd integer. Prove that $\mathbb{U}_n$ contains at least six elements.
11. Suppose $g = \gcd(a, b)$. Since g divides both a and b, there are integers A and B such that $a = Ag$ and $b = Bg$. Prove that A and B are relatively prime.
12. How many elements are there in $\mathbb{U}_{243}$? (Note that $243 = 3^5$.)
13. Suppose that $n > 1$ is an integer and that $(a, n) = 1 = (b, n)$. Use ideas from Section 3.3 to prove that $(ab, n) = 1$. Use this fact to give a different proof of Theorem 3.23.
14. Prove Theorem 3.24. (Let $W_n = \{[u] \cdot [a_i] : 1 \leq i \leq k\}$ and prove that $W_n = \mathbb{U}_n$.)
15. Prove that $(f_n, f_{n+2}) = 1$ for each positive integer n, where f_n is the nth Fibonacci number.

3.5 The GCD and the LCM

In this section, we present some further properties of the greatest common divisor and introduce the related notion of least common multiple. These two concepts are first introduced in middle school as an aid to adding and subtracting fractions. However, as is to be expected, we are going to look at some deeper properties of these concepts. The first result provides a complete characterization of the greatest common divisor.

THEOREM 3.25 Suppose that a and b are integers, not both 0. Then $g = (a, b)$ if and only if $g > 0$, $g|a$, $g|b$, and $d|g$ for every common divisor d of a and b.

Proof. Suppose that g is an integer that satisfies $g > 0$, $g|a$, $g|b$, and $d|g$ for every common divisor d of a and b. We must prove that g is the greatest common divisor of a and b. It is clear that g is a common divisor of a and b. By hypothesis, every common divisor d of a and b divides g and thus satisfies $|d| \leq g$ (see Theorem 2.8). It follows that g is in fact the greatest common divisor of a and b. A proof of the converse is left as an exercise. ∎

As a consequence of this theorem, we see that the entire collection of common divisors of a and b can be found by listing all of the divisors of (a, b). In other words, (a, b) is actually a multiple of every other common divisor of a and b. This is a somewhat surprising result since it is not obvious from the definition of the greatest common divisor. After all, from the definition all that we know about the greatest common divisor is that it is larger than all the other common divisors; we now see that it is not only larger, it is actually a multiple of every other common divisor.

Speaking of multiples, we now define another number which is 'dual' to the greatest common divisor. Consider once again the numbers 12 and 18. If we list the positive multiples of 12, we obtain 12, 24, 36, 48, 60, 72, and so on. Similarly, the positive multiples of 18 are 18, 36, 54, 72, 90, 108, and so on. If we want the common multiples of 12 and 18, we take the intersection of these two lists and obtain 36, 72, 108, and so on. The smallest number in this common list, namely 36, is called the least common multiple of 12 and 18.

DEFINITION 3.26 Suppose a and b are positive integers. The *least common multiple* of a and b, denoted by $[a, b]$ or $\text{lcm}(a, b)$, is the smallest positive integer that is a multiple of both a and b.

Returning to the discussion prior to the definition, we see that $[12, 18] = 36$. Omitting the simple details, it should be clear that $[2, 5] = 10$, $[4, 14] = 28$, and $[33, 77] = 231$. The next theorem, which is analogous to Theorem 3.10, records some simple facts related to $[a, b]$.

THEOREM 3.27 The least common multiple satisfies the following properties:

a) $[a, 1] = a$ for every positive integer a;

b) $[a, a] = a$ for every positive integer a;

c) $[a, b] = [b, a]$ for all positive integers a and b;

d) $[a, b] \geq \max\{a, b\}$ for all positive integers a and b;

e) If a and b are positive integers for which $a|b$, then $[a, b] = b$.

Proof. Parts (a), (b), and (c) follow very easily from the definition of the least common multiple. Proofs for parts (d) and (e) are left as exercises. ■

The following result is the analogue of Theorem 3.25 for least common multiples.

THEOREM 3.28 Suppose that a and b are positive integers. Then $\ell = [a, b]$ if and only if $\ell > 0$, $a|\ell$, $b|\ell$, and $\ell|m$ for every common multiple m of a and b.

Proof. Suppose that $\ell = [a, b]$. It is then obvious that $\ell > 0$, $a|\ell$, and $b|\ell$. Now suppose that m is a common multiple of a and b and, without loss of generality, assume that $m > 0$. Since ℓ is the least common multiple of a and b, we know that $\ell \leq m$. If $\ell = m$, then clearly $\ell|m$. Suppose that $\ell < m$. By the Division Algorithm, there exist integers q and r such that $m = q\ell + r$ and $0 \leq r < \ell$. A moment's glance at the equation $r = m - q\ell$ reveals that r is a multiple of both a and b. If r is positive, then we have found a positive common multiple of a and b that is less than ℓ, a contradiction. Hence, the remainder r is zero and ℓ divides m. A proof of the converse is left as an exercise. ■

Just as every common divisor of a and b is a divisor of (a, b), we now see that every common multiple of a and b is a multiple of $[a, b]$. As shown in the next theorem, there is also an interesting algebraic relationship between the greatest common divisor and the least common multiple.

THEOREM 3.29 If a and b are positive integers, then $(a, b) \cdot [a, b] = ab$.

Proof. To make the notation easier, let $g = (a, b)$. By Exercise 11 in Section 3.4, there exist integers A and B such that $a = Ag$, $b = Bg$, and $(A, B) = 1$. Let ℓ be the integer ABg and note that $aB = \ell = Ab$. We will show that the number ℓ satisfies the hypotheses of Theorem 3.28. It is easy to verify that $\ell > 0$, that $a|\ell$, and that $b|\ell$. Now suppose that m is any positive common multiple of a and b and choose integers x and y such that $ax = m = by$. Since $ax = by$, we find that $Agx = Bgy$ and consequently (since $g \neq 0$) that $Ax = By$. This last equation reveals that $A|By$ and thus $A|y$ since A and B are relatively prime (see Theorem 3.14). Writing $y = Av$ then yields

$$m = by = Abv = \ell v,$$

which shows that $\ell|m$. Since all of the hypotheses of Theorem 3.28 are satisfied, the number ℓ is the least common multiple of a and b. The proof is complete once we note that the product $(a, b) \cdot [a, b]$ is the same as $g\ell = g(ABg) = (Ag)(Bg) = ab$. ■

Illustrating this theorem with earlier examples, we find that $(12, 18) \cdot [12, 18] = 6 \cdot 36 = 12 \cdot 18$. The numbers used in this example are quite small. If we are given larger numbers as a and b, it may be more difficult to find the least common multiple $[a, b]$. However, the Euclidean Algorithm provides a systematic approach for finding (a, b) and once this is known, it is easy to use the preceding theorem to determine $[a, b]$.

Exercises 3.5.

1. Prove the other half of the biconditional statement of Theorem 3.25.

2. For each pair of integers a and b, find $[a, b]$.

a) $a = 28$, $b = 35$ **b)** $a = 51$, $b = 85$ **c)** $a = 132$, $b = 242$

3. Prove parts (d) and (e) of Theorem 3.27.

4. Prove the other half of the biconditional statement of Theorem 3.28.

5. Suppose $a > 0$, $(a, 42) = 6$, and $[a, 42] = 420$. Find a.

6. Let a, b, and n be positive integers. Prove that $(na, nb) = n(a, b)$ and $[na, nb] = n[a, b]$.

7. Prove that a and b are relatively prime if and only if $ab = [a, b]$.

8. Prove that $(a^2, b^2) = (a, b)^2$.

9. Suppose that g and ℓ are positive integers. Show that there are integers a and b with $(a, b) = g$ and $[a, b] = \ell$ if and only if $g|\ell$.

10. Suppose that a, b, and c are positive integers and let (a, b, c) represent the greatest common divisor of all three integers.

a) Prove that $(a, b, c) = ((a, b), c)$.

b) Prove that there exist integers x, y, and z such that $(a, b, c) = ax + by + cz$.

c) Find $(15, 21, 35)$ and represent this greatest common divisor as a linear combination of the integers 15, 21, and 35.

3.6 The Fundamental Theorem of Arithmetic

We are now ready to prove the uniqueness portion of the Fundamental Theorem of Arithmetic, that is, to prove that every positive integer greater than 1 can be factored as a product of primes in only one way (ignoring the order in which the factors are written). This fact seems completely obvious to most students; they are thus left wondering why a proof is even required. Therefore, before presenting the proof, we offer two examples of situations where unique factorization does not hold and thus show that there actually is something to prove.

Consider the set $T = \{3n-2 : n \in \mathbb{Z}^+\} = \{1, 4, 7, 10, \ldots\}$ and define multiplication in the usual way. It is easy to verify that the set T is closed under multiplication, that is, the product of any two elements of T is another element of T. (Note, however, that T is not closed under addition.) Prime numbers have the same meaning as before; an integer in T is prime if its only factors in T are itself and 1. So, for instance, the numbers 4, 7, and 10 are prime in T, but $28 = 4 \cdot 7$ is not. In this set, the number 100 has two different prime factorizations: $4 \cdot 25 = 100 = 10 \cdot 10$. Therefore, prime factorization is not unique in the set T.

For a different and more complicated example, consider the set $C = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$ with addition and multiplication defined in the usual way. The reader may verify that C is closed under both addition and multiplication. Without including any details, we note that it can be shown that the numbers 3, 7, $1 + 2\sqrt{-5}$, and $1 - 2\sqrt{-5}$ are all prime in C. It then follows that 21 has two distinct prime factorizations:

$$3 \cdot 7 = 21 = \left(1 + 2\sqrt{-5}\right)\left(1 - 2\sqrt{-5}\right).$$

So once again we have an example of a set that does not have unique factorizations. Since C apparently shares all of the algebraic properties of $\mathbb{Z}$, we thus realize that there is some other crucial property that $\mathbb{Z}$ satisfies in order to guarantee unique factorization. We encourage the reader to trace the origins of the facts needed in the following proof and thus determine what key results lie behind this property of $\mathbb{Z}$.

THEOREM 3.30 Fundamental Theorem of Arithmetic Every positive integer $n > 1$ is either a prime number or can be factored into a product of prime numbers. Furthermore, the factorization is unique except for the order in which the factors are written, that is, in any two factorizations of n into primes, every prime p occurs the same number of times in each factorization.

Proof. We already have seen that n can be factored in at least one way (see the proof of Theorem 2.22), so we need only prove uniqueness. Suppose that a positive integer $n > 1$ can be represented as a product of primes in two different ways as

$$p_1 p_2 \cdots p_j = n = q_1 q_2 \cdots q_k,$$

where, without loss of generality, we may assume that

$$1 \le j \le k, \quad p_1 \le p_2 \le \cdots \le p_j, \quad q_1 \le q_2 \le \cdots \le q_k.$$

Using Corollary 3.17, we find that

$$p_1 | n \;\Rightarrow\; p_1 | q_1 q_2 \cdots q_k \;\Rightarrow\; p_1 = q_i \text{ for some } 1 \le i \le k \;\Rightarrow\; p_1 \ge q_1;$$
$$q_1 | n \;\Rightarrow\; q_1 | p_1 p_2 \cdots p_j \;\Rightarrow\; q_1 = p_i \text{ for some } 1 \le i \le j \;\Rightarrow\; q_1 \ge p_1.$$

It follows that $p_1 = q_1$. We then have $p_2 p_3 \cdots p_j = q_2 q_3 \cdots q_k$, and the same argument can be repeated to show that $p_2 = q_2$. Continuing this process reveals that $p_i = q_i$ for $1 \le i \le j$. Now suppose that $j < k$. Then the last step leaves us with the equation $1 = q_{j+1} \cdots q_k$, a contradiction to the fact that the q_i's are primes. It follows that $j = k$ and the proof is complete. ■

Collecting like primes, this theorem says that any integer $n > 1$ can be expressed uniquely in the form $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, where $p_1 < p_2 < \cdots < p_k$ are distinct primes and the e_i's are positive integers. Often we wish to compare the prime factorizations of different integers. If we have two (positive) integers, say a and b, the prime factorization of a may use a different set of primes than the prime factorization of b; that is, some prime p may occur in the prime factorization of a but not b (or vice versa). If we wish to use the same set of primes in both factorizations, we simply include $p^0 = 1$ in the prime factorization of b. For example, if a factors as $2^2 \cdot 3^5 \cdot 7^3$ and b factors as $3^2 \cdot 5^4 \cdot 11^3$, then we can write

$$a = 2^2 \cdot 3^5 \cdot 5^0 \cdot 7^3 \cdot 11^0;$$
$$b = 2^0 \cdot 3^2 \cdot 5^4 \cdot 7^0 \cdot 11^3.$$

Such representations are not unique, of course, though they are unique except for the primes that appear with exponent 0. When using an expression like $p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$, be sure that you make clear whether or not the e_i's are positive or merely nonnegative; if the latter, remember not to invoke more uniqueness than is justified. Here's a simple but useful theorem that uses this approach.

THEOREM 3.31 If a and b are positive integers with prime factorizations $a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ and $b = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$ (where the p_i's are distinct and the exponents are nonnegative), then a divides b if and only if $e_i \le f_i$ for every i from 1 to k.

Proof. Suppose first that a divides b. Then there exists an integer x such that $ax = b$. Any prime that divides x must also divide b so we know that x must have the form $x = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}$, where $t_i \ge 0$ for each i. Since

$$ax = (p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k})(p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}) = p_1^{e_1+t_1} p_2^{e_2+t_2} \cdots p_k^{e_k+t_k}$$

and this product must be b, we find that $e_i + t_i = f_i$ for each i. Since $t_i \ge 0$ for each i, it follows that $e_i \le f_i$ for each i.

Now suppose that $e_i \le f_i$ for each i and let $t_i = f_i - e_i$ for each i. The number $x = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}$ is an integer since each t_i is nonnegative and it is clear that $ax = b$. By definition, a divides b. ■

Prime factorizations can be useful for finding greatest common divisors and least common multiples. These results, which are probably familiar to you, are given in the next two theorems.

THEOREM 3.32 Suppose integers a and b have prime factorizations $a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ and $b = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$, where the p_i's are distinct and the exponents are nonnegative. Then

- **a)** A positive integer $d = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}$ is a common divisor of a and b if and only if the inequality $t_i \le \min\{e_i, f_i\}$ is valid for $1 \le i \le k$.
- **b)** $(a, b) = p_1^{\min\{e_1, f_1\}} p_2^{\min\{e_2, f_2\}} \cdots p_k^{\min\{e_k, f_k\}}$.
- **c)** Every common divisor of a and b divides (a, b).

Proof. Although the notation is admittedly rather formidable, this result is a simple consequence of Theorem 3.31, which states that one number divides another if and only if the primes in the factorization of the first are present to lower powers than those in the second. Consequently, if d is a common divisor of a and b, then any prime in its factorization must occur less often (or equally) than it occurs in either the factorization of a or the factorization of b. This proves part (a). To determine the largest possible common factor, we clearly should choose the largest exponent possible for each prime; this is exactly what part (b) says. Finally, part (c) follows immediately from part (a), part (b), and Theorem 3.31. ■

THEOREM 3.33 Suppose integers a and b have prime factorizations $a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ and $b = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$, where the p_i's are distinct and the exponents are nonnegative. Then

a) A positive integer $m = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}$ is a common multiple of a and b if and only if the inequality $t_i \geq \max\{e_i, f_i\}$ is valid for $1 \leq i \leq k$.

b) $[a, b] = p_1^{\max\{e_1, f_1\}} p_2^{\max\{e_2, f_2\}} \cdots p_k^{\max\{e_k, f_k\}}$.

c) $[a, b]$ divides every common multiple of a and b.

Proof. The proof is left as an exercise. We note in passing that common multiples of a and b may involve primes other than the p_i's that appear in the statement of the theorem. In other words, common multiples of a and b may have the form $p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k} x$, where $(x, p_i) = 1$ for each i. ■

Notice that part (c) of both theorems is simply a restatement of portions of Theorems 3.25 and 3.28. However, it is interesting to see a different approach for proving these results. You may have used the ideas presented in these theorems to compute greatest common divisors and least common multiples in the past. For example, suppose that

$$a = 2^1 \cdot 3^3 \cdot 5^3 \cdot 13^0 \cdot 17^4 \cdot 23^3;$$
$$b = 2^2 \cdot 3^0 \cdot 5^6 \cdot 13^2 \cdot 17^0 \cdot 23^5.$$

By considering the sizes of the exponents, it then follows that

$$(a, b) = 2^1 \cdot 3^0 \cdot 5^3 \cdot 13^0 \cdot 17^0 \cdot 23^3;$$
$$[a, b] = 2^2 \cdot 3^3 \cdot 5^6 \cdot 13^2 \cdot 17^4 \cdot 23^5.$$

We note in passing that $(a, b) \cdot [a, b]$ is clearly equal to ab.

Exercises 3.6.

1. Let T be the set defined at the beginning of the section.

a) Find all of the elements of the set T that are composite in T and less than 100.

b) Find an element of T other than 100 that has two distinct prime factorizations. Can you find an example that does not involve a perfect square?

2. Let $a = 2 \cdot 3^2 \cdot 7^3 \cdot 13^4$ and $b = 2^5 \cdot 3^2 \cdot 5 \cdot 7^2 \cdot 11^3$. Find (a, b), $[a, b]$, and ab. (As should be clear, represent your answers as products.)

3. Let $a, b \in \mathbb{Z}^+$ and let p be a prime. Suppose that $(a, p^3) = p^2$ and $(b, p^3) = p$. Find $(a + b, p^3)$.

4. Prove Theorem 3.33.
5. Use theorems in this section to carefully prove Theorem 3.29.
6. Let $a = 3^2 \cdot 5 \cdot 7^3 \cdot 13$ and $b = 2^2 \cdot 3^2 \cdot 5^2 \cdot 7^3 \cdot 11 \cdot 13^4$. Show that $a|b$ by finding an x such that $b = ax$.
7. Suppose $a = 2^{e_1}3^{e_2} \cdots p_k^{e_k}$, where $\{p_i\}$ is a listing of the primes in increasing order, the exponents e_i are nonnegative, and k is some positive integer. Describe conditions on the exponents in the prime factorization of a that are equivalent to the following statements.
   a) a is even
   b) a is odd
   c) a is a perfect square
   d) a is a perfect cube
   e) a is square-free (the only divisor of a which is a perfect square is 1)
8. Suppose that a and b are positive integers. Prove that $a|b$ if and only if $a^2|b^2$.
9. Let p, q, and r be distinct primes and let $a = p^2qr^3$. Carefully list all of the positive divisors of a.
10. Suppose that $a = p_1^{e_1}p_2^{e_2} \cdots p_k^{e_k}$, where the p_i's are distinct primes and the e_i's are positive integers. How many positive divisors does a have?
11. When does a positive integer a have an odd number of positive divisors?
12. Suppose that $[a, b] = a^2$. What can you conclude?
13. Find the smallest positive integer x such that $2x$ is a perfect square and $3x$ is a perfect cube; prove that it is the smallest.
14. **a)** Show that $10|a^2$ implies $10|a$.
    b) What positive integers n have the property that for all $a \in \mathbb{N}$, $n|a^2$ implies $n|a$?
15. Determine the number of zeros on the end of 2015! when it is written in standard base ten form.
16. Suppose that n is a positive integer that is not a perfect square. Prove that $\sqrt{n}$ is an irrational number.

3.7 Wilson's Theorem and Euler's Theorem

In this section, we want to look more carefully at $\mathbb{U}_n$. To aid in this investigation, we introduce a new quantity, the **Euler phi function**, written $\phi(n)$, for positive integers n. This is a rather remarkable function, but we only need a few of its more basic properties for our purposes.

DEFINITION 3.34 Let n be a positive integer. The Euler phi function, denoted by the symbol $\phi(n)$, represents the number of positive integers less than or equal to n that are relatively prime to n. In other words, for each $n > 1$ the value of $\phi(n)$ is the number of elements in the set $\mathbb{U}_n$.

It is easy to verify that $\phi(1) = 1$, $\phi(2) = 1$, $\phi(4) = 2$, $\phi(12) = 4$, $\phi(15) = 8$, and $\phi(17) = 16$. (By the way, what makes $\phi(1)$ somewhat unusual?) In general, if p is a prime, then $\phi(p) = p - 1$ because 1, 2, ..., $p - 1$ are all relatively prime to p but p is not. The number $\phi(n)$ turns out to have a remarkably simple form; that is, there is a simple formula that gives the value of $\phi(n)$ for any positive integer n. Stating and proving this formula is the goal of the next few results.

THEOREM 3.35 If p is a prime and e is a positive integer, then $\phi(p^e) = p^e - p^{e-1}$.

