CHAPTER 3

ELEMENTARY NUMBER THEORY AND METHODS OF PROOF

The underlying content of this chapter is likely to be familiar to you. It consists of properties of integers (whole numbers), rational numbers (integer fractions), and real numbers. The underlying theme of this chapter is the question of how to determine the truth or falsity of a mathematical statement.

Here is an example involving a concept used frequently in computer science. Given any real number x, the floor of x, or greatest integer in x, denoted $\lfloor x \rfloor$, is the largest integer that is less than or equal to x. On the number line, $\lfloor x \rfloor$ is the integer immediately to the left of x (or equal to x if x is, itself, an integer). Thus $\lfloor 2.3 \rfloor = 2$, $\lfloor 12.99999 \rfloor = 12$, and $\lfloor -1.5 \rfloor = -2$. Consider the following two questions:

1. For any real number x, is $\lfloor x - 1 \rfloor = \lfloor x \rfloor - 1$?
2. For any real numbers x and y, is $\lfloor x - y \rfloor = \lfloor x \rfloor - \lfloor y \rfloor$?

Take a few minutes to try to answer these questions for yourself.

It turns out that the answer to (1) is yes, whereas the answer to (2) is no. Are these the answers you got? If not, don't worry. In Section 3.5 you will learn the techniques you need to answer these questions and more. If you did get the correct answers, congratulations! You have excellent mathematical intuition. Now ask yourself, "How sure am I of my answers? Were they plausible guesses or absolute certainties? Was there any difference in certainty between my answers to (1) and (2)? Would I have been willing to bet a large sum of money on the correctness of my answers?"

One of the best ways to think of a mathematical proof is as a carefully reasoned argument to convince a skeptical listener (often yourself) that a given statement is true. Imagine the listener challenging your reasoning every step of the way, constantly asking, "Why is that so?" If you can counter every possible challenge, then your proof as a whole will be correct.

As an example, imagine proving to someone not very familiar with mathematical notation that if x is a number with $5x + 3 = 33$, then $x = 6$. You could argue as follows:

> If $5x + 3 = 33$, then $5x + 3$ minus 3 will equal $33 - 3$ since subtracting the same number from two equal quantities gives equal results. But $5x + 3$ minus 3 equals $5x$ because adding 3 to $5x$ and then subtracting 3 just leaves $5x$. Also, $33 - 3 = 30$. Hence $5x = 30$. This means that x is a number which when multiplied by 5 equals 30. But the only number with this property is 6. Therefore, $x = 6$.

Of course there are other ways to phrase this proof, depending on the level of mathematical sophistication of the intended reader. In practice, mathematicians often omit reasons for certain steps of an argument when they are confident that the reader can easily supply them. When you are first learning to write proofs, however, it is better to err on the side of supplying too many reasons rather than too few. All too frequently, when even the best mathematicians carefully examine some "details" in their arguments, they discover that those details are actually false. Probably the most important reason for requiring proof in mathematics is that writing a proof forces us to become aware of weaknesses in our arguments and in the unconscious assumptions we have made.

Sometimes correctness of a mathematical argument can be a matter of life or death. Suppose, for example, that a mathematician is part of a team charged with designing a new type of airplane engine, and suppose that the mathematician is given the job of determining whether the thrust delivered by various engine types is adequate. If you knew that the mathematician was only fairly sure, but not positive, of the correctness of his analysis, you would probably not want to ride in the resulting aircraft.

At a certain point in Lewis Carroll's *Alice in Wonderland* (see exercise 28 in Section 1.2), the March Hare tells Alice to "say what you mean." In other words, she should be precise in her use of language: If she means a thing, then that is exactly what she should say. In this chapter, perhaps more than in any other mathematics course you have ever taken, you will find it necessary to say what you mean. Precision of thought and language is essential to achieve the mathematical certainty that is needed if you are to have complete confidence in your solutions to mathematical problems.

3.1 Direct Proof and Counterexample I: Introduction

Mathematics, as a science, commenced when first someone, probably a Greek, proved propositions about "any" things or about "some" things without specification of definite particular things. — Alfred North Whitehead, 1861–1947

Both discovery and proof are integral parts of problem solving. When you think you have discovered that a certain statement is true, try to figure out why it is true. If you succeed, you will know that your discovery is genuine. Even if you fail, the process of trying will give you insight into the nature of the problem and may lead to the discovery that the statement is false. For complex problems, the interplay between discovery and proof is not reserved to the end of the problem-solving process but, rather, is an important part of each step.

In this text we assume a familiarity with the laws of basic algebra, which are listed in Appendix A. We also use the three properties of equality: For all objects A, B, and C, (1) $A = A$, (2) if $A = B$ then $B = A$, and (3) if $A = B$ and $B = C$, then $A = C$. In addition, we assume that the set of integers is closed under addition, subtraction, and multiplication. This means that sums, differences, and products of integers are integers. Of course, most quotients of integers are not integers. For example, $3 \div 2$, which equals $3/2$, is not an integer, and $3 \div 0$ is not even a number.

The mathematical content of this section primarily concerns even and odd integers and prime and composite numbers.

Definitions

In order to evaluate the truth or falsity of a statement, you must understand what the statement is about. In other words, you must know the meanings of all terms that occur

in the statement. Mathematicians define terms very carefully and precisely and consider it important to learn definitions virtually word for word.

• Definitions

An integer n is **even** if, and only if, n equals twice some integer. An integer n is **odd** if, and only if, n equals twice some integer plus 1.

Symbolically, if n is an integer, then

$$n \text{ is even} \Leftrightarrow \exists \text{ an integer } k \text{ such that } n = 2k.$$
$$n \text{ is odd} \Leftrightarrow \exists \text{ an integer } k \text{ such that } n = 2k + 1.$$

It follows from the definition that if you are doing a problem in which you happen to know that a certain integer is even, you can deduce that it has the form 2 · (some integer). Conversely, if you know in some situation that a particular integer equals 2 · (some integer), then you can deduce that the integer is even.

Know a particular integer n is even. $\xrightarrow{\text{deduce}}$ n has the form 2 · (some integer).

Know n has the form 2 · (some integer). $\xrightarrow{\text{deduce}}$ n is even.

Example 3.1.1 Even and Odd Integers

Use the definitions of *even* and *odd* to justify your answers to the following questions.

a. Is 0 even?

b. Is −301 odd?

c. If a and b are integers, is $6a^2b$ even?

d. If a and b are integers, is $10a + 8b + 1$ odd?

e. Is every integer either even or odd?

Solution

a. Yes, $0 = 2 \cdot 0$.

b. Yes, $-301 = 2(-151) + 1$.

c. Yes, $6a^2b = 2(3a^2b)$, and since a and b are integers, so is $3a^2b$ (being a product of integers).

d. Yes, $10a + 8b + 1 = 2(5a + 4b) + 1$, and since a and b are integers, so is $5a + 4b$ (being a sum of products of integers).

e. The answer is yes, although the proof is not obvious. (Try giving a reason yourself.) We will show in Section 3.4 that this fact results from another fact known as the quotient-remainder theorem. ■

The integer 6, which equals 2 · 3, is a product of two smaller positive integers. On the other hand, 7 cannot be written as a product of two smaller positive integers; its only positive factors are 1 and 7. A positive integer, such as 7, that cannot be written as a product of two smaller positive integers is called *prime*.

• Definition

An integer n is **prime** if, and only if, $n > 1$ and for all positive integers r and s, if $n = r \cdot s$, then $r = 1$ or $s = 1$. An integer n is **composite** if, and only if, $n > 1$ and $n = r \cdot s$ for some positive integers r and s with $r \neq 1$ and $s \neq 1$.

Symbolically, if n is an integer that is greater than 1, then

$$n \text{ is prime} \Leftrightarrow \forall \text{ positive integers } r \text{ and } s, \text{ if } n = r \cdot s \text{ then } r = 1 \text{ or } s = 1.$$

$$n \text{ is composite} \Leftrightarrow \exists \text{ positive integers } r \text{ and } s \text{ such that } n = r \cdot s \text{ and } r \neq 1 \text{ and } s \neq 1.$$

Example 3.1.2 Prime and Composite Numbers

a. Is 1 prime?

b. Is it true that every integer greater than 1 is either prime or composite?

c. Write the first six prime numbers.

d. Write the first six composite numbers.

Solution

a. No. A prime number is required to be greater than 1.

b. Yes. For any integer greater than 1, the two definitions are negations of each other.

c. 2, 3, 5, 7, 11, 13

d. 4, 6, 8, 9, 10, 12 ■

Proving Existential Statements

According to the definition given in Section 2.1, a statement in the form

$$\exists x \in D \text{ such that } Q(x)$$

is true if, and only if,

$$Q(x) \text{ is true for at least one } x \text{ in } D.$$

One way to prove this is to find an x in D that makes $Q(x)$ true. Another way is to give a set of directions for finding such an x. Both of these methods are called **constructive proofs of existence.**

Example 3.1.3 Constructive Proofs of Existence

a. Prove the following: $\exists$ an even integer n that can be written in two ways as a sum of two prime numbers.

b. Suppose that r and s are integers. Prove the following: $\exists$ an integer k such that $22r + 18s = 2k$.

Solution

a. Let $n = 10$. Then $10 = 5 + 5 = 3 + 7$ and 3, 5, and 7 are all prime numbers.

b. Let $k = 11r + 9s$. Then k is an integer because it is a sum of products of integers; and by substitution, $2k = 2(11r + 9s)$, which equals $22r + 18s$ by the distributive law of algebra. ■

A **nonconstructive proof of existence** involves showing either (a) that the existence of a value of x that makes $Q(x)$ true is guaranteed by an axiom or a previously proved theorem or (b) that the assumption that there is no such x leads to a contradiction. The disadvantage of a nonconstructive proof is that it may give virtually no clue about where or how x may be found. The widespread use of digital computers in recent years has led to some dissatisfaction with this aspect of nonconstructive proofs and to increased efforts to produce constructive proofs containing directions for computer calculation of the quantity in question.

Disproving Universal Statements by Counterexample

To disprove a statement means to show that it is false. Consider the question of disproving a statement of the form

$$\forall x \text{ in } D, \text{ if } P(x) \text{ then } Q(x).$$

Showing that this statement is false is equivalent to showing that its negation is true. The negation of the statement is existential:

$$\exists x \text{ in } D \text{ such that } P(x) \text{ and not } Q(x).$$

But to show that an existential statement is true, we generally give an example, and because the example is used to show that the original statement is false, we call it a *counterexample*. Thus the method of disproof by *counterexample* can be written as follows:

Disproof by Counterexample

To disprove a statement of the form "$\forall x \in D$, if $P(x)$ then $Q(x)$," find a value of x in D for which $P(x)$ is true and $Q(x)$ is false. Such an x is called a **counterexample.**

Example 3.1.4 Disproof by Counterexample

Disprove the following statement by finding a counterexample:

$$\forall \text{ real numbers } a \text{ and } b, \text{ if } a^2 = b^2 \text{ then } a = b.$$

Solution To disprove this statement, you need to find real numbers a and b such that $a^2 = b^2$ and $a \neq b$. The fact that both positive and negative integers have positive squares helps in the search. If you flip through some possibilities in your mind, you will quickly see that 1 and -1 will work (or 2 and -2, or 0.5 and -0.5, and so forth).

Statement: $\forall$ real numbers a and b, if $a^2 = b^2$, then $a = b$.

Counterexample: Let $a = 1$ and $b = -1$. Then $a^2 = 1^2 = 1$ and $b^2 = (-1)^2 = 1$, and so $a^2 = b^2$. But $a \neq b$ since $1 \neq -1$.

■

It is a sign of intelligence to make generalizations. Frequently, after observing a property to hold in a large number of cases, you may guess that it holds in all cases. You may, however, run into difficulty when you try to prove your guess. Perhaps you just have not figured out the key to the proof. But perhaps your guess is false. Consequently, when you are having serious difficulty proving a general statement, you should interrupt your efforts to look for a counterexample. Analyzing the kinds of problems you are encountering in your proof efforts may help in the search. It may even happen that if

you find a counterexample and therefore prove the statement false, your understanding may be sufficiently clarified that you can formulate a more limited but true version of the statement. For instance, Example 3.1.4 shows that it is not always true that if the squares of two numbers are equal, then the numbers are equal. However, it is true that if the squares of two *positive* numbers are equal, then the numbers are equal.

Proving Universal Statements

The vast majority of mathematical statements to be proved are universal. In discussing how to prove such statements, it is helpful to imagine them in a standard form:

$$\forall x \in D, \text{ if } P(x) \text{ then } Q(x).$$

In Section 2.1 we showed that any universal statement can be written in this form and that when D is finite, such a statement can be proved by the method of exhaustion. This method can also be used when there are only a finite number of elements that satisfy the condition $P(x)$.

Example 3.1.5 The Method of Exhaustion

Use the method of exhaustion to prove the following statement:

$\forall n \in \mathbf{Z}$, if n is even and $4 \leq n \leq 30$, then n can be written as a sum of two prime numbers.

Solution

$$\begin{array}{llll} 4 = 2 + 2 & 6 = 3 + 3 & 8 = 3 + 5 & 10 = 5 + 5 \\ 12 = 5 + 7 & 14 = 11 + 3 & 16 = 5 + 11 & 18 = 7 + 11 \\ 20 = 7 + 13 & 22 = 5 + 17 & 24 = 5 + 19 & 26 = 7 + 19 \\ 28 = 11 + 17 & 30 = 11 + 19 & & \end{array}$$

■

In most cases in mathematics, however, the method of exhaustion cannot be used. For instance, can you prove by exhaustion that *every* even integer greater than 2 can be written as a sum of two prime numbers? No. To do that you would have to check every even integer, and because there are infinitely many such numbers, this is an impossible task.

Even when the domain is finite, it may be infeasible to use the method of exhaustion. Imagine, for example, trying to check by exhaustion that the multiplication circuitry of a particular computer gives the correct result for every pair of numbers in the computer's range. Since a typical computer would require thousands of years just to compute all possible products of all numbers in its range (not to mention the time it would take to check the accuracy of the answers), checking correctness by the method of exhaustion is obviously impractical.

The most powerful technique for proving a universal statement is one that works regardless of the size of the domain over which the statement is quantified. It is called the *method of generalizing from the generic particular*. Here is the idea underlying the method:

Method of Generalizing from the Generic Particular

To show that every element of a domain satisfies a certain property, suppose x is a *particular* but *arbitrarily chosen* element of the domain, and show that x satisfies the property.

Example 3.1.6 Generalizing from the Generic Particular

At some time you may have been shown a "mathematical trick" like the following. You ask a person to pick any number, add 5, multiply by 4, subtract 6, divide by 2, and subtract twice the original number. Then you astound the person by announcing that their final result was 7. How does this "trick" work? Let x stand for the number the person picks. Here is what happens when the person follows your directions:

Step	Result
Pick a number.	x
Add 5.	$x + 5$
Multiply by 4.	$(x + 5) \cdot 4 = 4x + 20$
Subtract 6.	$(4x + 20) - 6 = 4x + 14$
Divide by 2.	$\frac{4x + 14}{2} = 2x + 7$
Subtract twice the original number.	$(2x + 7) - 2x = 7$

Thus no matter what number the person starts with, the result will always be 7. Note that the x in the analysis above is *particular* (because it represents a single quantity), but it is also *arbitrarily chosen* or *generic* (because it can represent any number whatsoever). This illustrates the process of drawing a general conclusion from a particular but generic object. ■

The point of having x be arbitrarily chosen (or generic) is to make a proof that can be generalized to all elements of the domain. By choosing x arbitrarily, you are making no special assumptions about x that are not also true of all other elements of the domain. The word *generic* means "sharing all the common characteristics of a group or class." Thus everything you deduce about a generic element x of the domain is equally true of any other element of the domain.

When the method of generalizing from the generic particular is applied to a property of the form "If $P(x)$ then $Q(x)$," the result is the method of *direct proof*. Recall that the only way "If $P(x)$ then $Q(x)$" can be false is for $P(x)$ to be true and $Q(x)$ to be false. Thus to show that "If $P(x)$ then $Q(x)$" is true, suppose $P(x)$ is true and show that $Q(x)$ must also be true. It follows by the method of generalizing from the generic particular that to prove a statement of the form "$\forall x \in D$, if $P(x)$ then $Q(x)$," you suppose x is a particular but arbitrarily chosen element of D that satisfies $P(x)$, and then you show that x satisfies $Q(x)$.

Method of Direct Proof

1. Express the statement to be proved in the form "$\forall x \in D$, if $P(x)$ then $Q(x)$." (This step is often done mentally.)
2. Start the proof by supposing x is a particular but arbitrarily chosen element of D for which the hypothesis $P(x)$ is true. (This step is often abbreviated "Suppose $x \in D$ and $P(x)$.")
3. Show that the conclusion $Q(x)$ is true by using definitions, previously established results, and the rules for logical inference.

Example 3.1.7 A Direct Proof of a Theorem

Prove that the sum of any two even integers is even.

Caution! The word two in this statement does not necessarily refer to two distinct integers. If a choice of integers is made arbitrarily, the integers are very likely to be distinct, but they might be the same.

Solution Whenever you are presented with a statement to be proved, it is a good idea to ask yourself whether you believe it to be true. In this case you might imagine some pairs of even integers, say $2 + 4$, $6 + 10$, $12 + 12$, $28 + 54$, and mentally check that their sums are even. However, since you cannot possibly check all pairs of even numbers, you cannot know for sure that the statement is true in general by checking its truth in these particular instances. Many properties hold for a large number of examples and yet fail to be true in general.

To prove this statement in general, you need to show that no matter what even integers are given, their sum is even. But given any two even integers, it is possible to represent them as $2r$ and $2s$ for some integers r and s. And by the distributive law of algebra, $2r + 2s = 2(r + s)$, which is even. Thus the statement is true in general.

Suppose the statement to be proved were much more complicated than this. What is the statement method you could use to derive a proof?

Formal Restatement: $\forall$ integers m and n, if m and n are even then $m + n$ is even.

This statement is universally quantified over an infinite domain. Thus to prove it in general, you need to show that no matter what two integers you might be given, if both of them are even then their sum will also be even.

Next ask yourself, "Where am I starting from?" or "What am I supposing?" The answer to such a question gives you the starting point, or first sentence, of the proof.

Starting Point: Suppose m and n are particular but arbitrarily chosen integers that are even.

Or, in abbreviated form:

Suppose m and n are any even integers.

Then ask yourself, "What conclusion do I need to show in order to complete the proof?"

To Show: $m + n$ is even.

At this point you need to ask yourself, "How do I get from the starting point to the conclusion?" Since both involve the term *even integer,* you must use the definition of this term—and thus you must know what it means for an integer to be even. It follows from the definition that since m and n are even,

$$m = 2r, \text{ for some integer } r \quad \text{and} \quad n = 2s, \text{ for some integer } s.$$

(The reason you have to use two different letters r and s is that m and n are arbitrarily chosen—they could be any pair of even integers whatsoever. If you had set $m = 2r$ and $n = 2r$, then m would equal n, which need not be the case.)

Now what you want to show is that $m + n$ is even. In other words, you want to show something about the expression $m + n$. Having just found alternate representations for m (as $2r$) and n (as $2s$), it seems reasonable to substitute these representations in place of m and n:

$$m + n = 2r + 2s.$$

Your goal is to show that $m + n$ is even. By definition of even, this means that $m + n$ can be written in the form

$$2 \cdot (\text{some integer}).$$

This analysis narrows the gap between the starting point and what is to be shown to showing that

$$2r + 2s = 2 \cdot (\text{some integer}).$$

Why is this true? First, because of the distributive law from algebra, which says that

$$2r + 2s = 2(r + s),$$

and, second, because the sum of any two integers is an integer, which implies that $r + s$ is an integer.

This discussion is summarized by rewriting the statement as a theorem and giving a formal proof of it. (In mathematics, the word *theorem* refers to a statement that is known to be true because it has been proved.) The formal proof, as well as many others in this text, includes explanatory notes to make its logical flow apparent. Such comments are purely a convenience for the reader and could be omitted entirely. For this reason they are italicized and enclosed in square brackets: [ ].

Donald Knuth, one of the pioneers of the science of computing, has compared constructing a computer program from a set of specifications to writing a mathematical proof based on a set of axioms.* In keeping with this analogy, the bracketed comments can be thought of as similar to the explanatory documentation provided by a good programmer. Documentation is not necessary for a program to run, but it helps a human reader understand what is going on.

Theorem 3.1.1

The sum of any two even integers is even.

Proof:

Suppose m and n are [*particular but arbitrarily chosen*] even integers. [*We must show that $m + n$ is even.*] By definition of even, $m = 2r$ and $n = 2s$ for some integers r and s. Then

$$\begin{aligned} m + n &= 2r + 2s && \text{by substitution} \\ &= 2(r + s) && \text{by factoring out a 2.} \end{aligned}$$

Let $k = r + s$. Note that k is an integer because it is a sum of integers. Hence

$$m + n = 2k \quad \text{where } k \text{ is an integer.}$$

It follows by definition of even that $m + n$ is even. [*This is what we needed to show.*]†

■

Most theorems, like the one above, can be analyzed to a point where you realize that as soon as a certain thing is shown, the theorem will be proved. When that thing has been

*Donald E. Knuth, *The Art of Computer Programming*, 2nd ed., Vol. I (Reading, MA: Addison-Wesley, 1973), p. ix.

