CHAPTER 4

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 4.5 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 1 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, if $5x + 3 = 33$ then $x = 6$.

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. One of the most important reason's 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 2.2), 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.

4.1 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.

Assumptions

- 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 there is no integer between 0 and 1 and that the set of all 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 an 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 4.1.1 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 4.4 that this fact results from another fact known as the quotient-remainder theorem. ■

The integer 6, which equals $2 \cdot 3$, 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 $n = rs$, then either r or s equals n. An integer n is **composite** if, and only if, $n > 1$ and $n = rs$ for some integers r and s with $1 < r < n$ and $1 < s < n$.

In symbols:

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

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

Example 4.1.2 Prime and Composite Numbers

a. Is 1 prime?

b. Is every integer greater than 1 either prime or composite?

c. Write the first six prime numbers.

d. Write the first six composite numbers.

Solution

Note The reason for not allowing 1 to be prime is discussed in Section 4.3.

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

b. Yes. Let n be any integer that is greater than 1. Consider all pairs of positive integers r and s such that $n = rs$. There exist at least two such pairs, namely $r = n$ and $s = 1$ and $r = 1$ and $s = n$. Moreover, since $n = rs$, all such pairs satisfy the inequalities $1 \le r \le n$ and $1 \le s \le n$. If n is prime, then the two displayed pairs are the only ways to write n as rs. Otherwise, there exists a pair of positive integers r and s such that $n = rs$ and neither r nor s equals either 1 or n. Therefore, in this case $1 < r < n$ and $1 < s < n$, and hence n is composite.

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

d. 4, 6, 8, 9, 10, 12 ■

Proving Existential Statements

According to the definition given in Section 3.1, 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 4.1.3 Constructive Proofs of Existence

a. Prove the following: ∃ 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: ∃ 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 the hypothesis $P(x)$ is true and the conclusion $Q(x)$ is false. Such an x is called a **counterexample.**

Example 4.1.4 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 the hypothesis $a^2 = b^2$ is true and the conclusion $a = b$ is false. 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 4.1.4 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:

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

Sections 1.1 and 3.1 give examples showing how to write any universal statement in this form. When D is finite or when only a finite number of elements satisfy $P(x)$, such a statement can be proved by the method of exhaustion.

Example 4.1.5 The Method of Exhaustion

Use the method of exhaustion to prove the following statement:

$\forall n \in \mathbf{Z}$, if n is even and $4 \leq n \leq 26$, then n can be written as a sum of two prime numbers.

Solution

$$4 = 2 + 2 \qquad 6 = 3 + 3 \qquad 8 = 3 + 5 \qquad 10 = 5 + 5$$
$$12 = 5 + 7 \qquad 14 = 11 + 3 \qquad 16 = 5 + 11 \qquad 18 = 7 + 11$$
$$20 = 7 + 13 \qquad 22 = 5 + 17 \qquad 24 = 5 + 19 \qquad 26 = 7 + 19$$

■

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

Example 4.1.6 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 an empty box $\square$ or the symbol x stand for the number the person picks. Here is what happens when the person follows your directions:

Step	Visual Result	Algebraic Result
Pick a number.	$\square$	x
Add 5.	$\square$ | | | | |	$x + 5$
Multiply by 4.	$\square$ | | | | | $\square$ | | | | | $\square$ | | | | | $\square$ | | | | |	$(x + 5) \cdot 4 = 4x + 20$
Subtract 6.	$\square$ | | $\square$ | | $\square$ | | | | | $\square$ | | | | |	$(4x + 20) - 6 = 4x + 14$
Divide by 2.	$\square$ | | $\square$ | | | | |	$\frac{4x + 14}{2} = 2x + 7$
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 any number whatsoever can be put in its place). 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 an if-then statement can be false is for the hypothesis to be true and the conclusion to be false. Thus, given the statement "If $P(x)$ then $Q(x)$," if you can show that the truth of $P(x)$ compels the truth of $Q(x)$, then you will have proved the statement. It follows by the method of generalizing from the generic particular that to show that "$\forall x$, if $P(x)$ then $Q(x)$," is true for *all* elements x in a set D, you suppose x is a particular but arbitrarily chosen element of D that makes $P(x)$ true, and then you show that x makes $Q(x)$ true.

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 4.1.7 A Direct Proof of a Theorem

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.

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

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 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, each equals twice some integer. One of the basic laws of logic, called *existential instantiation*, says, in effect, that if you know something exists, you can give it a name. However, you cannot use the same name to refer to two different things, both of which are currently under discussion.

Existential Instantiation

If the existence of a certain kind of object is assumed or has been deduced then it can be given a name, as long as that name is not currently being used to denote something else.

Caution! Because m and n are arbitrarily chosen, they could be any pair of even integers whatsoever. Once r is introduced to satisfy $m = 2r$, then r is not available to represent something else. If you had set $m = 2r$, and $n = 2r$, then m would equal n, which need not be the case.