Proof. Let p be a prime and let e be a positive integer. To find $\phi(p^e)$, we need to calculate the number of positive integers less than or equal to p^e that are relatively prime to p^e. As is often the case, it turns out to be easier to calculate the number that are *not* relatively prime to p^e, and subtract from the total. The positive integers less than or equal to p^e are 1, 2, ..., p^e; there are p^e

of these integers. The numbers that are not relatively prime to p^e must be multiples of p, namely any number in the set $\{kp : 1 \le k \le p^{e-1}\}$. Since there are p^{e-1} numbers in this set, we find that $\phi(p^e) = p^e - p^{e-1}$. ■

For example, we see that $\phi(32) = 32 - 16 = 16$ and that $\phi(125) = 125 - 25 = 100$. As we will prove below, it turns out that $\phi(ab) = \phi(a)\phi(b)$ when a and b are relatively prime. Using this fact, we find that

$$\phi(4000) = \phi(2^5 \cdot 5^3) = \phi(2^5) \cdot \phi(5^3) = 16 \cdot 100 = 1600.$$

It is certainly evident how much easier it is to compute $\phi(4000)$ using these results than to use a direct approach. Note that once again, we are reducing a problem about positive integers to one for prime numbers.

LEMMA 3.36 Suppose that b and e are positive integers and that p is a prime. If b and p are relatively prime, then $\phi(bp^e) = \phi(b)\phi(p^e)$.

Proof. Let p be a prime and let e be a positive integer. There is nothing to prove when $b = 1$ so assume that $b > 1$ and $(b, p) = 1$, and let $n = bp^e$. We proceed to count the number of positive integers less than or equal to n that are not relatively prime to n. As a start, note that for $1 \le k \le n$,

$$(n, k) \neq 1 \quad \Leftrightarrow \quad \begin{cases} (b, k) \neq 1; \\ (b, k) = 1 \text{ and } (p, k) = p; \end{cases}$$

where the two options are mutually exclusive. To count these values, we list the numbers $1, 2, \ldots, n$ in p^e rows of b numbers each:

$$\begin{aligned} &1,\ 2,\ \ldots,\ b\,; \\ &b+1,\ b+2,\ \ldots,\ 2b\,; \\ &2b+1,\ 2b+2,\ \ldots,\ 3b\,; \\ &\quad\vdots \\ &(p^e-1)b+1,\ (p^e-1)b+2,\ \ldots,\ p^e b\,. \end{aligned}$$

To determine those values of k for which $(b, k) \neq 1$, we note that each row can be used to form a representation of $\mathbb{Z}_b$ (by writing i as $[i]$) and thus contains $b - \phi(b)$ values of k for which $(b, k) \neq 1$. It follows that there are a total of $p^e(b - \phi(b))$ values for integers k with $(b, k) \neq 1$. Now suppose that $(b, k) = 1$ and $(p, k) = p$. Then $k = xp$, where $(x, b) = 1$ and $1 \le x \le bp^{e-1}$. Referring once again to the listing given above, each row contains $\phi(b)$ integers that are relatively prime to b (those values of i for which $[i] \in \mathbb{U}_b$). Multiplying each of these numbers that appear in the first p^{e-1} rows by p generates a value of k for which $1 \le k \le n$, $(b, k) = 1$, and $(p, k) = p$. We thus find that there are $p^{e-1}\phi(b)$ values of k with this property. Putting this information together yields

$$\begin{aligned} \phi(bp^e) = \phi(n) &= n - p^e(b - \phi(b)) - p^{e-1}\phi(b) \\ &= n - bp^e + p^e\phi(b) - p^{e-1}\phi(b) \\ &= \phi(b)\big(p^e - p^{e-1}\big) = \phi(b)\phi(p^e), \end{aligned}$$

where the last step uses Theorem 3.35. ■

THEOREM 3.37 If $a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, where the p_i's are distinct primes and the e_i's are positive, then

$$\phi(a) = \prod_{i=1}^{k} (p_i^{e_i} - p_i^{e_i - 1}).$$

Proof. This result is a simple consequence of the Principle of Mathematical Induction, where the value of n represents the number of distinct primes in the product. When $n = 1$, the equation follows immediately from Theorem 3.35. Now suppose that the result holds for a product involving n distinct primes, where n is some positive integer. Consider the integer $a = \prod_{i=1}^{n+1} p_i^{e_i}$, where the p_i's are prime and the e_i's are positive. Note that the integers $\prod_{i=1}^{n} p_i^{e_i}$ and p_{n+1} are relatively prime. Using the lemma, the inductive hypothesis, and Theorem 3.35, we obtain

$$\phi(a) = \phi\Big(\prod_{i=1}^{n} p_i^{e_i}\Big)\phi(p_{n+1}^{e_{n+1}}) = \Big(\prod_{i=1}^{n} (p_i^{e_i} - p_i^{e_i - 1})\Big)(p_{n+1}^{e_{n+1}} - p_{n+1}^{e_{n+1}-1}) = \prod_{i=1}^{n+1} (p_i^{e_i} - p_i^{e_i - 1}).$$

This shows that the equation is valid for a product involving $n + 1$ distinct primes. The result now follows by the Principle of Mathematical Induction. ∎

COROLLARY 3.38 If a and b are relatively prime positive integers, then $\phi(ab) = \phi(a)\phi(b)$.

Proof. A proof of the corollary will be left as an exercise. ∎

Since every positive integer $n > 1$ can be written as a product of primes, Theorem 3.37 shows how to determine $\phi(n)$ for any positive integer $n > 1$. For example,

$$\phi(600) = \phi(2^3 \cdot 3 \cdot 5^2) = (2^3 - 2^2)(3 - 1)(5^2 - 5) = 160.$$

This is another illustration of how the prime numbers can be viewed as the building blocks for the positive integers; once we know how the Euler phi function behaves for prime numbers, we know how it behaves for all positive integers. Of course, there is the difficult computational problem of determining the prime factorizations of large integers, but that is an entirely different matter.

The defining characteristic of $\mathbb{U}_n$ is that every element has a unique multiplicative inverse (see Theorem 3.22). It is quite possible for an element of $\mathbb{U}_n$ to be its own inverse; for example, in $\mathbb{U}_{12}$, each of the elements [1], [5], [7], and [11] is its own inverse. This stands in contrast to arithmetic in $\mathbb{Z}$ or $\mathbb{R}$, where the only solutions to $x^2 = 1$ are ± 1. If n is prime, then this familiar fact is true in $\mathbb{U}_n$ as well.

THEOREM 3.39 If p is a prime, then the only elements of $\mathbb{U}_p$ which are their own inverses are $[1]$ and $[p - 1] = [-1]$.

Proof. Let p be a prime. It is certainly clear that $[1]$ and $[-1]$ are their own inverses in $\mathbb{U}_p$. Suppose that $[u] \in \mathbb{U}_p$ is its own inverse. The fact that $[u] \cdot [u] = [1]$ in $\mathbb{U}_p$ is equivalent to the statement $u^2 \equiv 1 \pmod{p}$. This means that $p|(u - 1)(u + 1)$. By Corollary 3.15, we know that either $p|(u - 1)$ or $p|(u + 1)$, which implies that either $[u] = [1]$ or $[u] = [-1]$, respectively. ∎

If $p > 2$ is prime, then $\mathbb{U}_p = \{[1], [2], \ldots, [p-1]\}$. Note that $\mathbb{U}_p$ contains an even number of elements since p is odd. The elements [2], [3], ..., $[p-2]$ all have unique inverses different from themselves, so it must be possible to pair up each element in this list with its inverse from the list. This means that if we multiply all of [2], [3], ..., $[p-2]$ together, we must get [1]. Illustrating this fact for $p = 11$, the pairing would be

$$\begin{aligned}[2] \cdot [3] \cdot [4] \cdot [5] \cdot [6] \cdot [7] \cdot [8] \cdot [9] &= ([2] \cdot [6]) \cdot ([3] \cdot [4]) \cdot ([5] \cdot [9]) \cdot ([7] \cdot [8]) \\ &= [1] \cdot [1] \cdot [1] \cdot [1] = [1].\end{aligned}$$

This observation suggests the following result, called **Wilson's Theorem**.

THEOREM 3.40 Wilson's Theorem If p is a prime, then $(p-1)! \equiv -1 \pmod{p}$.

Proof. The result is trivial for $p = 2$ and $p = 3$. Suppose that $p \geq 5$ is a prime and use the observation preceding the theorem to obtain

$$[(p-1)!] = [1] \cdot \big([2] \cdot [3] \cdot \cdots \cdot [p-2]\big) \cdot [p-1] = [1] \cdot \big([1]\big) \cdot [-1] = [-1].$$

It follows that $(p-1)! \equiv -1 \pmod{p}$. ■

To illustrate Wilson's Theorem with some simple examples, note that $4! + 1 = 25$ is a multiple of 5, $6! + 1 = 721$ is a multiple of 7, and that $10! + 1 = 3628801$ is divisible by 11. (How can you check this last divisibility result quickly?)

Similar in spirit to Wilson's Theorem, and very useful, is **Euler's Theorem** and its special case known as **Fermat's Little Theorem**. To motivate these results, let $n > 1$ be a positive integer and let $[u] \in \mathbb{U}_n$. Since the set $\{[u]^i : i \in \mathbb{Z}^+\}$ is a subset of $\mathbb{U}_n$ and since $\mathbb{U}_n$ contains at most $n-1$ elements, there must be distinct positive integers i and j such that $[u]^i = [u]^j$. Assuming that $j > i$, we find that $[u]^{j-i} = [1]$. In other words, for each $[u] \in \mathbb{U}_n$, there exists a positive integer k such that $[u]^k = [1]$. Euler's Theorem specifies a value of k with this property.

THEOREM 3.41 Euler's Theorem If n is a positive integer and $\gcd(u, n) = 1$, then $u^{\phi(n)} \equiv 1 \pmod{n}$.

Proof. The result is trivial when $n = 1$ so suppose that $n > 1$ and let $k = \phi(n)$. Since u and n are relatively prime, we know that $[u] \in \mathbb{U}_n$. If $[a_1], \ldots, [a_k]$ is a list of the elements of $\mathbb{U}_n$, then by Theorem 3.24 in Section 3.4, the collection $[u] \cdot [a_1], [u] \cdot [a_2], \ldots, [u] \cdot [a_k]$ is also a list of the elements of $\mathbb{U}_n$. Multiplying these two collections of terms together gives

$$[a_1] \cdot [a_2] \cdot \cdots \cdot [a_k] = ([u] \cdot [a_1]) \cdot ([u] \cdot [a_2]) \cdot \cdots \cdot ([u] \cdot [a_k]) = [u]^k \cdot [a_1] \cdot [a_2] \cdot \cdots \cdot [a_k].$$

Let $b = a_1 a_2 \cdots a_k$. Then $[b] \in \mathbb{U}_n$ and the displayed equation can be written as $[b] = [u]^k \cdot [b]$. Multiplying both sides of this equation by $[b]^{-1}$, we find that $[u]^k = [1]$. Given the value of k, it follows that $u^{\phi(n)} \equiv 1 \pmod{n}$. ■

COROLLARY 3.42 Fermat's Little Theorem Suppose that p is a prime and a is an integer. Then

a) $a^{p-1} \equiv 1 \pmod{p}$ if a and p are relatively prime;

b) $a^p \equiv a \pmod{p}$ for any a.

Proof. Since p is a prime, we know that $\phi(p) = p - 1$. If $(a, p) = 1$, then Euler's Theorem gives part (a). Multiplying both sides of $a^{p-1} \equiv 1 \pmod{p}$ by a gives $a^p \equiv a \pmod{p}$. If $(a, p) \neq 1$, then p divides both a and a^p. It follows easily that $a^p \equiv a \pmod{p}$. ■

To illustrate Euler's Theorem, note that

$$3^{\phi(8)} = 3^4 = 81 \equiv 1 \pmod{8} \qquad \text{and} \qquad 5^{\phi(14)} = 5^6 = (25)^3 = (-3)^3 \equiv -27 \equiv 1 \pmod{14}.$$

The second example indicates how modular arithmetic can simplify computations. Using similar ideas to avoid large numbers, we can verify Fermat's Little Theorem with $p = 17$:

$$\begin{aligned} 2^{16} &\equiv \left(2^4\right)^4 \equiv (-1)^4 \equiv 1; \\ 5^{16} &\equiv \left(5^2\right)^8 \equiv (8)^8 \equiv \left(2^4\right)^6 \equiv (-1)^6 \equiv 1; \\ 10^{16} &\equiv 2^{16} \cdot 5^{16} \equiv 1; \\ 7^{16} &\equiv (-10)^{16} \equiv 1. \end{aligned}$$

Notice that $2^8 \equiv 1 \pmod{17}$ and thus $4^4 \equiv 1 \pmod{17}$. In other words, Euler's Theorem gives a value of k for which $u^k \equiv 1 \pmod{n}$ but not necessarily the smallest such value. Finally, working with congruence modulo 7, we can verify part (b) of Fermat's Little Theorem:

$$\begin{aligned} 3^7 &\equiv 2187 \equiv 3 \pmod{7}; && \text{(the long way)} \\ 5^7 &\equiv (-2)(2^3)^2 \equiv -2 \equiv 5 \pmod{7}. && \text{(a shorter way)} \end{aligned}$$

It is good practice to do these computations without a calculator and looking for shortcuts.

Leonhard Euler. Euler (pronounced "oiler") was born in Basel in 1707 and died in 1783, following a life of stunningly prolific mathematical work. His complete bibliography runs to nearly 900 entries; his research amounted to some 800 pages a year over the whole of his career. He continued doing research right up until his sudden death while relaxing with a cup of tea. For almost all of the last 17 years of his life he was totally blind.

The breadth of Euler's knowledge may be as impressive as the depth of his mathematical work. He had a great facility with languages, and studied theology, medicine, astronomy, and physics. His first appointment was in medicine at the recently established St. Petersburg Academy. On the day that he arrived in Russia, the academy's patron, Catherine I, died, and the academy itself just managed to survive the transfer of power to the new regime. In the process, Euler ended up in the chair of natural philosophy instead of medicine.

Euler is best remembered for his contributions to analysis and number theory, especially for his use of infinite processes of various kinds (infinite sums and products, continued fractions), and for establishing much of the modern notation of mathematics. Euler originated the use of e for the base of the natural logarithms and i for $\sqrt{-1}$; the symbol π has been found in a book published in 1706, but it was Euler's adoption of the symbol, in 1737, that made it standard. He was also responsible for the use of $\sum$ to represent a sum, and for the modern notation for a function, $f(x)$.

Euler's greatest contribution to mathematics was the development of techniques for dealing with infinite operations. In the process, he established what has ever since been called the field of **analysis**, which includes and extends the differential and integral calculus of Newton and Leibniz. For example, by treating the familiar functions $\sin x$, $\cos x$, and e^x analytically (as infinite series), Euler could easily establish identities that became fundamental tools in analysis. One such is the well-known $e^{ix} = \cos x + i \sin x$; substituting $x = \pi$ gives $e^{i\pi} = -1$ or $e^{i\pi} + 1 = 0$, a remarkable equation containing perhaps the five most important constants in analysis.

Euler used infinite series to establish and exploit some remarkable connections between analysis and number theory. Many talented mathematicians before Euler had failed to discover the value of the sum of the reciprocals of the squares: $1^{-2} + 2^{-2} + 3^{-2} + \cdots$. Using the infinite series for $\sin x$, and assuming that it behaved like a finite polynomial, Euler showed that the sum is $\pi^2/6$. Euler's uncritical application of ordinary algebra to infinite series occasionally led him into trouble, but his results were overwhelmingly correct, and were later justified by more careful techniques as the need for increased rigor in mathematical arguments became apparent. We'll see Euler's name more than once in the remainder of the chapter.

The information here is taken from *A History of Mathematics*, by Carl Boyer, New York: John Wiley & Sons, 1968.

Exercises 3.7.

1. Verify the biconditional statement that is used in the proof of Lemma 3.36.

2. Prove Corollary 3.38.

3. Find $\phi(n)$ for each value of n.

a) $n = 49$ **b)** $n = 125$ **c)** $n = 222$

d) $n = 616$ **e)** $n = 980$ **f)** $n = 3^4 \cdot 7^3 \cdot 13^2$

4. Find a value of n for which $\phi(n) = 200$.

5. For $p = 13$ and $p = 19$, find the pairing of elements in $\mathbb{U}_p$ that is used implicitly in the proof of Wilson's Theorem.

6. Prove that if $e > 2$, then $\mathbb{U}_{2^e}$ has an element, other than $[2^e - 1]$ and $[1]$, which is its own inverse.

7. Let p be a prime and let $e > 0$. Suppose that $\mathbb{U}_{p^e}$ has an element other than $[p^e - 1]$ and $[1]$ which is its own inverse. Prove that $p = 2$.

8. Find all positive integers n which are the products of their proper positive divisors.

9. Suppose that $n > 4$ is a composite number. Prove that $(n-1)! \equiv 0 \pmod{n}$. (Compare this result with Wilson's Theorem.)

10. Verify Euler's Theorem in the following cases:

a) $u = 3$, $n = 10$ **b)** $u = 5$, $n = 6$ **c)** $u = 2$, $n = 15$

11. Verify Fermat's Little Theorem modulo 11 for the numbers 1 through 10. Do all of your computations without a calculator, using congruence properties as much as possible.

12. Suppose $n > 0$ and u is relatively prime to n.

a) If $m > 0$ and $\phi(n)|m$, prove that $u^m \equiv 1 \pmod{n}$.

b) If $m > 0$ is relatively prime to $\phi(n)$ and $u^m \equiv 1 \pmod{n}$, prove that $u \equiv 1 \pmod{n}$.

13. Let a and c be positive integers. Prove that the number $ac(c^4 - a^4)$ is divisible by 5.

14. Simplify each of the following.

a) $43! \pmod{47}$ **b)** $3^{70} \pmod{79}$ **c)** $2^{19} + 3^{21} \pmod{19}$

15. Solve the congruence $16x \equiv 75! \pmod{79}$.

16. Let p be a fixed prime. Use mathematical induction to prove that $n^p \equiv n \pmod{p}$ for each positive integer n and thus give an alternative proof of Fermat's Little Theorem.

3.8 Quadratic Residues

The prime numbers, their properties, and their relation to the composite numbers have fascinated mathematicians for thousands of years. A list of these results would fill volumes and new facts are continuing to be discovered. In this section and the next, we provide a glimpse into some of the problems that have been considered.

Most everyone is familiar with perfect squares. The list of perfect squares goes on indefinitely:

$$1,\ 4,\ 9,\ 16,\ 25,\ 36,\ 49,\ 64,\ 81,\ 100,\ 121,\ 144,\ 169,\ 196,\ 225,\ \ldots$$

Is it possible to extend the notion of perfect square to $\mathbb{Z}_n$? To determine the nature of this problem, we begin by considering the 1's digit of perfect squares. By one of the exercises in Section 3.1, any perfect square must end in 0, 1, 4, 5, 6, or 9. To verify this, we simply need to determine what happens in $\mathbb{Z}_{10}$:

$$\begin{aligned} [0]^2 &= [0], & [5]^2 &= [5], \\ [1]^2 &= [1], & [6]^2 &= [6], \\ [2]^2 &= [4], & [7]^2 &= [9], \\ [3]^2 &= [9], & [8]^2 &= [4], \\ [4]^2 &= [6], & [9]^2 &= [1]. \end{aligned}$$

As an illustration of this result, we immediately know that 56847 is not a perfect square. Another way to phrase what we have just done is to say that [0], [1], [4], [5], [6], and [9] are squares in $\mathbb{Z}_{10}$ and that [2], [3], [7], and [8] are not squares in $\mathbb{Z}_{10}$.

For a simpler, but slightly more abstract example, we can look at squares in $\mathbb{Z}_4$:

$$\begin{aligned} [0]^2 &= [0], & [2]^2 &= [0], \\ [1]^2 &= [1], & [3]^2 &= [1]. \end{aligned}$$

It follows that any perfect square has a remainder of 0 or 1 when divided by 4. (See Theorem 3.4 in Section 3.1.) In other words, [0] and [1] are squares in $\mathbb{Z}_4$, and [2] and [3] are not squares in $\mathbb{Z}_4$. The notion of quadratic residues extends this idea, but it does so with a focus on prime numbers.

DEFINITION 3.43 Suppose that p is an odd prime and that b and p are relatively prime. Then b is a **quadratic residue** modulo p if and only if the equation $x^2 \equiv b \pmod{p}$ has a solution. If the equation has no solution, then we say that b is a **quadratic nonresidue** modulo p.

This definition merely says that b is a quadratic residue modulo p if some perfect square (a quadratic) has a remainder (a residue) of b when divided by p. To phrase it another way, a quadratic residue is a "perfect square" in the world of modular arithmetic. However, by insisting that $\gcd(b, p) = 1$, we are excluding the trivial case of 0. An equivalent way of stating this is to say that b is a quadratic residue modulo p if the equation $[x]^2 = [b]$ has a solution in $\mathbb{U}_p$.