†See page 113 for a discussion of the role of universal modus ponens in this proof.

shown, it is natural to end the proof with the words "this is what we needed to show." The Latin words for this are *quod erat demonstrandum,* or Q.E.D. for short. Proofs in older mathematics books end with these initials.

Note that both the *if* and the *only if* parts of the definition of even were used in the proof of Theorem 3.1.1. Since m and n were known to be even, the *only if* ($\Rightarrow$) part of the definition was used to deduce that m and n had a certain general form. Then, after some algebraic substitution and manipulation, the *if* ($\Leftarrow$) part of the definition was used to deduce that $m + n$ was even.

Directions for Writing Proofs of Universal Statements

Think of a proof as a way to communicate a convincing argument for the truth of a mathematical statement. When you write a proof, imagine that you will be sending it to a capable classmate who has had to miss the last week or two of your course. Try to be clear and complete. Keep in mind that your classmate will see only what you actually write down, not any unexpressed thoughts behind it.

Over the years, the following rules of style have become fairly standard for writing the final versions of proofs:

1. **Copy the statement of the theorem to be proved on your paper.**
2. **Clearly mark the beginning of your proof with the word Proof.**
3. **Make your proof self-contained.**

   This means that you should identify each variable used in your proof in the body of the proof. Thus you will begin proofs by introducing the initial variables and stating what kind of objects they are. The first sentence of your proof would be something like "Suppose m and n are integers" or "Let x be a real number that is greater than 2." This is similar to declaring variables and their data types at the beginning of a computer program.

   At a later point in your proof, you may introduce a new variable to represent a quantity that is known to exist. For example, if you know that a particular integer n is even, then you know that n equals 2 times some integer. It is usually convenient to give this integer a name so that you can work with it concretely later in the proof. Thus if you decide to call the integer, say, s, you would write, "Since n is even, $n = 2s$ for some integer s."
4. **Write your proof in complete sentences.**

   This does not mean that you should avoid using symbols and shorthand abbreviations, just that you should incorporate them into sentences. For example, the proof of Theorem 3.1.1 contains the sentence

$$\begin{aligned} \text{Then } m + n &= 2r + 2s \\ &= 2(r + s). \end{aligned}$$

   To read this as a sentence, read the first equals sign as "equals" and each subsequent equals sign as "which equals."
5. **Give a reason for each assertion you make in your proof.**

   Each assertion in a proof should come directly from the hypothesis of the theorem, or follow from the definition of one of the terms in the theorem, or be a result obtained earlier in the proof, or be a mathematical result that has previously been established or is agreed to be assumed. Indicate the reason for each step of your proof using phrases such as *by hypothesis, by definition of . . .*, and *by theorem . . .*.

6. **Include the "little words" that make the logic of your arguments clear.**

When writing a mathematical argument, especially a proof, indicate how each sentence is related to the previous one. Does it follow from the previous sentence or from a combination of the previous sentence and earlier ones? If so, start the sentence by stating the reason why it follows or by writing *Then,* or *Thus,* or *So,* or *Hence,* or *Therefore,* or *It follows that,* and include the reason at the end of the sentence. For instance, in the proof of Theorem 3.1.1, once you know that m is even, you can write: "By definition of even, $m = 2k$ for some integer k," or you can write, "Then $m = 2k$ for some integer k by definition of even."

If a sentence expresses a new thought or fact that does not follow as an immediate consequence of the preceding statement but is needed for a later part of a proof, introduce it by writing *Observe that,* or *Note that,* or *But,* or *Now.*

Sometimes in a proof it is desirable to define a new variable in terms of previous variables. In such a case, introduce the new variable with the word *Let.* For instance, in the proof of Theorem 3.1.1, once it is known that $m + n = 2(r + s)$, where r and s are integers, a new variable k is introduced to represent $r + s$. The proof goes on to say, "Let $k = r + s$. Then k is an integer because it is a sum of two integers."

Variations among Proofs

It is rare that two proofs of a given statement, written by two different people, are identical. Even when the basic mathematical steps are the same, the two people may use different notation or may give differing amounts of explanation for their steps, or may choose different words to link the steps together into paragraph form. An important question is how detailed to make the explanations for the steps of a proof. This must ultimately be worked out between the writer of a proof and the intended reader, whether they be student and teacher, teacher and student, student and fellow student, or mathematician and colleague. Your teacher may provide explicit guidelines for you to use in your course. Or you may follow the example of the proofs in this book (which are generally explained rather fully in order to be understood by students at various stages of mathematical development). Remember that the phrases written inside brackets [ ] are intended to elucidate the logical flow or underlying assumptions of the proof and need not be written down at all. It is entirely your decision whether to include such phrases in your own proofs.

Common Mistakes

The following are some of the most common mistakes people make when writing mathematical proofs.

1. **Arguing from examples.**

Looking at examples is one of the most helpful practices a problem solver can engage in and is encouraged by all good mathematics teachers. However, it is a mistake to think that a general statement can be proved by showing it to be true for some special cases. A universal statement may be true in many instances without being true in general.

Here is an example of this mistake. It is an incorrect "proof" of the fact that the sum of any two even integers is even. (Theorem 3.1.1).

> This is true because if $m = 14$ and $n = 6$, which are both even,
> then $m + n = 20$, which is also even.

Some people find this kind of argument convincing because it does, after all, consist of evidence in support of a true conclusion. But remember that when we discussed

valid arguments, we pointed out that an argument may be invalid and yet have a true conclusion. In the same way, an argument from examples may be mistakenly used to "prove" a true statement. In the example above, it is not sufficient to show that the conclusion "$m + n$ is even" is true for $m = 14$ and $n = 6$. You must give an argument to show that the conclusion is true for any even integers m and n.

2. **Using the same letter to mean two different things.**
   Some beginning theorem provers give a new variable quantity the same letter name as a previously introduced variable. Consider the following "proof" fragment:

   > Suppose m and n are odd integers. Then by definition of odd, $m = 2k + 1$ and $n = 2k + 1$ for some integer k.

   This is incorrect. Using the same symbol, k, in the expressions for both m and n implies that $m = 2k + 1 = n$. It follows that the rest of the proof applies only to integers m and n that equal each other. This is inconsistent with the supposition that m and n are arbitrarily chosen odd integers. For instance, the proof would not show that the sum of 3 and 5 is even.

3. **Jumping to a conclusion.**
   To jump to a conclusion means to allege the truth of something without giving an adequate reason. Consider the following "proof" that the sum of any two even integers is even.

   > Suppose m and n are any even integers. By definition of even, $m = 2r$ and $n = 2s$ for some integers r and s. Then $m + n = 2r + 2s$. So $m + n$ is even.

   The problem with this "proof" is that the crucial calculation

   $$2r + 2s = 2(r + s)$$

   is missing. The author of the "proof" has jumped prematurely to a conclusion.

4. **Begging the question.**
   To beg the question means to assume what is to be proved; it is a variation of jumping to a conclusion. As an example, consider the following "proof" of the fact that the product of any two odd integers is odd:

   > Suppose m and n are any odd integers. When any odd integers are multiplied, their product is odd. Hence mn is odd.

   Here is another, more subtle example of the same mistake.

   > Suppose m and n are odd integers. If mn is odd, then $mn = 2k + 1$ for some integer k. Also by definition of odd, $m = 2a + 1$ and $n = 2b + 1$ for some integers a and b. Then $mn = (2a + 1)(2b + 1) = 2k + 1$, which is odd by definition of odd. This is what was to be shown.

   The problem with this "proof" is that the author first states what it means for the conclusion to be true (that $m \cdot n$ can be expressed as $2k + 1$ for some integer k) and later just assumes it to be true (by setting $(2a + 1) \cdot (2b + 1)$ equal to $2k + 1$). Thus the author of the "proof" begs the question.

5. **Misuse of the word *if*.**
   Another common error is not serious in itself, but it reflects imprecise thinking that sometimes leads to problems later in a proof. This error involves using the word *if* when the word *because* is really meant. Consider the following proof fragment:

> Suppose p is a prime number. If p is prime, then p cannot be written as a product of two smaller positive integers.

The use of the word *if* in the second sentence is inappropriate. It suggests that the primeness of p is in doubt. But p is known to be prime by the first sentence. It cannot be written as a product of two smaller positive integers *because* it is prime. Here is a correct version of the fragment:

> Suppose p is a prime number. Because p is prime, p cannot be written as a product of two smaller positive integers.

Getting Proofs Started

Believe it or not, once you understand the idea of generalizing from the generic particular and the method of direct proof, you can write the beginnings of proofs even for theorems you do not understand. The reason is that the starting point and what is to be shown in a proof depend only on the linguistic form of the statement to be proved, not on the content of the statement.

Example 3.1.8 Identifying the "Starting Point" and the "Conclusion to Be Shown"

Write the first sentence of a proof of the following statement (the "starting point") and the last sentence of a proof (the "conclusion to be shown"):

> Every complete, bipartite graph is connected. You are not expected to understand this statement.

Solution It is helpful to rewrite the statement formally using a quantifier and a variable:

Formal Restatement: $\forall$ graphs G, if G is complete and bipartite, then G is connected.
(domain; hypothesis; conclusion)

The first sentence, or starting point, of a proof supposes the existence of an object (in this case G) in the domain (in this case the set of all graphs) that satisfies the hypothesis of the if-then part of the statement (in this case that G is complete and bipartite). The conclusion to be shown is just the conclusion of the if-then part of the statement (in this case that G is connected).

Starting Point: Suppose G is a [*particular but arbitrarily chosen*] graph such that G is complete and bipartite.

Conclusion to Be Shown: G is connected.

Thus the proof has the following first and last sentences:

First sentence of proof: Suppose G is a [*particular but arbitrarily chosen*] graph such that G is complete and bipartite.

Last sentence of proof: Therefore G is connected.

Of course, to reach the last sentence of the proof, the definitions of the terms will have to be used. ■

Showing That an Existential Statement Is False

Recall that the negation of an existential statement is universal. It follows that to prove an existential statement is false, you must prove a universal statement (its negation) is true.

Example 3.1.9 Disproving an Existential Statement

Show that the following statement is false:

There is a positive integer n such that $n^2 + 3n + 2$ is prime.

Solution Proving that the given statement is false is equivalent to proving its negation is true. The negation is

For all positive integers n, $n^2 + 3n + 2$ is not prime.

Because the negation is universal, it is proved by generalizing from the generic particular.

Claim: The statement "There is a positive integer n such that $n^2 + 3n + 2$ is prime" is false.

Proof:

Suppose n is any [*particular but arbitrarily chosen*] positive integer. [*We will show that $n^2 + 3n + 2$ is not prime.*] We can factor $n^2 + 3n + 2$ to obtain $n^2 + 3n + 2 = (n + 1)(n + 2)$. We also note that $n + 1$ and $n + 2$ are integers (because they are sums of integers) and that both $n + 1 > 1$ and $n + 2 > 1$ (because $n \geq 1$). Thus $n^2 + 3n + 2$ is a product of two integers each greater than 1, and so $n^2 + 3n + 2$ is not prime. ■

Conjecture, Proof, and Disproof

CORBIS

Pierre de Fermat (1601–1665)

Andrew Wiles/Princeton University

Andrew Wiles (born 1953)

More than 350 years ago, the French mathematician Pierre de Fermat claimed that it is impossible to find positive integers x, y, and z with $x^n + y^n = z^n$ if n is an integer that is at least 3. (For $n = 2$, the equation has many integer solutions, such as $3^2 + 4^2 = 5^2$ and $5^2 + 12^2 = 13^2$.) Fermat wrote his claim in the margin of a book, along with the comment "I have discovered a truly remarkable proof of this theorem which this margin is too small to contain." No proof, however, was found among his papers, and over the years some of the greatest mathematical minds tried and failed to discover a proof or a counterexample, for what came to be known as Fermat's last theorem.

In 1986 Kenneth Ribet of the University of California at Berkeley showed that if a certain other statement, the Taniyama–Shimura conjecture, could be proved, then Fermat's theorem would follow. Andrew Wiles, an English mathematician and faculty member at Princeton University, had become intrigued by Fermat's claim while still a child and, as an adult, had come to work in the branch of mathematics to which the Taniyama–Shimura conjecture belonged. As soon as he heard of Ribet's result, Wiles immediately set to work to prove the conjecture. In June of 1993, after 7 years of concentrated effort, he presented a proof to worldwide acclaim.

During the summer of 1993, however, while every part of the proof was being carefully checked to prepare for formal publication, Wiles found that he could not justify one step and that that step might actually be wrong. He worked unceasingly for another year to resolve the problem, finally realizing that the gap in the proof was a genuine error but that an approach he had worked on years earlier and abandoned provided a way around the difficulty. By the end of 1994, the revised proof had been thoroughly checked and pronounced correct in every detail by experts in the field. It was published in the *Annals of Mathematics* in 1995. Several books and an excellent documentary television show have been produced that convey the drama and excitement of Wiles's discovery.*

*"The Proof," produced in 1997, for the series *Nova* on the Public Broadcasting System; *Fermat's Enigma: The Epic Quest to Solve the World's Greatest Mathematical Problem*, by Simon Singh and John Lynch (New York: Bantam Books, 1998); *Fermat's Last Theorem: Unlocking the Secret of an Ancient Mathematical Problem* by Amir D. Aczel (New York: Delacorte Press, 1997).

One of the oldest problems in mathematics that remain unsolved is the Goldbach conjecture. In Example 3.1.5 it was shown that every even integer from 4 to 30 can be represented as a sum of two prime numbers. More than 250 years ago, Christian Goldbach (1690–1764) conjectured that every even integer greater than 2 can be so represented. Explicit computer-aided calculations have shown the conjecture to be true up to at least 10^{16}. But there is a huge chasm between 10^{16} and infinity. As pointed out by James Gleick of the *New York Times*, many other plausible conjectures in number theory have proved false. Leonhard Euler (1707–1783), for example, proposed in the eighteenth century that $a^4 + b^4 + c^4 = d^4$ had no nontrivial whole number solutions. In other words, no three perfect fourth powers add up to another perfect fourth power. For small numbers, Euler's conjecture looked good. But in 1987 a Harvard mathematician, Noam Elkies, proved it wrong. One counterexample, found by Roger Frye of Thinking Machines Corporation in a long computer search, is $95{,}800^4 + 217{,}519^4 + 414{,}560^4 = 422{,}481^4$.*

In May 2000, "to celebrate mathematics in the new millennium," the Clay Mathematics Institute of Cambridge, Massachusetts, announced that it would award prizes of $1 million each for the solutions to seven longstanding, classical mathematical questions. One of them, "P vs. NP," asks whether problems belonging to a certain class can be solved on a computer using more efficient methods than the very inefficient methods that are presently known to work for them. This question is discussed briefly at the end of Chapter 9.

Exercise Set 3.1†

In 1–3, use the definitions of even, odd, prime, and composite to justify each of your answers.

1. Assume that k is a particular integer.
   a. Is -17 an odd integer? b. Is 0 an even integer?
   c. Is $2k - 1$ odd?

2. Assume that m and n are particular integers.
   a. Is $6m + 8n$ even? b. Is $10mn + 7$ odd?
   c. If $m > n > 0$, is $m^2 - n^2$ composite?

3. Assume that r and s are particular integers.
   a. Is $4rs$ even? b. Is $6r + 4s^2 + 3$ odd?
   c. If r and s are both positive, is $r^2 + 2rs + s^2$ composite?

Prove the statements in 4–10.

4. There are integers m and n such that $m > 1$ and $n > 1$ and $\frac{1}{m} + \frac{1}{n}$ is an integer.

5. There are distinct integers m and n such that $\frac{1}{m} + \frac{1}{n}$ is an integer.

6. There are real numbers a and b such that
$$\sqrt{a+b} = \sqrt{a} + \sqrt{b}.$$

7. There is an integer $n > 5$ such that $2^n - 1$ is prime.

8. There is a real number x such that $x > 1$ and $2^x > x^{10}$.

Definition: An integer n is called a **perfect square** if, and only if, $n = k^2$ for some integer k.

9. There is a perfect square that can be written as a sum of two other perfect squares.

10. There is an integer n such that $2n^2 - 5n + 2$ is prime.

Disprove the statements in 11–13 by giving a counterexample.

11. For all real numbers a and b, if $a < b$ then $a^2 < b^2$.

12. For all integers n, if n is odd then $\frac{n-1}{2}$ is odd.

13. For all integers m and n, if $2m + n$ is odd then m and n are both odd.

In 14–16, determine whether the property is true for all integers, true for no integers, or true for some integers and false for other integers. Justify your answers.

14. $(a + b)^2 = a^2 + b^2$ 15. $3n^2 - 4n + 1$ is prime.

16. The average of any two odd integers is odd.

Prove the statements in 17 and 18 by the method of exhaustion.

17. Every positive even integer less than 26 can be expressed as a sum of three or fewer perfect squares. (For instance, $10 = 1^2 + 3^2$ and $16 = 4^2$.)

*James Gleick, "Fermat's Last Theorem Still Has Zero Solutions," *New York Times*, 17 April 1988.

†For exercises with blue numbers, solutions are given in Appendix B. The symbol **H** indicates that only a hint or partial solution is given. The symbol * signals that an exercise is more challenging than usual.

18. For each integer n with $1 \le n \le 10$, $n^2 - n + 11$ is a prime number.

19. a. Rewrite the following theorem in the form $\forall$ _____, if _____ then _____.

b. Fill in the blanks in the proof.

Theorem: The sum of any even integer and any odd integer is odd.

Proof: Suppose m is any even integer and n is (a) _____. By definition of even, $m = 2r$ for some (b) _____, and by definition of odd, $n = 2s + 1$ for some integer s. By substitution and algebra, $m + n =$ (c) _____ $= 2(r + s) + 1$. Since r and s are both integers, so is their sum $r + s$. Hence $m + n$ has the form 2 · (some integer) + 1, and so (d) _____ by definition of odd.

Each of the statements in 20–23 is true. For each, (a) rewrite the statement using a variable or variables and the form $\forall$ _____, if _____ then _____, and (b) write the first sentence of a proof (the "starting point") and the last sentence of a proof (the "conclusion to be shown"). Note that you do not need to understand the statements in order to be able to do these exercises.

20. For all integers m, if $m > 1$ then $0 < \dfrac{1}{m} < 1$.

21. For all real numbers x, if $x > 1$ then $x^2 > x$.

22. For all integers m and n, if $mn = 1$ then $m = n = 1$ or $m = n = -1$.

23. For all real numbers x, if $0 < x < 1$ then $x^2 < x$.

Prove the statements in 24–30. Follow the directions given in this section for writing proofs of universal statements.

24. The negative of any even integer is even.

25. The difference of any even integer minus any odd integer is odd.

26. The difference of any odd integer minus any even integer is odd. (*Note:* The "proof" shown in exericse 35 contains an error. Can you spot it?)

27. The sum of any two odd integers is even.

28. For all integers n, if n is odd then n^2 is odd.

29. If n is any even integer, then $(-1)^n = 1$.

30. If n is any odd integer, then $(-1)^n = -1$.

Prove that the statements in 31–33 are false.

31. There exists an integer $m \ge 3$ such that $m^2 - 1$ is prime.

32. There exists an integer n such that $6n^2 + 27$ is prime.

33. There exists an integer k such that $k \ge 4$ and $2k^2 - 5k + 2$ is prime.

Find the mistakes in the "proofs" shown in 34–38.

34. Theorem: For all integers k, if $k > 0$ then $k^2 + 2k + 1$ is composite.

"**Proof:** For $k = 2$, $k^2 + 2k + 1 = 2^2 + 2 \cdot 2 + 1 = 9$. But $9 = 3 \cdot 3$, and so 9 is composite. Hence the theorem is true."

35. Theorem: The difference between any odd integer and any even integer is odd.

"**Proof:** Suppose n is any odd integer, and m is any even integer. By definition of odd, $n = 2k + 1$ where k is an integer, and by definition of even, $m = 2k$ where k is an integer. Then $n - m = (2k + 1) - 2k = 1$. But 1 is odd. Therefore, the difference between any odd integer and any even integer is odd."

36. Theorem: For all integers k, if $k > 0$ then $k^2 + 2k + 1$ is composite.

"**Proof:** Suppose k is any integer such that $k > 0$. If $k^2 + 2k + 1$ is composite, then $k^2 + 2k + 1 = r \cdot s$ for some integers r and s such that $1 < r < (k^2 + 2k + 1)$ and $1 < s < (k^2 + 2k + 1)$. Since $k^2 + 2k + 1 = r \cdot s$ and both r and s are strictly between 1 and $k^2 + 2k + 1$, then $k^2 + 2k + 1$ is not prime. Hence $k^2 + 2k + 1$ is composite as was to be shown."

37. **Theorem:** The product of an even integer and an odd integer is even.

"**Proof:** Suppose m is an even integer and n is an odd integer. If $m \cdot n$ is even, then by definition of even there exists an integer r such that $m \cdot n = 2r$. Also since m is even, there exists an integer p such that $m = 2p$, and since n is odd there exists an integer q such that $n = 2q + 1$. Thus

$$m \cdot n = (2p) \cdot (2q + 1) = 2r,$$

where r is an integer. By definition of even, then, $m \cdot n$ is even, as was to be shown."