Thus since m equals twice some integer, you can give that integer a name, and since n equals twice some integer, you can also give that integer a name:

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

Now what you want to show is that $m + n$ is even. In other words, you want to show that $m + n$ equals $2 \cdot$(some integer). Having just found alternative 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 italic 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 4.1.1

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

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

Note Introducing t to equal $r + s$ is another use of existential instantiation.

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

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

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 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 4.1.1. 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. Ideally, your proof will lead your classmate to understand *why* the given statement is true.

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

†See page 134 for a discussion of the role of universal modus ponens in this proof.

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 explain the meaning of 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 any even integers" or "Let x be a real number such that x 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 at that point to exist. For example, if you have assumed that a particular integer n is even, then you know that n equals 2 times some integer, and you can 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," or "since n is even, there exists an integer s such that $n = 2s$."
4. **Write your proof in complete, gramatically correct 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 4.1.1 contains the sentence

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

   To read such text as a sentence, read the first equals sign as "equals" and each subsequent equals sign as "which equals."
5. **Keep your reader informed about the status of each statement in your proof.**

   Your reader should never be in doubt about whether something in your proof has been assumed or established or is still to be deduced. If something is assumed, preface it with a word like *Suppose* or *Assume*. If it is still to be shown, preface it with words like, *We must show that* or *In other words, we must show that*. This is especially important if you introduce a variable in rephrasing what you need to show. (See Common Mistakes on the next page.)
6. **Give a reason for each assertion 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 . . .*.
7. **Include the "little words and phrases" 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 *Consequently*, or *It follows that,* and include the reason at the end of the sentence. For instance, in the proof of Theorem 4.1.1, once you know that m is even, you can write: "By definition of even, $m = 2r$ for some integer r," or you can write, "Then $m = 2r$ for some integer r 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 4.1.1, once it is known that $m + n = 2(r + s)$, where r and s are integers, a new variable t is introduced to represent $r + s$. The proof goes on to say, "Let $t = r + s$. Then t is an integer because it is a sum of two integers."

8. **Display equations and inequalities.**

The convention is to display equations and inequalities on separate lines to increase readability, both for other people and for ourselves so that we can more easily check our work for accuracy. We follow the convention in the text of this book, but in order to save space, we violate it in a few of the exercises and in many of the solutions contained in Appendix B. So you may need to copy out some parts of solutions on scratch paper to understand them fully. Please follow the convention in your own work. Leave plenty of empty space, and don't be stingy with paper!

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 property referred to in 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 4.1.1).

> 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 previous example, 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 any 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. **Circular reasoning.**
   To engage in circular reasoning 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.

5. **Confusion between what is known and what is still to be shown.**
   A more subtle way to engage in circular reasoning occurs when the conclusion to be shown is restated using a variable. Here is an example in a "proof" that the product of any two odd integers is odd:

   Suppose m and n are any odd integers. We must show that mn is odd. This means that there exists an integer s such that

   $$mn = 2s + 1.$$

   Also by definition of odd, there exist integers a and b such that

   $$m = 2a + 1 \text{ and } n = 2b + 1.$$

   Then

   $$mn = (2a + 1)(2b + 1) = 2s + 1.$$

   So, since s is an integer, mn is odd by definition of odd.

   In this example, when the author restated the conclusion to be shown (that mn is odd), the author wrote "there exists an integer s such that $mn = 2s + 1$." Later the author jumped to an unjustified conclusion by assuming the existence of this s when

that had not, in fact, been established. This mistake might have been avoided if the author had written "This means that we must show that there exists an integer s such that

$$mn = 2s + 1.$$

An even better way to avoid this kind of error is not to introduce a variable into a proof unless it is either part of the hypothesis or deducible from it.

6. **Use of *any* rather than *some*.**
   There are a few situations in which the words *any* and *some* can be used interchangeably. For instance, in starting a proof that the square of any odd integer is odd, one could correctly write "Suppose m is any odd integer" or "Suppose m is some odd integer." In most situations, however, the words *any* and *some* are not interchangeable. Here is the start of a "proof" that the square of any odd integer is odd, which uses *any* when the correct word is *some*:

   > Suppose m is a particular but arbitrarily chosen odd integer.
   > By definition of odd, $m = 2a + 1$ for any integer a.

   In the second sentence it is incorrect to say that "$m = 2a + 1$ for any integer a" because a cannot be just "any" integer; in fact, solving $m = 2a + 1$ for a shows that the only possible value for a is $(m - 1)/2$. The correct way to finish the second sentence is, "$m = 2a + 1$ for some integer a" or "there exists an integer a such that $m = 2a + 1$."

7. **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 4.1.8 Identifying the "Starting Point" and the "Conclusion to Be Shown"

Note You are not expected to know anything about complete, bipartite graphs.