Given the equation $x^2 \equiv b \pmod{p}$, we may, without loss of generality, assume that $1 \leq b < p$ and seek solutions x that satisfy $1 \leq x < p$. Hence, to find the quadratic residues of a prime number p, we simply need to check the squares of the numbers $1, 2, \ldots, p-1$. Since p is an odd prime, this is equivalent to checking the squares of the numbers $\pm 1, \pm 2, \ldots, \pm(p-1)/2$. Using this idea, it is easy to check that the quadratic residues of 7 are 1, 2, and 4, and that the quadratic residues of 11 are 1, 3, 4, 5, and 9. For a more complicated illustration of the notion of quadratic residue, the equation $13^2 = 169 = 5 \cdot 31 + 14$ reveals that 14 is a quadratic residue modulo 31. The following result indicates how many quadratic residues a prime number may have.

THEOREM 3.44 If p is an odd prime, then exactly half of the numbers $1, 2, 3, \ldots, p-1$ are quadratic residues modulo p. In other words, half of the elements of $\mathbb{U}_p$ are perfect squares in $\mathbb{U}_p$.

Proof. Let p be an odd prime. To determine the quadratic residues of p, we need to compute the numbers $x^2 \pmod{p}$ as x runs through the integers 1 to $p-1$. Since $x^2 \equiv (p-x)^2$ for any integer x, at most half of the elements that belong to the set $\{1, 2, 3, \ldots, p-1\}$ are quadratic residues modulo p. The result then follows from the fact that $x^2 \equiv y^2$ implies $y \equiv x$ or $y \equiv p - x$. The details are left as an exercise. ■

For small primes, it is not difficult to find all of the quadratic residues by computing squares. However, to determine whether or not, say, 111 is a quadratic residue of the prime 947 would be rather challenging to attempt by brute force (that is, to write out all of the possible options for squares in $\mathbb{U}_{947}$). It is thus convenient to have an easy and arithmetic way to identify whether a given integer b is a quadratic residue of a prime p. It turns out to be most useful to define a function $\mathrm{QR}(b, p)$ that gives the quadratic character of b modulo p. We write $\mathrm{QR}(b, p) = 1$ when b is a quadratic residue modulo p and $\mathrm{QR}(b, p) = -1$ when it is not. The standard notation for this function is the **Legendre symbol**:

$$\mathrm{QR}(b, p) = \left(\frac{b}{p}\right), \quad \text{where} \quad \left(\frac{b}{p}\right) = \begin{cases} 1, & \text{if } x^2 \equiv b \pmod{p} \text{ has a solution;} \\ -1, & \text{if } x^2 \equiv b \pmod{p} \text{ does not have a solution.} \end{cases}$$

We should emphasize here that the notation "QR" is completely nonstandard, introduced in the hope that first expressing this concept as a function makes the idea easier to understand. The Legendre symbol is not an ideal choice, since it looks exactly like a fraction, but it is the standard notation used in number theory. Whenever this notation is used, it is implicitly assumed that p is an odd prime and that b and p are relatively prime.

The following result is known as **Euler's Criterion**. It states that $\left(\frac{b}{p}\right) \equiv b^{(p-1)/2} \pmod{p}$ when b and p are relatively prime. To illustrate the ideas used in the proof for a particular case, let $b = 7$ and $p = 13$. We then list all of the solutions to the equation $xy \equiv 7 \pmod{13}$ for values of x and y between 1 and 12:

$$1 \cdot 7 \equiv 7; \quad 2 \cdot 10 \equiv 7; \quad 4 \cdot 5 \equiv 7; \quad 3 \cdot 11 \equiv 7; \quad 6 \cdot 12 \equiv 7; \quad 8 \cdot 9 \equiv 7.$$

Multiplying all these equations together gives $12! \equiv 7^6 \pmod{13}$ and thus $-1 \equiv 7^{(13-1)/2} \pmod{13}$ by Wilson's Theorem. Since $x \neq y$ for each pair of products, we see that 7 is a quadratic nonresidue of 13, that is, $-1 = \left(\frac{7}{13}\right) \equiv 7^{(13-1)/2} \pmod{13}$. Now let $b = 3$ and $p = 13$. The solutions to the equation $xy \equiv 3 \pmod{13}$ in this case are:

$$4 \cdot 4 \equiv 3; \quad 9 \cdot 9 \equiv 3; \quad 1 \cdot 3 \equiv 3; \quad 2 \cdot 8 \equiv 3; \quad 5 \cdot 11 \equiv 3; \quad 6 \cdot 7 \equiv 3; \quad 10 \cdot 12 \equiv 3.$$

It is clear that 3 is a quadratic residue of 13 since there are two solutions to $x^2 = 3 \pmod{13}$. Putting in the proper numbers and using Wilson's Theorem once again, we find that

$$-1 \equiv 12! \equiv 4 \cdot 9 \cdot 3^5 \equiv 4 \cdot (-4) \cdot 3^5 \equiv (-1)3 \cdot 3^5 \equiv (-1)3^6 \pmod{13}.$$

It follows that $1 = \left(\frac{3}{13}\right) \equiv 3^{(13-1)/2} \pmod{13}$. The proof of Euler's Criterion merely extends these ideas to the general case. As indicated by the above examples, for each integer $x \in \{1, 2, 3, \ldots, p-1\}$ there is a unique integer $y \in \{1, 2, 3, \ldots, p-1\}$ such that $xy \equiv b \pmod{p}$. If b is a quadratic residue modulo p, then y may be equal to x, but if b is not a quadratic residue modulo p, then x and y are always distinct. We leave a proof of this fact as an exercise.

THEOREM 3.45 Euler's Criterion Suppose that p is an odd prime and that b is an integer. If b and p are relatively prime, then

$$\left(\frac{b}{p}\right) \equiv b^{(p-1)/2} \pmod{p}.$$

Proof. Although it is not necessary, we can, without loss of generality, assume that $1 \leq b \leq p-1$. We first note that $(p-1)/2$ is an integer since p is odd and that $b^{p-1} \equiv 1 \pmod{p}$ by Fermat's Little Theorem. It follows that p divides the product

$$\left(b^{(p-1)/2} - 1\right)\left(b^{(p-1)/2} + 1\right),$$

which means that either $b^{(p-1)/2} \equiv 1 \pmod{p}$ or $b^{(p-1)/2} \equiv -1 \pmod{p}$. This shows that the conclusion of the theorem makes sense; both sides assume the values ± 1.

Suppose that b is a quadratic nonresidue modulo p. Then the numbers 1, 2, ..., $p-1$ can be grouped into $(p-1)/2$ pairs $\{x_i, y_i\}$ with $x_i y_i \equiv b$ and it follows that

$$(p-1)! = \prod_{i=1}^{(p-1)/2} x_i y_i \equiv b^{(p-1)/2} \pmod{p}.$$

By Wilson's Theorem, we find that $b^{(p-1)/2} \equiv -1 \pmod{p}$, as desired.

Now suppose that b is a quadratic residue modulo p. There are precisely two numbers in $\{1, 2, 3, \ldots, p-1\}$, say c and $p-c$, such that $c^2 \equiv (p-c)^2 \equiv b$. The remaining $p-3$ numbers can be paired up as before. Since $c(p-c) \equiv -c^2 \equiv -b$, we find that

$$(p-1)! = c(p-c) \prod_{i=1}^{(p-3)/2} x_i y_i \equiv (-b)b^{(p-3)/2} = -b^{(p-1)/2}.$$

Using Wilson's Theorem once again, we find that $b^{(p-1)/2} \equiv 1 \pmod{p}$, which agrees with the value of the Legendre symbol. This completes the proof. ■

COROLLARY 3.46 Suppose that p is an odd prime and that $n = \prod_{i=1}^{k} b_i$. If n and p are relatively prime, then

$$\left(\frac{n}{p}\right) = \prod_{i=1}^{k} \left(\frac{b_i}{p}\right).$$

Proof. We first note that the hypotheses imply that p does not divide any of the b_i's. By the theorem, it follows that

$$\left(\frac{n}{p}\right) \equiv n^{(p-1)/2} \equiv \prod_{i=1}^{k} b_i^{(p-1)/2} \equiv \prod_{i=1}^{k} \left(\frac{b_i}{p}\right) \pmod{p}.$$

Now the number represented by

$$\left(\frac{n}{p}\right) - \prod_{i=1}^{k} \left(\frac{b_i}{p}\right)$$

is a multiple of p and can only assume the values 0, -2, or 2. Since p is an odd prime, the value must be 0. ■

To illustrate Euler's Criterion, note that

$$\left(\frac{5}{19}\right) \equiv 5^9 \equiv 5 \cdot (5^2)^4 \equiv 5 \cdot 6^4 \equiv 5 \cdot (-2)^2 \equiv 1;$$
$$\left(\frac{17}{29}\right) \equiv 17^{14} \equiv 289^7 \equiv (-1)^7 \equiv -1.$$

Thus 5 is a quadratic residue modulo 19 (with a little patience, we find that $9^2 \equiv 5 \pmod{19}$) and 17 is a quadratic nonresidue modulo 29. The corollary once again reduces a problem about integers to a problem concerning primes. As an example, the second problem above could be solved as follows:

$$\begin{aligned}\left(\frac{17}{29}\right) = \left(\frac{-12}{29}\right) &= \left(\frac{-1}{29}\right)\left(\frac{4}{29}\right)\left(\frac{3}{29}\right) \\ &\equiv (-1)^{14}(1)(3^{14}) \equiv (3^3)^4 \cdot 3^2 \\ &\equiv (-2)^4 \cdot 3^2 \equiv 144 \equiv -1.\end{aligned}$$

As you can imagine, as the numbers become larger, the computations become more challenging.

The following remarkable result shows how the quadratic character of larger primes can be computed quite easily. This deep result, known as the *Quadratic Reciprocity Theorem*, was discovered (but not proved) by Leonhard Euler. It was proved first by Gauss in the early 1800's and reproved many times thereafter (at least eight different ways by Gauss alone). The beautiful proof of this result given below is due to the brilliant young mathematician Gotthold Eisenstein, who died tragically young, at 29, of tuberculosis. The proof is similar to one by Gauss, but it replaces a complicated lemma by an ingenious geometrical argument. For each real number x, the symbols $\lfloor x \rfloor$ represent the greatest integer less than or equal to x. For example, $\lfloor 58/7 \rfloor = 8$ and $\lfloor \pi \rfloor = 3$.

THEOREM 3.47 Quadratic Reciprocity Theorem If p and q are distinct odd primes, then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)}.$$

Proof. Let p and q be distinct odd primes and let $E = \{2, 4, 6, \ldots, p-1\}$. For each $e \in E$, use the Division Algorithm to write $eq = pn_e + r_e$, where $n_e = \lfloor eq/p \rfloor$ and $1 \leq r_e \leq p-1$. It is easy to verify that $r_e = r_f$ if and only if $e = f$. For each $e \in E$, define

$$s_e = \begin{cases} r_e, & \text{if } r_e \text{ is even;} \\ p - r_e, & \text{if } r_e \text{ is odd;} \end{cases}$$

and note that $\{s_e : e \in E\} \subseteq E$. We claim that these two sets are actually equal. The only way for them not to be equal would be if $r_e = p - r_f$ for distinct integers e and f in E. But then

$$0 \equiv r_e + r_f \equiv q(e+f) \pmod{p},$$

which implies that p divides $e + f$, a contradiction to the fact that $2 < e + f < 2p$ and $e + f$ is even. As we will use this fact momentarily, note that $s_e \equiv (-1)^{r_e} r_e \pmod{p}$ for each $e \in E$.

Let $x = \sum_{e\in E} r_e$ and $y = \sum_{e\in E} n_e$. We claim that $(-1)^x \equiv q^{(p-1)/2} \equiv (-1)^y \pmod{p}$. To see this, first consider the following string of equivalences modulo p:

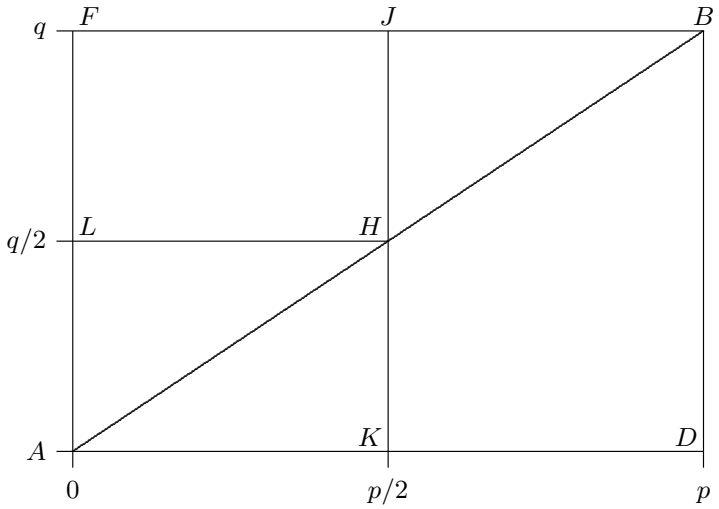
$$\prod_{e\in E} r_e \equiv \prod_{e\in E} eq \equiv q^{(p-1)/2} \prod_{e\in E} e \equiv q^{(p-1)/2} \prod_{e\in E} s_e \equiv q^{(p-1)/2} \prod_{e\in E} (-1)^{r_e} r_e \equiv q^{(p-1)/2}(-1)^x \prod_{e\in E} r_e.$$

Since p does not divide $\prod_{e\in E} r_e$, it follows that $q^{(p-1)/2} \equiv (-1)^x$. We next note that

$$\sum_{e\in E} eq = \sum_{e\in E} (pn_e + r_e) = py + x.$$

Since the sum is even and p is odd, we find that the integers x and y have the same parity (that is, x and y are either both even or both odd) and thus $(-1)^x = (-1)^y$. This establishes the claim. By Euler's Criterion, we conclude that $\left(\frac{q}{p}\right) = (-1)^y$. Note that thus far in the proof, the only property of q that we have used is that q is a positive integer that is relatively prime to p. In particular, the results thus far are valid if $q = 2$.

We have thus reduced the problem of determining $\left(\frac{q}{p}\right)$ to that of determining whether y is even or odd, where $y = \sum_{e \in E} \left\lfloor \frac{eq}{p} \right\rfloor$. For each $e \in E$, we need to count the number of integers k that satisfy $1 \le k < eq/p$. Interpreting an allowed value of e and k as the ordered pair (e, k), we can view the problem as counting lattice points (points with integer coordinates) in a certain region of the plane. In particular, we are interested in lattice points with even abscissas and lying below the line through the origin with slope q/p, that is, lattice points that lie completely inside triangle ABD in the figure.



Note that (excluding the endpoints) there are no integer lattice points on the line segment AB. The number of integer lattice points inside rectangle $ADBF$ with a given integer abscissa is even (namely, $q - 1$), so the number of these points above line AB has the same parity as the number below AB. Suppose $e \in E$ and $e > p/2$. The number of integer lattice points with abscissa e above line AB is the same as the number of integer lattice points with abscissa $p - e$ below AB (via the correspondence $(e, k) \to (p - e, q - k)$). Since $p - e$ is odd,

$$\begin{aligned} y = \sum_{e \in E} \left\lfloor \frac{qe}{p} \right\rfloor &= \sum_{\substack{e < p/2 \\ e \text{ even}}} \left\lfloor \frac{qe}{p} \right\rfloor + \sum_{\substack{e > p/2 \\ e \text{ even}}} \left\lfloor \frac{qe}{p} \right\rfloor \\ &= (\text{the number of lattice points with even abscissa in } AKH) + \\ &\qquad (\text{the number of lattice points with even abscissa in } KDBH) \\ &\equiv (\text{the number of lattice points with even abscissa in } AKH) + \\ &\qquad (\text{the number of lattice points with even abscissa in } HJB) \\ &= (\text{the number of lattice points with even abscissa in } AKH) + \\ &\qquad (\text{the number of lattice points with odd abscissa in } AKH) \\ &= (\text{the number of lattice points in } AKH) \doteq \mu, \end{aligned}$$

where the equivalence on the second line is (mod 2). (The symbol $\doteq$ indicates that we are defining a new variable μ equal to the number of lattice points in AKH.) Since μ and y have the same

parity, we find that $\left(\frac{q}{p}\right) = (-1)^{\mu}$. By an analogous argument, it can be shown that $\left(\frac{p}{q}\right) = (-1)^{\nu}$, where ν is the number of lattice points that lie completely inside triangle ALH. Since there are $\frac{1}{2}(p-1) \cdot \frac{1}{2}(q-1)$ lattice points inside the rectangle $AKHL$, we have

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\mu+\nu} = (-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)}.$$

This completes the proof. ■

Since the Quadratic Reciprocity Theorem does not include the lone even prime 2, its quadratic character is stated in a separate theorem.

THEOREM 3.48 If p is an odd prime, then

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{if } p \equiv \pm 1 \pmod 8; \\ -1, & \text{if } p \equiv \pm 3 \pmod 8. \end{cases}$$

Proof. The proof depends on the observation made at the end of the second paragraph in the proof of the Quadratic Reciprocity Theorem. The details are left as an exercise. ■

The value of $\left(\frac{q}{p}\right)$ is ± 1. Multiplying both sides of the equation in the general theorem by this value gives

$$\left(\frac{p}{q}\right) = (-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)}\left(\frac{q}{p}\right).$$

It may not be immediately apparent how much this equation simplifies the problem of determining quadratic residues. Repeating the examples from above with this new result, we find that

$$\left(\frac{5}{19}\right) = \left(\frac{19}{5}\right) = \left(\frac{4}{5}\right) = 1;$$
$$\left(\frac{17}{29}\right) = \left(\frac{29}{17}\right) = \left(\frac{12}{17}\right) = \left(\frac{4}{17}\right)\left(\frac{3}{17}\right) = \left(\frac{17}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

To show how to handle much larger numbers, suppose we want to determine whether or not 73 is a quadratic residue of 419. Using results in this section, we obtain

$$\left(\frac{73}{419}\right) = \left(\frac{419}{73}\right) = \left(\frac{54}{73}\right) = \left(\frac{9}{73}\right)\left(\frac{2}{73}\right)\left(\frac{3}{73}\right) = \left(\frac{73}{3}\right) = \left(\frac{1}{3}\right) = 1.$$

(Be certain you follow each of the steps that appear in this equation.) In other words, the equation $x^2 \equiv 73 \pmod{419}$ has a solution. (Can you find the value of x that solves this equation?) Although these computations take some care, they are certainly much easier than using Euler's Criterion and attempting to compute 73^{209}.

We have certainly not exhausted the topic of quadratic residues and the ramifications of the Quadratic Reciprocity Theorem, but we have sufficient information to solve an interesting problem. This is the content of the next section.

Ferdinand Gotthold Max Eisenstein. Eisenstein (1823-1852) was born to parents of limited means and remained near poverty throughout his life. He had five younger siblings, all of whom died in childhood—most of meningitis, which also afflicted Eisenstein. He suffered from poor health and depression for most of his life.

Eisenstein first became interested in mathematics when he was six, thanks to a family acquaintance. In his autobiography, Eisenstein wrote, "As a boy of six I could understand the proof of a mathematical theorem more readily than that meat had to be cut with one's knife, not one's fork." He also had a lifelong interest in music—he played the piano and composed.

Eisenstein had some excellent and encouraging teachers in mathematics, and began reading the work of Euler, Lagrange and Gauss at an early age. In 1843 he passed his secondary school examinations, though he already knew far more mathematics than the standard secondary fare. He enrolled at the University of Berlin and submitted his first paper in January of 1844. In that year, volumes 27 and 28 of Crelle's mathematical journal contained *twenty-five* works by Eisenstein, making him an overnight sensation in mathematical circles. Gauss was very impressed by Eisenstein's early work, and wrote the preface for an 1847 collection of work by Eisenstein.

Through Crelle, Eisenstein met Alexander von Humboldt, who became his mentor, champion and financial lifeline. Humboldt secured a series of small grants for Eisenstein, and sometimes contributed his own funds to help Eisenstein through times between grants.

Eisenstein was minimally involved in the political unrest of 1848. He was arrested and detained overnight, suffering severe mistreatment that hurt his already poor health. The incident also made it even more difficult for him to find financial support; Humboldt was just barely able to find some funding for him. Eisenstein's health deteriorated and his depression increased, so that he was often unable to deliver his lectures, but he continued to publish papers.

In 1851 Eisenstein was elected to the Göttingen Society, and in 1852 to the Berlin Academy. In July of 1852, his health declined precipitously when he suffered a hemorrhage. Humboldt raised enough money to send him to recuperate in Italy for a year, but it came too late. Eisenstein died in October of tuberculosis.

Our exposition of Eisenstein's proof is taken from *Eisenstein's Misunderstood Geometric Proof of the Quadratic Reciprocity Theorem*, by Reinhard Laubenbacher and David Pengelley, in The College Mathematics Journal, volume 25, number 1, January 1994. Biographical information is from the same paper, and from the article on Eisenstein, by Kurt-R. Biermann, in Biographical Dictionary of Mathematicians, New York: Charles Scribner's Sons, 1991.

Exercises 3.8.

1. Find the "perfect squares" in $\mathbb{Z}_{15}$. How many are there? Compare your answer with the result in Theorem 3.44.
2. Find the quadratic residues for 11 and 17.
3. Fill in the details missing in the proof of Theorem 3.44.
4. Give a proof of the fact mentioned just before the statement of Euler's Criterion.
5. Give examples like those preceding Euler's Criterion using $xy \equiv 5 \pmod{17}$ and $xy \equiv 13 \pmod{17}$.