38. **Theorem:** The sum of any two even integers equals $4k$ for some integer k.

"**Proof:** Suppose m and n are any two even integers. By definition of even, $m = 2k$ for some integer k and $n = 2k$ for some integer k. By substitution, $m + n = 2k + 2k = 4k$. This is what was to be shown."

In 39–56 determine whether the statement is true or false. Justify your answer with a proof or a counterexample, as appropriate.

39. The product of any two odd integers is odd.

40. The negative of any odd integer is odd.

41. The difference of any two odd integers is odd.

42. The product of any even integer and any integer is even.

43. If a sum of two integers is even, then one of the summands is even. (In the expression $a + b$, a and b are called **summands.**)

44. The difference of any two even integers is even.

45. The difference of any two odd integers is even.

46. For all integers n and m, if $n - m$ is even then $n^3 - m^3$ is even.

47. For all integers n, if n is prime then $(-1)^n = -1$.

48. For all integers m, if $m > 2$ then $m^2 - 4$ is composite.

49. For all integers n, $n^2 - n + 11$ is a prime number.

50. For all integers n, $4(n^2 + n + 1) - 3n^2$ is a perfect square.

51. Every positive integer can be expressed as a sum of three or fewer perfect squares.

52. (Two integers are **consecutive** if, and only if, one is one more than the other.) Any product of four consecutive integers is one less than a perfect square.

53. If m and n are positive integers and mn is a perfect square, then m and n are perfect squares.

54. The difference of the squares of any two consecutive integers is odd.

55. For all nonnegative real numbers a and b, $\sqrt{ab} = \sqrt{a}\sqrt{b}$. (Note that if x is a nonnegative real number, then there is a unique nonnegative real number y, denoted $\sqrt{x}$, such that $y^2 = x$.)

56. For all nonnegative real numbers a and b,

$$\sqrt{a+b} = \sqrt{a} + \sqrt{b}.$$

57. If m and n are perfect squares, then $m + n + 2\sqrt{mn}$ is also a perfect square. Why?

H ★58. If p is a prime number, must $2^p - 1$ also be prime? Prove or give a counterexample.

★59. If n is a nonnegative integer, must $2^{2^n} + 1$ be prime? Prove or give a counterexample.

60. When expressions of the form $(x - r)(x - s)$ are multiplied out, a quadratic polynomial is obtained. For instance, $(x - 2)(x - (-7)) = (x - 2)(x + 7) = x^2 + 5x - 14$.

H a. What can be said about the coefficients of the polynomial obtained by multiplying out $(x - r)(x - s)$ when both r and s are odd integers? when both r and s are even integers? when one of r and s is even and the other is odd?

b. It follows from part (a) that $x^3 - 1253x + 255$ cannot be written as a product of two polynomials with integer coefficients. Explain why this is so.

★61. Observe that $(x - r)(x - s)(x - t)$

$$= x^3 - (r + s + t)x^2 + (rs + rt + st)x - rst.$$

a. Derive a result for cubic polynomials similar to the result in part (a) of exercise 60 for quadratic polynomials.

b. Can $15x^3 + 7x^2 - 8x - 27$ be written as a product of three polynomials with integer coefficients? Explain.

3.2 Direct Proof and Counterexample II: Rational Numbers

Such, then, is the whole art of convincing. It is contained in two principles: to define all notations used, and to prove everything by replacing mentally the defined terms by their definitions. — Blaise Pascal, 1623–1662

Sums, differences, and products of integers are integers. But most quotients of integers are not integers. Quotients of integers are, however, important; they are known as *rational numbers.*

• Definition

A real number r is **rational** if, and only if, it can be expressed as a quotient of two integers with a nonzero denominator. A real number that is not rational is **irrational.** More formally, if r is a real number, then

$$r \text{ is rational} \Leftrightarrow \exists \text{ integers } a \text{ and } b \text{ such that } r = \frac{a}{b} \text{ and } b \neq 0.$$

The word *rational* contains the word *ratio,* which is another word for quotient. A rational number is a fraction or ratio of integers.

Example 3.2.1 Determining Whether Numbers Are Rational or Irrational

a. Is $10/3$ a rational number?

b. Is $-(5/39)$ a rational number?

c. Is 0.281 a rational number?

d. Is 7 a rational number?

e. Is 0 a rational number?

f. Is $2/0$ a rational number?

g. Is $2/0$ an irrational number?

h. Is $0.12121212\ldots$ a rational number (where the digits 12 are assumed to repeat forever)?

i. If m and n are integers and neither m nor n is zero, is $(m+n)/mn$ a rational number?

Solution

a. Yes, $10/3$ is a quotient of the integers 10 and 3 and hence is rational.

b. Yes, $-(5/39) = -5/39$, which is a quotient of the integers -5 and 39 and hence is rational.

c. Yes, $0.281 = 281/1000$. Note that the real numbers represented on a typical calculator display are all finite decimals. An explanation similar to the one in this example shows that any such number is rational. It follows that a calculator with such a display can represent only rational numbers.

d. Yes, $7 = 7/1$.

e. Yes, $0 = 0/1$.

f. No, $2/0$ is not a number (division by 0 is not allowed).

g. No, because every irrational number is a number, and $2/0$ is not a number. We discuss additional techniques for determining whether numbers are irrational in Sections 3.6, 3.7, and 7.4.

h. Yes. Let $x = 0.12121212\ldots$. Then $100x = 12.12121212\ldots$. Hence

$$100x - x = 12.12121212\ldots - 0.12121212\ldots = 12.$$

But also

$$100x - x = 99x \quad \text{by basic algebra}$$

Hence

$$99x = 12,$$

and so

$$x = \frac{12}{99}.$$

Therefore, $0.12121212\ldots = 12/99$, which is a ratio of two nonzero integers and thus is a rational number.

Note that you can use an argument similar to this one to show that any repeating decimal is a rational number. In Section 7.3 we show that any rational number can be written as a repeating or terminating decimal.

i. Yes, since m and n are integers, so are $m + n$ and mn (because sums and products of integers are integers). Also $mn \neq 0$ by the **zero product property.** (One version of this property says that if neither of two real numbers is 0, then their product is also not 0. See exercise 8 at the end of this section.) It follows that $(m + n)/mn$ is a quotient of two integers with a nonzero denominator and hence is a rational number. ■

More on Generalizing from the Generic Particular

Some people like to think of the method of generalizing from the generic particular as a challenge process. If you claim a property holds for all elements in a domain, then someone can challenge your claim by picking any element in the domain whatsoever and asking you to prove that that element satisfies the property. To prove your claim, you must be able to meet all such challenges. That is, you must have a way to convince the challenger that the property is true for an *arbitrarily chosen* element in the domain.

For example, suppose "A" claims that every integer is a rational number. "B" challenges this claim by asking "A" to prove it for $n = 7$. "A" observes that

$$7 = \frac{7}{1} \quad \text{which is a quotient of integers and hence rational.}$$

"B" accepts this explanation but challenges again with $n = -12$. "A" responds that

$$-12 = \frac{-12}{1} \quad \text{which is a quotient of integers and hence rational.}$$

Next "B" tries to trip up "A" by challenging with $n = 0$, but "A" answers that

$$0 = \frac{0}{1} \quad \text{which is a quotient of integers and hence rational.}$$

As you can see, "A" is able to respond effectively to all "B"s challenges because "A" has a general procedure for putting integers into the form of rational numbers: "A" just divides whatever integer "B" gives by 1. That is, no matter what integer n "B" gives "A", "A" writes

$$n = \frac{n}{1} \quad \text{which is a quotient of integers and hence rational.}$$

This discussion proves the following theorem.

Theorem 3.2.1

Every integer is a rational number.

In exercise 11 at the end of this section you are asked to condense the above discussion into a formal proof.

Proving Properties of Rational Numbers

The next example shows how to use the method of generalizing from the generic particular to prove a property of rational numbers.

Example 3.2.2 A Sum of Rationals Is Rational

Prove that the sum of any two rational numbers is rational.

Solution Begin by mentally or explicitly rewriting the statement to be proved in the form "$\forall$ _____, if _____ then _____."

Formal Restatement: $\forall$ real numbers r and s, if r and s are rational then $r + s$ is rational.

Next ask yourself, "Where am I starting from?" or "What am I supposing?" The answer gives you the starting point, or first sentence, of the proof.

Starting Point: Suppose r and s are particular but arbitrarily chosen real numbers such that r and s are rational; or, more simply,

Suppose r and s are rational numbers.

Then ask yourself, "What must I show to complete the proof?"

To Show: $r + s$ is rational.

Finally you ask, "How do I get from the starting point to the conclusion?" or "Why must $r + s$ be rational if both r and s are rational?" The answer depends in an essential way on the definition of rational.

Rational numbers are quotients of integers, so to say that r and s are rational means that

$$r = \frac{a}{b} \quad \text{and} \quad s = \frac{c}{d} \qquad \begin{array}{l}\text{for some integers } a, b, c, \text{ and } d \\ \text{where } b \neq 0 \text{ and } d \neq 0.\end{array}$$

It follows by substitution that

$$r + s = \frac{a}{b} + \frac{c}{d}.$$

Hence you must show that the right-hand sum can be written as a single fraction or ratio of two integers with a nonzero denominator. But

$$\begin{aligned} \frac{a}{b} + \frac{c}{d} &= \frac{ad}{bd} + \frac{bc}{bd} && \text{rewriting the fraction with a common denominator} \\ &= \frac{ad + bc}{bd} && \text{adding fractions with a common denominator.} \end{aligned}$$

Is this fraction a ratio of integers? Yes. Because products and sums of integers are integers, $ad + bc$ and bd are both integers. Is the denominator $bd \neq 0$? Yes, by the zero product property (since $b \neq 0$ and $d \neq 0$). Thus $r + s$ is a rational number.

This discussion is summarized as follows:

Theorem 3.2.2

The sum of any two rational numbers is rational.

Proof:

Suppose r and s are rational numbers. [*We must show that $r + s$ is rational.*] Then, by definition of rational, $r = a/b$ and $s = c/d$ for some integers a, b, c, and d with $b \neq 0$ and $d \neq 0$. Thus

$$r + s = \frac{a}{b} + \frac{c}{d} \qquad \text{by substitution}$$

$$= \frac{ad + bc}{bd} \qquad \text{by basic algebra.}$$

Let $p = ad + bc$ and $q = bd$. Then p and q are integers because products and sums of integers are integers and because a, b, c, and d are all integers. Also $q \neq 0$ by the zero product property. Thus

$$r + s = \frac{p}{q} \text{ where } p \text{ and } q \text{ are integers and } q \neq 0.$$

Therefore, $r + s$ is rational by definition of a rational number. [*This is what was to be shown.*]

■

Deriving New Mathematics from Old

Section 3.1 focused on establishing truth and falsity of mathematical theorems using only the basic algebra normally taught in secondary school; the fact that the integers are closed under addition, subtraction, and multiplication; and the definitions of the terms in the theorems themselves. In the future, when we ask you to **prove something directly from the definitions,** we will mean that you should restrict yourself to this approach. However, once a collection of statements has been proved directly from the definitions, another method of proof becomes possible. The statements in the collection can be used to derive additional results.

Example 3.2.3 Deriving Additional Results about Even and Odd Integers

Suppose that you have already proved the following properties of even and odd integers:

1. The sum, product, and difference of any two even integers are even.
2. The sum and difference of any two odd integers are even.
3. The product of any two odd integers is odd.
4. The product of any even integer and any odd integer is even.
5. The sum of any odd integer and any even integer is odd.
6. The difference of any odd integer minus any even integer is odd.
7. The difference of any even integer minus any odd integer is odd.

Use the properties listed above to prove that if a is any odd integer and b is any given integer, then $\dfrac{a^2 + b^2 + 1}{2}$ is an integer.

Solution Suppose a is any odd integer and b is any even integer. By property 3, b^2 is odd, and by property 1, a^2 is even. Then by property 5, $a^2 + b^2$ is odd, and because 1 is also odd, the sum $(a^2 + b^2) + 1 = a^2 + b^2 + 1$ is even by property 2. Hence, by definition of even, there exists an integer k such that $a^2 + b^2 + 1 = 2k$. Dividing both sides by 2 gives $\dfrac{a^2 + b^2 + 1}{2} = k$, which is an integer. Thus $\dfrac{a^2 + b^2 + 1}{2}$ is an integer [*as was to be shown*]. ■

A **corollary** is a statement whose truth can be immediately deduced from a theorem that has already been proved.

Example 3.2.4 The Double of a Rational Number

Derive the following as a corollary of Theorem 3.2.2.

Corollary 3.2.3

The double of a rational number is rational.

Solution The double of a number is just its sum with itself. But since the sum of any two rational numbers is rational (Theorem 3.2.2), the sum of a rational number with itself is rational. Hence the double of a rational number is rational. Here is a formal version of this argument:

Proof:

Suppose r is any rational number. Then $2r = r + r$ is a sum of two rational numbers. So, by Theorem 3.2.2, $2r$ is rational. ■

Exercise Set 3.2

The numbers in 1–7 are all rational. Write each number as a ratio of two integers.

1. $-\dfrac{35}{6}$
2. 4.6037
3. $\dfrac{4}{5} + \dfrac{2}{9}$
4. 0.37373737...
5. 0.56565656...
6. 320.5492492492...
7. 52.4672167216721...
8. The zero product property says that if a product of two real numbers is 0, then one of the numbers must be 0.
   a. Write this property formally using quantifiers and variables.
   b. Write the contrapositive of your answer to part (a).
   c. Write an informal version (without quantifier symbols or variables) for your answer to part (b).
9. Assume that a and b are both integers and that $a \neq 0$ and $b \neq 0$. Explain why $(b - a)/(ab^2)$ must be a rational number.
10. Assume that m and n are both integers and that $n \neq 0$. Explain why $(5m + 12n)/(4n)$ must be a rational number.
11. Prove that every integer is a rational number.
12. Fill in the blanks in the following proof that the square of any rational number is rational:

    Proof: Suppose that r is $\underline{\text{(a)}}$. By definition of rational, $r = a/b$ for some $\underline{\text{(b)}}$ with $b \neq 0$. By substitution, $r^2 = \underline{\text{(c)}} = a^2/b^2$. Since a and b are both integers, so are the products a^2 and $\underline{\text{(d)}}$. Also $b^2 \neq 0$ by the $\underline{\text{(e)}}$. Hence r^2 is a ratio of two integers with a nonzero denominator, and so $\underline{\text{(f)}}$ by definition of rational.

Determine which of the statements in 13–19 are true and which are false. Prove each true statement directly from the definitions, and give a counterexample for each false statement. In case the statement is false, determine whether a small change would make it true. If so, make the change and prove the new statement.

13. The product of any two rational numbers is a rational number.
14. The quotient of any two rational numbers is a rational number.
15. The difference of any two rational numbers is a rational number.

16. Given any rational number r, $-r$ is also a rational number.

17. If r and s are any two rational numbers with $r < s$, then $\dfrac{r+s}{2}$ is rational.

18. For all real numbers a and b, if $a < b$ then $a < \dfrac{a+b}{2} < b$. (You may use the properties of inequalities in T16-T25 of Appendix A.)

19. Given any two rational numbers r and s with $r < s$, there is another rational number between r and s. (*Hint:* Use the results of exercises 17 and 18.)

Use the properties of even and odd integers that are listed in Example 3.2.3 to do exercises 20–22. Indicate which properties you use to justify your reasoning.

20. True or false? If m is any even integer and n is any odd integer, then $m^2 + 3n$ is odd. Explain.

21. True or false? If a is any odd integer, then $a^2 + a$ is even. Explain.

22. True or false? If k is any even integer and m is any odd integer, then $(k+2)^2 - (m-1)^2$ is even. Explain.

Derive the statements in 23–25 as corollaries of Theorems 3.2.1, 3.2.2, and the results of exercises 12, 13, 15, and 16.

23. For any rational numbers r and s, $2r + 3s$ is rational.

24. If r is any rational number, then $3r^2 - 2r + 4$ is rational.

25. For any rational number s, $5s^3 + 8s^2 - 7$ is rational.

26. It is a fact that if n is any nonnegative integer, then

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

(A more general form of this statement is proved in Section 4.2). Is a number of this form rational? If so, express it as a ratio of two integers.

27. Suppose a, b, c, and d are integers and $a \neq c$. Suppose also that x is a real number that satisfies the equation

$$\frac{ax+b}{cx+d} = 1.$$

Must x be rational? If so, express x as a ratio of two integers.

28. Suppose a, b, and c are integers and x, y, and z are nonzero real numbers that satisfy the following equations:

$$\frac{xy}{x+y} = a \quad \text{and} \quad \frac{xz}{x+z} = b \quad \text{and} \quad \frac{yz}{y+z} = c.$$

Is x rational? If so, express it as a ratio of two integers.

29. Prove that if one solution for a quadratic equation of the form $x^2 + bx + c = 0$ is rational (where b and c are rational), then the other solution is also rational. (Use the fact that if the solutions of the equation are r and s, then $x^2 + bx + c = (x-r)(x-s)$.)

30. Prove that if a real number c satisfies a polynomial equation of the form

$$r_3x^3 + r_2x^2 + r_1x + r_0 = 0,$$

where r_0, r_1, r_2, and r_3 are rational numbers, then c satisfies an equation of the form

$$n_3x^3 + n_2x^2 + n_1x + n_0 = 0,$$

where n_0, n_1, n_2, and n_3 are integers.

Definition: A number c is called a **root** of a polynomial $p(x)$ if, and only if, $p(c) = 0$.

31. Prove that for all real numbers c, if c is a root of a polynomial with rational coefficients, then c is a root of a polynomial with integer coefficients.

In 32–36 find the mistakes in the "proofs" that the sum of any two rational numbers is a rational number.

32. "**Proof:** Let rational numbers $r = \frac{1}{4}$ and $s = \frac{1}{2}$ be given. Then $r + s = \frac{1}{4} + \frac{1}{2} = \frac{3}{4}$, which is a rational number. This is what was to be shown."

33. "**Proof:** Any two rational numbers produce a rational number when added together. So if r and s are particular but arbitrarily chosen rational numbers, then $r + s$ is rational."

34. "**Proof:** Suppose r and s are rational numbers. By definition of rational, $r = a/b$ for some integers a and b with $b \neq 0$, and $s = a/b$ for some integers a and b with $b \neq 0$. Then $r + s = a/b + a/b = 2a/b$. Let $p = 2a$. Then p is an integer since it is a product of integers. Hence $r + s = p/b$, where p and b are integers and $b \neq 0$. Thus $r + s$ is a rational number by definition of rational. This is what was to be shown."

35. "**Proof:** Suppose r and s are rational numbers. Then $r = a/b$ and $s = c/d$ for some integers a, b, c, and d with $b \neq 0$ and $d \neq 0$ (by definition of rational). Then $r + s = a/b + c/d$. But this is a sum of two fractions, which is a fraction. So $r + s$ is a rational number since a rational number is a fraction."

36. "**Proof:** Suppose r and s are rational numbers. If $r + s$ is rational, then by definition of rational $r + s = a/b$ for some integers a and b with $b \neq 0$. Also since r and s are rational, $r = i/j$ and $s = m/n$ for some integers i, j, m, and n with $j \neq 0$ and $n \neq 0$. It follows that $r + s = i/j + m/n = a/b$, which is a quotient of two integers with a nonzero denominator. Hence it is a rational number. This is what was to be shown."

3.3 Direct Proof and Counterexample III: Divisibility

The essential quality of a proof is to compel belief. — Pierre de Fermat

When you were first introduced to the concept of division in elementary school, you were probably taught that 12 divided by 3 is 4 because if you separate 12 objects into groups of 3, you get 4 groups with nothing left over.

You may also have been taught to describe this fact by saying that "12 is evenly divisible by 3" or "3 divides 12 evenly."

The notion of divisibility is the central concept of one of the most beautiful subjects in advanced mathematics: **number theory,** the study of properties of integers.

• Definition

If n and d are integers, then

n is **divisible by** d if, and only if, $n = dk$ for some integer k.

Alternatively, we say that

n **is a multiple of** d, or
d **is a factor of** n, or
d **is a divisor of** n, or
d **divides** n.

The notation $\mathbf{d \mid n}$ is read "d divides n." Symbolically, if n and d are integers and $d \neq 0$,

$$d \mid n \quad \Leftrightarrow \quad \exists \text{ an integer } k \text{ such that } n = dk.$$

Example 3.3.1 Divisibility

a. Is 21 divisible by 3?
b. Does 5 divide 40?
c. Does $7 \mid 42$?
d. Is 32 a multiple of -16?
e. Is 6 a factor of 54?
f. Is 7 a factor of -7?

Solution

a. Yes, $21 = 3 \cdot 7$.
b. Yes, $40 = 5 \cdot 8$.
c. Yes, $42 = 7 \cdot 6$.
d. Yes, $32 = (-16) \cdot (-2)$.
e. Yes, $54 = 6 \cdot 9$.
f. Yes, $-7 = 7 \cdot (-1)$. ■

Example 3.3.2 Divisors of Zero

If k is any integer, does k divide 0?

