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

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

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.]*†

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

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.