6. Use Euler's Criterion and its corollary to determine each of the following. Try to do the computations without technology, simplifying as much as possible.

a) $\left(\frac{7}{23}\right)$ **b)** $\left(\frac{10}{31}\right)$ **c)** $\left(\frac{3}{83}\right)$ **d)** $\left(\frac{23}{47}\right)$

7. There are several statements in the opening paragraph of the proof of Theorem 3.47 that may require more detail. Give careful details for each of the following.

a) Why may we assume $1 \leq r_e \leq p-1$ rather than the usual $0 \leq r_e < p$?

b) Prove that $r_e = r_f$ if and only if $e = f$.

c) What exactly is the contradiction that appears in the proof that $\{s_e : e \in E\} = E$?

8. Prove Theorem 3.48 by considering the cases $p = 4k+1$ and $p = 4k+3$ separately. You should be able to find the value of y explicitly for these two cases.

9. Use Theorems 3.47 and 3.48 to determine each of the following. (All of the integers are primes.)

a) $\left(\frac{13}{41}\right)$ **b)** $\left(\frac{61}{113}\right)$ **c)** $\left(\frac{283}{577}\right)$

d) $\left(\frac{107}{149}\right)$ **e)** $\left(\frac{379}{947}\right)$ **f)** $\left(\frac{1973}{2153}\right)$

10. Determine (as mentioned in the text) whether or not 111 is a quadratic residue of 947.

11. For which odd primes p is -1 a quadratic residue modulo p? You must justify your answer.

12. Determine $\left(\frac{3}{p}\right)$, where $p > 3$ is an odd prime. Your solution (which must involve a proof) should look something like the result in Theorem 3.48. (Look at primes of the form $12k + r$.)

3.9 Sums of Two Squares

The Pythagorean Theorem states that $a^2 + b^2 = c^2$ for a right triangle with legs a and b and hypotenuse c. A search for integer solutions to this equation can be traced back more than two thousand years; some general solutions appear in *The Elements*. Simple examples include

$$5^2 = 3^2 + 4^2, \qquad 13^2 = 5^2 + 12^2, \qquad 17^2 = 8^2 + 15^2, \qquad 29^2 = 20^2 + 21^2.$$

More generally, the equation

$$(n^2+1)^2 = n^4 + 2n^2 + 1 = n^4 - 2n^2 + 1 + 4n^2 = (n^2-1)^2 + (2n)^2$$

provides an infinite number of examples. A vast number of results are known about integer solutions to the equation $a^2 + b^2 = c^2$, but our goal is more modest. The examples above show that some perfect squares are sums of two other perfect squares. Trivially, any perfect square n^2 can be written as the sum of two perfect squares, namely, $n^2 = n^2 + 0^2$. However, there are many other integers that can be written as the sum of two perfect squares; $13 = 2^2 + 3^2$ is a simple example. We can thus ask which positive integers are the sums of two squares. To approach a problem such as this, it is best to gather some information first. An initial list of integers that can be written as a sum of two squares is given below; a blank equation indicates that the integer cannot be represented as a sum of two squares. (For 25, we have used the more interesting option rather than $5^2 + 0^2$.)

$1 = 0^2 + 1^2$	$17 = 1^2 + 4^2$	$33 =$
$2 = 1^2 + 1^2$	$18 = 3^2 + 3^2$	$34 = 3^2 + 5^2$
$3 =$	$19 =$	$35 =$
$4 = 0^2 + 2^2$	$20 = 2^2 + 4^2$	$36 = 0^2 + 6^2$
$5 = 1^2 + 2^2$	$21 =$	$37 = 1^2 + 6^2$
$6 =$	$22 =$	$38 =$
$7 =$	$23 =$	$39 =$
$8 = 2^2 + 2^2$	$24 =$	$40 = 2^2 + 6^2$
$9 = 0^2 + 3^2$	$25 = 3^2 + 4^2$	$41 = 4^2 + 5^2$
$10 = 1^2 + 3^2$	$26 = 1^2 + 5^2$	$42 =$
$11 =$	$27 =$	$43 =$
$12 =$	$28 =$	$44 =$
$13 = 2^2 + 3^2$	$29 = 2^2 + 5^2$	$45 = 3^2 + 6^2$
$14 =$	$30 =$	$46 =$
$15 =$	$31 =$	$47 =$
$16 = 0^2 + 4^2$	$32 = 4^2 + 4^2$	$48 =$

We mentioned in the last section that a perfect square is congruent to either 0 or 1 modulo 4. It follows that the sum of two perfect squares must be congruent to either 0, 1, or 2 modulo 4. In other words, any integer that is congruent to 3 modulo 4 cannot be represented as a sum of two squares. This accounts for the fact that the numbers 3, 7, 11, 15, and so on, have blank equations in the table. However, there are quite a few other integers that also have blank equations. Our goal is to characterize all positive integers that can be represented as a sum of two squares.

As we have done several times before, we break the problem down into simpler parts. We first make note of the following pair of algebraic identities:

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2;$$
$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.$$

These equalities show that the product of two integers that can be represented as a sum of two squares can also be represented as a sum of two squares (and often the product has two such representations). For example, using these identities and results from the table, we find that

$$1189 = 29 \cdot 41 = (2^2 + 5^2)(4^2 + 5^2) = \begin{cases} (8 + 25)^2 + (10 - 20)^2 & = 33^2 + 10^2; \\ (8 - 25)^2 + (10 + 20)^2 & = 17^2 + 30^2. \end{cases}$$

Notice that determining whether or not 1189 can be represented as a sum of two squares reduces to determining whether or not its prime factors 29 and 41 can be represented as sums of two squares. In general, if the factors of a number can be represented as a sum of two squares, then the number itself can be represented as a sum of two squares.

What can we say about the integers that cannot be represented as a sum of two squares? The product equation given above, along with the Fundamental Theorem of Arithmetic, makes it possible to focus on prime numbers and their powers. Using 0^2 as one of the perfect squares, it is easy to see that any even power of a prime number can be represented as a sum of squares. Let's look at a few of the numbers that have blank equations in our table (and are not of the form $4k+3$ since these have already been ruled out) and consider their prime factorizations:

$$\begin{array}{lll} 6 = 2 \cdot 3 & 24 = 2^3 \cdot 3 & 42 = 2 \cdot 3 \cdot 7 \\ 12 = 2^2 \cdot 3 & 28 = 2^2 \cdot 7 & 44 = 4 \cdot 11 \\ 14 = 2 \cdot 7 & 30 = 2 \cdot 3 \cdot 5 & 46 = 2 \cdot 23 \\ 21 = 3 \cdot 7 & 33 = 3 \cdot 11 & 48 = 2^4 \cdot 3 \\ 22 = 2 \cdot 11 & 38 = 2 \cdot 19 & 54 = 2 \cdot 3^3 \end{array}$$

We notice that each of these nonrepresentable numbers contains an odd power of a prime of the form $4k + 3$. It turns out that this property completely characterizes those integers that can be represented as a sum of two squares.

THEOREM 3.49 A positive integer n can be represented as a sum of two squares if and only if every prime divisor of n of the form $4k + 3$ appears in the canonical representation of n with an even exponent.

Proof. Suppose first that $n \geq 1$ can be represented as a sum of two squares and, to exclude the trivial case, assume that n is not a perfect square. Let $n = a^2 + b^2$, where a and b are positive integers, and let $g = (a, b)$. It follows easily that g^2 divides n so we may write

$$N = A^2 + B^2, \quad \text{where} \quad n = Ng^2,\ a = Ag,\ b = Bg.$$

Note that $(A, B) = 1$ (see Exercise 11 in Section 3.4). Assume that a prime number p of the form $4k + 3$ appears with an odd exponent in the canonical representation of n. Since g^2 contains only even powers of primes that divide n, we know (by the Fundamental Theorem of Arithmetic) that p must divide N, and hence p divides $A^2 + B^2$. If p divides either of the integers A or B, then p also divides the other and we would have $(A, B) \geq p$, a contradiction. Thus p does not divide either A or B. Since $(-B^2, p) = 1$ and the equation $x^2 \equiv -B^2 (\text{mod } p)$ has a solution (namely, A), the number $-B^2$ is a quadratic residue of p. By Euler's Criterion and Fermat's Little Theorem, we find that (using modulo p)

$$1 \equiv (-B^2)^{(p-1)/2} \equiv (-1)^{(2k+1)} B^{p-1} \equiv -1,$$

a contradiction. It follows that p must appear in the canonical representation of n with an even exponent.

Now suppose that every prime divisor of n of the form $4k + 3$ appears in the canonical representation of n with an even exponent. It is thus possible to write n as

$$n = N^2 \cdot p_1 \cdot p_2 \cdot \cdots \cdot p_m,$$

where $N \geq 1$ and the p_i's are distinct primes of the form $4k + 1$ with the possible exception that one of them might be 2. As noted earlier, the product of two positive integers each of which can be

represented as a sum of two squares also can be represented as a sum of two squares. Since both N^2 and 2 can be represented as a sum of two squares, it is sufficient to prove that each prime of the form $4k+1$ can be represented as a sum of two squares.

Let p be a prime of the form $4k+1$. By Euler's Criterion, we find that -1 is a quadratic residue of p. Consequently, there exist positive integers z and s such that $2 \le z \le (p-1)/2$ and $sp = z^2+1$. In other words, a multiple of p can be written as a sum of two squares and the multiplier s satisfies $1 \le s < p$ since

$$sp = z^2 + 1 \le \left(\frac{p-1}{2}\right)^2 + 1 < \left(\frac{p+1}{2}\right)^2 < p^2.$$

Since the collection of all positive multiples of p that can be written as a sum of two squares is nonempty, it contains a least element (by the Well-Ordering Property), call it $s_1 p$. If $s_1 = 1$, then we are finished. Suppose then that $s_1 > 1$ and choose positive integers x and y so that $s_1 p = x^2+y^2$. By a modification of the Division Algorithm (see Exercise 10 in Section 2.7), there exist integers q_1, r_1, q_2, and r_2 such that

$$x = q_1 s_1 + r_1 \quad \text{and} \quad y = q_2 s_1 + r_2,$$

where $0 \le |r_i| \le s_1/2$ for each i. Note that r_1 and r_2 cannot both be 0 since then s_1 would divide p, an impossibility since $1 < s_1 \le s < p$. We then have

$$s_1 p = x^2 + y^2 = s_1^2(q_1^2 + q_2^2) + 2s_1(q_1 r_1 + q_2 r_2) + (r_1^2 + r_2^2), \tag{1}$$

which reveals that $r_1^2 + r_2^2$ is a multiple of s_1. Since

$$0 < r_1^2 + r_2^2 \le 2\left(\frac{s_1}{2}\right)^2 < s_1^2,$$

we see that $r_1^2 + r_2^2 = s_1 s_2$ with $0 < s_2 < s_1$. Canceling s_1 from both sides of equation (1), then multiplying by s_2 and using the sum of squares product identity, we obtain

$$\begin{aligned} s_2 p &= s_1 s_2(q_1^2 + q_2^2) + 2s_2(q_1 r_1 + q_2 r_2) + s_2^2 \\ &= s_2^2 + 2s_2(q_1 r_1 + q_2 r_2) + (r_1^2 + r_2^2)(q_1^2 + q_2^2) \\ &= s_2^2 + 2s_2(q_1 r_1 + q_2 r_2) + (q_1 r_1 + q_2 r_2)^2 + (q_2 r_1 - q_1 r_2)^2 \\ &= (s_2 + q_1 r_1 + q_2 r_2)^2 + (q_2 r_1 - q_1 r_2)^2. \end{aligned}$$

This shows that $s_2 p$ is a multiple of p that can be represented as a sum of two squares, a contradiction to the fact that $s_1 p$ was the least multiple of p that could be represented as a sum of two squares. Thus s_1 must be 1 and the proof is complete. ■

Although it would take some work to actually find the representation, the integer

$$n = 3^4 \cdot 11^2 \cdot 17 \cdot 29 \cdot 53 \cdot 71^6$$

can be represented as a sum of two squares. However, the integer

$$m = 5 \cdot 13^3 \cdot 17 \cdot 29 \cdot 31^5 \cdot 41$$

has no such representation due to the appearance of the $4k+3$ prime 31 with an odd exponent.

Using ideas similar to those discussed in this section, it can be shown that every positive integer can be represented as the sum of at most four squares. From here, you can branch off in several directions. You can ask which integers can be represented as a sum of three squares or how many different ways an integer can be written as a sum of four squares. You can then look at sums of cubes, sums of fourth powers, and so on. Many such problems have been studied over the years and continue to be studied today.

The topics considered in the last three sections of this chapter provide a glimpse at the wonderful but difficult and subtle areas of the field of number theory. We hope these ideas make you want to explore number theory further. You can use the bibliography for a list of some books to get you started but there are many other sources of information on these topics.

Exercises 3.9.

1. Use the product identity to write $697 = 17 \cdot 41$ as a sum of two squares in two different ways.

2. Extend the table in this section by including the numbers from 49 to 64.

3. Use the product identity to write $3233 = 53 \cdot 61$ as a sum of two squares in two different ways.

4. Use the product identity to express $26129 = 17 \cdot 29 \cdot 53$ as a sum of two squares in four different ways. Use one of your answers to show how to write the integer n that appears near the end of this section as a sum of two squares.

5. Suppose that p is a prime of the form $4k + 1$. Prove that there exist nonzero integers a and b such that $p^2 = a^2 + b^2$. (Hint: Begin by writing $p = u^2 + v^2$, which follows from Theorem 3.49, and noting some properties of u and v.)

6. Suppose that p is a prime of the form $4k+3$. We know that p^2 can be written as a sum of two squares, namely, $p^2 = 0^2 + p^2$. Show that this is essentially (that is, ignore $p^2 = 0^2 + (-p)^2$) the only way to do this. In other words, prove that if $p^2 = a^2 + b^2$, then either $a = 0$ or $b = 0$. (Hint: Read carefully the first part of the proof of Theorem 3.49.)

7. Determine the integers (there are seven of them) in the range 1–48 that cannot be represented as a sum of three or fewer nonzero squares.

8. Suppose that n is a multiple of 4 and that $n = a^2 + b^2 + c^2$. Prove that a, b, and c must all be even.

9. Use a modulo 8 argument to prove that any positive integer of the form $8k + 7$ cannot be represented as a sum of three or fewer squares.

10. Referring to the two previous exercises, prove that any number of the form $4^j(8k + 7)$, where j and k are nonnegative integers, cannot be represented as a sum of three or fewer squares.

11. Write each of the integers in the range 1–24 as a sum of positive cubes, using the least number of cubes possible. What appears to be the minimum number of cubes that is needed?

12. Consider writing integers as sums of fourth powers and determine a two-digit number that requires as many positive fourth powers as possible. In a similar vein, can you find a number that requires a large number of positive fifth powers? (Hint: Do some thinking, not trial and error.)

4

Functions

The reader has certainly dealt with functions before, primarily in calculus, where functions from $\mathbb{R}$ to $\mathbb{R}$ or from $\mathbb{R}^2$ to $\mathbb{R}$ are studied extensively. Most students think of functions as formulas such as $f(x) = x^2 \sin x$ or $g(x, y) = x^2 + 2xy + y^3$, but there is much more to the concept than these simple formulas might indicate. Perhaps you have encountered functions in a more abstract setting as well; this is our focus. We consider the general notion of a function and examine some of its properties. In the last few sections of the chapter, we use functions to study some interesting topics in set theory. In particular, we explore the notion of infinity and determine ways in which to compare the sizes of infinite sets.

4.1 Definition and Examples

As with sets, the notion of a function is a fundamental concept in mathematics. It is possible to define functions in terms of sets and concepts that involve sets. The advantage of defining functions in this way is that it keeps the number of undefined terms to a minimum, but a disadvantage is that the notion of a function becomes more abstract. As the reader has had a great deal of experience with functions, at least real-valued functions, we treat the term "function" as another undefined term and simply explain how the concept is used.

DEFINITION 4.1 Let A and B be two nonempty sets. A **function** f from A to B is an *assignment* or *rule* that assigns to each element of the set A exactly one element of the set B. If f assigns the element b of B to the element a of A, then we write $f(a) = b$. The set A is called the **domain** of f and the set B is called the **codomain** of f. We say two functions f and g are **equal** if they have the same domain and the same codomain, and if for every a in the domain, $f(a) = g(a)$. In symbols, this last phrase can be written as $\forall a \in A\,(f(a) = g(a))$.

To see why this "definition" is not really a definition, note that the words "assignment" and "rule" are synonyms for "function." As mentioned above, this problem can be resolved by defining a function using the undefined term 'set'; a function from A to B is a subset of the Cartesian product $A \times B$ that satisfies certain properties. For our purposes, all that is needed is an intuitive understanding of the concept and a way of showing two functions are equal.

We often write $f\colon A \to B$ to indicate that f is a function from A to B. For the record, whenever we write $f\colon A \to B$, it is always assumed that A and B are nonempty sets. Sometimes the word "map" or "mapping" is used instead of "function." If $f\colon A \to B$ and $f(a) = b$, then we say b is the **image of** a **under** f and a is a **preimage of** b **under** f. When the function is clear from the context, the phrase 'under f' may be dropped. The elements of A are sometimes referred to as the **inputs** for the function f and the values $f(a)$ are the **outputs** of the function f.

It is important to note that a function consists of three parts; a domain, a codomain, and a rule of correspondence, that is, a function is not just a rule of correspondence or a formula. In calculus, it is common to see something like "consider the function $f(x) = \sqrt{5 - x}$." For situations such as this, the codomain is assumed to be $\mathbb{R}$ and the domain is assumed to be the set of all real numbers for which the formula for $f(x)$ is defined. In this case, we see that the domain is the interval $(-\infty, 5]$. Using our new notation, we would write "consider the function $f\colon (-\infty, 5] \to \mathbb{R}$ defined by $f(x) = \sqrt{5 - x}$." When a domain is defined implicitly like this, it is often referred to as the *natural domain* of the function. To emphasize the first sentence of this paragraph, the function $g\colon [0, 5] \to [0, \infty)$ defined by $g(x) = \sqrt{5 - x}$ is not the same as the function f; the rule is the same but both the domain and the codomain are different. In practice, however, the sets A and B are often clear from the context and we refer to the function f as opposed to always writing "the function $f\colon A \to B$."

Let A and B be nonempty sets. A rule of correspondence that attempts to define a function $f\colon A \to B$ is **well-defined** if for each $a \in A$ there is exactly one value for $f(a)$. To illustrate what is meant by this, consider the following attempt to define a function: "for each real number x, let $f(x)$ be a real number whose square is x." There are two problems with this definition. First of all, if $x < 0$, then there is no value for $f(x)$. This problem can be eliminated by writing "for each nonnegative real number x, let $f(x)$ be a real number whose square is x." However, this does not remove the second problem; for each $x > 0$, there are two real numbers whose square is x. Hence, all positive inputs generate two outputs, something that is not allowed in the definition of a function. The bottom line is that this rule of correspondence does not define a function. However, the function $f\colon [0, \infty) \to \mathbb{R}$ defined by $f(x) = \sqrt{x}$ is a valid function. (By convention, the symbol $\sqrt{x}$ means the positive square root of x.)

As a final comment before considering some examples, it is important to note that the symbols f and $f(x)$ are not interchangeable (although not everyone agrees on this matter). The symbol f represents a function, whereas the symbol $f(x)$ represents the value of f at x. A good way to illustrate this is with a calculator. The symbol x represents the number that is entered into the calculator, the symbol f represents the function key that is used (the squaring key, the sine key, etc.), and $f(x)$ represents the displayed output. There is a clear distinction between the function keys of the calculator (the function f) and the displayed outputs (the values $f(x)$).

The reader should be familiar with many functions of the form $f: \mathbb{R} \to \mathbb{R}$: polynomial functions, trigonometric functions, exponential functions, and so on. Usually these functions have codomain $\mathbb{R}$ and their domain is some subset of $\mathbb{R}$. For example, $f(x) = \sqrt{x}$ has domain $[0, \infty)$ and $f(x) = 1/x$ has domain $\{x \in \mathbb{R} : x \neq 0\}$. (The domain of these functions is the natural domain discussed earlier.) It is easy to see that a subset of the plane is the graph of a function $f: \mathbb{R} \to \mathbb{R}$ if and only if every vertical line intersects the graph at exactly one point. If this point is (a, b), then $f(a) = b$.

Functions on finite sets can be defined by listing all the assignments. If $A = \{1, 2, 3, 4\}$ and $B = \{r, s, t, u, v\}$, then "$f(1) = t, f(2) = s, f(3) = u, f(4) = t$" defines a function from A to B. The assignment can be done quite arbitrarily, without recourse to any particular formula. Note that the images of both 1 and 4 are t. This is consistent with the definition of a function. The definition insists that each input have exactly one output, but different inputs may have the same output; this is an important distinction to remember.