Solution Yes, because $0 = k \cdot 0$. ■

Example 3.3.3 The Positive Divisors of a Positive Number

Suppose a and b are positive integers and $a \mid b$. Is $a \leq b$?

Solution Yes. To say that $a \mid b$ means that $b = ka$ for some integer k. Now k must be a positive integer because both a and b are positive. It follows that

$$1 \leq k$$

because every positive integer is greater than or equal to 1. Multiplying both sides by a gives

$$a \leq k \cdot a = b$$

(since multiplying both sides of an inequality by a positive number preserves the inequality—property T19 of Appendix A). ■

Example 3.3.4 Divisors of 1

Which integers divide 1?

Solution By Example 3.3.3 any positive integer that divides 1 is less than or equal to 1. Since $1 = 1 \cdot 1$, 1 divides 1, and there are no positive integers that are less than 1. So the only positive divisor of 1 is 1.

On the other hand, if d is a negative integer that divides 1, then $1 = dk$, and so $1 = |d| \cdot |k|$. Hence $|d|$ is a positive integer that divides 1. Thus $|d| = 1$, and so $d = -1$. It follows that the only divisors of 1 are 1 and -1. ■

Example 3.3.5 Divisibility of Algebraic Expressions

a. If a and b are integers, is $3a + 3b$ divisible by 3?

b. If k and m are integers, is $10km$ divisible by 5?

Solution

a. Yes. By the distributive law of algebra, $3a + 3b = 3(a + b)$ and $a + b$ is an integer because it is a sum of two integers.

b. Yes. By the associative law of algebra, $10km = 5 \cdot (2km)$ and $2km$ is an integer because it is a product of three integers. ■

When the definition of divides is rewritten formally using the existential quantifier, the result is

$$d \mid n \quad \Leftrightarrow \quad \exists \text{ an integer } k \text{ such that } n = dk.$$

Since the negation of an existential statement is universal, it follows that d does not divide n (denoted $d \nmid n$) if, and only if, $\forall$ integers k, $n \neq dk$, or, in other words, the quotient n/d is not an integer.

For all integers n and d, $\quad d \nmid n \quad \Leftrightarrow \quad \dfrac{n}{d}$ is not an integer.

Example 3.3.6 Checking Nondivisibility

Does $4 \mid 15$?

Solution No, $\frac{15}{4} = 3.75$, which is not an integer. ■

Caution! Be careful to distinguish between the notation $a \mid b$ and the notation a/b. The notation $a \mid b$ stands for the sentence "a divides b," which means that there is an integer k such that $b = a \cdot k$. Dividing both sides by a gives $b/a = k$, an integer. Thus, when $d \neq 0$, $a \mid b$ if, and only if, b/a is an integer. On the other hand, the notation a/b stands for the fractional number a/b (the inverse fraction!), which may or may not be an integer.

Example 3.3.7 Prime Numbers and Divisibility

An alternative way to define a prime number is to say that an integer $n > 1$ is prime if, and only if, its only positive integer divisors are 1 and itself. ■

Proving Properties of Divisibility

One of the most useful properties of divisibility is that it is transitive. If one number divides a second and the second number divides a third, then the first number divides the third.

Example 3.3.8 Transitivity of Divisibility

Prove that for all integers a, b, and c, if $a \mid b$ and $b \mid c$, then $a \mid c$.

Solution Since the statement to be proved is already written formally, you can immediately pick out the starting point, or first sentence of the proof, and the conclusion that must be shown.

Starting Point: Suppose a, b, and c are particular but arbitrarily chosen integers such that $a \mid b$ and $b \mid c$.

To Show: $a \mid c$.

You need to show that $a \mid c$, or, in other words, that

$$c = a \cdot (\text{some integer}).$$

But since $a \mid b$,

$$b = ar \quad \text{for some integer } r. \tag{3.3.1}$$

And since $b \mid c$,

$$c = bs \quad \text{for some integer } s. \tag{3.3.2}$$

Equation 3.3.2 expresses c in terms of b, and equation 3.3.1 expresses b in terms of a. Thus if you substitute 3.3.1 into 3.3.2, you will have an equation that expresses c in terms of a.

$$\begin{aligned} c &= bs && \text{by equation 3.3.2} \\ &= (ar)s && \text{by equation 3.3.1.} \end{aligned}$$

But $(ar)s = a(rs)$ by the associative law for multiplication. Hence

$$c = a(rs).$$

Now you are almost finished. You have expressed c as $a \cdot$ (something). It remains only to verify that that something is an integer. But of course it is, because it is a product of two integers.

This discussion is summarized as follows:

Theorem 3.3.1 Transitivity of Divisibility

For all integers a, b, and c, if a divides b and b divides c, then a divides c.

Proof:

Suppose a, b, and c are [*particular but arbitrarily chosen*] integers such that a divides b and b divides c. [*We must show that a divides c.*] By definition of divisibility,

$$b = ar \quad \text{and} \quad c = bs \quad \text{for some integers } r \text{ and } s.$$

By substitution

$$\begin{aligned} c &= bs \\ &= (ar)s \\ &= a(rs) \qquad \text{by basic algebra.} \end{aligned}$$

Let $k = rs$. Then k is an integer since it is a product of integers, and therefore

$$c = ak \quad \text{where } k \text{ is an integer.}$$

Thus a divides c by definition of divisibility. [*This is what was to be shown.*]

■

It would appear from the definition of prime that to show that an integer is prime you would need to show that it is not divisible by any integer greater than 1 and less than itself. In fact, you need only check divisibility by prime numbers. This follows from Theorem 3.3.1, Example 3.3.3, and the following theorem, which says that any integer greater than 1 is divisible by a prime number. The idea of the proof is quite simple. You start with a positive integer. If it is prime, you are done; if not, it is a product of two smaller positive factors. If one of these is prime, you are done; if not, you can pick one of the factors and write it as a product of still smaller positive factors. You can continue in this way, factoring the factors of the number you started with, until one of them turns out to be prime. This must happen eventually because all the factors can be chosen to be positive and each is smaller than the preceding one.

Theorem 3.3.2 Divisibility by a Prime

Any integer $n > 1$ is divisible by a prime number.

Proof:

Suppose n is a [*particular but arbitrarily chosen*] integer that is greater than 1. [*We must show that there is a prime number that divides n.*] If n is prime, then n is divisible by a prime number (namely itself), and we are done. If n is not prime, then, as discussed in Example 3.1.2b,

$$n = r_0 s_0 \quad \text{where } r_0 \text{ and } s_0 \text{ are integers and } 1 < r_0 < n \text{ and } 1 < s_0 < n.$$

It follows by definition of divisibility that $r_0 \mid n$.

continued on page 152

If r_0 is prime, then r_0 is a prime number that divides n, and we are done. If r_0 is not prime, then

$$r_0 = r_1 s_1 \quad \text{where } r_1 \text{ and } s_1 \text{ are integers and } 1 < r_1 < r_0 \text{ and } 1 < s_1 < r_0.$$

It follows by the definition of divisibility that $r_1 \mid r_0$. But we already know that $r_0 \mid n$. Consequently, by transitivity of divisibility, $r_1 \mid n$.

If r_1 is prime, then r_1 is a prime number that divides n, and we are done. If r_1 is not prime, then

$$r_1 = r_2 s_2 \quad \text{where } r_2 \text{ and } s_2 \text{ are integers and } 1 < r_2 < r_1 \text{ and } 1 < s_2 < r_1.$$

It follows by definition of divisibility that $r_2 \mid r_1$. But we already know that $r_1 \mid n$. Consequently, by transitivity of divisibility, $r_2 \mid n$.

If r_2 is prime, then r_2 is a prime number that divides n, and we are done. If r_2 is not prime, then we may repeat the above process by factoring r_2 as $r_3 s_3$.

We may continue in this way, factoring successive factors of n until we find a prime factor. We must succeed in a finite number of steps because each new factor is both less than the previous one (which is less than n) and greater than 1, and there are fewer than n integers strictly between 1 and n.* Thus we obtain a sequence

$$r_0, r_1, r_2, \ldots, r_k,$$

where $k \geq 0$, $1 < r_k < r_{k-1} < \cdots < r_2 < r_1 < r_0 < n$, and $r_i \mid n$ for each $i = 0, 1, 2, \ldots, k$. The condition for termination is that r_k should be prime. Hence r_k is a prime number that divides n. [*This is what we were to show.*]

Counterexamples and Divisibility

To show that a proposed divisibility property is not universally true, you need to find some integers for which it is false.

Example 3.3.9 Checking a Proposed Divisibility Property

Is it true or false that for all integers a and b, if $a \mid b$ and $b \mid a$ then $a = b$?

Solution This proposed property is false. Can you think of a counterexample just by concentrating for a minute or so?

The following discussion describes a mental process that may take just a few seconds. It is helpful to be able to use it consciously, however, to solve more difficult problems.

To discover the truth or falsity of a statement such as the one given above, start off much as you would if you were trying to prove it.

Starting Point: Suppose a and b are integers such that $a \mid b$ and $b \mid a$.

Ask yourself, "*Must* it follow that $a = b$, or *could* it happen that $a \neq b$ for some a and b?" Focus on the supposition. What does it mean? By definition of divisibility, the conditions $a \mid b$ and $b \mid a$ mean that

$$b = ka \quad \text{and} \quad a = lb \quad \text{for some integers } k \text{ and } l.$$

*Strictly speaking, this statement is justified by an axiom for the integers called the well-ordering principle, which is discussed in Section 4.4. Theorem 3.3.2 can also be proved using strong mathematical induction, as shown in Example 4.4.1.

Must it follow that $a = b$, or can you find integers a and b that satisfy these equations for which $a \neq b$? The equations imply that

$$b = ka = k(lb) = (kl)b.$$

Since $b \mid a$, $b \neq 0$, and so you can cancel b from the extreme left and right sides to obtain

$$1 = kl.$$

In other words, k and l are divisors of 1. But the only divisors of 1 are 1 and -1 (see Example 3.3.4). Thus k and l are both 1 or -1. If $k = l = 1$, then $b = a$. But if $k = l = -1$, then $b = -a$ and so $a \neq b$. This analysis suggests that you can find a counterexample by taking $b = -a$. Here is a formal answer:

Statement: For all integers a and b, if $a \mid b$ and $b \mid a$ then $a = b$.

Counterexample: Let $a = 2$ and $b = -2$. Then

$$a \mid b \text{ since } 2 \mid (-2) \text{ and } b \mid a \text{ since } (-2) \mid 2, \text{ but } a \neq b \text{ since } 2 \neq -2.$$

Therefore, the proposed divisibility property is false. ■

The search for a proof will frequently help you discover a counterexample (provided the statement you are trying to prove is, in fact, false). Conversely, in trying to find a counterexample for a statement, you may come to realize the reason why it is true (if it is, in fact, true). The important thing is to keep an open mind until you are convinced by the evidence of your own careful reasoning.

The Unique Factorization Theorem

The most comprehensive statement about divisibility of integers is contained in a theorem known as the *unique factorization theorem* for the integers. Because of its importance, this theorem is also called the *fundamental theorem of arithmetic*. Although Euclid, who lived about 300 B.C., seems to have been acquainted with the theorem, it was first stated precisely by the great German mathematician Carl Friedrich Gauss (rhymes with *house*) in 1801.

The unique factorization theorem says that any integer greater than 1 either is prime or can be written as a product of prime numbers in a way that is unique except, perhaps, for the order in which the primes are written. For example,

$$72 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 = 2 \cdot 3 \cdot 3 \cdot 2 \cdot 2 = 3 \cdot 2 \cdot 2 \cdot 3 \cdot 2$$

and so forth. The three 2's and two 3's may be written in any order, but any factorization of 72 as a product of primes must contain exactly three 2's and two 3's—no other collection of prime numbers besides three 2's and two 3's multiplies out to 72.

Theorem 3.3.3 Unique Factorization Theorem for the Integers (Fundamental Theorem of Arithmetic)

Given any integer $n > 1$, there exist a positive integer k, distinct prime numbers $p_1, p_2, \ldots, p_k$, and positive integers $e_1, e_2, \ldots, e_k$ such that

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_k^{e_k},$$

and any other expression of n as a product of prime numbers is identical to this except, perhaps, for the order in which the factors are written.

The proof of the unique factorization theorem is included in Section 10.4.

Because of the unique factorization theorem, any integer $n > 1$ can be put into a *standard factored form* in which the prime factors are written in ascending order from left to right.

• Definition

Given any integer $n > 1$, the **standard factored form** of n is an expression of the form

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_k^{e_k},$$

where k is a positive integer; $p_1, p_2, \ldots, p_k$ are prime numbers; $e_1, e_2, \ldots, e_k$ are positive integers; and $p_1 < p_2 < \cdots < p_k$.

Example 3.3.10 Writing Integers in Standard Factored Form

Write 3,300 in standard factored form.

Solution First find all the factors of 3,300. Then write them in ascending order:

$$\begin{aligned} 3{,}300 &= 100 \cdot 33 = 4 \cdot 25 \cdot 3 \cdot 11 \\ &= 2 \cdot 2 \cdot 5 \cdot 5 \cdot 3 \cdot 11 = 2^2 \cdot 3^1 \cdot 5^2 \cdot 11^1. \end{aligned}$$

■

Example 3.3.11 Using Unique Factorization to Solve a Problem

Suppose m is an integer such that

$$8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot m = 17 \cdot 16 \cdot 15 \cdot 14 \cdot 13 \cdot 12 \cdot 11 \cdot 10.$$

Does $17 \mid m$?

Solution Since 17 is one of the prime factors of the right-hand side of the equation, it is also a prime factor of the left-hand side (by the unique factorization theorem). But 17 does not equal any prime factor of 8, 7, 6, 5, 4, 3, or 2 (because it is too large). Hence 17 must occur as one of the prime factors of m, and so $17 \mid m$. ■

Exercise Set 3.3

Give a reason for your answer in each of 1–13. Assume that all variables represent integers.

1. Is 52 divisible by 13?
2. Is 54 divisible by 18?
3. Does $5 \mid 0$?
4. Is $(3k + 1)(3k + 2)(3k + 3)$ divisible by 3?
5. Is $6m(2m + 10)$ divisible by 4?
6. Is 29 a multiple of 3?
7. Is -3 a factor of 66?
8. Is $6a(a + b)$ a multiple of $3a$?
9. Is 4 a factor of $2a \cdot 34b$?
10. Does $7 \mid 34$?
11. Does $13 \mid 73$?
12. If $n = 4k + 1$, does 8 divide $n^2 - 1$?
13. If $n = 4k + 3$, does 8 divide $n^2 - 1$?
14. Fill in the blanks in the following proof that for all integers a and b, if $a \mid b$ then $a \mid (-b)$.

    Proof: Suppose a and b are any integers such that $\underline{\text{(a)}}$. By definition of divisibility, $b = \underline{\text{(b)}}$ for some $\underline{\text{(c)}}$ k. By substitution, $-b = \underline{\text{(d)}} = a \cdot (-k)$. But $-k = (-1) \cdot k$ is an integer since -1 and k are integers. Hence, by definition of divisibility, $\underline{\text{(e)}}$, as was to be shown.

Prove statements 15 and 16 directly from the definition of divisibility.

15. For all integers a, b, and c, if $a \mid b$ and $a \mid c$ then $a \mid (b + c)$.
16. For all integers a, b, and c, if $a \mid b$ and $a \mid c$ then $a \mid (b - c)$.

For each statement in 17–28, determine whether the statement is true or false. Prove the statement directly from the definitions if it is true, and give a counterexample if it is false.

17. The sum of any three consecutive integers is divisible by 3. (Two integers are **consecutive** if, and only if, one is one more than the other.)

18. The product of any two even integers is a multiple of 4.

19. A necessary condition for an integer to be divisible by 6 is that it be divisible by 2.

20. A sufficient condition for an integer to be divisible by 8 is that it be divisible by 16.

21. For all integers a, b, and c, if $a \mid b$ and $a \mid c$ then $a \mid (2b - 3c)$.

22. For all integers a, b, and c, if $ab \mid c$ then $a \mid c$ and $b \mid c$.

23. For all integers a, b, and c, if a is a factor of c then ab is a factor of c.

24. For all integers a, b, and c, if $a \mid (b + c)$ then $a \mid b$ or $a \mid c$.

25. For all integers a, b, and c, if $a \mid bc$ then $a \mid b$ or $a \mid c$.

26. For all integers a and b, if $a \mid b$ then $a^2 \mid b^2$.

27. For all integers a and n, if $a \mid n^2$ and $a \leq n$ then $a \mid n$.

28. For all integers a and b, if $a \mid 10b$ then $a \mid 10$ or $a \mid b$.

29. A fast-food chain has a contest in which a card with numbers on it is given to each customer who makes a purchase. If some of the numbers on the card add up to 100, then the customer wins \$100. A certain customer receives a card containing the numbers

    72, 21, 15, 36, 69, 81, 9, 27, 42, and 63.

    Will the customer win \$100? Why or why not?

30. Is it possible to have a combination of nickels, dimes, and quarters that add up to \$4.72? Explain.

31. Is it possible to have 50 coins, made up of pennies, dimes, and quarters, that add up to \$3? Explain.

32. Two athletes run a circular track at a steady pace so that the first completes one round in 8 minutes and the second in 10 minutes. If they both start from the same spot at 4 P.M., when will be the first time they return to the start together?

33. It can be shown (see exercises 41–45) that an integer is divisible by 3 if, and only if, the sum of its digits is divisible by 3. An integer is divisible by 9 if, and only if, the sum of its digits is divisible by 9. An integer is divisible by 5 if, and only if, its right-most digit is a 5 or a 0. And an integer is divisible by 4 if, and only if, the number formed by its right-most two digits is divisible by 4. Check the following integers for divisibility by 3, 4, 5 and 9.
    a. 637,425,403,705,125 b. 12,858,306,120,312
    c. 517,924,440,926,512 d. 14,328,083,360,232

34. Use the unique factorization theorem to write the following integers in standard factored form.
    a. 1176 b. 5377 c. 3675

35. Suppose that in standard factored form $a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, where k is a positive integer; $p_1, p_2, \ldots, p_k$ are prime numbers; and $e_1, e_2, \ldots, e_k$ are positive integers.
    a. What is the standard factored form for a^2?
    b. Find the least positive integer n such that $2^5 \cdot 3 \cdot 5^2 \cdot 7^3 \cdot n$ is a perfect square. Write the resulting product as a perfect square.
    c. Find the least positive integer m such that $2^2 \cdot 3^5 \cdot 7 \cdot 11 \cdot m$ is a perfect square. Write the resulting product as a perfect square.

36. Suppose that in standard factored form $a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, where k is a positive integer; $p_1, p_2, \ldots, p_k$ are prime numbers; and $e_1, e_2, \ldots, e_k$ are positive integers.
    a. What is the standard factored form for a^3?
    b. Find the least positive integer k such that $2^4 \cdot 3^5 \cdot 7 \cdot 11^2 \cdot k$ is a perfect cube (i.e., equals an integer to the third power). Write the resulting product as a perfect cube.

37. **a.** If a and b are integers and $12a = 25b$, does $12 \mid b$? does $25 \mid a$? Explain.
    b. If x and y are integers and $10x = 9y$, does $10 \mid y$? does $9 \mid x$? Explain.

38. How many zeros are at the end of $45^8 \cdot 88^5$? Explain how you can answer this question without actually computing the number. (*Hint:* $10 = 2 \cdot 5$.)

39. If n is an integer and $n > 1$, then $n!$ is the product of n and every other positive integer that is less than n. For example, $5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$.
    a. Write 6! in standard factored form.
    b. Write 20! in standard factored form.
    c. Without computing the value of $(20!)^2$ determine how many zeros are at the end of this number when it is written in decimal form. Justify your answer.

★40. In a certain town 2/3 of the adult men are married to 3/5 of the adult women. Assume that all marriages are monogamous (no one is married to more than one other person). Also assume that there are at least 100 adult men in the town. What is the least possible number of adult men in the town? of adult women in the town?

Definition: Given any nonnegative integer n, the **decimal representation** of n is an expression of the form

$$d_k d_{k-1} \cdots d_2 d_1 d_0,$$

where k is a nonnegative integer; $d_0, d_1, d_2, \ldots, d_k$ (called the **decimal digits** of n) are integers from 0 to 9 inclusive; $d_k \neq 0$ unless $n = 0$ and $k = 0$; and

$$n = d_k \cdot 10^k + d_{k-1} \cdot 10^{k-1} + \cdots + d_2 \cdot 10^2 + d_1 \cdot 10 + d_0.$$

(For example, $2{,}503 = 2 \cdot 10^3 + 5 \cdot 10^2 + 0 \cdot 10 + 3$.)

41. Prove that if n is any nonnegative integer whose decimal representation ends in 0, then $5 \mid n$. (*Hint:* If the decimal representation of a nonnegative integer n ends in d_0, then $n = 10m + d_0$ for some integer m.)

42. Prove that if n is any nonnegative integer whose decimal representation ends in 5, then $5 \mid n$.

43. Prove that if the decimal representation of a nonnegative integer n ends in d_1d_0 and if $4 \mid (10d_1 + d_0)$, then $4 \mid n$. (*Hint:* If the decimal representation of a nonnegative integer n ends in d_1d_0, then there is an integer s such that $n = 100s + 10d_1 + d_0$.)