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

> Every complete, bipartite graph is connected.

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: graphs G; hypothesis: G is complete and bipartite; conclusion: G is connected)

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 shape:

Proof:

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

⋮

Therefore, G is connected. ■

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 4.1.9 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

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

Bettmann/CORBIS

Pierre de Fermat
(1601–1665)

Andrew Wiles/Princeton University

Andrew Wiles
(born 1953)

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.*

One of the oldest problems in mathematics that remains unsolved is the Goldbach conjecture. In Example 4.1.5 it was shown that every even integer from 4 to 26 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^{18}. But there is a huge chasm between 10^{18} 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 11.

Test Yourself

Answers to Test Yourself questions are located at the end of each section.

1. An integer is even if, and only if, _____.
2. An integer is odd if, and only if, _____.
3. An integer n is prime if, and only if, _____.
4. The most common way to disprove a universal statement is to find _____.

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

5. According to the method of generalizing from the generic particular, to show that every element of a set satisfies a certain property, suppose x is a _____, and show that _____.

6. To use the method of direct proof to prove a statement of the form, "For all x in a set D, if $P(x)$ then $Q(x)$," one supposes that _____ and one shows that _____.

Exercise Set 4.1*

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. $(a + b)^2 = a^2 + b^2$ ***H*** 15. $-a^n = (-a)^n$

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 $16 = 4^2$.)

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 three different ways: as $\forall$ _____, if _____ then _____, as $\forall$ _____, _____ (without using the words *if* or *then*), and as If _____, then _____ (without using an explicit universal quantifier).

b. Fill in the blanks in the proof of the theorem.

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

Proof: Suppose m is any even integer and n is $\underline{\text{(a)}}$. By definition of even, $m = 2r$ for some $\underline{\text{(b)}}$, and by definition of odd, $n = 2s + 1$ for some integer s. By substitution and algebra,

$$m + n = \underline{\text{(c)}} = 2(r + s) + 1.$$

Since r and s are both integers, so is their sum $r + s$. Hence $m + n$ has the form twice some integer plus one, and so $\underline{\text{(d)}}$ by definition of odd.

Each of the statements in 20–23 is true. For each, (a) rewrite the statement with the quantification implicit as 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 $0 < \frac{1}{m} < 1$.

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 $x^2 < x$.

*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.

Prove the statements in 24–34. In each case use only the definitions of the terms and the Assumptions listed on page 146, not any previously established properties of odd and even integers. 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.

***H* 26.** The difference between any odd integer and any even integer is odd. (*Note:* The "proof" shown in exericse 39 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. For all integers n, if n is odd then $3n + 5$ is even.

30. For all integers m, if m is even then $3m + 5$ is odd.

31. If k is any odd integer and m is any even integer, then, $k^2 + m^2$ is odd.

32. If a is any odd integer and b is any even integer, then, $2a + 3b$ is even.

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

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

Prove that the statements in 35–37 are false.

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

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

37. There exists an integer $k \geq 4$ such that $2k^2 - 5k + 2$ is prime.

Find the mistakes in the "proofs" shown in 38–42.

38. **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."

39. **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."

40. **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 $k^2 + 2k + 1 = rs$ for some integers r and s such that

$$1 < r < (k^2 + 2k + 1)$$

and

$$1 < s < (k^2 + 2k + 1).$$

Since

$$k^2 + 2k + 1 = rs$$

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."

41. **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

$$mn = (2p)(2q + 1) = 2r,$$

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

42. **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 43–60 determine whether the statement is true or false. Justify your answer with a proof or a counterexample, as appropriate. In each case use only the definitions of the terms and the Assumptions listed on page 146 not any previously established properties.

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

44. The negative of any odd integer is odd.

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

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

47. 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.**)

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

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

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

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

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

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

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

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

H ✶56. (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.

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

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

59. 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 $y^2 = x$.)

60. For all nonnegative real numbers a and b,

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

61. Suppose that integers m and n are perfect squares. Then $m + n + 2\sqrt{mn}$ is also a perfect square. Why?

H ✶62. If p is a prime number, must $2^p - 1$ also be prime? Prove or give a counterexample.

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

Answers for Test Yourself

1. it equals twice some integer 2. it equals twice some integer plus 1 3. n is greater than 1 and if n equals the product of any two positive integers, then one of the integers equals 1 and the other equals n. 4. a counterexample 5. particular but arbitrarily chosen element of the set; x satisfies the given property 6. x is a particular but arbitrarily chosen element of the set D that makes the hypothesis $P(x)$ true; x makes the conclusion $Q(x)$ true.

4.2 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 can be written as a ratio of integers.

Example 4.2.1 Determining Whether Numbers Are Rational or Irrational

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

b. Is $-\frac{5}{39}$ a rational number?

c. Is 0.281 a rational number?

d. Is 7 a rational number?

e. Is 0 a rational number?