In calculus and analysis, the rule of correspondence for a function is often given by an explicit formula. For example, we can define a function $h: \mathbb{R} \to \mathbb{R}$ by $h(x) = x^2$. This function assigns the real number x^2 to the real number x. However, any rule of correspondence that assigns to each element of A a unique element of B is a function, even if it does not involve a formula. As an example of this situation from a calculus perspective, for each real number x, let $u(x)$ be the real number for which

$$(u(x))^7 + (u(x))^5 + (u(x))^3 + u(x) + 1 = x.$$

It can be shown that this defines a function $u: \mathbb{R} \to \mathbb{R}$. There is no explicit formula that gives the values of this function, but it still satisfies the definition of a function; for each real number x there is exactly one real number $u(x)$. (What theorems from calculus are necessary to prove this?)

EXAMPLE 4.2 For $A = \{1, 2, 3, 4, 5\}$ and $B = \{r, s, t, u\}$, consider the following correspondences f, g, and h:

$f(1) = t;$	$g(1) = u;$	$h(1) = r;$
$f(2) = s;$	$g(2) = r;$	$h(2) = r;$
$f(3) = r;$	$g(4) = s;$	$h(3) = s;$
$f(3) = u;$	$g(5) = t;$	$h(4) = s;$
$f(4) = u;$		$h(5) = s.$
$f(5) = r;$		

The correspondences f and g are not functions from A to B. The problem is that f maps 3 to two values and g doesn't map 3 to any values. When listing the assignments for a function the elements of the domain must appear exactly once. Elements of the codomain may appear more than once or not at all; the correspondence h is a function from A to B even though the element s of the codomain has three preimages and t has none. We discuss this situation at length in later sections.

Some functions are common enough to be given special names. Suppose that A and B are nonempty sets. We define the **identity** function $i_A: A \to A$ by the rule $i_A(a) = a$ for all $a \in A$. In other words, the identity function maps every element to itself. Though this seems like a rather trivial concept, it is useful and important. As we will see, identity functions behave in much the same way that 0 does with respect to addition or 1 does with respect to multiplication. If b_0 is a fixed element of B, we can define a **constant** function $f: A \to B$ by the formula $f(a) = b_0$ for all

$a \in A$. There are as many constant functions from A to B as there are elements of B. Finally, if $A \subseteq B$, define the **inclusion** function $f: A \to B$ by $f(a) = a$ for every $a \in A$. This is very similar to i_A; the only difference is the codomain.

DEFINITION 4.3 If $f: A \to B$ and $g: B \to C$ are functions, define $g \circ f: A \to C$ by the rule $(g \circ f)(a) = g(f(a))$ for all $a \in A$. This is called the **composition** of the two functions.

Note that the domain of $g \circ f$ is the same as the domain of f and that the codomain of $g \circ f$ is the same as the codomain of g. Observe that f is the first function that is applied to an element a though it is listed on the right. This violation of the usual left-to-right convention sometimes causes confusion so be careful. Composite functions appear frequently in calculus. If $f: [0, \infty) \to \mathbb{R}$ is given by $f(x) = \sqrt{x}$ and $g: \mathbb{R} \to \mathbb{R}$ is given by $g(x) = \sin x$, then $g \circ f: [0, \infty) \to \mathbb{R}$ is given by $(g \circ f)(x) = \sin \sqrt{x}$. Note that the function $f \circ g$, which is defined by the formula $(f \circ g)(x) = \sqrt{\sin x}$, makes sense only for those values of x such that $\sin x \geq 0$. In general, the functions $f \circ g$ and $g \circ f$ are not equal, and (as in this case) they need not be defined at the same points. Thus the operation of composition is not commutative.

If A, B, and C are nonempty sets for which $A \subseteq B$, $f: A \to B$ is the inclusion function, and $g: B \to C$ is a function, then $g \circ f: A \to C$ is called the **restriction** of g to A and is usually written $g|_A$. For all $a \in A$,

$$g|_A(a) = g(f(a)) = g(a),$$

that is, the rule for $g|_A$ is the same as it is for the function g but the domain of $g|_A$ is a smaller set. In particular, the functions g and $g|_A$ are not the same unless $A = B$.

EXAMPLE 4.4 Let $A = \{1, 2, 3, 4\}$, $B = \{r, s, t, u\}$, and $C = \{\$, \%, \#, \&\}$, then for the functions $f: A \to B$ and $g: B \to C$ defined by

$$\begin{array}{lll} f(1) = u; & g(r) = \%; & \\ f(2) = r; & g(s) = \#; & \text{we have} \\ f(3) = s; & g(t) = \$; & \\ f(4) = u; & g(u) = \$; & \end{array} \qquad \begin{array}{ll} (g \circ f)(1) & = \$; \\ (g \circ f)(2) & = \%; \\ (g \circ f)(3) & = \#; \\ (g \circ f)(4) & = \$. \end{array}$$

Note that $g \circ f$ maps A into C.

The following two results record simple but important observations. A proof of the second result, which states that function composition is an associative operation, is similar to the first and is left as an exercise.

THEOREM 4.5 If $f: A \to B$, then $f \circ i_A = f$ and $i_B \circ f = f$.

Proof. All three functions f, $f \circ i_A$, and $i_B \circ f$ have domain A and codomain B; these sets are implicitly assumed for the composite functions. For every $a \in A$,

$$(f \circ i_A)(a) = f(i_A(a)) = f(a) \qquad \text{and} \qquad (i_B \circ f)(a) = i_B(f(a)) = f(a).$$

Since the values of these functions are the same for each a in the domain A, the functions are equal. ∎

THEOREM 4.6 If $f: C \to D$, $g: B \to C$, and $h: A \to B$ are functions, then the functions $(f \circ g) \circ h$ and $f \circ (g \circ h)$ are equal. ■

Exercises 4.1.

1. Decide if the following three assignments, referred to as f, g, and h, define functions from the set $A = \{1, 2, 3, 4\}$ to the set $B = \{r, s, t, u, v\}$.

$$\begin{array}{lll} f(1) = s; & g(1) = t; & h(1) = v; \\ f(2) = t; & g(2) = r; & h(2) = u; \\ f(4) = u; & g(3) = s; & h(3) = t; \\ & g(4) = r; & h(2) = s; \\ & & h(4) = r. \end{array}$$

2. Let $f: \{s, t, u, v, w, x\} \to \{1, 2, 3, 4, 5\}$ and $g: \{1, 2, 3, 4, 5\} \to \{m, n, o, p\}$ be given by

$$\begin{array}{ll} f(s) = 2; & g(1) = m; \\ f(t) = 1; & g(2) = n; \\ f(u) = 4; & g(3) = p; \\ f(v) = 2; & g(4) = o; \\ f(w) = 1; & g(5) = m. \\ f(x) = 2; & \end{array}$$

Find the following:

a) $h = g \circ f$; **b)** the image of u under f;

c) the image of 2 under g; **d)** the image of v under h;

e) the preimage(s) of p under g; **f)** the preimage(s) of 1 under f;

g) the preimage(s) of n under h; **h)** the preimage(s) of 5 under f.

3. Find the natural domains of each of the following functions:

a) $f(x) = \dfrac{1}{x^2 - x}$ **b)** $g(x) = \sqrt{x - 8}$ **c)** $h(x) = \dfrac{x}{\sqrt{5 - 4x - x^2}}$

4. Suppose that $f: \mathbb{R} \to \mathbb{R}$ is given by $f(x) = \cos x$ and $g: \mathbb{R} \to \mathbb{R}$ is given by $g(x) = x^2$. Find the following:

a) $h = g \circ f$; **b)** the image of 4π under f;

c) the image of $-\sqrt{2}$ under g; **d)** the image of $\pi/4$ under h;

e) the preimage(s) of $\frac{\sqrt{3}}{2}$ under f; **f)** the preimage(s) of $9/25$ under g;

g) the preimage(s) of 1 under h; **h)** the preimage(s) of 2 under f.

5. Suppose f and g are both functions from A to A. If $f \circ f = g \circ g$, does it follow that $f = g$?

6. Suppose A and B are nonempty sets with m and n elements, respectively. How many different functions are there from A to B?

7. Suppose that f and g are two functions from A to B and that $A = X \cup Y$. Prove that $f = g$ if and only if $f|_X = g|_X$ and $f|_Y = g|_Y$.

8. Prove Theorem 4.6. What are the (implicitly assumed) domains and codomains for these functions?

4.2 Induced Set Functions

As we will see throughout this chapter, sets and functions are intimately related. In this section, we begin to explore some basic connections between them. Suppose $f: A \to B$ is a function. If $X \subseteq A$, define a set $f(X) \subseteq B$ by

$$f(X) = \{b \in B : \exists\, a \in X (b = f(a))\} \quad \text{or} \quad f(X) = \{f(a) : a \in X\}.$$

The set $f(X)$ is called the **image** of X. If $Y \subseteq B$, define a set $f^{-1}(Y) \subseteq A$ by

$$f^{-1}(Y) = \{a \in A : f(a) \in Y\}.$$

This set is called the **preimage** of Y. Note that we are inputting sets into f and f^{-1} and obtaining other sets as outputs; this is why these functions are known as induced set functions.

There is real cause for confusion here: the letter f is being used in two different, though related, ways. We can apply f to *elements* of A to get *elements* of B, or we can apply f to *subsets* of A to get *subsets* of B. In other words, we can interpret f as a function from A to B or as a function from $\mathcal{P}(A)$ to $\mathcal{P}(B)$ (see Section 1.6 for a discussion of power sets). Similarly, we can talk about preimages of either elements or subsets; the function f^{-1} maps $\mathcal{P}(B)$ to $\mathcal{P}(A)$. To be explicit, given a function $f\colon A \to B$, define functions $f\colon \mathcal{P}(A) \to \mathcal{P}(B)$ and $f^{-1}\colon \mathcal{P}(B) \to \mathcal{P}(A)$ by

$$f(X) = \{f(a) : a \in X\} \text{ for each } X \in \mathcal{P}(A);$$
$$f^{-1}(Y) = \{a \in A : f(a) \in Y\} \text{ for each } Y \in \mathcal{P}(B).$$

Context should always make it clear what is meant by the function f, but you should be aware of the potential misinterpretation.

EXAMPLE 4.7 Suppose $A = \{1, 2, 3, 4, 5, 6\}$ and $B = \{r, s, t, u, v, w\}$ and define a function $f\colon A \to B$ by $f(1) = r,\ f(2) = s,\ f(3) = v,\ f(4) = t,\ f(5) = r,\ f(6) = v$.
Then

$$f(\{1, 3, 5\}) = \{r, v\}; \qquad f^{-1}(\{r, t, u\}) = f^{-1}(\{r, t\}) = \{1, 4, 5\};$$
$$f(\{4, 5, 6\}) = \{r, t, v\}; \qquad f^{-1}(\{u, w\}) = \emptyset.$$

EXAMPLE 4.8 Suppose $g\colon \mathbb{R} \to \mathbb{R}$ is given by $g(x) = x^2$. Then (using standard interval notation to represent sets in $\mathbb{R}$)

$$g([2, 3]) = [4, 9]; \qquad g^{-1}([0, 1]) = [-1, 1];$$
$$g((-2, 1]) = [0, 4); \qquad g^{-1}([-1, 0]) = \{0\};$$
$$g(\{1, 2, 3\}) = \{1, 4, 9\}; \qquad g^{-1}((-\infty, 0)) = \emptyset.$$

By the **range** (or **image**) of a function $f\colon A \to B$, we mean the set

$$f(A) = \{f(a) : a \in A\} = \{b \in B : \exists a \in A\,(b = f(a))\}.$$

The range is a subset of the codomain, but it may be considerably smaller than the codomain. Referring to the two previous examples, the range of the function f is $\{r, s, v, t\}$, which is a proper subset of the codomain, and the range of the function g is $[0, \infty)$. As a further example, the range of the function $h\colon \mathbb{R} \to \mathbb{R}$ defined by $h(x) = \sin x$ is $[-1, 1]$.

The next two theorems show how induced set functions behave with respect to the set operations of intersection and union.

THEOREM 4.9 Suppose $f: A \to B$ is a function and Y and Z are subsets of B. Then

a) $f^{-1}(Y \cup Z) = f^{-1}(Y) \cup f^{-1}(Z)$,

b) $f^{-1}(Y \cap Z) = f^{-1}(Y) \cap f^{-1}(Z)$.

Proof. We prove part (b) and leave a proof of part (a) as an exercise. Note that the three sets that appear in part (b) are all subsets of A. Suppose that $a \in A$. We then have

$$\begin{aligned} a \in f^{-1}(Y \cap Z) &\Leftrightarrow f(a) \in Y \cap Z && \text{definition of } f^{-1} \\ &\Leftrightarrow f(a) \in Y \text{ and } f(a) \in Z && \text{definition of } \cap \\ &\Leftrightarrow a \in f^{-1}(Y) \text{ and } a \in f^{-1}(Z) && \text{definition of } f^{-1} \\ &\Leftrightarrow a \in f^{-1}(Y) \cap f^{-1}(Z), && \text{definition of } \cap \end{aligned}$$

showing that $f^{-1}(Y \cap Z) = f^{-1}(Y) \cap f^{-1}(Z)$. ■

THEOREM 4.10 Suppose $f: A \to B$ is a function and W and X are subsets of A. Then

a) $f(W \cup X) = f(W) \cup f(X)$,

b) $f(W \cap X) \subseteq f(W) \cap f(X)$.

Proof. Once again, we prove part (b) and leave part (a) as an exercise. The three sets that appear in part (b) are all subsets of B. If $f(W \cap X)$ is empty, we are done. Otherwise, suppose that $b \in f(W \cap X)$. This means that $b = f(a)$ for some $a \in W \cap X$. Since $a \in W \cap X$, it follows that a is in both W and X. Thus $b = f(a)$ belongs to both $f(W)$ and $f(X)$, that is, $b \in f(W) \cap f(X)$. Since every b that belongs to the set $f(W \cap X)$ also belongs to the set $f(W) \cap f(X)$, we find that $f(W \cap X) \subseteq f(W) \cap f(X)$. ■

It is perhaps surprising to compare these two theorems and observe that of the two induced set functions, it is f^{-1} that is "better behaved" with respect to the usual set operations.

Exercises 4.2.

In the first two exercises, use the function $f: \{1, 2, 3, 4, 5, 6, 7\} \to \{A, B, C, D, E, F, G, H\}$ given by:

$$\begin{array}{llll} f(1) = D; & f(3) = F; & f(5) = B; & f(7) = F. \\ f(2) = E; & f(4) = A; & f(6) = E. & \end{array}$$

1. For the function f given above, find the following:

a) $f(\{2, 4, 6\})$ **b)** $f(\{1, 3, 5, 7\})$ **c)** $f(\emptyset)$

d) $f^{-1}(\{D, E, H\})$ **e)** $f^{-1}(\{A, B, C, F\})$ **f)** $f^{-1}(\{F\})$

2. Refer to the function f given above.

a) If $Y = \{A, B, C, E, F\}$ and $Z = \{A, D, E, G, H\}$, verify the statements in Theorem 4.9.

b) If $W = \{1, 2, 3, 4\}$ and $X = \{2, 4, 5, 7\}$, verify the statements in Theorem 4.10.

3. Suppose $f: \mathbb{R} \to \mathbb{R}$ is given by $f(x) = |x - 1|$. Find the following:

a) $f([-1, 1])$ **b)** $f((0, 3))$ **c)** $f(\{-4, -2, 0, 1, 5\})$

d) $f^{-1}((0, 2))$ **e)** $f^{-1}([-1, 2])$ **f)** $f^{-1}(\{-2, 0, 4, 5\})$

4. Suppose $f: \mathbb{R} \to \mathbb{R}$ is given by $f(x) = x^3 - 3x$. Find the following:

a) $f([-1, 1])$ **b)** $f([-2, 4))$ **c)** $f(\{-4, -3, 1, 2\})$

d) $f^{-1}([0, 2])$ **e)** $f^{-1}((-2, 18))$ **f)** $f^{-1}(\{-2, 0, \frac{46}{27}\})$

5. Suppose $f: \mathbb{R} \to \mathbb{R}$ is given by $f(x) = x^2$.

a) If $Y = (1, \infty)$ and $Z = (-\infty, 4)$, verify the statements in Theorem 4.9.

b) If $W = [-3, 2]$, and $X = (0, 4]$, verify the statements in Theorem 4.10.

6. Prove part (a) of Theorem 4.9.

7. Prove part (a) of Theorem 4.10.

8. Give several examples of a function f and sets W and X for which the inclusion in part (b) of Theorem 4.10 is proper.

4.3 Injections and Surjections

Two simple properties that functions may have turn out to be exceptionally useful. If the codomain of a function is also its range, then the function is **onto** or **surjective**. If a function does not map two different elements in the domain to the same element in the range, it is **one-to-one** or **injective**. In this section, we define these concepts "officially" in terms of preimages, and explore some easy examples and consequences. Recall that a function is a rule of correspondence along with two sets, a domain and a codomain; it is not just a rule. This distinction is very important to remember.

DEFINITION 4.11 Let A and B be nonempty sets. A function $f: A \to B$ is **injective** if each $b \in B$ has at most one preimage in A.

An injective function is called an **injection**. An injection may also be referred to as a one-to-one (or 1–1) function; some people consider this term to be less formal than "injection." Note that the definition has several equivalent formulations:

$$\begin{aligned} f \text{ is injective} &\Leftrightarrow \text{each } b \text{ in } B \text{ has at most one preimage in } A \\ &\Leftrightarrow \text{for each } b \in B, \text{ the set } f^{-1}(\{b\}) \text{ contains at most one element} \\ &\Leftrightarrow \forall b \in f(A)\ \exists!\, a \in A\ (f(a) = b) \\ &\Leftrightarrow (\forall a_1 \in A)(\forall a_2 \in A)(f(a_1) = f(a_2) \Rightarrow a_1 = a_2) \\ &\Leftrightarrow (\forall a_1 \in A)(\forall a_2 \in A)(a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)). \end{aligned}$$

Sometimes one form of the definition is preferable over another.

To illustrate this concept, suppose $A = \{1, 2, 3\}$ and $B = \{r, s, t, u, v\}$ are sets and f and g are two functions mapping A into B defined by

$$\begin{aligned} f(1) &= s; & g(1) &= r; \\ f(2) &= t; & g(2) &= t; \\ f(3) &= r; & g(3) &= r. \end{aligned}$$

The function f is injective since r, s, and t each have one preimage and u and v each have no preimages. On the other hand, the function g fails to be injective since r has more than one

preimage. In general, if $A \subseteq B$, then the inclusion map from A to B is injective. In particular, the identity function is injective.

To illustrate injective functions with functions from calculus, define functions $f\colon \mathbb{R} \to \mathbb{R}$ and $g\colon \mathbb{R} \to \mathbb{R}$ by $f(x) = x^2$ and $g(x) = 2^x$, respectively. The function f fails to be injective because any positive number has two preimages (its positive and negative square roots). On the other hand, the function g is injective. To see this, note that $g(x) = b$ has one solution when $b > 0$ (namely, $\log_2 b$) and no solution when $b \leq 0$. The reader might find it helpful to formulate a "horizontal line test" to determine if a function of the form $h\colon \mathbb{R} \to \mathbb{R}$ is injective or not.

Referring to the list of equivalent formulations for the definition of an injection, the third one shows that a proof that a function is injective is essentially a uniqueness proof. Hence, a common way to prove that a function $f\colon A \to B$ is injective is to assume that $f(a_1) = f(a_2)$ for two elements a_1 and a_2 of A, then prove that $a_1 = a_2$. It follows that each element of the codomain has at most one preimage. This method of proof is illustrated in the following example.

EXAMPLE 4.12 Consider the function $f\colon \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^3 + 4x + 7$. To prove that f is injective, suppose that there exist two real numbers x and y such that $f(x) = f(y)$. Then

$$\begin{aligned} x^3 + 4x + 7 &= y^3 + 4y + 7; \\ (x^3 - y^3) + 4(x - y) &= 0; \\ (x - y)(x^2 + xy + y^2 + 4) &= 0; \\ (x - y)\Big(\frac{x^2 + y^2 + (x + y)^2 + 8}{2}\Big) &= 0. \end{aligned}$$

Since the second term in the last product is clearly positive, we find that $x = y$. It follows that f is injective. (We have presented a proof that involves algebra only. It is possible to prove that f is injective using some theorems from calculus, but calculus results are deeper than algebra results so some people might view such a proof as "cheating.")

The next result shows how injections behave under composition.

THEOREM 4.13 If $f\colon A \to B$ and $g\colon B \to C$ are injective functions, then $g \circ f\colon A \to C$ is an injective function.

Proof. Suppose there exist elements u and v in A for which $g(f(u)) = g(f(v))$. Since g is injective, we know that $f(u) = f(v)$. Since f is injective, it follows that $u = v$. Hence, the function $g \circ f\colon A \to C$ is injective. ■

We now turn to the other property of functions that we mentioned in the introduction of this section. The notion of a surjective function is 'dual' to that of an injective function.