H ✶44. Observe that

$$\begin{aligned}7524 &= 7\cdot1000 + 5\cdot100 + 2\cdot10 + 4\\ &= 7(999+1) + 5(99+1) + 2(9+1) + 4\\ &= (7\cdot999 + 7) + (5\cdot99 + 5) + (2\cdot9 + 2) + 4\\ &= (7\cdot999 + 5\cdot99 + 2\cdot9) + (7+5+2+4)\\ &= (7\cdot111\cdot9 + 5\cdot11\cdot9 + 2\cdot9) + (7+5+2+4)\\ &= (7\cdot111 + 5\cdot11 + 2)\cdot9 + (7+5+2+4)\\ &= \text{(an integer divisible by 9)}\\ &\qquad + \text{(the sum of the digits of 7524).}\end{aligned}$$

Since the sum of the digits of 7524 is divisible by 9, 7524 can be written as a sum of two integers each of which is divisible by 9. It follows from exercise 15 that 7524 is divisible by 9.

Generalize the argument given in this example to any nonnegative integer n. In other words, prove that for any nonnegative integer n, if the sum of the digits of n is divisible by 9, then n is divisible by 9.

✶45. Prove that for any nonnegative integer n, if the sum of the digits of n is divisible by 3, then n is divisible by 3.

✶46. Given a positive integer n written in decimal form, the alternating sum of the digits of n is obtained by starting with the right-most digit, subtracting the digit immediately to its left, adding the next digit to the left, subtracting the next digit, and so forth. For example, the alternating sum of the digits of 180,928 is $8 - 2 + 9 - 0 + 8 - 1 = 22$. Justify the fact that for any nonnegative integer n, if the alternating sum of the digits of n is divisible by 11, then n is divisible by 11.

3.4 Direct Proof and Counterexample IV: Division into Cases and the Quotient-Remainder Theorem

Be especially critical of any statement following the word "obviously."
— Anna Pell Wheeler 1883–1966

When you divide 11 by 4, you get a quotient of 2 and a remainder of 3.

$$\begin{array}{r} 2 \leftarrow \text{quotient} \\ 4\overline{)\,11} \\ \underline{8} \\ 3 \leftarrow \text{remainder} \end{array}$$

Another way to say this is that 11 equals 2 groups of 4 with 3 left over:

$$\underbrace{\boxed{\text{XXXX}}\ \boxed{\text{XXXX}}}_{\text{2 groups of 4}}\ \underbrace{\text{XXX}}_{\text{3 left over}}$$

Or,

$$11 = \underbrace{2}_{\text{2 groups of 4}} \cdot 4 + \underbrace{3}_{\text{3 left over}}.$$

Of course, the number left over (3) is less than the size of the groups (4) because if more than 4 were left over, another group of 4 could be separated off.

The quotient-remainder theorem says that when any integer n is divided by any positive integer d, the result is a quotient q and a nonnegative remainder r that is smaller than d.

Theorem 3.4.1 The Quotient-Remainder Theorem

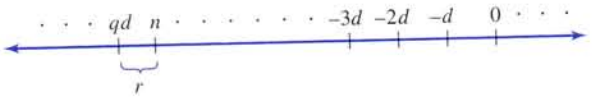
Given any integer n and positive integer d, there exist unique integers q and r such that

$$n = dq + r \quad \text{and} \quad 0 \leq r < d.$$

We give a proof of the quotient-remainder theorem in Section 4.4.

If n is positive, the quotient-remainder theorem can be illustrated on the number line as follows:

If n is negative, the picture changes. Since $n = dq + r$, where r is nonnegative, d must be multiplied by a negative integer q to go below n. Then the nonnegative integer r is added to come back up to n. This is illustrated as follows:



Example 3.4.1 The Quotient-Remainder Theorem

For each of the following values of n and d, find integers q and r such that $n = dq + r$ and $0 \leq r < d$.

a. $n = 54$, $d = 4$ b. $n = -54$, $d = 4$ c. $n = 54$, $d = 70$

Solution

a. $54 = 4 \cdot 13 + 2$; hence $q = 13$ and $r = 2$.

b. $-54 = (-14) \cdot 4 + 2$; hence $q = -14$ and $r = 2$.

c. $54 = 70 \cdot 0 + 54$; hence $q = 0$ and $r = 54$. ■

div and mod

A number of computer languages have built-in functions that enable you to compute many values of q and r for the quotient-remainder theorem. These functions are called **div** and **mod** in Pascal, are called / and % in C and C++, are called / and % in Java, and are called / (or \) and **mod** in .NET. The functions give the values that satisfy the quotient-remainder theorem when a *nonnegative* integer n is divided by a positive integer d and the result is assigned to an integer variable. However, they do not give the values that satisfy the quotient-remainder theorem when a negative integer n is divided by a positive integer d (see exercise 16 at the end of this section). So we restrict our definitions for *div* (short for "divided by") and *mod* (short for "modulo") to division of a nonnegative integer. The modulo concept is discussed in greater detail in Sections 10.3 and 10.4.

• Definition

Given a nonnegative integer n and a positive integer d,

$$\textbf{\textit{n div d}} = \text{the integer quotient obtained when } n \text{ is divided by } d, \text{ and}$$
$$\textbf{\textit{n mod d}} = \text{the integer remainder obtained when } n \text{ is divided by } d.$$

Symbolically, if n and d are positive integers, then

$$n \text{ div } d = q \quad \text{and} \quad n \text{ mod } d = r \quad \Leftrightarrow \quad n = dq + r$$

where q and r are integers and $0 \le r < d$.

Note that it follows from the quotient-remainder theorem that $n \text{ mod } d$ equals one of the integers from 0 through $d - 1$ (since the remainder of the division of n by d must be one of these integers). Note also that a necessary and sufficient condition for an integer n to be divisible by an integer d is that $n \text{ mod } d = 0$. You are asked to prove this in the exercises at the end of this section.

You can also use a calculator to compute values of *div* and *mod*. To compute $n \text{ div } d$ for a nonnegative integer n and a positive integer d, you just divide n by d and ignore the fractional part of the answer. To find $n \text{ mod } d$, you can use the fact that if $n = dq + r$, then $r = n - dq$. Thus since $n = d \cdot (n \text{ div } d) + n \text{ mod } d$, we have that

$$n \text{ mod } d = n - d \cdot (n \text{ div } d).$$

So you can compute $n \text{ div } d$, multiply by d, and subtract the result from n, to obtain $n \text{ mod } d$.

Example 3.4.2 *div* and *mod*

Compute 32 *div* 9 and 32 *mod* 9.

Solution

$$\begin{array}{r} 3 \\ 9\overline{)\,32} \\ \underline{27} \\ 5 \end{array} \quad \begin{array}{l} \leftarrow 32 \textit{ div } 9 \\ \\ \\ \leftarrow 32 \textit{ mod } 9 \end{array}$$

Thus 32 *div* 9 = 3 and 32 *mod* 9 = 5. ■

Example 3.4.3 Computing the Day of the Week

Suppose today is Tuesday, and neither this year nor next year is a leap year. What day of the week will it be 1 year from today?

Solution There are 365 days in a year that is not a leap year, and each week has 7 days. Now

$$365 \textit{ div } 7 = 52 \quad \text{and} \quad 365 \textit{ mod } 7 = 1$$

because $365 = 52 \cdot 7 + 1$. Thus 52 weeks, or 364 days, from today will be a Tuesday, and so 365 days from today will be 1 day later, namely Wednesday.

More generally, if *DayT* is the day of the week today and *DayN* is the day of the week in N days, then

$$DayN = (DayT + N) \bmod 7, \tag{3.4.1}$$

where Sunday $= 0$, Monday $= 1, \ldots,$ Saturday $= 6$. ■

Representations of Integers

In Section 3.1 we defined an even integer to have the form $2k$ for some integer k. At that time we could have defined an odd integer to be one that was not even. Instead, because it was more useful for proving theorems, we specified that an odd integer has the form $2k + 1$ for some integer k. The quotient-remainder theorem brings these two ways of describing odd integers together by guaranteeing that any integer is either even or odd. To see why, let n be any integer, and consider what happens when n is divided by 2. By the quotient-remainder theorem (with $d = 2$), there exist integers q and r such that

$$n = 2q + r \quad \text{and} \quad 0 \leq r < 2.$$

But the only integers that satisfy $0 \leq r < 2$ are $r = 0$ and $r = 1$. It follows that given any integer n, there exists an integer q with

$$n = 2q + 0 \quad \text{or} \quad n = 2q + 1.$$

In the case that $n = 2q + 0 = 2q$, n is even. In the case that $n = 2q + 1$, n is odd. Hence n is either even or odd.

The *parity* of an integer refers to whether the integer is even or odd. For instance, 5 has odd parity and 28 has even parity. We call the fact that any integer is either even or odd the **parity property.**

Example 3.4.4 Consecutive Integers Have Opposite Parity

Prove that given any two consecutive integers, one is even and the other is odd.

Solution Two integers are called *consecutive* if, and only if, one is one more than the other. So if one integer is m, the next consecutive integer is $m + 1$.

To prove the given statement, start by supposing that you have two particular but arbitrarily chosen consecutive integers. If the smaller is m, then the larger will be $m + 1$. How do you know for sure that one of these is even and the other is odd? You might imagine some examples: 4, 5; 12, 13; 1,073, 1,074. In the first two examples, the smaller of the two integers is even and the larger is odd; in the last example, it is the reverse. These observations suggest dividing the analysis into two cases.

Case 1: The smaller of the two integers is even.

Case 2: The smaller of the two integers is odd.

In the first case, when m is even, it appears that the next consecutive integer is odd. Is this always true? If an integer m is even, must $m + 1$ necessarily be odd? Of course the answer is yes. Because if m is even, then $m = 2k$ for some integer k, and so $m + 1 = 2k + 1$, which is odd.

In the second case, when m is odd, it appears that the next consecutive integer is even. Is this always true? If an integer m is odd, must $m + 1$ necessarily be even? Again, the answer is yes. For if m is odd, then $m = 2k + 1$ for some integer k, and so $m + 1 = (2k + 1) + 1 = 2k + 2 = 2(k + 1)$, which is even.

This discussion is summarized as follows.

Theorem 3.4.2

Any two consecutive integers have opposite parity.

Proof:

Suppose that two [*particular but arbitrarily chosen*] consecutive integers are given; call them m and $m + 1$. [*We must show that one of m and $m + 1$ is even and that the other is odd.*] By the parity property, either m is even or m is odd. [*We break the proof into two cases depending on whether m is even or odd.*]

Case 1 (m is even): In this case, $m = 2k$ for some integer k, and so $m + 1 = 2k + 1$, which is odd [*by definition of odd*]. Hence in this case, one of m and $m + 1$ is even and the other is odd.

Case 2 (m is odd): In this case, $m = 2k + 1$ for some integer k, and so $m + 1 = (2k + 1) + 1 = 2k + 2 = 2(k + 1)$. But $k + 1$ is an integer because it is a sum of two integers. Therefore, $m + 1$ equals twice some integer, and thus $m + 1$ is even. Hence in this case also, one of m and $m + 1$ is even and the other is odd.

It follows that regardless of which case actually occurs for the particular m and $m + 1$ that are chosen, one of m and $m + 1$ is even and the other is odd. [*This is what was to be shown.*]

■

The division into cases in a proof is like the transfer of control for an **if-then-else** statement in a computer program. If m is even, control transfers to case 1; if not, control transfers to case 2. For any given integer, only one of the cases will apply. You must consider both cases, however, to obtain a proof that is valid for an arbitrarily given integer whether even or not.

There are times when division into more than two cases is called for. Suppose that at some stage of developing a proof, you know that a statement of the form

$$A_1 \text{ or } A_2 \text{ or } A_3 \text{ or } \ldots \text{ or } A_n$$

is true, and suppose you want to deduce a conclusion C. By definition of *or*, you know that at least one of the statements A_i is true (although you may not know which). In this situation, you should use the method of division into cases. First assume A_1 is true and deduce C; next assume A_2 is true and deduce C; and so forth until you have assumed A_n is true and deduced C. At that point, you can conclude that regardless of which statement A_i happens to be true, the truth of C follows. In symbols,

Given that A_1 or A_2 or A_3 or $\cdots$ or A_n, to show that
$(A_1$ or A_2 or A_3 or $\cdots$ or $A_n) \rightarrow C$, show all the implications

$$\begin{aligned} A_1 &\rightarrow C, \\ A_2 &\rightarrow C, \\ A_3 &\rightarrow C, \\ &\vdots \\ A_n &\rightarrow C. \end{aligned}$$

Note that this form of argument is a generalization of the one given in Example 1.3.8. Its validity was proved in exercise 21 of Section 1.3.

The procedure used to derive the parity property can be applied with other values of d to obtain a variety of alternative representations of integers.

Example 3.4.5 Representations of Integers Modulo 4

Show that any integer can be written in one of the four forms

$$n = 4q \quad \text{or} \quad n = 4q + 1 \quad \text{or} \quad n = 4q + 2 \quad \text{or} \quad n = 4q + 3$$

for some integer q.

Solution Given any integer n, apply the quotient-remainder theorem to n with $d = 4$. This implies that there exist an integer quotient q and a remainder r such that

$$n = 4q + r \quad \text{and} \quad 0 \le r < 4.$$

But the only nonnegative remainders r that are less than 4 are 0, 1, 2, and 3. Hence

$$n = 4q \quad \text{or} \quad n = 4q + 1 \quad \text{or} \quad n = 4q + 2 \quad \text{or} \quad n = 4q + 3$$

for some integer q. ■

The next example illustrates how alternative representations for integers can help establish results in number theory. The solution is broken into two parts: a discussion and a formal proof. These correspond to the stages of actual proof development. Very few people, when asked to prove an unfamiliar theorem, immediately write down the kind of formal proof you find in a mathematics text. Most need to experiment with several possible approaches before they find one that works. A formal proof is much like the ending of a mystery story—the part in which the action of the story is systematically reviewed and all the loose ends are carefully tied together.

Example 3.4.6 The Square of an Odd Integer

Prove that the square of any odd integer has the form $8m + 1$ for some integer m.

Solution Begin by asking yourself, "Where am I starting from?" and "What do I need to show?" To help answer these questions, introduce variables to represent the quantities in the statement to be proved.

Formal Restatement: $\forall$ odd integers n, $\exists$ an integer m such that $n^2 = 8m + 1$.

From this, you can immediately identify the starting point and what is to be shown.

Starting Point: Suppose n is a particular but arbitrarily chosen odd integer.

To Show: $\exists$ an integer m such that $n^2 = 8m + 1$.

This looks tough. Why should there be an integer m with the property that $n^2 = 8m + 1$? That would say that $(n^2 - 1)/8$ is an integer, or that 8 divides $n^2 - 1$. Perhaps you could make use of the fact that $n^2 - 1 = (n - 1)(n + 1)$. Does 8 divide $(n - 1)(n + 1)$? Since n is odd, both $(n - 1)$ and $(n + 1)$ are even. That means that their product is divisible by 4. But that's not enough. You need to show that the product is divisible by 8. This seems to be a blind alley.

You could try another tack. Since n is odd, you could represent n as $2q + 1$ for some integer q. Then $n^2 = (2q + 1)^2 = 4q^2 + 4q + 1 = 4(q^2 + q) + 1$. It is clear from this analysis that n^2 can be written in the form $4m + 1$, but it may not be clear that it can be written as $8m + 1$. This also seems to be a blind alley.*

Yet another possibility is to use the result of Example 3.4.5. That example showed that any integer can be written in one of the four forms $4q$, $4q + 1$, $4q + 2$, or $4q + 3$. Two of these, $4q + 1$ and $4q + 3$, are odd. Thus any odd integer can be written in the

*See exercise 25 for a different perspective.

form $4q + 1$ or $4q + 3$ for some integer q. You could try breaking into cases based on these two different forms.*

It turns out that this last possibility works! In each of the two cases, the conclusion follows readily by direct calculation. The details are shown in the following formal proof:

Theorem 3.4.3

The square of any odd integer has the form $8m + 1$ for some integer m.

Proof:

Suppose n is a [*particular but arbitrarily chosen*] odd integer. By the quotient-remainder theorem, n can be written in one of the forms

$$4q \quad \text{or} \quad 4q + 1 \quad \text{or} \quad 4q + 2 \quad \text{or} \quad 4q + 3$$

for some integer q. In fact, since n is odd and $4q$ and $4q + 2$ are even, n must have one of the forms

$$4q + 1 \quad \text{or} \quad 4q + 3.$$

Case 1 ($n = 4q + 1$ for some integer q): [*We must find an integer m such that $n^2 = 8m + 1$.*] Since $n = 4q + 1$,

$$\begin{aligned} n^2 &= (4q + 1)^2 && \text{by substitution} \\ &= (4q + 1)(4q + 1) && \text{by definition of square} \\ &= 16q^2 + 8q + 1 \\ &= 8(2q^2 + q) + 1 && \text{by the laws of algebra.} \end{aligned}$$

Let $m = 2q^2 + q$. Then m is an integer since 2 and q are integers and sums and products of integers are integers. Thus, substituting,

$$n^2 = 8m + 1 \quad \text{where } m \text{ is an integer.}$$

Case 2 ($n = 4q + 3$ for some integer q): [*We must find an integer m such that $n^2 = 8m + 1$.*] Since $n = 4q + 3$,

$$\begin{aligned} n^2 &= (4q + 3)^2 && \text{by substitution} \\ &= (4q + 3)(4q + 3) && \text{by definition of square} \\ &= 16q^2 + 24q + 9 \\ &= 16q^2 + 24q + (8 + 1) \\ &= 8(2q^2 + 3q + 1) + 1 && \text{by the laws of algebra.} \end{aligned}$$

[*The motivation for the choice of algebra steps was the desire to write the expression in the form $8 \cdot$ (some integer) $+ 1$.*]

Let $m = 2q^2 + 3q + 1$. Then m is an integer since 1, 2, 3, and q are integers and sums and products of integers are integers. Thus, substituting,

$$n^2 = 8m + 1 \quad \text{where } m \text{ is an integer.}$$

Cases 1 and 2 show that given any odd integer, whether of the form $4q + 1$ or $4q + 3$, $n^2 = 8m + 1$ for some integer m. [*This is what we needed to show.*]

■

*Desperation can spur creativity. When you have tried all the obvious approaches without success and you really care about solving a problem, you reach into the odd corners of your memory for *anything* that may help.

Note that the result of Theorem 3.4.3 can also be written, "For any odd integer n, $n^2 \ mod \ 8 = 1$."

Exercise Set 3.4

For each of the values of n and d given in 1–6, find integers q and r such that $n = dq + r$ and $0 \le r < d$.

1. $n = 70, d = 9$
2. $n = 62, d = 7$
3. $n = 36, d = 40$
4. $n = 3, d = 11$
5. $n = -45, d = 11$
6. $n = -27, d = 8$

Evaluate the expressions in 7–10.

7. a. 43 *div* 9 b. 43 *mod* 9
8. a. 50 *div* 7 b. 50 *mod* 7
9. a. 28 *div* 5 b. 28 *mod* 5
10. a. 30 *div* 2 b. 30 *mod* 2
11. Check the correctness of formula (3.4.1) given in Example 3.4.3 for the following values of *DayT* and N.
    a. $DayT = 6$ (Saturday) and $N = 15$
    b. $DayT = 0$ (Sunday) and $N = 7$
    c. $DayT = 4$ (Thursday) and $N = 12$
12. Justify formula (3.4.1) for general values of *DayT* and N.
13. On a Monday a friend says he will meet you again in 30 days. What day of the week will that be?
14. If today is Tuesday, what day of the week will it be 1,000 days from today?
15. January 1, 2000 was a Saturday, and 2000 was a leap year. What day of the week will January 1, 2050 be?
16. The / and % functions in Java operate as follows: If q and r are the integers obtained from the quotient-remainder theorem when a negative integer n is divided by a positive integer d, then n/d is $q + 1$ and $n\%d$ is $r - d$, provided that these values are assigned to an integer variable. Show that n/d and $n\%d$ satisfy one of the conclusions of the quotient-remainder theorem but not the other. To be specific, show that the equation $n = d \cdot n/d + n\%d$ is true but the condition $0 \le n\%d < d$ is false. (The functions **div** and **mod** in Pascal, / and % in C and C++, and / (or \ ) and **mod** in .NET operate similarly to / and % in Java.)
17. When an integer a is divided by 7, the remainder is 4. What is the remainder when $5a$ is divided by 7?
18. When an integer b is divided by 12, the remainder is 5. What is the remainder when $8b$ is divided by 12?
19. When an integer c is divided by 15, the remainder is 3. What is the remainder when $10c$ is divided by 15?
20. Suppose d is a positive integer and n is any integer. If $d \mid n$, what is the remainder obtained when the quotient-remainder theorem is applied to n with divisor d?
21. Prove that a necessary and sufficient condition for a nonnegative integer n to be divisible by a positive integer d is that $n \ mod \ d = 0$.
22. A matrix **M** has 3 rows and 4 columns.

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \end{bmatrix}$$

    The 12 entries in the matrix are to be stored in *row major* form in locations 7,609 to 7,620 in a computer's memory. This means that the entries in the first row (reading left to right) are stored first, then the entries in the second row, and finally the entries in the third row.
    a. Which location will a_{22} be stored in?
    b. Write a formula (in i and j) that gives the integer n so that a_{ij} is stored in location $7{,}609 + n$.
    c. Find formulas (in n) for r and s so that a_{rs} is stored in location $7{,}609 + n$.
23. Let **M** be a matrix with m rows and n columns, and suppose that the entries of **M** are stored in a computer's memory in row major form (see exercise 22) in locations $N, N + 1, N + 2, \ldots, N + mn - 1$. Find formulas in k for r and s so that a_{rs} is stored in location $N + k$.
24. Prove that the product of any two consecutive integers is even.
25. The result of exercise 24 suggests that the second apparent blind alley in the discussion of Example 3.4.6 might not be a blind alley after all. Write a new proof of Theorem 3.4.3 based on this observation.
26. Prove that for all integers n, $n^2 - n + 3$ is odd.
27. Show that any integer n can be written in one of the three forms

$$n = 3q \quad \text{or} \quad n = 3q + 1 \quad \text{or} \quad n = 3q + 2$$

    for some integer q.
28. a. Use the quotient-remainder theorem with $d = 3$ to prove that the product of any three consecutive integers is divisible by 3.
    b. Use the *mod* notation to rewrite the result of part (a).
29. Use the quotient-remainder theorem with $d = 3$ to prove that the square of any integer has the form $3k$ or $3k + 1$ for some integer k.
30. Use the quotient-remainder theorem with $d = 3$ to prove that the product of any two consecutive integers has the form $3k$ or $3k + 2$ for some integer k.

31. a. Prove that for all integers m and n, $m + n$ and $m - n$ are either both odd or both even.
    b. Find all solutions to the equation $m^2 - n^2 = 56$ for which both m and n are positive integers.
    c. Find all solutions to the equation $m^2 - n^2 = 88$ for which both m and n are positive integers.

32. Given any integers a, b, and c, if $a - b$ is even and $b - c$ is even, what can you say about the parity of $2a - (b + c)$? Prove your answer. You may use the properties listed in Example 3.2.3.

33. Given any integers a, b, and c, if $a - b$ is odd and $b - c$ is even, what can you say about the parity of $a - c$? Prove your answer.

H 34. Given any integer n, if $n > 3$, could n, $n + 2$, and $n + 4$ all be prime? Prove or give a counterexample.

35. The fourth power of any integer has the form $8m$ or $8m + 1$ for some integer m.

Prove each of the statements in 36–43.

H 36. The product of any four consecutive integers is divisible by 8.

37. The square of any integer has the form $4k$ or $4k + 1$ for some integer k.

H 38. For any integer $n \geq 1$, $n^2 + 1$ has the form $4k + 1$ or $4k + 2$ for some integer k.

H 39. The sum of any four consecutive integers has the form $4k + 2$ for some integer k.

40. For any integer n, $n(n^2 - 1)(n + 2)$ is divisible by 4.

41. For all integers m, $m^2 = 5k$, or $m^2 = 5k + 1$, or $m^2 = 5k + 4$ for some integer k.

H 42. Every prime number except 2 and 3 has the form $6q + 1$ or $6q + 5$ for some integer q.

43. If n is an odd integer, then $n^4 \bmod 16 = 1$.

✶44. If m, n, and d are integers and $m \bmod d = n \bmod d$, does it necessarily follow that $m = n$? That $m - n$ is divisible by d? Prove your answers.

✶45. If m, n, and d are integers and $d \mid (m - n)$, what is the relation between $m \bmod d$ and $n \bmod d$? Prove your answer.

✶46. If m, n, a, b, and d are integers and $m \bmod d = a$ and $n \bmod d = b$, is $(m + n) \bmod d = a + b$? Is $(m + n) \bmod d = (a + b) \bmod d$? Prove your answers.

✶47. If m, n, a, b, and d are integers and $m \bmod d = a$ and $n \bmod d = b$, is $(mn) \bmod d = ab$? Is $(mn) \bmod d = ab \bmod d$? Prove your answers.

48. Prove that if m, d, and k are integers and $d \neq 0$, then $(m + dk) \bmod d = m \bmod d$.

Use the following definition to prove each statement in 49–53.

Definition: For any real number x, the **absolute value of x**, denoted $|x|$, is defined as follows:

$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}.$$

49. For all real numbers x, $|-x| = |x|$.

50. For all real numbers x and y, $|x| \cdot |y| = |xy|$.

51. For all real numbers x, $-|x| \leq x \leq |x|$.

52. If c is a positive real number and x is any real number, then $-c \leq x \leq c$ if, and only if, $|x| \leq c$. (To prove a statement of the form "A if, and only if, B," you must prove "if A then B" and "if B then A.")

53. For all real numbers x and y, $|x + y| \leq |x| + |y|$. This result is called the **triangle inequality.** (*Hint:* Use 51 and 52 above.)

3.5 Direct Proof and Counterexample V: Floor and Ceiling

Proof serves many purposes simultaneously. In being exposed to the scrutiny and judgment of a new audience, [a] proof is subject to a constant process of criticism and revalidation. Errors, ambiguities, and misunderstandings are cleared up by constant exposure. Proof is respectability. Proof is the seal of authority.

Proof, in its best instances, increases understanding by revealing the heart of the matter. Proof suggests new mathematics. The novice who studies proofs gets closer to the creation of new mathematics. Proof is mathematical power, the electric voltage of the subject which vitalizes the static assertions of the theorems.

Finally, proof is ritual, and a celebration of the power of pure reason.

— Philip J. Davis and Reuben Hersh, *The Mathematical Experience*, 1981

Imagine a real number sitting on a number line. The *floor* and *ceiling* of the number are the integers to the immediate left and to the immediate right of the number (unless the number is, itself, an integer, in which case its floor and ceiling both equal the number itself). Many computer languages have built-in functions that compute floor and ceiling automatically. These functions are very convenient to use when writing certain kinds of computer programs. In addition, the concepts of floor and ceiling are important in analyzing the efficiency of many computer algorithms.

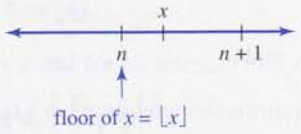
• Definition

Given any real number x, the **floor of x,** denoted $\lfloor x \rfloor$, is defined as follows:

$$\lfloor x \rfloor = \text{that unique integer } n \text{ such that } n \leq x < n + 1.$$

Symbolically, if x is a real number and n is an integer, then

$$\lfloor x \rfloor = n \quad \Leftrightarrow \quad n \leq x < n + 1.$$



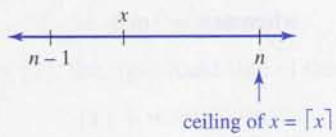
• Definition

Given any real number x, the **ceiling of x,** denoted $\lceil x \rceil$, is defined as follows:

$$\lceil x \rceil = \text{that unique integer } n \text{ such that } n - 1 < x \leq n.$$

Symbolically, if x is a real number and n is an integer, then

$$\lceil x \rceil = n \quad \Leftrightarrow \quad n - 1 < x \leq n.$$



Example 3.5.1 Computing Floors and Ceilings

Compute $\lfloor x \rfloor$ and $\lceil x \rceil$ for each of the following values of x:

a. $25/4$ b. 0.999 c. -2.01

Solution

a. $25/4 = 6.25$ and $6 < 6.25 < 7$; hence $\lfloor 25/4 \rfloor = 6$ and $\lceil 25/4 \rceil = 7$.

b. $0 < 0.999 < 1$; hence $\lfloor 0.999 \rfloor = 0$ and $\lceil 0.999 \rceil = 1$.

c. $-3 < -2.01 < -2$; hence $\lfloor -2.01 \rfloor = -3$ and $\lceil -2.01 \rceil = -2$.

Note that on some calculators $\lfloor x \rfloor$ is denoted INT (x). ■

Example 3.5.2 An Application

The 1,370 soldiers at a military base are given the opportunity to take buses into town for an evening out. Each bus holds a maximum of 40 passengers.

a. For reasons of economy, the base commander will send only full buses. What is the maximum number of buses the base commander will send?

b. If the base commander is willing to send a partially filled bus, how many buses will the commander need to allow all the soldiers to take the trip?

Solution

a. $\lfloor 1370/40 \rfloor = \lfloor 34.25 \rfloor = 34$ b. $\lceil 1370/40 \rceil = \lceil 34.25 \rceil = 35$ ■

Example 3.5.3 Some General Values of Floor

If k is an integer, what are $\lfloor k \rfloor$ and $\lfloor k + 1/2 \rfloor$? Why?

Solution Suppose k is an integer. Then

$$\lfloor k \rfloor = k \text{ because } k \text{ is an integer and } k \leq k < k + 1,$$

and

$$\left\lfloor k + \frac{1}{2} \right\rfloor = k \text{ because } k \text{ is an integer and } k \leq k + \frac{1}{2} < k + 1.$$ ■

Example 3.5.4 Disproving an Alleged Property of Floor

Is the following statement true or false?

For all real numbers x and y, $\lfloor x + y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor$.

Solution The statement is false. As a counterexample, take $x = y = \frac{1}{2}$. Then

$$\lfloor x \rfloor + \lfloor y \rfloor = \left\lfloor \frac{1}{2} \right\rfloor + \left\lfloor \frac{1}{2} \right\rfloor = 0 + 0 = 0,$$

whereas

$$\lfloor x + y \rfloor = \left\lfloor \frac{1}{2} + \frac{1}{2} \right\rfloor = \lfloor 1 \rfloor = 1.$$

Hence $\lfloor x + y \rfloor \neq \lfloor x \rfloor + \lfloor y \rfloor$.

To arrive at this counterexample, you could have reasoned as follows: Suppose x and y are real numbers. Must it necessarily be the case that $\lfloor x + y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor$, or could x and y be such that $\lfloor x + y \rfloor \neq \lfloor x \rfloor + \lfloor y \rfloor$? Imagine values that the various quantities could take. For instance, if both x and y are positive, then $\lfloor x \rfloor$ and $\lfloor y \rfloor$ are the integer parts of $\lfloor x \rfloor$ and $\lfloor y \rfloor$ respectively; just as

$$2\frac{3}{5} = 2 + \frac{3}{5}$$

integer part fractional part

so is

$$x = \lfloor x \rfloor + \text{fractional part of } x$$

and

$$y = \lfloor y \rfloor + \text{fractional part of } y.$$

Thus if x and y are positive,

$$x + y = \lfloor x \rfloor + \lfloor y \rfloor + \textit{the sum of the fractional parts of } x \textit{ and } y.$$

But also

$$x + y = \lfloor x + y \rfloor + \textit{the fractional part of } (x + y).$$

These equations show that if there exist numbers x and y such that the sum of the fractional parts of x and y is at least 1, then a counterexample can be found. But there do exist such x and y; for instance, $x = \frac{1}{2}$ and $y = \frac{1}{2}$ as before. ■

The analysis of Example 3.5.4 indicates that if x and y are positive and the sum of their fractional parts is less than 1, then $\lfloor x + y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor$. In particular, if x is positive and m is a positive integer, then $\lfloor x + m \rfloor = \lfloor x \rfloor + \lfloor m \rfloor = \lfloor x \rfloor + m$. (The fractional part of m is 0; hence the sum of the fractional parts of x and m equals the fractional part of x, which is less than 1.) It turns out that you can use the definition of floor to show that this equation holds for all real numbers x and for all integers m.

Example 3.5.5 Proving a Property of Floor

Prove that for all real numbers x and for all integers m, $\lfloor x + m \rfloor = \lfloor x \rfloor + m$.

Solution Begin by supposing that x is a particular but arbitrarily chosen real number and that m is a particular but arbitrarily chosen integer. You must show that $\lfloor x + m \rfloor = \lfloor x \rfloor + m$. Since this is an equation involving $\lfloor x \rfloor$ and $\lfloor x + m \rfloor$, it is reasonable to give one of these quantities a name: Let $n = \lfloor x \rfloor$. By definition of floor,

$$n \text{ is an integer} \quad \text{and} \quad n \le x < n + 1.$$

This double inequality enables you to compute the value of $\lfloor x + m \rfloor$ in terms of n by adding m to all sides:

$$n + m \le x + m < n + m + 1.$$

Thus the left-hand side of the equation to be shown is

$$\lfloor x + m \rfloor = n + m.$$

On the other hand, since $n = \lfloor x \rfloor$, the right-hand side of the equation to be shown is

$$\lfloor x \rfloor + m = n + m$$

also. Thus $\lfloor x + m \rfloor = \lfloor x \rfloor + m$. This discussion is summarized as follows:

Theorem 3.5.1

For all real numbers x and all integers m, $\lfloor x + m \rfloor = \lfloor x \rfloor + m$.

Proof:

Suppose a real number x and an integer m are given. [*We must show that* $\lfloor x + m \rfloor = \lfloor x \rfloor + m$.] Let $n = \lfloor x \rfloor$. By definition of floor, n is an integer and

$$n \le x < n + 1.$$

Add m to all sides to obtain

$$n + m \le x + m < n + m + 1$$

continued on page 168

[*since adding a number to both sides of an inequality does not change the direction of the inequality*].

Now $n + m$ is an integer [*since n and m are integers and a sum of integers is an integer,*] and so, by definition of floor, the left-hand side of the equation to be shown is

$$\lfloor x + m \rfloor = n + m.$$

But $n = \lfloor x \rfloor$. Hence, by substitution,

$$n + m = \lfloor x \rfloor + m,$$

which is the right-hand side of the equation to be shown. Thus $\lfloor x + m \rfloor = \lfloor x \rfloor + m$ [*as was to be shown*].

■

The analysis of a number of computer algorithms, such as the binary search and merge sort algorithms, requires that you know the value of $\lfloor n/2 \rfloor$, where n is an integer. The formula for computing this value depends on whether n is even or odd.

Theorem 3.5.2 The Floor of $n/2$

For any integer n,

$$\left\lfloor \frac{n}{2} \right\rfloor = \begin{cases} \dfrac{n}{2} & \text{if } n \text{ is even} \\ \dfrac{n-1}{2} & \text{if } n \text{ is odd} \end{cases}$$

Proof:

Suppose n is a [*particular but arbitrarily chosen*] integer. By the quotient-remainder theorem, n is odd or n is even.

Case 1 (n is odd): In this case, $n = 2k + 1$ for some integer k. [*We must show that* $\lfloor n/2 \rfloor = (n-1)/2$.] But the left-hand side of the equation to be shown is

$$\left\lfloor \frac{n}{2} \right\rfloor = \left\lfloor \frac{2k+1}{2} \right\rfloor = \left\lfloor \frac{2k}{2} + \frac{1}{2} \right\rfloor = \left\lfloor k + \frac{1}{2} \right\rfloor = k$$

because k is an integer and $k \le k + 1/2 < k + 1$. And the right-hand side of the equation to be shown is

$$\frac{n-1}{2} = \frac{(2k+1)-1}{2} = \frac{2k}{2} = k$$

also. So since both the left-hand and right-hand sides equal k, they are equal to each other. That is, $\left\lfloor \dfrac{n}{2} \right\rfloor = \dfrac{n-1}{2}$ [*as was to be shown*].

Case 2 (n is even): In this case, $n = 2k$ for some integer k. [*We must show that* $\lfloor n/2 \rfloor = n/2$]. The rest of the proof of this case is left as an exercise.

Given a nonnegative integer n and a positive integer d, the quotient-remainder theorem guarantees the existence of unique integers q and r such that

$$n = dq + r \quad \text{and} \quad 0 \leq r < d.$$

The following theorem states that the floor notation can be used to describe q and r as follows:

$$q = \left\lfloor \frac{n}{d} \right\rfloor \quad \text{and} \quad r = n - d\left\lfloor \frac{n}{d} \right\rfloor.$$

Thus if, on a calculator or in a computer language, floor is built in but *div* and *mod* are not, *div* and *mod* can be defined as follows: For a nonnegative integer n and a positive integer d,

$$n \text{ div } d = \left\lfloor \frac{n}{d} \right\rfloor \quad \text{and} \quad n \bmod d = n - d\left\lfloor \frac{n}{d} \right\rfloor. \tag{3.5.1}$$

Note that d divides n if, and only if, $n \bmod d = 0$, or, in other words, $n = d\lfloor n/d \rfloor$. You are asked to prove this in exercise 13.

Theorem 3.5.3

If n is a nonnegative integer and d is a positive integer, and if $q = \lfloor n/d \rfloor$ and $r = n - d\lfloor n/d \rfloor$, then

$$n = dq + r \quad \text{and} \quad 0 \leq r < d.$$

Proof:

Suppose n is a nonnegative integer, d is a positive integer, $q = \lfloor n/d \rfloor$, and $r = n - d\lfloor n/d \rfloor$. [*We must show that* $n = dq + r$ *and* $0 \leq r < d$.] By substitution,

$$dq + r = d\left\lfloor \frac{n}{d} \right\rfloor + \left(n - d\left\lfloor \frac{n}{d} \right\rfloor\right) = n.$$

So it remains only to show that $0 \leq r < d$. But $q = \lfloor n/d \rfloor$. Thus, by definition of floor,

$$q \leq \frac{n}{d} < q + 1.$$

Then

$$dq \leq n < dq + d \qquad \text{by multiplying all parts by } d$$

and so

$$0 \leq n - dq < d \qquad \text{by subtracting } dq \text{ from all parts.}$$

But

$$r = n - d\left\lfloor \frac{n}{d} \right\rfloor = n - dq.$$

Hence

$$0 \leq r < d \qquad \text{by substitution.}$$

[*This is what was to be shown.*]

Example 3.5.6 Computing *div* and *mod*

Use the floor notation to compute 3850 *div* 17 and 3850 *mod* 17.

Solution By formula (3.5.1),

$$\begin{aligned} 3850 \textit{ div } 17 &= \lfloor 3850/17 \rfloor = \lfloor 226.47 \rfloor = 226 \\ 3850 \textit{ mod } 17 &= 3850 - 17 \cdot \lfloor 3850/17 \rfloor \\ &= 3850 - 17 \cdot 226 \\ &= 3850 - 3842 = 8. \end{aligned}$$

Exercise Set 3.5

Compute $\lfloor x \rfloor$ and $\lceil x \rceil$ for each of the values of x in 1–4.

1. 37.999
2. 17/4
3. −14.00001
4. −32/5
5. Use the floor notation to express 259 *div* 11 and 259 *mod* 11.
6. If k is an integer, what is $\lceil k \rceil$? Why?
7. If k is an integer, what is $\lceil k + \frac{1}{2} \rceil$? Why?
8. Seven pounds of raw material are needed to manufacture each unit of a certain product. Express the number of units that can be produced from n pounds of raw material using either the floor or the ceiling notation. Which notation is more appropriate?
9. Boxes, each capable of holding 36 units, are used to ship a product from the manufacturer to a wholesaler. Express the number of boxes that would be required to ship n units of the product using either the floor or the ceiling notation. Which notation is more appropriate?
10. If 0 = Sunday, 1 = Monday, 2 = Tuesday, . . . , 6 = Saturday, then January 1 of year n occurs on the day of the week given by the following formula:

$$\left(n + \left\lfloor \frac{n-1}{4} \right\rfloor - \left\lfloor \frac{n-1}{100} \right\rfloor + \left\lfloor \frac{n-1}{400} \right\rfloor\right) \textit{ mod } 7.$$

   a. Use this formula to find January 1 of
      i. 2050 ii. 2100 iii. the year of your birth.

   H b. Interpret the different components of this formula.

11. State a necessary and sufficient condition for the floor of a real number to equal that number.
12. Prove that if n is any even integer, then $\lfloor n/2 \rfloor = n/2$.
13. Suppose n and d are integers and $d \neq 0$. Prove each of the following.
   a. If $d \mid n$, then $n = \lfloor n/d \rfloor \cdot d$.
   b. If $n = \lfloor n/d \rfloor \cdot d$, then $d \mid n$.
   c. Use the floor notation to state a necessary and sufficient condition for an integer n to be divisible by an integer d.

Some of the statements in 14–22 are true and some are false. Prove each true statement and find a counterexample for each false statement.

14. For all real numbers x and y, $\lfloor x - y \rfloor = \lfloor x \rfloor - \lfloor y \rfloor$.
15. For all real numbers x, $\lfloor x - 1 \rfloor = \lfloor x \rfloor - 1$.
16. For all real numbers x, $\lfloor x^2 \rfloor = \lfloor x \rfloor^2$.

H 17. For all integers n,

$$\lfloor n/3 \rfloor = \begin{cases} n/3 & \text{if } n \textit{ mod } 3 = 0 \\ (n-1)/3 & \text{if } n \textit{ mod } 3 = 1 \\ (n-2)/3 & \text{if } n \textit{ mod } 3 = 2 \end{cases}.$$

H 18. For all real numbers x and y, $\lceil x + y \rceil = \lceil x \rceil + \lceil y \rceil$.

H 19. For all real numbers x, $\lceil x + 1 \rceil = \lceil x \rceil + 1$.