DEFINITION 4.14 Let A and B be nonempty sets. A function $f\colon A \to B$ is **surjective** if each $b \in B$ has at least one preimage in A.

A surjective function is called a **surjection**. A surjection may also be called an onto function; some people consider this term to be less formal than "surjection." As with injective functions, the

the definition has several equivalent formulations:

$$\begin{aligned} f \text{ is surjective} &\Leftrightarrow \text{each } b \text{ in } B \text{ has at least one preimage in } A \\ &\Leftrightarrow \text{for each } b \in B, \text{ the set } f^{-1}(\{b\}) \text{ is nonempty} \\ &\Leftrightarrow \forall b \in B\, \exists\, a \in A\, (f(a) = b) \\ &\Leftrightarrow B = f(A) \\ &\Leftrightarrow \text{the range of } f \text{ is } B. \end{aligned}$$

As the last form indicates, a function $f: A \to B$ is a surjection if its range is the same as its codomain. For example, let $A = \{1, 2, 3, 4, 5\}$ and $B = \{r, s, t\}$ be sets and define functions f and g mapping A into B by

$$\begin{aligned} f(1) &= s; & g(1) &= t; \\ f(2) &= r; & g(2) &= r; \\ f(3) &= s; & g(3) &= r; \\ f(4) &= t; & g(4) &= t; \\ f(5) &= r; & g(5) &= t. \end{aligned}$$

For the function f, the elements r, s, and t have 2, 2, and 1 preimages, respectively, so f is surjective. For the function g, the element s has no preimages. It follows that g is not surjective. For any nonempty set A, the identity map $i_A: A \to A$ is both injective and surjective.

To illustrate surjective functions with functions from calculus, define functions $f: \mathbb{R} \to \mathbb{R}$ and $g: \mathbb{R} \to \mathbb{R}$ by $f(x) = 3^x$ and $g(x) = x^3$, respectively. Since 3^x is always positive, the function f is not surjective (any $b \leq 0$ has no preimages). On the other hand, for any $b \in \mathbb{R}$, the equation $b = g(x)$ has a solution (namely $x = \sqrt[3]{b}$) so b has a preimage under g. Therefore, the function g is surjective. As with injective functions, the reader might find it helpful to formulate a "horizontal line test" to determine if a function of the form $h: \mathbb{R} \to \mathbb{R}$ is surjective or not.

As we have mentioned before, a function consists of two nonempty sets and a rule of correspondence. Since the definitions of an injection and a surjection depend on the domain and codomain, it is important to be clear what these sets are. For example, we cannot use the formula $f(x) = x^2$ to decide if f is injective or surjective; we need to know the domain and codomain. To be specific,

1. the function $f_1: \mathbb{R} \to \mathbb{R}$ defined by $f_1(x) = x^2$ is neither injective nor surjective;
2. the function $f_2: [0, \infty) \to \mathbb{R}$ defined by $f_2(x) = x^2$ is injective but not surjective;
3. the function $f_3: [-1, 1] \to [0, 1]$ defined by $f_3(x) = x^2$ is surjective but not injective;
4. the function $f_4: [0, \infty) \to [0, \infty)$ defined by $f_4(x) = x^2$ is both injective and surjective.

The following result is the analogue of Theorem 4.13. Its proof is left as an exercise.

THEOREM 4.15 If $f: A \to B$ and $g: B \to C$ are surjective functions, then $g \circ f: A \to C$ is a surjective function. ■

Exercises 4.3.

1. Determine if the given function $f: \mathbb{R} \to \mathbb{R}$ is an injection, a surjection, neither, or both.

a) $f(x) = 2x + 1$ **b)** $f(x) = (x + 1)^3$ **c)** $f(x) = 1/2^x$

d) $f(x) = x^3 - x$ **e)** $f(x) = \sin x$ **f)** $f(x) = |x|$

2. Use algebra similar to the algebra used in Example 4.12 to prove that the function $f: \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^3 + 4x^2 + 26x$ is injective. Then give another proof using results from calculus.

3. **a)** Find an example of an injection $f: A \to B$ and a surjection $g: B \to C$ such that $g \circ f$ is neither injective nor surjective.

b) Find an example of a surjection $f: A \to B$ and an injection $g: B \to C$ such that $g \circ f$ is neither injective nor surjective.

4. Suppose that $f: A \to B$ is a function and that the sets A and B contain m and n elements, respectively, where m and n are positive integers.

a) If f is injective, what conclusion is possible regarding the integers m and n?

b) If f is surjective, what conclusion is possible regarding the integers m and n?

c) If f is both injective and surjective, what conclusion is possible regarding the integers m and n?

d) Suppose that $m = n$ and f is injective. Must f be surjective?

e) Suppose that $m = n$ and f is surjective. Must f be injective?

5. **a)** Find a function $f: \mathbb{N} \to \mathbb{N}$ that is injective, but not surjective.

b) Find a function $g: \mathbb{N} \to \mathbb{N}$ that is surjective, but not injective.

6. Suppose A and B are nonempty sets with m and n elements respectively, where $m \leq n$. How many injective functions are there from A to B?

7. Find an injection $f: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. (Hint: You might want to consider prime factorizations.)

8. Consider the function $f: \mathbb{N} \times \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ defined by $f(a, b, c) = 2^a + 3^b + 5^c$. Determine whether or not f is injective.

9. If $f: A \to B$ is a function, $A = X \cup Y$ and $f|_X$ and $f|_Y$ are both injective, can we conclude that f is injective?

10. Prove Theorem 4.15.

11. Suppose that A and B are nonempty sets. The function $p: A \times B \to B$ defined by $p((a, b)) = b$ is called the **projection onto** B. Prove that p is surjective. Under what conditions is p injective?

4.4 More Properties of Injections and Surjections

Injections and surjections are 'alike but different,' much as intersection and union are 'alike but different.' This is another example of *duality.*

THEOREM 4.16 Suppose $f: A \to B$ and $g: B \to C$ are functions.

a) If $g \circ f$ is injective, then f is injective.

b) If $g \circ f$ is surjective, then g is surjective.

Proof. To prove part (a), assume that $g \circ f: A \to C$ is injective. Suppose that $f(a_1) = f(a_2)$ for two elements a_1 and a_2 of A. It is then clear that

$$(g \circ f)(a_1) = g(f(a_1)) = g(f(a_2)) = (g \circ f)(a_2).$$

Since $g \circ f$ is injective, we find that $a_1 = a_2$. Hence, the function f is injective. We leave a proof of part (b) as an exercise. ■

Let A be a nonempty set and let $\mathcal{F}$ represent the collection of all functions mapping A into A. Define an operation $*$ on $\mathcal{F}$ by $f * g = f \circ g$. As we have seen, this operation is associative but it may not be commutative. For this operation, we can ask questions such as

if $f * g_1 = f * g_2$, does it follow that $g_1 = g_2$?
if $f_1 * g = f_2 * g$, does it follow that $f_1 = f_2$?

The next result shows that such "cancellations" are valid for injective and surjective functions in certain circumstances. The results are given in a more general setting than in this brief introduction to function spaces. As in Theorem 4.16, the result in the two cases is 'the same, but different.'

THEOREM 4.17 Suppose that f_1 and f_2 are functions mapping A into B, that g is a function mapping B into C, and that h_1 and h_2 are functions mapping C into D.

a) If g is injective and $g \circ f_1 = g \circ f_2$, then $f_1 = f_2$.

b) If g is surjective and $h_1 \circ g = h_2 \circ g$, then $h_1 = h_2$.

Proof. To prove part (b), assume that g is surjective and that $h_1 \circ g = h_2 \circ g$. We must show that $h_1(c) = h_2(c)$ for each $c \in C$. Let $c \in C$. Since the function g is surjective, there exists $b \in B$ such that $g(b) = c$. It then follows that

$$h_1(c) = h_1(g(b)) = h_2(g(b)) = h_2(c).$$

Since this equality is valid for every $c \in C$, the functions h_1 and h_2 are equal. We leave a proof of part (a) as an exercise. ■

Exercises 4.4.

1. Prove part (b) of Theorem 4.16.

2. Let $f: A \to B$ and $g: B \to C$ be functions. For the requested examples, find several options for f and g. In particular, find at least one pair of examples in which the sets A, B, and C finite and another pair of examples in which all of the sets are $\mathbb{R}$.

a) Find functions f and g such that $g \circ f$ is injective but g is not injective.

b) Find functions f and g such that $g \circ f$ is surjective but f is not surjective.

3. Prove part (a) of Theorem 4.17.

4. For this exercise, assume all functions map $\mathbb{R}$ into $\mathbb{R}$.

a) Find functions f_1, f_2, and g such that $g \circ f_1 = g \circ f_2$ but $f_1 \neq f_2$.

b) Find functions f, g_1, and g_2 such that $g_1 \circ f = g_2 \circ f$ but $g_1 \neq g_2$.

5. Let $A = \{1, 2, 3\}$ and let $\mathcal{F}$ be the set of six functions from A to A defined by

$$\begin{array}{llllll} i(1) = 1; & f(1) = 1; & s(1) = 3; & t(1) = 2; & o(1) = 2; & e(1) = 3; \\ i(2) = 2; & f(2) = 3; & s(2) = 2; & t(2) = 1; & o(2) = 3; & e(2) = 1; \\ i(3) = 3; & f(3) = 2; & s(3) = 1; & t(3) = 3; & o(3) = 1; & e(3) = 2; \end{array}$$

Assuming that multiplication is defined as composition (so, for instance, $t * s$ means $t \circ s$), write out the complete multiplication table for $\mathcal{F}$ (similar to the way multiplication tables were written for $\mathbb{U}_n$). To make solutions easier to check, write your table with the functions in the order they are listed.

6. Suppose that $f: A \to B$ and that $Y \subseteq B$.

a) Prove that $f(f^{-1}(Y)) \subseteq Y$. Give an example for which the inclusion is proper.

b) Suppose that f is a surjection. Prove that $f(f^{-1}(Y)) = Y$.

7. Suppose that $f: A \to B$ and that $X \subseteq A$. Explore the relationship between the sets X and $f^{-1}(f(X))$. (Your solution should be 'dual' to the previous exercise.)

8. Suppose that $f: A \to B$ and that W and X are subsets of A. Referring to part (b) of Theorem 4.10, we know that $f(W \cap X) \subseteq f(W) \cap f(X)$. Prove that equality holds when f is injective.

4.5 Pseudo-Inverses

Suppose $f: A \to B$ is a function with range $R \subseteq B$. Given an element $b \in R$, we are often interested in the values of a in A with the property that $f(a) = b$. The induced set function f^{-1} and the set $f^{-1}(\{b\}) = \{a \in A : f(a) = b\}$ are relevant to this question. However, as a function mapping B into A, the expression f^{-1} may not represent a well-defined function. The notion of a pseudo-inverse is sometimes useful in this context.

DEFINITION 4.18 Let $f: A \to B$ be a function and let $R = f(A)$ denotes its range. A function $g: B \to A$ is a **pseudo-inverse** of f if $g(b) \in f^{-1}(\{b\})$ for each $b \in R$. In other words, for all $b \in R$, $g(b)$ is a preimage of b.

Note that the values of g at points of $B \setminus R$ are completely arbitrary. For each $b \in R$, we find that $f(g(b)) = b$, that is, the function $f \circ g|_R$ is the inclusion map from R to B. (Note that $f \circ g|_R$ is the identity i_B when $B = R$.) If $a \in A$, it is not necessarily true that $g(f(a)) = a$. The reader should check these equations for the functions in the following example.

EXAMPLE 4.19 If $A = \{1, 2, 3, 4\}$, $B = \{r, s, t\}$, and $f: A \to B$ is defined by

$$f(1) = r, \qquad f(2) = t, \qquad f(3) = t, \qquad f(4) = r,$$

then $R = \{r, t\}$ and

$$g(r) = 4, \qquad g(s) = 3, \qquad g(t) = 2,$$

is one of several pseudo-inverses of f. The important point is that g must map r to either 1 or 4, and t to either 2 or 3.

As this example illustrates, any $f: A \to B$ has a pseudo-inverse. We are usually interested in a pseudo-inverse when f is either injective or surjective. The next result indicates some of the useful information that can be obtained in these cases.

THEOREM 4.20 Let A and B be nonempty sets and let $f: A \to B$ be a function.

a) If f is injective, then any pseudo-inverse of f is surjective.

b) If f is surjective, then any pseudo-inverse of f is injective.

Proof. Suppose first that $f: A \to B$ is injective and let $g: B \to A$ be any pseudo-inverse of f. Let a be an element of A. Then $b = f(a)$ is an element of the range of f. Since g is a pseudo-inverse

of f, we know that $g(b)$ must belong to the set $f^{-1}(\{b\})$. However, since f is injective, this set contains a only so we must have $g(b) = a$. It follows that g is surjective. Note that $g \circ f = i_A$; we say g is a **left inverse** of f.

Now suppose that $f\colon A \to B$ is surjective and let $g\colon B \to A$ be any pseudo-inverse of f. To prove that g is injective, suppose that $g(b_1) = g(b_2)$ for two elements b_1 and b_2 in B. By the definition of a function, we know that $f(g(b_1)) = f(g(b_2))$. Since f is surjective, it follows from the definition of a pseudo-inverse that $g(b_1)$ is a pre-image under f of b_1 and $g(b_2)$ is a pre-image under of f of b_2. This means that $b_1 = f(g(b_1)) = f(g(b_2)) = b_2$ and we conclude that g is injective. Note that $f \circ g = i_B$; we say g is a **right inverse** of f. ∎

EXAMPLE 4.21 Let $A = \{1, 2, 3, 4\}$ and $B = \{r, s, t, u, v, w\}$, then define functions $f\colon A \to B$ and $g\colon B \to A$ by

$$f(1) = s, \quad f(2) = v, \quad f(3) = w, \quad f(4) = r;$$
$$g(r) = 4, \quad g(s) = 1, \quad g(t) = 2, \quad g(u) = 4, \quad g(v) = 2, \quad g(w) = 3.$$

It is easy to verify that f is injective, that g is a pseudo-inverse of f, and that $g \circ f = i_A$.

EXAMPLE 4.22 For the sets $A = \{1, 2, 3, 4, 5\}$ and $B = \{r, s, t\}$, define two functions $f\colon A \to B$ and $g\colon B \to A$ by

$$f(1) = r, \quad f(2) = t, \quad f(3) = t, \quad f(4) = r, \quad f(5) = s;$$
$$g(r) = 4, \quad g(s) = 5, \quad g(t) = 2.$$

It is easy to verify that f is surjective, that g is a pseudo-inverse of f, and that $f \circ g = i_B$.

Exercises 4.5.

1. Find pseudo-inverses for the following functions:

a) the function $f\colon A \to B$, with $A = \{1, 2, 3, 4, 5, 6\}$ and $B = \{r, s, t, u\}$, defined by

$$f(1) = t; \quad f(3) = u; \quad f(5) = u;$$
$$f(2) = t; \quad f(4) = s; \quad f(6) = s;$$

b) the function $f\colon A \to B$, with $A = \{1, 2, 3, 4, 5, 6\}$ and $B = \{r, s, t\}$, defined by

$$f(1) = r; \quad f(3) = t; \quad f(5) = s;$$
$$f(2) = s; \quad f(4) = t; \quad f(6) = s;$$

c) the function $f\colon A \to B$, with $A = \{1, 2, 3, 4\}$ and $B = \{r, s, t, u, v, w\}$, defined by

$$f(1) = t; \quad f(3) = u;$$
$$f(2) = r; \quad f(4) = s;$$

d) the function $f\colon \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$;

e) the function $f\colon \mathbb{R} \to \mathbb{R}$ defined by $f(x) = e^x$.

2. Determine whether the pseudo-inverses for the functions listed in Exercise 1 are right inverses, left inverses, both, or neither. (Use your specific answers to Exercise 1, but then check to see if the same result holds for other choices.)

3. Give a proof of Theorem 4.17 using pseudo-inverses. (Focus on left and right inverses.)

4. How many pseudo-inverses do each of the functions in parts (a), (b), and (c) of Exercise 1 have?

5. Suppose that g is a pseudo-inverse of f. Find $f \circ g \circ f$.
6. If the set A has four elements and the set B has three elements, what is the least number of pseudo-inverses that a function $f: A \to B$ might have? What is the greatest number?
7. Determine whether or not the following partial converses of Theorem 4.20 are true.
   a) If f has a left inverse, then f is injective.
   b) If f has a right inverse, then f is surjective.

4.6 Bijections and Inverse Functions

As we have seen, functions that are injections or surjections have special properties that a general function does not have. What happens if a function is both injective and surjective?

DEFINITION 4.23 A function $f: A \to B$ is **bijective** if each $b \in B$ has exactly one preimage. A bijective function is called a **bijection**.

Since *"at least one"* combined with *"at most one"* gives *"exactly one,"* a function f is a bijection if and only if it is both an injection and a surjection. Consider the following examples of bijections.

- If $A = \{1, 2, 3, 4\}$ and $B = \{r, s, t, u\}$, then the function $f: A \to B$ defined by
$$f(1) = u, \qquad f(2) = r, \qquad f(3) = t, \qquad f(4) = s,$$
is a bijection.
- The functions $f: \mathbb{R} \to \mathbb{R}$ and $F: \mathbb{R} \to \mathbb{R}^+$ (where $\mathbb{R}^+$ denotes the set of positive real numbers) given by $f(x) = x^5$ and $F(x) = 5^x$ are bijections.
- For a nonempty set A, the identity function $i_A: A \to A$ is a bijection.

It should be clear why a bijection is also called a **one-to-one correspondence**.

DEFINITION 4.24 If $f: A \to B$ and $g: B \to A$ are functions, we say g is an *inverse* of f (and f is an inverse of g) if and only if $f \circ g = i_B$ and $g \circ f = i_A$.

The idea behind an inverse is that f sends an element a in A to an element b in B and then g sends it right back. Referring to the examples given above, we have the following:

- For the function $f: A \to B$, a function $g: B \to A$ defined by
$$g(r) = 2, \qquad g(s) = 4, \qquad g(t) = 3, \qquad g(u) = 1,$$
is an inverse of f. For example, $f(g(r)) = f(2) = r$ and $g(f(3)) = g(t) = 3$.
- An inverse to the function $f: \mathbb{R} \to \mathbb{R}$ is the function $g: \mathbb{R} \to \mathbb{R}$ defined by $g(x) = \sqrt[5]{x}$, while an inverse to the function $F: \mathbb{R} \to \mathbb{R}^+$ is the function $G: \mathbb{R}^+ \to \mathbb{R}$ defined by $G(x) = \log_5 x$. These follow from the identities
$$(\sqrt[5]{x}\,)^5 = x, \quad \sqrt[5]{x^5} = x, \qquad \text{and} \qquad \log_5 5^x = x, \quad 5^{\log_5 x} = x,$$
respectively. Note carefully the domains and codomains of the functions f and g and the functions F and G and the corresponding values of x for which the above equations are valid.

- The identity function $i_A: A \to A$ is its own inverse.

If you understand these examples and think about one-to-one correspondences, the following result should come as no surprise.

THEOREM 4.25 A function $f: A \to B$ has an inverse if and only if it is bijective.

Proof. Suppose first that f has an inverse and let g be an inverse of f. Since $g \circ f = i_A$ is injective, the function f is injective (see part (a) of Theorem 4.16). Since $f \circ g = i_B$ is surjective, the function f is surjective (see part (b) of Theorem 4.16). Since f is injective and surjective, it is bijective.

Conversely, suppose f is bijective. For each $b \in B$ there exists (the surjective part) a unique (the injective part) $a \in A$ such that $f(a) = b$. Let $g(b) = a$; this defines a function $g: B \to A$. It is easy to verify that $f \circ g = i_B$ and $g \circ f = i_A$, showing that g is an inverse of f. ■

We have talked about "an" inverse of f, but really there is only one.

THEOREM 4.26 If $f: A \to B$ has an inverse function, then the inverse is unique.

Proof. Suppose $g_1: B \to A$ and $g_2: B \to A$ are both inverses of f. By the definition of inverse functions, we know that $f \circ g_2 = i_B$ and $g_1 \circ f = i_A$. Since composition of functions is associative,

$$g_1 = g_1 \circ i_B = g_1 \circ (f \circ g_2) = (g_1 \circ f) \circ g_2 = i_A \circ g_2 = g_2.$$

This completes the proof. ■

Because of Theorem 4.26, we can talk about "the" inverse of f, assuming it has one; we write f^{-1} for the inverse of f. Note well that this extends the meaning of the symbol "f^{-1}" in a potentially confusing way. No matter what function f we are given, the induced set function f^{-1} is defined, but the inverse function f^{-1} is defined only if f is bijective. In other words, f^{-1} is always defined for *subsets* of the codomain, but it is defined for *elements* of the codomain only if f is a bijection.

We close this section with a pair of easy observations.

THEOREM 4.27

a) The composition of two bijections is a bijection.

b) The inverse of a bijection is a bijection.

Proof. The proof is left as an exercise. ■

Exercises 4.6.