20. For all real numbers x and y, $\lceil xy \rceil = \lceil x \rceil \cdot \lceil y \rceil$.
21. For all odd integers n, $\lceil n/2 \rceil = (n+1)/2$.
22. For all real numbers x and y, $\lceil xy \rceil = \lceil x \rceil \cdot \lfloor y \rfloor$.

Prove each of the statements in 23–29.

23. For any real number x, if x is not an integer, then $\lfloor x \rfloor + \lfloor -x \rfloor = -1$.
24. For any integer m and any real number x, if x is not an integer, then $\lfloor x \rfloor + \lfloor m - x \rfloor = m - 1$.

H 25. For all real numbers x, $\lfloor \lfloor x/2 \rfloor / 2 \rfloor = \lfloor x/4 \rfloor$.

26. For all real numbers x, if $x - \lfloor x \rfloor < 1/2$ then $\lfloor 2x \rfloor = 2\lfloor x \rfloor$.
27. For all real numbers x, if $x - \lfloor x \rfloor \geq 1/2$ then $\lfloor 2x \rfloor = 2\lfloor x \rfloor + 1$.
28. For any odd integer n,

$$\left\lfloor \frac{n^2}{4} \right\rfloor = \left(\frac{n-1}{2}\right)\left(\frac{n+1}{2}\right).$$

29. For any odd integer n,

$$\left\lceil \frac{n^2}{4} \right\rceil = \frac{n^2+3}{4}.$$

30. Find the mistake in the following "proof" that $\lfloor n/2 \rfloor = (n-1)/2$ if n is an odd integer.

"**Proof:** Suppose n is any odd integer. Then $n = 2k + 1$ for some integer k. Consequently,

$$\left\lfloor \frac{2k+1}{2} \right\rfloor = \frac{(2k+1)-1}{2} = \frac{2k}{2} = k.$$

But $n = 2k + 1$. Solving for k gives $k = (n-1)/2$. Hence, by substitution, $\lfloor n/2 \rfloor = (n-1)/2$."

3.6 Indirect Argument: Contradiction and Contraposition

Reductio ad absurdum is one of a mathematician's finest weapons. It is a far finer gambit than any chess gambit: a chess player may offer the sacrifice of a pawn or even a piece, but the mathematician offers the game. — G. H. Hardy, 1877–1947

In a direct proof you start with the hypothesis of a statement and make one deduction after another until you reach the conclusion. Indirect proofs are more roundabout. One kind of indirect proof, *argument by contradiction,* is based on the fact that either a statement is true or it is false but not both. Suppose you can show that the assumption that a given statement is not true leads logically to a contradiction, impossibility, or absurdity. Then that assumption must be false; hence, the given statement must be true. This method of proof is also known as *reductio ad impossible* or *reductio ad absurdum* because it relies on reducing a given assumption to an impossibility or absurdity.

Argument by contradiction occurs in many different settings. For example, if a man accused of holding up a bank can prove that he was some place else at the time the crime was committed, he will certainly be acquitted. The logic of his defense is as follows:

> Suppose I did commit the crime. Then at the time of the crime, I would have had to be at the scene of the crime. In fact, at the time of the crime I was in a meeting with 20 people far from the crime scene, as they will testify. This contradicts the assumption that I committed the crime, since it is impossible to be in two places at one time. Hence that assumption is false.

Another example occurs in debate. One technique of debate is to say, "Suppose for a moment that what my opponent says is correct." Starting from this supposition, the debater then deduces one statement after another until finally arriving at a statement that is completely ridiculous and unacceptable to the audience. By this means the debater shows the opponent's statement to be false.

The point of departure for a proof by contradiction is the supposition that the statement to be proved is false. The goal is to reason to a contradiction. Thus proof by contradiction has the following outline:

Method of Proof by Contradiction

1. Suppose the statement to be proved is false. That is, suppose that the negation of the statement is true. (Be very careful when writing the negation!)
2. Show that this supposition leads logically to a contradiction.
3. Conclude that the statement to be proved is true.

There are no clear-cut rules for when to try a direct proof and when to try a proof by contradiction. There are some general guidelines, however. Proof by contradiction is indicated if you want to show that there is no object with a certain property, or if you want to show that a certain object does not have a certain property. The next two examples illustrate these situations.

Example 3.6.1 There Is No Greatest Integer

Use proof by contradiction to show that there is no greatest integer.

Solution Most small children believe there is a greatest integer—they often call it a "zillion." But with age and experience, they change their belief. At some point they realize that if there were a greatest integer, they could add 1 to it to obtain an integer that was greater still. Since that is a contradiction, no greatest integer can exist. This line of reasoning is the heart of the formal proof.

For the proof, the certain property is the property of being the greatest integer. To prove that there is no object with this property, begin by supposing the negation: that there is an object with the property.

Starting Point: Suppose not. Suppose there is a greatest integer; call it N.

This means that $N \geq n$ for all integers n.

To Show: This supposition leads logically to a contradiction.

Theorem 3.6.1

There is no greatest integer.

Proof:

[*We take the negation of the theorem and suppose it to be true.*] Suppose not. That is, suppose there is a greatest integer N. [*We must deduce a contradiction.*] Then $N \geq n$ for every integer n. Let $M = N + 1$. Now M is an integer since it is a sum of integers. Also $M > N$ since $M = N + 1$.

Thus M is an integer that is greater than N. So N is the greatest integer and N is not the greatest integer, which is a contradiction. [*This contradiction shows that the supposition is false and, hence, that the theorem is true.*]

■

After a contradiction has been reached, the logic of the argument is always the same: "This is a contradiction. Hence the supposition is false and the theorem is true." Because of this, most mathematics texts end proofs by contradiction at the point at which the contradiction has been obtained.

The contradiction in the next example is based on the fact that $1/2$ is not an integer.

Example 3.6.2 No Integer Can Be Both Even and Odd

Is it possible for an integer to be both even and odd? The intuitive answer is "Of course not." What justifies this certainty? A proof by contradiction!

Theorem 3.6.2

There is no integer that is both even and odd.

Proof:

[*We take the negation of the theorem and suppose it to be true.*] Suppose not. That is, suppose there is an integer n that is both even and odd. [*We must deduce a contradiction.*] By definition of even, $n = 2a$ for some integer a, and by definition of odd, $n = 2b + 1$ for some integer b. Consequently,

$$2a = 2b + 1 \quad \text{by equating the two expressions for } n$$

and so

$$\begin{aligned} 2a - 2b &= 1 \\ 2(a - b) &= 1 \\ (a - b) &= 1/2 \quad \text{by algebra.} \end{aligned}$$

Now since a and b are integers, the difference $a - b$ must also be an integer. But $a - b = 1/2$, and $1/2$ is not an integer. Thus $a - b$ is an integer and $a - b$ is not an integer, which is a contradiction. [*This contradiction shows that the supposition is false and, hence, that the theorem is true.*]

■

The next example asks you to show that the sum of any rational number and any irrational number is irrational. One way to think of this is in terms of a certain object (the sum of a rational and an irrational) not having a certain property (the property of being rational). This suggests trying a proof by contradiction: suppose the object has the property and deduce a contradiction.

Example 3.6.3 The Sum of a Rational Number and an Irrational Number

Use proof by contradiction to show that the sum of any rational number and any irrational number is irrational.

Solution Begin by supposing the negation of what you are to prove. Be very careful when writing down what this means. If you take the negation incorrectly, the entire rest of the proof will be flawed. In this example, the statement to be proved can be written formally as

$$\begin{aligned} &\forall \text{ real numbers } r \text{ and } s, \text{ if } r \text{ is rational and} \\ &s \text{ is irrational, then } r + s \text{ is irrational.} \end{aligned}$$

From this you can see that the negation is

$$\begin{aligned} &\exists \text{ a rational number } r \text{ and an irrational} \\ &\text{number } s \text{ such that } r + s \text{ is rational.} \end{aligned}$$

Caution! The negation of "The sum of any irrational number and any rational number is irrational" is NOT "The sum of any irrational number and any rational number is rational."

It follows that the starting point and what is to be shown are as follows:

Starting Point: Suppose not. That is, suppose there is a rational number r and an irrational number s such that $r + s$ is rational.

To Show: This supposition leads to a contradiction.

To derive a contradiction, you need to understand what you are supposing: There are numbers r and s such that r is rational, s is irrational, and $r + s$ is rational. By definition of rational and irrational, this means that s cannot be written as a quotient of any two integers but that r and $r + s$ can:

$$r = \frac{a}{b} \quad \text{for some integers } a \text{ and } b \text{ with } b \neq 0, \text{ and} \tag{3.6.1}$$

$$r + s = \frac{c}{d} \quad \text{for some integers } c \text{ and } d \text{ with } d \neq 0. \tag{3.6.2}$$

If you substitute (3.6.1) into (3.6.2), you obtain

$$\frac{a}{b} + s = \frac{c}{d}.$$

Subtracting a/b from both sides gives

$$\begin{aligned} s &= \frac{c}{d} - \frac{a}{b} \\ &= \frac{bc}{bd} - \frac{ad}{bd} && \text{by rewriting } c/d \text{ and } a/b \text{ as equivalent fractions} \\ &= \frac{bc - ad}{bd} && \text{by the rule for subtracting fractions with the same denominator.} \end{aligned}$$

But both $bc - ad$ and bd are integers because products and differences of integers are integers, and $bd \neq 0$ by the zero product property. Hence s can be expressed as a quotient of two integers with a nonzero denominator, and so s is rational, which contradicts the supposition that it is irrational.

This discussion is summarized in a formal proof.

Theorem 3.6.3

The sum of any rational number and any irrational number is irrational.

Proof:

[*We take the negation of the theorem and suppose it to be true.*] Suppose not. That is, suppose there is a rational number r and an irrational number s such that $r + s$ is rational. [*We must deduce a contradiction.*] By definition of rational, $r = a/b$ and $r + s = c/d$ for some integers a, b, c, and d with $b \neq 0$ and $d \neq 0$. By substitution,

$$\frac{a}{b} + s = \frac{c}{d},$$

and so

$$\begin{aligned} s &= \frac{c}{d} - \frac{a}{b} && \text{by subtracting } a/b \text{ from both sides} \\ &= \frac{bc - ad}{bd} && \text{by the laws of algebra.} \end{aligned}$$

Now $bc - ad$ and bd are both integers [*since a, b, c, and d are, and since products and differences of integers are integers*], and $bd \neq 0$ [*by the zero product property*]. Hence s is a quotient of the two integers $bc - ad$ and bd with $bd \neq 0$. Thus, by definition of rational, s is rational, which contradicts the supposition that s is irrational. [*Hence the supposition is false and the theorem is true.*]

■

Argument by Contraposition

A second form of indirect argument, *argument by contraposition,* is based on the logical equivalence between a statement and its contrapositive. To prove a statement by contraposition, you take the contrapositive of the statement, prove the contrapositive by a direct proof, and conclude that the original statement is true. The underlying reasoning is that since a conditional statement is logically equivalent to its contrapositive, if the contrapositive is true then the statement must also be true.

Method of Proof by Contraposition

1. Express the statement to be proved in the form

   $$\forall x \text{ in } D, \text{ if } P(x) \text{ then } Q(x).$$

   (This step may be done mentally.)

2. Rewrite this statement in the contrapositive form

   $$\forall x \text{ in } D, \text{ if } Q(x) \text{ is false then } P(x) \text{ is false.}$$

   (This step may also be done mentally.)

3. Prove the contrapositive by a direct proof.

   a. Suppose x is a (particular but arbitrarily chosen) element of D such that $Q(x)$ is false.

   b. Show that $P(x)$ is false.

Example 3.6.4 If the Square of an Integer Is Even, Then the Integer Is Even

Prove that for all integers n, if n^2 is even then n is even.

Solution First form the contrapositive of the statement to be proved.

Contrapositive: For all integers n, if n is not even then n^2 is not even.

By the quotient-remainder theorem with $d = 2$, any integer is even or odd, so any integer that is not even is odd. Also by Theorem 3.6.2, no integer can be both even and odd. So if an integer is odd, then it is not even. Thus the contrapositive can be restated as follows:

Contrapositive: For all integers n, if n is odd then n^2 is odd.

A straightforward computation is the heart of a direct proof for this statement, as shown below.

Proposition 3.6.4

For all integers n, if n^2 is even then n is even.

Proof (by contraposition):

Suppose n is any odd integer. [*We must show that* n^2 *is odd.*] By definition of odd, $n = 2k + 1$ for some integer k. By substitution and algebra, $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. But $2k^2 + 2k$ is an integer because products and sums of integers are integers. So $n^2 = 2 \cdot (\text{an integer}) + 1$, and thus, by definition of odd, n^2 is odd [*as was to be shown*]. ■

We used the word *proposition* here rather than *theorem* because although the word *theorem* can refer to any statement that has been proved, mathematicians often restrict it to especially important statements that have many and varied consequences. Then they use the word **proposition** to refer to a statement that is somewhat less consequential but nonetheless worth writing down. We will use Proposition 3.6.4 in Section 3.7 to prove that $\sqrt{2}$ is irrational.

Relation between Proof by Contradiction and Proof by Contraposition

Observe that any proof by contraposition can be recast in the language of proof by contradiction. In a proof by contraposition, the statement

$$\forall x \text{ in } D, \text{ if } P(x) \text{ then } Q(x)$$

is proved by giving a direct proof of the equivalent statement

$$\forall x \text{ in } D, \text{ if } \sim Q(x) \text{ then } \sim P(x).$$

To do this, you suppose you are given an arbitrary element x of D such that $\sim Q(x)$. You then show that $\sim P(x)$. This is illustrated in Figure 3.6.1.

Figure 3.6.1 Proof by Contraposition

Exactly the same sequence of steps can be used as the heart of a proof by contradiction for the given statement. The only thing that changes is the context in which the steps are written down.

To rewrite the proof as a proof by contradiction, you suppose there is an x in D such that $P(x)$ and $\sim Q(x)$. You then follow the steps of the proof by contraposition to deduce the statement $\sim P(x)$. But $\sim P(x)$ is a contradiction to the supposition that $P(x)$ and $\sim Q(x)$. (Because to contradict a conjunction of statement, it is only necessary to contradict one component.) This process is illustrated in Figure 3.6.2.

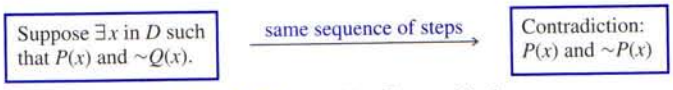


Figure 3.6.2 Proof by Contradiction

As an example, here is a proof by contradiction of Proposition 3.6.4, namely that for any integer n, if n^2 is even then n is even.

Proposition 3.6.4

For all integers n, if n^2 is even then n is even.

Proof (by contradiction):

[*We take the negation of the theorem and suppose it to be true.*] Suppose not. That is, suppose there is an integer n such that n^2 is even and n is not even. [*We must deduce a contradiction.*] By the quotient-remainder theorem with $d = 2$, any integer is even or odd. Hence, since n is not even it is odd, and thus, by definition of odd, $n = 2k + 1$ for some integer k. By substitution and algebra: $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. But $2k^2 + 2k$ is an integer because products and sums of integers are integers. So $n^2 = 2 \cdot (\text{an integer}) + 1$, and so, by definition of odd, n^2 is odd. Therefore, n^2 is both even and odd. This contradicts Theorem 3.6.2, which states that no integer can be both even and odd. [*This contradiction shows that the supposition is false and, hence, that the proposition is true.*]

Note that when you use proof by contraposition, you know exactly what conclusion you need to show, namely the negation of the hypothesis; whereas in proof by contradiction, it may be difficult to know what contradiction to head for. On the other hand, when you use proof by contradiction, once you have deduced any contradiction whatsoever, you are done. The main advantage of contraposition over contradiction is that you avoid having to take (possibly incorrectly) the negation of a complicated statement. The disadvantage of contraposition as compared with contradiction is that you can use contraposition only for a specific class of statements—those that are universal and conditional. The discussion above shows that any statement that can be proved by contraposition can be proved by contradiction. But the converse is not true. Statements such as "$\sqrt{2}$ is irrational" (discussed in the next section) can be proved by contradiction but not by contraposition.

Proof as a Problem-Solving Tool

Direct proof, disproof by counterexample, proof by contradiction, and proof by contraposition are all tools that may be used to help determine whether statements are true or false. Given a statement of the form

For all elements in a domain, if (hypothesis) then (conclusion),

imagine elements in the domain that satisfy the hypothesis. Ask yourself: Must they satisfy the conclusion? If you can see that the answer is "yes" in all cases, then the statement is true and your insight will form the basis for a direct proof. If after some thought it is not clear that the answer is "yes," try to think whether there are elements of the domain that satisfy the hypothesis and *not* the conclusion. If you are successful in finding some, then the statement is false and you have a counterexample. On the other hand, if you are not successful in finding such elements, perhaps none exist. Perhaps you can show that assuming the existence of elements in the domain that satisfy the hypothesis and not the conclusion leads logically to a contradiction. If so, then the given statement is true and you have the basis for a proof by contradiction. Alternatively, you could imagine elements of the domain for which the conclusion is false and ask whether such elements also fail to satisfy the hypothesis. If the answer in all cases is "yes," then you have a basis for a proof by contraposition.

Solving problems, especially difficult problems, is rarely a straightforward process. At any stage of following the guidelines above, you might want to try the method of a previous stage again. If, for example, you fail to find a counterexample for a certain statement, your experience in trying to find it might help you decide to reattempt a direct argument rather than trying an indirect one. Psychologists who have studied problem solving have found that the most successful problem solvers are those who are flexible and willing to use a variety of approaches without getting stuck in any one of them for very long. Mathematicians sometimes work for months (or longer) on difficult problems. Don't be discouraged if some problems in this book take you quite a while to solve.

Learning the skills of proof and disproof is much like learning other skills, such as those used in swimming, tennis, or playing a musical instrument. When you first start out, you may feel bewildered by all the rules, and you may not feel confident as you attempt new things. But with practice the rules become internalized and you can use them in conjunction with all your other powers—of balance, coordination, judgment, aesthetic sense—to concentrate on winning a meet, winning a match, or playing a concert successfully.

Now that you have worked through the first six sections of this chapter, return to the idea that, above all, a proof or disproof should be a convincing argument. You need to know how direct and indirect proofs and counterexamples are structured. But to use this knowledge effectively, you must use it in conjunction with your imaginative powers, your intuition, and especially your common sense.

Exercise Set 3.6

1. Fill in the blanks in the following proof that there is no least positive real number.

Proof: [*We take the negation of the statement and suppose it to be true.*] Suppose not. That is, suppose that there is a real number x such that x is positive and $\underline{\text{(a)}}$ for all positive real numbers y. [*We must deduce* $\underline{\text{(b)}}$.] Consider the number $x/2$. Then $\underline{\text{(c)}}$ because x is positive, and $x/2 < x$ because $\underline{\text{(d)}}$. Hence $\underline{\text{(e)}}$, which is a contradiction. [*Thus the supposition is false, and so there is no least positive real number.*]

2. Is $\dfrac{1}{0}$ an irrational number? Explain.

3. Use proof by contradiction to show that for all integers n, $3n + 2$ is not divisible by 3.

4. Use proof by contradiction to show that for all integers m, $7m + 4$ is not divisible by 7.

Carefully formulate the negations of each of the statements in 5–8. Then prove each statement by contradiction.

5. There is no greatest even integer.

6. There is no greatest negative real number.

7. There is no least positive rational number.

8. a. When asked to prove that the difference of any rational number and any irrational number is irrational, a student begins, "Suppose not. Suppose the difference of any rational number and any irrational number is rational." Comment.

b. Prove by contradiction that the difference of any rational number and any irrational numbr is irrational.

Prove each statement in 9–15 by contradiction.

9. For all real numbers x and y, if x is irrational and y is rational then $x - y$ is irrational.

10. The product of any nonzero rational number and any irrational number is irrational.

11. If a and b are rational numbers, $b \neq 0$, and r is an irrational number, then $a + br$ is irrational.

***H* 12.** For any integer n, $n^2 - 2$ is not divisible by 4.

***H* 13.** For all prime numbers a, b, and c, $a^2 + b^2 \neq c^2$.

***H* 14.** If a, b, and c are integers and $a^2 + b^2 = c^2$, then at least one of a and b is even.

***H* ★ 15.** For all odd integers a, b, and c, if z is a solution of $ax^2 + bx + c = 0$ then z is irrational.

16. Fill in the blanks in the following proof by contraposition that for all integers n, if $5 \nmid n^2$ then $5 \nmid n$.

Proof (by contraposition): [*The contrapositive is: For all integers n, if $5 \mid n$ then $5 \mid n^2$.*] Suppose n is any integer such that $\underline{\text{(a)}}$. [*We must show that* $\underline{\text{(b)}}$.] By definition of divisibility, $n = \underline{\text{(c)}}$ for some integer k. By substitution, $n^2 = \underline{\text{(d)}} = 5(5k^2)$. But $5k^2$ is an integer because it is a product of integers. Hence $n^2 = 5 \cdot$ (an integer), and so $\underline{\text{(e)}}$ [*as was to be shown*].

Prove the statements in 17 and 18 by contraposition.

17. If a product of two positive real numbers is greater than 100, then at least one of the numbers is greater than 10.

18. If a sum of two real numbers is less than 50, then at least one of the numbers is less than 25.

19. Consider the statement "For all integers n, if n^2 is odd then n is odd."
   a. Write what you would suppose and what you would need to show to prove this statement by contradiction.
   b. Write what you would suppose and what you would need to show to prove this statement by contraposition.

20. Consider the statement "For all real numbers r, if r^2 is irrational then r is irrational."
   a. Write what you would suppose and what you would need to show to prove this statement by contradiction.
   b. Write what you would suppose and what you would need to show to prove this statement by contraposition.

Prove each of the statements in 21–26 in two ways: (a) by contraposition and (b) by contradiction.

21. The negative of any irrational number is irrational.

22. The reciprocal of any irrational number is irrational. (The **reciprocal** of a nonzero real number x is $1/x$.)

H 23. For all integers n, if n^2 is odd then n is odd.

24. For all integers a, b, and c, if $a \nmid bc$ then $a \nmid b$. (Recall that the symbol $\nmid$ means "does not divide.")

H 25. For all integers m and n, if $m + n$ is even then m and n are both even or m and n are both odd.

26. For all integers a, b, and c, if $a \mid b$ and $a \nmid c$, then $a \nmid (b + c)$. (*Hint:* To prove $p \to q \vee r$, it suffices to prove either $p \wedge \sim q \to r$ or $p \wedge \sim r \to q$. See exercise 14 in Section 1.2.)

27. The following "proof" that every integer is rational is incorrect. Find the mistake.

"**Proof (by contradiction):** Suppose not. Suppose every integer is irrational. Then the integer 1 is irrational. But $1 = 1/1$, which is rational. This is a contradiction. [*Hence the supposition is false and the theorem is true.*]"

28. **a.** Use the properties of inequalities in Appendix A to prove that for all integers r, s, and n, if $r > \sqrt{n}$ and $s > \sqrt{n}$ then $rs > n$.

H **b.** Use proof by contraposition and the result of part (a) to show that for all integers $n > 1$, if n is not divisible by any positive integer that is greater than 1 and less than or equal to $\sqrt{n}$, then n is prime.

c. Use proof by contraposition and the result of part (b) to show that for all integers $n > 1$, if n is not divisible by any prime number less than or equal to $\sqrt{n}$, then n is prime.

29. Use the result of exercise 28 to determine whether the following numbers are prime.
a. 667 **b.** 557 c. 527 d. 613

30. The sieve of Eratosthenes, named after its inventor, the Greek scholar Eratosthenes (276–194 B.C.), provides a way to find all prime numbers less than or equal to some fixed number n. To construct it, write out all the integers from 2 to n. Cross out all multiples of 2 except 2 itself, then all multiples of 3 except 3 itself, then all multiples of 5 except 5 itself, and so forth. Continue crossing out the multiples of each successive prime number up to $\sqrt{n}$. The numbers that are not crossed out are all the prime numbers from 2 to n. Here is a sieve of Eratosthenes that includes the numbers from 2 to 27. The multiples of 2 are crossed out with a /, the multiples of 3 with a \, and the multiples of 5 with a —.

2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~
~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~ ~~21~~ ~~22~~ 23 ~~24~~ ~~25~~ ~~26~~ ~~27~~

Use the sieve of Eratosthenes to find all prime numbers less than 100.

31. Use the results of exercises 28 and 30 to determine whether the following numbers are prime.
a. 9,269 **b.** 9,103 c. 8,623 d. 7,917

H ✶ 32. Use proof by contradiction to show that every integer greater than 11 is a sum of two composite numbers.

3.7 Two Classical Theorems

How flat and dead would be a mind that saw nothing in a negation but an opaque barrier! A live mind can see a window onto a world of possibilities.
— Douglas Hofstadter, *Gödel, Escher, Bach,* 1979

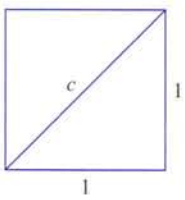
This section contains proofs of two of the most famous theorems in mathematics: that $\sqrt{2}$ is irrational and that there are infinitely many prime numbers. Both proofs are examples of indirect arguments and were well known more than 2,000 years ago, but they remain exemplary models of mathematical argument to this day.

The Irrationality of $\sqrt{2}$

When mathematics flourished at the time of the ancient Greeks, mathematicians believed that given any two line segments, say A: ——— and B: ————, two integers, say a and b, could be found so that the ratio of the lengths of A and B would be in the same proportion as the ratio of a and b. Symbolically:

$$\frac{\text{length } A}{\text{length } B} = \frac{a}{b}.$$

Now it is easy to find a line segment of length $\sqrt{2}$; just take the diagonal of the unit square:



By the Pythagorean theorem, $c^2 = 1^2 + 1^2 = 2$, and so $c = \sqrt{2}$. If the belief of the ancient Greeks were correct, there would be integers a and b such that

$$\frac{\text{length (diagonal)}}{\text{length (side)}} = \frac{a}{b}.$$

And this would imply that

$$\frac{c}{1} = \frac{\sqrt{2}}{1} = \sqrt{2} = \frac{a}{b}.$$

But then $\sqrt{2}$ would be a ratio of two integers, or, in other words, $\sqrt{2}$ would be rational.


CORBIS

Euclid
(fl. 300 B.C.)

In the fourth or fifth century B.C., the followers of the Greek mathematician and philosopher Pythagoras discovered that $\sqrt{2}$ was not rational. This discovery was very upsetting to them, for it undermined their deep, quasi-religious belief in the power of whole numbers to describe phenomena.

The following proof of the irrationality of $\sqrt{2}$ was known to Aristotle and is similar to that in the tenth book of Euclid's *Elements of Geometry*. The Greek mathematician Euclid is best known as a geometer. In fact, knowledge of the geometry in the first six books of his *Elements* has been considered an essential part of a liberal education for more than 2,000 years. Books 7–10 of his *Elements*, however, contain much that we would now call number theory.

The proof begins by supposing the negation: $\sqrt{2}$ is rational. This means that there exist integers m and n such that $\sqrt{2} = m/n$. Now if m and n have any common factors, these may be factored out to obtain a new fraction, equal to m/n, in which the numerator and denominator have no common factors. (For example, $18/12 = (6 \cdot 3)/(6 \cdot 2) = 3/2$, which is a fraction whose numerator and denominator have no common factors.) Thus, without loss of generality, we may assume that m and n had no common factors in the first place.* We will then derive the contradiction that m and n *do* have a common factor of 2. The argument makes use of Proposition 3.6.4: If the square of an integer is even, then that integer is even.

*Strictly speaking, this deduction is a consequence of an axiom called the "well-ordering principle," which is discussed in Section 4.4.

Theorem 3.7.1 Irrationality of $\sqrt{2}$

$\sqrt{2}$ is irrational.

Proof:

[*We take the negation and suppose it to be true.*] Suppose not. That is, suppose $\sqrt{2}$ is rational. Then there are integers m and n with no common factors such that

$$\sqrt{2} = \frac{m}{n} \qquad 3.7.1$$

[*by dividing m and n by any common factors if necessary*]. [*We must derive a contradiction.*] Squaring both sides of equation (3.7.1) gives

$$2 = \frac{m^2}{n^2}.$$

Or, equivalently,

$$m^2 = 2n^2. \qquad 3.7.2$$

Note that equation (3.7.2) implies that m^2 is even (by definition of even). It follows that m is even (by Proposition 3.6.4). We file this fact away for future reference and also deduce (by definition of even) that

$$m = 2k \quad \text{for some integer } k. \qquad 3.7.3$$

Substituting equation (3.7.3) into equation (3.7.2), we see that

$$m^2 = (2k)^2 = 4k^2 = 2n^2.$$

Dividing both sides of the right-most equation by 2 gives

$$n^2 = 2k^2.$$

Consequently, n^2 is even, and so n is even (by Proposition 3.6.4). But we also know that m is even. [*This is the fact we filed away.*] Hence both m and n have a common factor of 2. But this contradicts the supposition that m and n have no common factors. [*Hence the supposition is false and so the theorem is true.*]

Now that you have seen the proof that $\sqrt{2}$ is irrational, you can easily derive the irrationality of certain other real numbers.

Example 3.7.1 Irrationality of $1 + 3\sqrt{2}$

Prove by contradiction that $1 + 3\sqrt{2}$ is irrational.

Solution The essence of the argument is the observation that if $1 + 3\sqrt{2}$ could be written as a fraction, then so could $\sqrt{2}$. But by Theorem 3.7.1, we know that to be impossible.

Proposition 3.7.2

$1 + 3\sqrt{2}$ is irrational.

Proof:

Suppose not. Suppose $1 + 3\sqrt{2}$ is rational. [*We must derive a contradiction.*] Then by definition of rational,

$$1 + 3\sqrt{2} = \frac{a}{b} \quad \text{for some integers } a \text{ and } b \text{ with } b \neq 0.$$

It follows that

$$\begin{aligned} 3\sqrt{2} &= \frac{a}{b} - 1 && \text{by subtracting 1 from both sides} \\ &= \frac{a}{b} - \frac{b}{b} && \text{by substitution} \\ &= \frac{a-b}{b} && \text{by the rule for subtracting fractions with a common denominator.} \end{aligned}$$

Hence

$$\sqrt{2} = \frac{a-b}{3b} \qquad \text{by dividing both sides by 3.}$$

But $a - b$ and $3b$ are integers (since a and b are integers and differences and products of integers are integers), and $3b \neq 0$ by the zero product property. Hence $\sqrt{2}$ is a quotient of the two integers $a - b$ and $3b$ with $3b \neq 0$, and so $\sqrt{2}$ is rational (by definition of rational.) This contradicts the fact that $\sqrt{2}$ is irrational. [*This contradiction shows that the supposition is false.*] Hence $1 + 3\sqrt{2}$ is irrational.

■

The Infinitude of the Set of Prime Numbers

You know that a prime number is a positive integer that cannot be factored as a product of two smaller positive integers. Is the set of all such numbers infinite, or is there a largest prime number? The answer was known to Euclid, and a proof that the set of all prime numbers is infinite appears in Book 9 of his *Elements of Geometry*.

Euclid's proof requires one additional fact we have not yet established: If a prime number divides an integer a, then it does not divide $a + 1$.

Proposition 3.7.3

For any integer a and any prime number p, if $p \mid a$ then $p \nmid (a + 1)$.

Proof:

Suppose not. That is, suppose there exists an integer a and a prime number p such that $p \mid a$ and $p \mid (a + 1)$. Then, by definition of divisibility, there exist integers r and s such that $a = pr$ and $a + 1 = ps$. It follows that $1 = (a + 1) - a = ps - pr = p(s - r)$, and so (since $s - r$ is an integer) $p \mid 1$. But the only integer divisors of 1 are 1 and -1 (see Example 3.3.4), and since p is prime, $p > 1$. Thus $p \leq 1$ and $p > 1$, which is a contradiction. [*Hence the supposition is false, and the proposition is true.*]

The idea of Euclid's proof is this: Suppose the set of prime numbers were finite. Then you could take the product of all the prime numbers and add one. By Theorem 3.3.2 this number must be divisible by some prime number. But by Proposition 3.7.3, this number is not divisible by any of the prime numbers in the set. Hence there must be a prime number that is not in the set of all prime numbers, which is impossible.

The following formal proof fills in the details of this outline.

Theorem 3.7.4 Infinitude of the Primes

The set of prime numbers is infinite.

Proof (by contradiction):

Suppose not. Suppose the set of prime numbers is finite. [*We must deduce a contradiction.*] Then all the prime numbers can be listed, say, in ascending order:

$$p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ p_4 = 7,\ p_5 = 11, \ldots, p_n.$$

Consider the integer

$$N = p_1 p_2 p_3 \cdots p_n + 1.$$

Then $N > 1$, and so, by Theorem 3.3.2, N is divisible by some prime number p. Also, since p is prime, p must equal one of the prime numbers $p_1, p_2, p_3, \ldots, p_n$. Thus $p \mid (p_1 p_2 p_3 \cdots p_n)$. By Proposition 3.7.3, $p \nmid (p_1 p_2 p_3 \cdots p_n + 1)$, and so $p \nmid N$. Hence $p \mid N$ and $p \nmid N$, which is a contradiction. [*Hence the supposition is false and the theorem is true.*]

The proof of Theorem 3.7.4 shows that if you form the product of all prime numbers up to a certain point and add one, the result, N, is divisible by a prime number not on the list. The proof does not show that N is, itself, prime. In the exercises at the end of this section you are asked to find an example of an integer N constructed in this way that is not prime.

When to Use Indirect Proof

The examples in this section and Section 3.6 have not provided a definitive answer to the question of when to prove a statement directly and when to prove it indirectly. Many theorems can be proved either way. Usually, however, when both types of proof are possible, indirect proof is clumsier than direct proof. In the absence of obvious clues suggesting indirect argument, try first to prove a statement directly. Then, if that does not succeed, look for a counterexample. If the search for a counterexample is unsuccessful, look for a proof by contradiction or contraposition.

Open Questions in Number Theory

In this section we proved that there are infinitely many prime numbers. There is no known formula for obtaining primes, but a few formulas have been found to be more successful at producing them than other formulas. One such is due to Marin Mersenne, a French monk who lived from 1588–1648. *Mersenne primes* have the form $2^p - 1$, where p is prime. Not all numbers of this form are prime, but because of the greater likelihood of finding primes among them, those seeking large prime numbers often test these for primality. As a result, many of the largest known prime numbers are Mersenne primes.

An interesting question is whether there are infinitely many Mersenne primes. As of the date of publication of this book, the answer is not known, but new mathematical discoveries are being made every day and by the time you read this someone may have discovered the answer. Another formula that seems to produce a relatively large number of prime numbers is due to Fermat. *Fermat primes* are prime numbers of the form $2^{2^n} + 1$, where n is a positive integer. Are there infinitely many Fermat primes? Again, as of now, no one knows. Similarly unknown are whether there are infinitely many primes of the form $n^2 + 1$, where n is a positive integer, and whether there is always a prime number between integers n^2 and $(n + 1)^2$.

Another famous open question involving primes is the *twin primes conjecture,* which states that there are infinitely many pairs of prime numbers of the form p and $p + 2$. As with other well-known problems in number theory, this conjecture has withstood computer testing up to extremely large numbers. But compared with infinity, any number, no matter how large, is less than a drop in the ocean.

In 1844, the Belgian mathematician Eugène Catalan conjectured that the only solutions to the equation $x^n - y^m = 1$, where x, y, n, and m are all integers greater than 1, is $3^2 - 2^3 = 1$. This conjecture also remains unresolved to this day.

In 1993, while trying to prove Fermat's last theorem, an amateur number theorist, Andrew Beal, became intrigued by the equation $x^m + y^n = z^k$, where no two of x, y, or z have any common factor other than ± 1. When diligent effort, first by hand and then by computer, failed to reveal any solutions, Beal conjectured that no solutions exist. His conjecture has become known as *Beal's conjecture,* and he has offered a prize of $100,000 to anyone who can either prove or disprove it.

These are just a few of a large number of open questions in number theory. Many people believe that mathematics is a fixed subject that changes very little from one century to the next. In fact, more mathematical questions are being raised and more results are being discovered now than ever before in history.

Exercise Set 3.7

1. A calculator display shows that $\sqrt{2} = 1.414213562$, and $1.414213562 = \dfrac{1414213562}{1000000000}$. This suggests that $\sqrt{2}$ is a rational number, which contradicts Theorem 3.7.1. Explain the discrepancy.

2. Example 3.2.1(h) illustrates a technique for showing that any repeating decimal number is rational. A calculator display shows the result of a certain calculation as 40.72727272727. Can you be sure that the result of the calculation is a rational number? Explain.

Determine which statements in 3–13 are true and which are false. Prove those that are true and disprove those that are false.

3. $6 - 7\sqrt{2}$ is irrational.
4. $3\sqrt{2} - 7$ is irrational.
5. $\sqrt{4}$ is irrational.
6. $\sqrt{2}/6$ is rational.
7. The sum of any two irrational numbers is irrational.
8. The difference of any two irrational numbers is irrational.
9. The square root of an irrational number is irrational.
10. If r is any rational number and s is any irrational number, then r/s is irrational.
11. The sum of any two positive irrational numbers is irrational.
12. The product of any two irrational numbers is irrational.
13. If an integer greater than 1 is a perfect square, then its cube root is irrational.
14. Consider the following sentence: If x is rational then $\sqrt{x}$ is irrational. Is this sentence always true, sometimes true and sometimes false, or always false? Justify your answer.
15. a. Prove that for all integers a, if a^3 is even then a is even.
    b. Prove that $\sqrt[3]{2}$ is irrational.
16. a. Use proof by contradiction to show that for any integer n, it is impossible for n to equal both $3q_1 + r_1$ and $3q_2 + r_2$, where q_1, q_2, r_1, and r_2, are integers, $0 \le r_1 < 3$, $0 \le r_2 < 3$, and $r_1 \ne r_2$.
    b. Use proof by contradiction, the quotient-remainder theorem, division into cases, and the result of part (a) to prove that for all integers n, if n^2 is divisible by 3 then n is divisible by 3.
    c. Prove that $\sqrt{3}$ is irrational.
17. Give an example to show that if d is not prime and n^2 is divisible by d, then n need not be divisible by d.

H 18. The quotient-remainder theorem says not only that there exist quotients and remainders but also that the quotient and remainder of a division are unique. Prove the uniqueness. That is, prove that if a and d are integers with $d > 0$ and if q_1, r_1, q_2, and r_2 are integers such that

$$a = dq_1 + r_1 \quad \text{where } 0 \le r_1 < d$$

and

$$a = dq_2 + r_2 \quad \text{where } 0 \le r_2 < d,$$

then

$$q_1 = q_2 \quad \text{and} \quad r_1 = r_2.$$

H 19. Prove that $\sqrt{5}$ is irrational.

H 20. Prove that for any integer a, $9 \nmid (a^2 - 3)$.

21. **a.** Use the unique factorization theorem to answer the following question: If the prime factorization of an integer n contains k occurrences of a prime number p, how many occurrences of p are contained in the prime factorization of n^2?

b. An alternative proof of the irrationality of $\sqrt{2}$ counts the number of 2's on the two sides of the equation $2n^2 = m^2$ and deduces a contradiction. Write a proof that uses this approach.

22. Use the proof technique illustrated in exercise 21(b) to prove that if n is any integer that is not a perfect square, then $\sqrt{n}$ is irrational.

H 23. Prove that $\sqrt{2} + \sqrt{3}$ is irrational.

H 24. Prove that $\log_5(2)$ is irrational.

H 25. Let $N = 2 \cdot 3 \cdot 5 \cdot 7 + 1$. What remainder is obtained when N is divided by 2? 3? 5? 7? Is N prime? Justify your answer.

H 26. Suppose a is an integer and p is a prime number such that $p \mid a$ and $p \mid (a + 3)$. What can you deduce about p? Why?

27. Let $p_1, p_2, p_3, \ldots$ be a list of all prime numbers in ascending order. Here is a table of the first six:

p_1	p_2	p_3	p_4	p_5	p_6
2	3	5	7	11	13

H **a.** For each $i = 1, 2, 3, 4, 5, 6$, let $N_i = p_1 p_2 \cdots p_i + 1$. Calculate N_1, N_2, N_3, N_4, N_5, and N_6.

b. For each $i = 1, 2, 3, 4, 5, 6$, find the smallest prime number q_i such that q_i divides N_i.

28. An alternative proof of the infinitude of the prime numbers begins as follows:

Proof: Suppose there are only finitely many prime numbers. Then one is the largest. Call it p. Let $M = p! + 1$. We will show that there is a prime number q such that $q > p$.

Complete this proof.

H ★ **29.** Prove that if $p_1, p_2, \ldots$, and p_n are distinct prime numbers with $p_1 = 2$ and $n > 1$, then $p_1 p_2 \cdots p_n + 1$ can be written in the form $4k + 3$ for some integer k.

H ★ **30.** Prove that for all integers n, if $n > 2$ then there is a prime number p such that $n < p < n!$.

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

H **31.** a. Fermat's last theorem says that for all integers $n > 2$, the equation $x^n + y^n = z^n$ has no positive integer solution (solution for which x, y, and z are positive integers). Prove the following: If for all prime numbers $p > 2$, $x^p + y^p = z^p$ has no positive integer solution, then for any integer $n > 2$ that is not a power of 2, $x^n + y^n = z^n$ has no positive integer solution.

b. Fermat proved that there are no integers x, y, and z such that $x^4 + y^4 = z^4$. Use this result to remove the restriction in part (a) that n not be a power of 2. That is, prove that if n is a power of 2 and $n > 4$, then $x^n + y^n = z^n$ has no positive integer solution.

For exercises 32–35 note that to show there is a unique object with a certain property, show that (1) there is an object with the property and (2) if objects A and B have the property, then $A = B$.

32. Prove that there exists a unique prime number of the form $n^2 - 1$, where n is an integer that is greater than or equal to 2.

33. Prove that there exists a unique prime number of the form $n^2 + 2n - 3$, where n is a positive integer.

34. Prove that there is at most one real number a with the property that $a + r = r$ for all real numbers r. (Such a number is called an *additive identity*.)

35. Prove that there is at most one real number b with the property that $br = r$ for all real numbers r. (Such a number is called a *multiplicative identity*.)