1. Find examples of functions $f: A \to B$ and $g: B \to A$ such that $f \circ g = i_B$, but f and g are not inverse functions. Give examples involving finite sets A and B and examples using $A = \mathbb{N} = B$.
2. Suppose $[a]$ is a fixed element of $\mathbb{Z}_n$. Define $f: \mathbb{Z}_n \to \mathbb{Z}_n$ by $f([x]) = [a] + [x]$. Show that f is a bijection by finding an inverse of f.
3. Suppose $[u]$ is a fixed element of $\mathbb{U}_n$. Define $f: \mathbb{U}_n \to \mathbb{U}_n$ by $f([x]) = [u] \cdot [x]$. Show that f is a bijection by finding an inverse of f.

4. Suppose that m and b are real numbers with $m \neq 0$ and define a function $L: \mathbb{R} \to \mathbb{R}$ by $L(x) = mx + b$. Prove that L is a bijection, then find the inverse of L.
5. Show how Theorem 4.26 is simply a special case of Theorem 4.17.
6. Prove Theorem 4.27.
7. Referring to Exercise 5 in Section 4.4, find the inverse of each of the six functions in $\mathcal{F}$.
8. Let a, b, c, and d be real numbers for which $ad \neq bc$. Consider the function f defined by the formula $f(x) = (ax + b)/(cx + d)$, where the domain of f is the subset of $\mathbb{R}$ for which $f(x)$ is defined and the codomain of f is the range of f.
   a) Prove directly (that is, use algebra) that f is one-to-one.
   b) Find a formula for the inverse function f^{-1}. What are the domain and range of f^{-1}?
   c) Find conditions on a, b, c, and d so that $f = f^{-1}$.
9. Suppose $f: A \to A$ is a function and $f \circ f$ is bijective. Is f necessarily bijective?
10. Find a bijection $f: \mathbb{N} \to \mathbb{Z}$.
11. Suppose that $f: A \to B$ and $g: B \to C$ are bijections. Prove that $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.
12. Suppose that n is a positive integer and that $n = ab$, where a and b are relatively prime positive integers. Define a function $f: \mathbb{Z}_n \to \mathbb{Z}_a \times \mathbb{Z}_b$ by $f([x]) = ([x], [x])$. It is important to note that the symbol $[x]$ means different things in $\mathbb{Z}_n$, $\mathbb{Z}_a$, and $\mathbb{Z}_b$.
   a) Prove that f is a well-defined function.
   b) Prove that f is a bijection.
   c) Prove that f also gives a bijection between $\mathbb{U}_n$ and $\mathbb{U}_a \times \mathbb{U}_b$.
   d) Show how part (c) gives another proof of Corollary 3.38.

4.7 Cardinality and Countability

Consider the seemingly innocuous statement "The set of real numbers is 'larger' than the set of rational numbers." On the surface, this appears to be a simplistic observation. Since every rational number is a real number and there are real numbers that are not rational numbers, it seems clear that the set of real numbers contains more elements than the set of rational numbers. However, consider the statement, "there are more irrational numbers than there are rational numbers." Since these two sets are disjoint, this question is not as easy to dismiss; for that matter, since the sets are both infinite, it is not all that clear what it even means. How can one set be "more infinite" than another set? To answer this question, we must first agree on a definition of size for infinite sets.

For the usual sorts of sets we encounter every day, the question "When are two sets A and B the same size?" has a simple answer; the sets A and B have the same size when A and B have the same number of elements. When entering the realm of infinite sets, we need to be much more careful than this. A good way to motivate the definition of size for infinite sets is with a thought experiment. Consider a large auditorium that is filled with people. The fire code states that each person must have a seat, while the management wants every seat full in order to maximize revenue. How can you determine if both conditions are met? One method is to actually count the number of people and to count the number of seats. If there are 9852 people and 9852 seats, then everyone is satisfied. This would be a tedious task, and errors in counting could easily occur. A much more efficient method is to have everyone take a seat. If each person has a seat and if no seat is empty,

then there are the same number of people as seats. This is a true statement even if you do not know either the number of people or the number of seats.

It is thus possible to show that two sets have the same size without knowing the number of elements in each set: simply pair off the elements of each set. This method easily extends to infinite sets. Two infinite sets have the same size if their elements can be put into a one-to-one correspondence. We thus make the following definition.

DEFINITION 4.28 The sets A and B have the same size or **cardinality** if there is a bijection $f: A \to B$. When A and B have the same cardinality, we write $A \approx B$.

The difficulty, if one can call it that, is that this definition leads to intuitively bizarre results. For example, the set of positive integers and the set of even positive integers have the same size. This follows from the pairing (top to bottom)

$$\begin{array}{cccccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & \dots \\ 2 & 4 & 6 & 8 & 10 & 12 & 14 & 16 & 18 & 20 & \dots \end{array}$$

which establishes a one-to-one correspondence between the two sets. The fact that this pairing is a one-to-one correspondence is clear, but it seems just as clear that there are more positive integers than there are even positive integers. If a definition leads to contradictions (in the logical sense), it must be discarded; if it leads to results that seem to violate common sense, then the definition can either be left aside or intuition can rise to the occasion. In this case, it is intuition that must find a way to grapple with these strange properties of infinite sets. In other words, we will accept this definition and see where it leads.

Due to the fact that counterintuitive results appear to occur when working with the definition of cardinality, especially when dealing with infinite sets, we must proceed very carefully. For this reason, even "obvious" results require careful proofs using the definition of this new concept. The following theorem presents one of these "obvious" results.

THEOREM 4.29 For each positive integer n, we have $\{1, 2, \dots, n\} \not\approx \mathbb{N}$.

Proof. Suppose that $\{1, 2, \dots, n\} \approx \mathbb{N}$ for some positive integer n and let $f: \{1, 2, \dots, n\} \to \mathbb{N}$ be a bijection. It is easy to verify that the positive integer p defined by $p = \sum_{i=1}^{n} f(i)$ is not in the range of f. This is a contradiction to the fact that f is a bijection and the theorem follows. (Do you see how mathematical induction has implicitly entered the proof?) ■

We now record some simple but important properties of cardinality. Taken together, they reveal that the notion of cardinality determines an equivalence relation on a collection of sets.

THEOREM 4.30 Suppose A, B, and C are sets. Then

a) $A \approx A$;

b) if $A \approx B$, then $B \approx A$;

c) if $A \approx B$ and $B \approx C$, then $A \approx C$.

Proof. Let A and B be sets. Since $i_A: A \to A$ is a bijection, part (a) follows. Suppose that $A \approx B$ and let $f: A \to B$ be a bijection. By Theorem 4.27, the function $f^{-1}: B \to A$ is also a bijection. It follows that $B \approx A$, proving part (b). Part (c) follows from the fact that the composition of two bijections is a bijection; the details are left to the reader. ■

The next definition formalizes the introductory discussion concerning the relative sizes of arbitrary sets. It also introduces some adjectives that describe the various sizes of sets that are to be considered in these last two sections of the text.

DEFINITION 4.31 Let A be an arbitrary set.

a) The set A is **finite** if it is empty or if its elements can be put in a one-to-one correspondence with the set $\{1, 2, \ldots, n\}$ for some positive integer n.

b) The set A is **infinite** if it is not finite.

c) The set A is **countably infinite** if its elements can be put in a one-to-one correspondence with the set of positive integers.

d) The set A is **countable** if it is either finite or countably infinite.

e) The set A is **uncountable** if it is not countable.

The distinction between finite sets and infinite sets is generally easy to grasp: a finite set is eventually exhausted when you start listing out its elements, whereas an infinite set is not. For instance, the number of license plates using three letters (from the alphabet) and three single-digit numbers is finite. There are many of them, but in theory if you start writing down all of the possibilities, eventually the list would end. Intuitively, the set of positive integers is infinite because a list of positive integers never ends; Theorem 4.29 provides a rigorous proof of this fact. It then follows (see part (3) of Theorem 4.33) that the set of rational numbers is an infinite set, as is the set of real numbers.

According to the definition, a set A is countably infinite if $\mathbb{N} \approx A$, that is, A has the same cardinality as the natural numbers. If $f: \mathbb{N} \to A$ is a bijection, then

$$A = \{f(1), f(2), f(3), \ldots\}.$$

In other words, a set is countably infinite if and only if it can be arranged as an infinite sequence of distinct terms.

As indicated earlier, the set of even positive integers is countably infinite. Letting E^+ be the set of even positive integers, the function $f: \mathbb{N} \to E^+$ defined by $f(n) = 2n$ is a bijection. The set of all integers greater than -1000 is also countably infinite; the function g defined on $\mathbb{N}$ by $g(n) = n - 1000$ provides a one-to-one correspondence between these two sets. Since it is often difficult to express a correspondence between two sets as a function, a pairing of the elements of two sets is sometimes just written down as a pattern, with the assumption that the pattern continues. For example, the pairing

1	2	3	4	5	6	7	8	9	10	...
0	1	−1	2	−2	3	−3	4	−4	5	...

shows that the set $\mathbb{Z}$ is countably infinite. This pairing is probably easier to grasp than defining a function $f: \mathbb{N} \to \mathbb{Z}$ by

$$f(n) = \begin{cases} n/2, & \text{if } n \text{ is even;} \\ (1-n)/2, & \text{if } n \text{ is odd;} \end{cases}$$

and showing that it is a bijection.

The above examples show that a proper subset of an infinite set can have the same cardinality as the entire set. In fact, this is sometimes taken as the definition of an infinite set. In other words, this seeming paradox is actually part of the nature of an infinite set. This fact is stated precisely in the following theorem; be aware that understanding the proof requires some effort.

THEOREM 4.32 A set is infinite if and only if it has the same cardinality as one of its proper subsets.

Proof. Suppose first that X is an infinite set. Let x_1 be an arbitrary element of X, let x_2 be an arbitrary element of $X \setminus \{x_1\}$, let x_3 be an arbitrary element of $X \setminus \{x_1, x_2\}$, and so on. Since the set X is infinite, this process can be repeated for each positive integer n. Hence (by the strong form of the Principle of Mathematical Induction), the set X contains a countably infinite subset $\{x_n : n \in \mathbb{Z}^+\}$. Let $X_1 = X \setminus \{x_n : n \in \mathbb{Z}^+\}$ and let $Y = X_1 \cup \{x_{2n} : n \in \mathbb{Z}^+\}$. (Note that the set X_1 may be empty.) Then Y is a proper subset of X and the function $f: X \to Y$ defined by

$$f(x) = \begin{cases} x, & \text{if } x \in X_1; \\ x_{2n}, & \text{if } x = x_n; \end{cases}$$

is a bijection. It follows that X has the same cardinality as one of its proper subsets.

For the converse, we must prove that a finite set cannot have the same cardinality as any of its proper subsets. Since cardinality is an equivalence relation, we need only consider sets of positive integers. For each positive integer n, let $\pi_n = \{1, 2, \ldots, n\}$. We must show that for each n, the set π_n does not have the same cardinality as any of its proper subsets. To prove this, we apply the Principle of Mathematical Induction. It is obvious that the statement is true for both π_1 and π_2. Suppose that for some positive integer k, the set π_k does not have the same cardinality as any of its proper subsets. Let A be a proper subset of π_{k+1} and suppose that $f: \pi_{k+1} \to A$ is a bijection. There are two cases to consider.

i) Suppose that $k+1 \notin A$. Then $A \subseteq \pi_k$ and $f(k+1) \in \pi_k$. The function $g: \pi_k \to A \setminus \{f(k+1)\}$ defined by $g(i) = f(i)$ for each $i \in \pi_k$ is a bijection between π_k and one of its proper subsets, namely, the set $A \setminus \{f(k+1)\}$.

ii) Suppose that $k+1 \in A$. Without loss of generality, we may assume that $f(k+1) = k+1$. For if $f(p) = k+1$ for some $1 \leq p < k+1$, the function $f_1 : \pi_{k+1} \to A$ defined by

$$f_1(i) = \begin{cases} f(i), & \text{if } i \notin \{p, k+1\}; \\ f(p), & \text{if } i = k+1; \\ f(k+1), & \text{if } i = p; \end{cases}$$

is a bijection that satisfies $f_1(k+1) = k+1$. Now the function $g : \pi_k \to A \setminus \{k+1\}$ defined by $g(i) = f(i)$ for each $i \in \pi_k$ is a bijection between π_k and one of its proper subsets.

In either case the induction hypothesis is contradicted. Hence, the set π_{k+1} does not have the same cardinality as any of its proper subsets. By the Principle of Mathematical Induction, for each positive integer n, the set π_n does not have the same cardinality as any of its proper subsets. This completes the proof. ■

The next theorem lists some results that are easy to believe based upon the definitions of the concepts and intuition. However, careful proofs are once again required to establish the results.

THEOREM 4.33 The following results on finite and infinite sets are valid.

1. A subset of a finite set is finite.
2. The union of two finite sets is a finite set.
3. A set that contains an infinite subset is infinite.
4. Every infinite set contains a countably infinite subset.
5. The union of two countably infinite sets is a countably infinite set.
6. A subset of a countably infinite set is countable.
7. An infinite subset of a countably infinite set is countably infinite.
8. A set that contains an uncountable subset is uncountable.

Proof. The reader should note that parts (3), (7), and (8) are logical consequences of other parts of the theorem. In addition, part (4) was proved as the first step in the proof of Theorem 4.32. In what follows, we prove parts (1) and (6), leaving proofs for parts (2) and (5) as exercises.

For each positive integer n, let $\pi_n = \{1, 2, \ldots, n\}$. To establish (1), it is sufficient to prove the following fact: for each positive integer n, if $B \subseteq \pi_n$, then B is finite. We proceed to do so with mathematical induction. The statement is trivial for $n = 1$ and $n = 2$. Suppose that for some positive integer k, the statement "if $B \subseteq \pi_k$, then B is finite" is valid. Suppose that $B \subseteq \pi_{k+1}$. If $B \subseteq \pi_k$, then B is finite by the induction hypothesis. If B contains the element $k + 1$, then the set $B_1 = B \setminus \{k + 1\}$ is a subset of π_k and thus finite. Omitting the trivial case in which $B = \emptyset$, there exists a positive integer j and a bijection $f: B_1 \to \pi_j$. It follows easily that the function $g: B \to \pi_{j+1}$ defined by $g(x) = f(x)$ if $x \in B_1$ and $g(k + 1) = j + 1$ is a bijection, and we conclude that the set B is finite. We have thus shown that each subset of π_{k+1} is finite. By the Principle of Mathematical Induction, for each positive integer n, any subset of π_n is finite. This proves (1).

Since any countably infinite set can be put in a one-to-one correspondence with the set of positive integers, for (6) it is sufficient to prove that every subset of positive integers is countable. Let A be a subset of the positive integers. If A is finite, then A is countable and the proof is complete. Suppose that A is an infinite set. By the Well-Ordering Property of the positive integers, the set A contains a least element. Let $f(1)$ be the smallest integer in A. Similarly, let $f(2)$ be the smallest integer in $A \setminus \{f(1)\}$. In general, let $f(n + 1)$ be the smallest integer in $A \setminus \{f(1), \ldots, f(n)\}$. Since the set A is infinite, the function f is defined for each positive integer n, that is, the function f maps $\mathbb{N}$ into A. It is clear from the definition of f that f is a one-to-one function. To show that f is onto, let $a \in A$. The number of integers in A that are less than a is finite (there are at most $a - 1$ such integers). Let p be the number of elements in the set A that are less than a. By the definition

of the function f, we find that a is the smallest integer in the set $A \setminus \{f(1), f(2), \ldots, f(p)\}$. Then $f(p+1) = a$, and it follows that f is onto. Therefore, the function f establishes a one-to-one correspondence between $\mathbb{N}$ and A. This shows that A is countably infinite. ■

The assertion that there are more irrational numbers than there are rational numbers can now be stated precisely as follows: the set of rational numbers is countably infinite and the set of irrational numbers is uncountable. This fact, which was first published by Georg Cantor (see the next section for his biography), came as a surprise to mathematicians of the time. As a first step toward a proof, we prove that the union of a countable number of countable sets is a countable set. (The formation of a set of this type is explained in the proof of the theorem.)

THEOREM 4.34 A countable union of countable sets is countable.

Proof. It is sufficient to prove that a countably infinite union of disjoint countably infinite sets is countably infinite (see the exercises). In order to have a countably infinite number of sets, there must be one set corresponding to each positive integer n. Let $\{A_n : n \in \mathbb{N}\}$ be a countably infinite collection of sets. Suppose that each A_n is a countably infinite set and that none of the sets have any elements in common. We must prove that the set $A = \bigcup_{n=1}^{\infty} A_n$ is countably infinite. Since each A_n is countably infinite, its elements can be put into a one-to-one correspondence with the set of positive integers. For each n, let $A_n = \{x_{n,k} : k = 1, 2, \ldots\}$, that is,

$$A_1 = \{x_{1,1}, x_{1,2}, x_{1,3}, x_{1,4}, \ldots\},$$
$$A_2 = \{x_{2,1}, x_{2,2}, x_{2,3}, x_{2,4}, \ldots\},$$
$$A_3 = \{x_{3,1}, x_{3,2}, x_{3,3}, x_{3,4}, \ldots\},$$

and so on. By the Fundamental Theorem of Arithmetic, the pairing $x_{n,k} \longleftrightarrow 2^n 3^k$ is a one-to-one correspondence between A and an infinite subset of the positive integers. By part (7) of Theorem 4.33, the set A is countably infinite. ■

The previous theorem is often used to prove that an infinite set is countably infinite. If it is possible to decompose the set into a countably infinite number of subsets, each of which is countable, then the set is countably infinite. The advantage of this method for proving that a set is countably infinite is that there is no need to find a formula of correspondence or even to illustrate how the elements of the set can be paired with the positive integers. To illustrate the use of Theorem 4.34, we use it to prove that the set of rational numbers is countably infinite. (For the record, there are other ways to prove that $\mathbb{Q}$ is countably infinite.) The method of proof, which is summarized in the next few sentences, is quite typical. Let A be a set. For each positive integer n, define a subset A_n of A. The sets A_n must be defined in such a way that $A = \bigcup_{n=1}^{\infty} A_n$ and that a method for proving that each A_n is a countable set is apparent. It is this step of the proof that may require some creativity. The conclusion that A is countable then follows from Theorem 4.34. For the record, the ratio p/q of two integers is said to be in **simplest form** if p and q are relatively prime.

THEOREM 4.35 The set of rational numbers is countably infinite.

Proof. Let A_1 be the set of all rational numbers that in simplest form have a denominator of 1. The set A_1 is actually the set of integers and is thus countably infinite. Let A_2 be the set of all rational numbers that in simplest form have a denominator of 2. Since the only possible choices for the numerators are odd integers, the set A_2 is also countably infinite. In general, for each positive integer n, let A_n be the set of all rational numbers that in simplest form have a denominator of n. For instance,

$$A_3 = \left\{\ldots, -\frac{4}{3}, -\frac{2}{3}, -\frac{1}{3}, \frac{1}{3}, \frac{2}{3}, \frac{4}{3}, \ldots\right\} \quad \text{and} \quad A_4 = \left\{\ldots, -\frac{5}{4}, -\frac{3}{4}, -\frac{1}{4}, \frac{1}{4}, \frac{3}{4}, \frac{5}{4}, \ldots\right\}.$$

It should be clear that $\mathbb{Q} = \bigcup_{n=1}^{\infty} A_n$. Since the numerators that appear in the elements of A_n are integers that are relatively prime to n, each A_n can be put into a one-to-one correspondence with an infinite subset of $\mathbb{Z}$, that is, each of the sets A_n is countably infinite. By Theorem 4.34, the set $\mathbb{Q}$ is countably infinite. ■

Exercises 4.7.

1. For each pair of sets, find an explicit bijection from one set to the other.

- **a)** the positive integers and the odd positive integers
- **b)** the even integers and the odd integers
- **c)** the positive integers and the integers
- **d)** the interval $(1, 2)$ and the interval $(1, 6)$
- **e)** the interval $(0, 1)$ and the interval $(4, 50)$
- **f)** the set of real numbers and the interval $(0, \infty)$
- **g)** the set of real numbers and the interval $(0, 1)$
- **h)** the interval $(0, 1)$ and the interval $[0, 1]$

2. Define a function $f: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by $f(m, n) = 2^{m-1}(2n - 1)$. Prove that f is a bijection and conclude that $\mathbb{N} \times \mathbb{N}$ is countably infinite.

3. Suppose that A is a nonempty finite set. Prove that there exists a unique integer n with the property that $A \approx \{1, 2, \ldots, n\}$.

4. Prove part (2) of Theorem 4.33.

5. Give an induction argument to prove that the union of a finite number of finite sets is a finite set.

6. Prove part (5) of Theorem 4.33. (Although this result is a simple consequence of Theorem 4.34, the intention here is to give a direct proof of this one special case.)

7. Explain how parts (3), (7), and (8) of Theorem 4.33 are logical consequences of other parts of the theorem.

8. Prove that the union of a countable set and an uncountable set is uncountable.

9. Explain why the opening sentence in the proof of Theorem 4.34 is valid.

10. Let B be the collection of all sequences of 0's and 1's for which the number of 1's is finite. One example of an element of the set B is the sequence

$$1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, \ldots.$$

Use Theorem 4.34 to show that the set B is countably infinite. Can you prove that B is countably infinite in other ways?

4.8 Uncountability of the Reals

Since a countably infinite union of countably infinite sets is still countably infinite, it is difficult to imagine a set that is uncountable. However, such sets do exist. To prove that a set is uncountable, it is necessary to verify that there is no one-to-one correspondence between the given set and the set of positive integers. The following list of equivalent statements provides a common way to prove that an infinite set is uncountable:

$$\begin{aligned} A \text{ is an uncountable set} &\Leftrightarrow \neg(\exists f\colon \mathbb{N} \to A)\ (f \text{ is injective and } f \text{ is surjective}) \\ &\Leftrightarrow (\forall f\colon \mathbb{N} \to A)\ (f \text{ is not injective or } f \text{ is not surjective}) \\ &\Leftrightarrow (\forall f\colon \mathbb{N} \to A)\ (f \text{ is injective } \Rightarrow\ f \text{ is not surjective}) \end{aligned}$$

Hence, to prove that a set A is uncountable, it is sufficient to prove that every injection mapping $\mathbb{N}$ into A is not a surjection. This is the approach taken in the proof of the next theorem. In addition, the proof uses a famous technique known as the *Cantor diagonalization process*, named after the mathematician Georg Cantor.

THEOREM 4.36 The set of real numbers $\mathbb{R}$ is uncountable.

Proof. It is sufficient to prove that the open interval $(0, 1)$ is uncountable. Suppose that a function $f\colon \mathbb{N} \to (0, 1)$ is an injection. In other words, we can express the range of f as an infinite sequence $f(1)$, $f(2)$, $f(3)$, ... of distinct real numbers. To show that f is not a surjection, we show that this sequence cannot be a listing of all the real numbers in $(0, 1)$ by finding a real number that is not in the list. We begin by writing the numbers $f(i)$ in decimal form; the list might start something like this:

$$\begin{aligned} f(1) &= 0.\underline{2}3454167\ldots, \\ f(2) &= 0.1\underline{5}367843\ldots, \\ f(3) &= 0.86\underline{9}54367\ldots, \\ f(4) &= 0.199\underline{1}9423\ldots, \\ f(5) &= 0.2245\underline{3}665\ldots, \\ &\vdots \end{aligned}$$

Let r be the real number with decimal expansion $0.d_1d_2d_3d_4d_5\ldots$, where $d_i = 1$ unless the decimal expansion of $f(i)$ has a 1 in the ith place to the right of the decimal point, in which case $d_i = 5$. (For the list above, the expansion would be $0.11151\ldots$; the 'diagonal' entries are underlined. However, note that our method is completely general and not dependent on any particular listing.) This decimal expansion is different than *every* expansion in the list and it corresponds to a real number between 0 and 1. Therefore, the real number r determined in this way is not on the list; that is, the function f is not surjective. Since $f\colon \mathbb{N} \to (0, 1)$ was an arbitrary injective function, we conclude that the interval $(0, 1)$ is uncountable. ■

For the record, the fact that every real number has a decimal expansion requires proof. Since the proof of this fact requires properties of the real numbers that we have not discussed, it is not

included here. Furthermore, as the reader may recall, some real numbers have two different decimal expansions; for example,

$$0.274999999999\ldots = 0.275000000000\ldots$$

In the proof of Theorem 4.36, we may insist that the decimal expansion of each $f(i)$ does not end in all 9's. Our method for choosing a number not in the list (which is just one of many ways to accomplish this) guarantees that no number whose decimal expansion ends in all 0's or all 9's can appear. This means that there is no way our generated number could appear in the list but in a different form. It should be clear how the term "Cantor diagonalization process" appears. The listing of the decimal expansions can be interpreted as a very large (infinite in fact) matrix and the key step is moving along the diagonal and writing down a number that is different than the diagonal entry. It is a clever technique, one that is both simple and subtle.

COROLLARY 4.37 The set of irrational numbers is uncountable.

Proof. Suppose, by way of contradiction, that the set K of irrational numbers is countably infinite. Since the rational numbers $\mathbb{Q}$ are countably infinite and $\mathbb{R} = \mathbb{Q} \cup K$, it follows from Theorem 4.34 that the set of real numbers is countably infinite. As this is a contradiction to Theorem 4.36, the set of irrational numbers is uncountable. ■

Since the set of irrational numbers is uncountable and the set of rational numbers is countably infinite, it is certainly clear that there are more irrational numbers than there are rational numbers. It is not difficult to prove that between any two distinct rational numbers there is an irrational number and between any two distinct irrational numbers there is a rational number. Yet the set of irrational numbers is, in some sense, much larger than the set of rational numbers. It is difficult to make sense of these two statements at the same time. Nevertheless, both statements are valid and both statements are consequences of properties of the real number system.

We have seen that many infinite sets that might seem to have different sizes are in fact the same size and we have just seen that there are infinite sets that are not the same size. It turns out that there are infinitely many different sizes of infinite sets. In order to talk about the "size" of an infinite set, in much the same way that we talk about the size of a finite set (as in, "The set $\{a, b, c, d, e\}$ has size 5."), with every set A we associate a symbol $\overline{A}$, called the **cardinal number** of A, and we say that $\overline{A} = \overline{B}$ if and only if $A \approx B$.

Some cardinal numbers occur so frequently that they have been given special names: $\overline{\mathbb{N}} = \aleph_0$ ("aleph-naught") and $\overline{\mathbb{R}} = c$ (the size of the "continuum"). In this language, we can say that the "size" of $\mathbb{Q}$ or of $\mathbb{Z}$ is $\aleph_0$, and that the size of the open interval $(0, 1)$ is c.

One familiar feature of finite 'sizes' is that they come in a particular order—that is, if two sizes are different, then one is bigger than the other. When can we say that one infinite cardinal number is bigger than another? Here is a natural way: If $\overline{A}$ and $\overline{B}$ are cardinal numbers, define $\overline{A} \leq \overline{B}$ to mean that there is an injection $f: A \to B$. There is a potential, but somewhat subtle, problem with this definition. We are defining a relationship between 'sizes' by referring to *particular* sets that have those sizes. What if we were to choose different sets, say A_1 and B_1, with the same sizes? The following lemma shows that there is no cause for concern.

LEMMA 4.38 Suppose $\overline{A}_1 = \overline{A}_2$ and $\overline{B}_1 = \overline{B}_2$. There is an injection $f_1 \colon A_1 \to B_1$ if and only if there is an injection $f_2 \colon A_2 \to B_2$.

Proof. Suppose there is an injection $f_1 \colon A_1 \to B_1$. By hypothesis, there are bijections $\theta \colon A_2 \to A_1$ and $\phi \colon B_1 \to B_2$. By Theorem 4.16, the function $f_2 = \phi \circ f_1 \circ \theta$ is an injection from A_2 to B_2. Since the converse only requires a change of letters, the proof is complete. ∎

The upshot of this lemma is that the definition for $\overline{A} \leq \overline{B}$ does not depend upon which particular set is chosen to represent these two cardinal numbers, that is, "$\leq$" as used in this context is **well-defined**. This ordering of the cardinal numbers has some familiar properties.

THEOREM 4.39 Suppose that A, B, and C are sets. Then

a) $\overline{A} \leq \overline{A}$;

b) if $\overline{A} \leq \overline{B}$ and $\overline{B} \leq \overline{C}$, then $\overline{A} \leq \overline{C}$.

Proof. Part (a) follows from the simple observation that the identity map $i_A \colon A \to A$ is an injection. For part (b), the hypotheses imply that there exist injective functions $f \colon A \to B$ and $g \colon B \to C$. By Theorem 4.16, the function $g \circ f \colon A \to C$ is an injection. It follows that $\overline{A} \leq \overline{C}$. ∎

Theorem 4.39 shows that '$\leq$', as applied to infinite cardinal numbers, shares some properties with '$\leq$' in more familiar settings such as the integers or the real numbers. Another property that we rely on when dealing with real numbers is **anti-symmetry**: if $x \leq y$ and $y \leq x$, then $x = y$. We state without proof the following result. For the record, the proof is not exceptionally difficult, but it is rather abstract and hard to grasp.

THEOREM 4.40 Schröder-Bernstein Theorem If $\overline{A} \leq \overline{B}$ and $\overline{B} \leq \overline{A}$, then $\overline{A} = \overline{B}$. ∎

It is sometimes tempting to react to a result like this with, "Of course! How could it be otherwise?" This may be due in part to the use of the familiar symbol '$\leq$'—but just using the symbol hardly guarantees that it acts like '$\leq$' in more familiar contexts. Even paying attention to the new meaning, this theorem may seem "obvious." Perhaps the best way to see that it might not be so obvious is to look at a special case, one in which the injections f and g are easy to find, but there does not seem to be any "obvious" bijection. See Exercise 5 for a similar example.

EXAMPLE 4.41 Suppose $D = \{\, (x, y) : x^2 + y^2 \leq 1 \,\}$ is the unit disk in the plane and S is the square $\{\, (x, y) : x \in [-1, 1], y \in [-1, 1] \,\}$. Since $D \subseteq S$, it is clear that $\overline{D} \leq \overline{S}$. Since the function $f \colon S \to D$ defined by $f\big((x, y)\big) = (x/2, y/2)$ is an injection, we see that $\overline{S} \leq \overline{D}$. By the Schröder-Bernstein Theorem, $\overline{S} = \overline{D}$. It is an interesting exercise to seek an explicit bijection mapping D onto S; such a search provides an appreciation for the power of Theorem 4.40.

Thus far, we have seen infinite sets of two different sizes, $\aleph_0$ and c. Are there others? Is there a largest infinite size, that is, a largest cardinal number? Recall that for any set A, the **power set** of A, written $\mathcal{P}(A)$, is the collection of all subsets of A. For example, $\mathcal{P}(\{1, 2\}) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$. For finite sets, the power set is not just larger than the original set, it is *much* larger (see Exercise 7). This makes it natural to think that perhaps the power set of an infinite set will be larger than

the base set, that is, $\overline{A} < \overline{\mathcal{P}(A)}$. To be clear what this last statement is saying, let $\overline{A} < \overline{B}$ mean that $\overline{A} \leq \overline{B}$, but that A and B do not have the same cardinality. The next theorem answers both questions posed at the beginning of this paragraph.

THEOREM 4.42 Cantor's Theorem If A is any set, then $\overline{A} < \overline{\mathcal{P}(A)}$.

Proof. Since the function $f: A \to \mathcal{P}(A)$ defined by $f(a) = \{a\}$ is an injection, we find that $\overline{A} \leq \overline{\mathcal{P}(A)}$. To prove that $\overline{A} < \overline{\mathcal{P}(A)}$, we need to show that there is no bijection $g: A \to \mathcal{P}(A)$. To obtain a contradiction, suppose that g is such a bijection. Let $S = \{a \in A : a \notin g(a)\}$ and note that $S \subseteq A$. Since g is a surjection and $S \in \mathcal{P}(A)$, there exists some $x \in A$ such that $S = g(x)$. There are two possibilities to consider: $x \in S$ and $x \notin S$.

1. If $x \in S$, then $x \notin g(x)$, that is, $x \notin S$, a contradiction.

2. If $x \notin S$, then $x \in g(x)$, that is, $x \in S$, a contradiction.

Therefore, no such bijection is possible. (Compare the ideas in this proof with the concept of a normal set introduced in Exercise 11 in Section 1.5.) ■

Cantor's theorem implies that there are infinitely many infinite cardinal numbers, and that there is no largest cardinal number. It also has the following interesting consequence:

There is no such thing as the "set of all sets."

Suppose A were the set of all sets. Since every element of $\mathcal{P}(A)$ is a set, we would have $\mathcal{P}(A) \subseteq A$, which then implies that

$$\overline{\mathcal{P}(A)} \leq \overline{A} \leq \overline{\mathcal{P}(A)}.$$

By the Schröder–Bernstein Theorem, $\overline{\mathcal{P}(A)} = \overline{A}$, but this contradicts Cantor's Theorem.

Many questions about the cardinal numbers remain. Since we know that $\mathbb{Z}$ and $\mathbb{Q}$ are the same size, and that $\mathbb{R}$ is larger, one very natural question is whether there are any sets 'between' $\mathbb{Z}$ and $\mathbb{R}$, that is, strictly bigger than $\mathbb{Z}$ (and $\mathbb{Q}$) but strictly smaller than $\mathbb{R}$. The **continuum hypothesis** says:

There is no set A with $\aleph_0 < \overline{A} < c$.

That is, the continuum hypothesis asserts that c is the first cardinal number larger than $\aleph_0$; in symbols, this means that $\aleph_1 = c$. Assuming the usual axioms for our number systems, it is a remarkable fact that the continuum hypothesis *cannot be proved to be true and cannot be proved to be false*. In the 1920's, Kurt Gödel showed that the continuum hypothesis cannot be *disproved*, and in the early 1960's, Paul Cohen showed that it cannot be *proved* either. Hence, mathematicians can choose to add the continuum hypothesis as an axiom or to add the denial of the continuum hypothesis as an axiom. In each case, different results can be proved. With this conundrum, we bring to a close our introduction to higher mathematics.

Georg Cantor. Cantor (1845–1918) was born in St. Petersburg and grew up in Germany. He took an early interest in theological arguments about continuity and the infinite, and as a result studied philosophy, mathematics, and physics at universities in Zurich, Göttingen, and Berlin, though his father encouraged him to pursue engineering. He did his doctorate in number theory and then worked in analysis before doing his pioneering work in the theory of sets.

The prevailing opinion in the nineteenth century was that 'completed' infinities could not be studied rigorously; only 'potential' infinity made sense—for example, the process of repeatedly adding one, starting at 1, would never finish and was therefore infinite, but most mathematicians viewed the completed set of positive integers (or any other infinite set) as a dubious concept at best. An infinite set can be placed in one-to-one correspondence with a proper subset of itself; most mathematicians saw this as a paradox, and 'solved' the problem by declaring that 'infinite sets' simply make no sense.

A few mathematicians went against the grain; Dedekind realized that the 'paradoxical' correspondence between a set and one of its proper subsets could be taken as the *definition* of an infinite set. Cantor took this notion much further, showing that infinite sets come in an infinite number of sizes. Cantor knew most of what we have seen in this chapter: he showed that the rational numbers are countable, that $\mathbb{R}$ is not countable, and that $\mathcal{P}(A)$ is always bigger than A. The **algebraic numbers** are those real numbers that are roots of polynomials with rational coefficients—for example, $\sqrt{2}$ is a solution of $x^2 - 2 = 0$, and is therefore both irrational and algebraic (see Exercise 10 for further results concerning algebraic numbers). There are 'more' algebraic numbers than rational numbers, in the sense that the algebraic numbers form a proper superset of the rationals, but Cantor showed that the set of algebraic numbers is countable. This means that the **transcendental** numbers (that is, the non-algebraic numbers, like π and e) form an uncountable set—so in fact almost all real numbers are transcendental.

In addition to the arithmetic of infinite cardinal numbers, Cantor developed the theory of infinite ordinal numbers. The two concepts are practically the same for finite numbers, so the idea that infinite ordinals and infinite cardinals are different takes some getting used to. Since there is essentially only one way to make a total order out of four objects (namely, pick a first, a second, a third and a fourth), the cardinal number 4 ('how many') and the ordinal number 4 ('what order') are easily confused. For infinite sets the situation is radically different. The **ordinal** number of the positive integers, called ω, is simply the usual total ordering of the positive integers. 'Addition' of ordinals is accomplished by placing the orders side by side: $1 + \omega$ 'looks like' one item followed by a countable number of items *in the same order as the positive integers*—this looks just like the positive integers. On the other hand, $\omega + 1$ looks like the positive integers followed by a single item, and is much different than the usual ordering of the positive integers, even though the size of the two ordered sets is the same. (The easiest way to see that there is a crucial difference between the two orderings is to note that one element of $\omega + 1$ has an infinite number of predecessors, while all of the elements of $1 + \omega$ have a finite number of predecessors.)

Cantor was unable to secure a position at a major university, including Berlin, where he most desired to be. This failure was due in large part to the influence of Kronecker, a mathematician at Berlin, who ridiculed all talk of completed infinities, convinced that only finite processes could be justified. (As a result, he didn't believe in irrational numbers, since they could not be 'produced'

by a finite process.) Beginning in 1884, Cantor suffered a series of nervous breakdowns, presumably related to the refusal of so many mathematicians to accept his work; Cantor himself had occasional doubts about his results—the proofs were clear and rigorous, but the results still seemed paradoxical. Cantor died in a mental institution in 1918, though he did get some positive recognition for his work before his death. Writing a few years after Cantor's death, the great mathematician David Hilbert called Cantor's work "the most astonishing product of mathematical thought, one of the most beautiful realizations of human activity in the domain of the purely intelligible." The years since have more than justified this assessment of Cantor's work.

The information here is taken from *A History of Mathematics*, by Carl Boyer, New York: John Wiley & Sons, 1968. For a more detailed account of Cantor's life and work, see *Georg Cantor, His Mathematics and Philosophy of the Infinite*, by Joseph Dauben, Harvard University Press, 1979.

Exercises 4.8.

1. Prove that the set of real numbers that have more than one decimal expansion is countably infinite.

2. Let A be the collection of all sequences of 0's and 1's. One simple example of an element of the set A is the sequence

$$1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, \ldots.$$

a) Use Cantor's diagonal process to prove that the set A is uncountable.

b) Prove that the collection of all subsets of positive integers is uncountable by establishing a one-to-one correspondence between $\mathcal{P}(\mathbb{Z}^+)$ and the set A.

c) Explain and prove the statement $2^{\aleph_0} = c$. (Compare with Exercise 7 below.)

3. Suppose A and B are nonempty sets. Show that $\overline{A} \leq \overline{B}$ if and only if there is a surjection $g\colon B \to A$.

4. If A is countable and $f\colon A \to B$ is a surjection, prove that B is countable.

5. Find simple injections from $[0, 1]$ to $\mathbb{R}$ and from $\mathbb{R}$ to $[0, 1]$. Then find an explicit bijection from $[0, 1]$ to $\mathbb{R}$.

6. Let $I = (0, 1)$ and let $S = (0, 1) \times (0, 1)$. Use the Schröder-Bernstein Theorem to prove that $\overline{I} = \overline{S}$. (You might consider using decimal expansions for the injection from S to I.) This result implies that there is a one-to-one correspondence between one-dimensional space and two-dimensional space, a rather counter-intuitive idea.

7. Verify Cantor's Theorem for finite sets by showing that if A has n elements, then $\mathcal{P}(A)$ has 2^n elements.

8. Let S be an uncountable set and let B be a countably infinite subset of S. Prove that there is a one-to-one correspondence between S and $S \setminus B$.

9. Since the set of rational number is countably infinite, it is possible to write $\mathbb{Q} = \{r_n : n \in \mathbb{Z}^+\}$. Let ϵ be any positive number and for each n, let I_n be the interval

$$\left(r_n - \frac{\epsilon}{2^n}, r_n - \frac{\epsilon}{2^n}\right).$$

Show that $Q \subseteq \bigcup_{n=1}^{\infty} I_n$ and that $\sum_{n=1}^{\infty} \ell(I_n) = 2\epsilon$. What does this result say about the size of $\mathbb{Q}$?

10. The set of real numbers is composed of the rational numbers and the irrational numbers. Another classification of real numbers involves algebraic and transcendental numbers. An **algebraic number** is any number that is a root of a polynomial with integer coefficients. For example, the number $\sqrt{2}$ is algebraic since it is a root of the polynomial $x^2 - 2$. A **transcendental number** is a real number that is not an algebraic number.

a) Prove that every rational number is an algebraic number.

b) Prove that the square root and cube root of every positive integer is an algebraic number.

c) Prove that $2 - \sqrt{3}$ and $\sqrt{4 + \sqrt[3]{3}}$ are algebraic numbers.

d) Prove that the set of all algebraic numbers is countably infinite.

e) Prove that there exist transcendental numbers.

Bibliography

American Council of Learned Societies. *Biographical Dictionary of Mathematicians*. Charles Scribner's Sons, New York, 1991.

Carl B. Boyer. *A History of Mathematics*. John Wiley and Sons, New York, 1968.

Joseph Dauben. *Georg Cantor, His Mathematics and Philosophy of the Infinite*. Harvard University Press, Cambridge, MA, 1979.

Howard Eves. *An Introduction to the History of Mathematics*. Holt, Rinehart and Winston, New York, 1976.

G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. Oxford University Press, London, fourth edition, 1960.

William Judson LeVeque. *Topics in Number Theory*. Addison–Wesley, Reading, MA, 1956.

Calvin Long. *Elementary Introduction to Number Theory*. D. C. Heath, Lexington, MA, second edition, 1972.

Alexander Macfarlane. *Lectures on Ten British Mathematicians of the Nineteenth Century*. John Wiley & Sons, New York, 1916.

Index

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W