20. Determine whether these are valid arguments.
   a) If a is a positive real number, then \( a^2 \) is a positive real number. Therefore, if \( a^2 \) is positive, where \( a \) is a real number, then \( a \) is a positive real number.
b) If \( a \neq 0 \), where \( a \) is a real number, then \( x \neq 0 \). Let \( a \) be a real number with \( a^2 \neq 0 \); then \( a \neq 0 \).

21. Which rules of inference are used to establish the conclusion of Lewis Carroll's argument described in Example 26 of Section 1.4?

22. Which rules of inference are used to establish the conclusion of Lewis Carroll's argument described in Example 27 of Section 1.4?

23. Identify the error or errors in this argument that supposedly shows that if \( \exists x (P(x) \land Q(x)) \) is true then \( \exists x (P(x) \land Q(x)) \) is true.

24. Identify the error or errors in this argument that supposedly shows that if \( \forall x (P(x) \lor Q(x)) \) is true then \( \forall x (P(x) \lor Q(x)) \) is true.

25. Justify the rule of universal modus tollens by showing that the premises \( \forall x (P(x) \rightarrow Q(x)) \) and \( \neg Q(a) \) for a particular element \( a \) in the domain, imply \( \neg P(a) \).

26. Justify the use of universal modus tollens by showing that if \( \forall x (P(x) \rightarrow Q(x)) \) and \( \forall x (P(x) \rightarrow R(x)) \) are true, then \( \forall x (R(x) \rightarrow S(x)) \) is true, where the domains of all quantifiers are the same.

27. Use rules of inference to show that if \( \forall x (P(x) \rightarrow (Q(x) \lor S(x))) \) and \( \forall x (P(x) \land R(x)) \) are true, then \( \forall x (R(x) \land S(x)) \) is true.

28. Use rules of inference to show that if \( \forall x (P(x) \lor Q(x)) \) and \( \forall x (\neg (P(x) \lor Q(x)) \rightarrow R(x)) \) is true, then \( \forall x (\neg R(x) \rightarrow P(x)) \) is also true, where the domains of all quantifiers are the same.

29. Use rules of inference to show that if \( \forall x (P(x) \lor Q(x)) \), \( \forall x (\neg (Q(x) \lor S(x))) \), \( \forall x (R(x) \rightarrow \neg S(x)) \), and \( \exists x \neg P(x) \) are true, then \( \exists x \neg R(x) \) is true.

30. Use resolution to show the hypotheses “Allen is a bad boy or Hillary is a good girl” and “Allen is a good boy or David is happy” imply the conclusion “Hillary is a good girl or David is happy.”

31. Use resolution to show that the hypotheses “It is not raining or Yvette has her umbrella,” “Yvette does not have her umbrella or she does not get wet,” and “It is raining or Yvette does not get wet” imply that “Yvette does not get wet.”

32. Show that the equivalence \( p \land \neg q \equiv F \) can be derived using resolution together with the fact that a conditional statement with a false hypothesis is true. [Hint: Let \( q = r = F \) in resolution.]

33. Use resolution to show that the compound proposition \( (p \lor q) \land (\neg p \lor q) \land (\neg p \lor \neg q) \) is not satisfiable.

34. The Logic Problem, taken from WFF\’N PROOF: The Game of Logic, has these two assumptions:
   1. “Logic is difficult or not many students like logic.”
   2. “If mathematics is easy, then logic is not difficult.”
   By translating these assumptions into statements involving propositional variables and logical connectives, determine whether each of the following are valid conclusions of these assumptions:
   a) That mathematics is not easy, if many students like logic.
   b) That not many students like logic, if mathematics is not easy.
   c) That mathematics is not easy or logic is difficult.
   d) That logic is not difficult or mathematics is not easy.
   e) That if not many students like logic, then either mathematicians are not easy or logic is not difficult.

35. Determine whether this argument, taken from Kalish and Montague [KaMo64], is valid.
   - If Superman were able and willing to prevent evil, he would do so. If Superman were unable to prevent evil, he would be impotent; if he were unwilling to prevent evil, he would be malevolent. Superman does not prevent evil. If Superman exists, he is neither impotent nor malevolent. Therefore, Superman does not exist.

### 1.7 Introduction to Proofs

**Introduction**

In this section we introduce the notion of a proof and describe methods for constructing proofs. A proof is a valid argument that establishes the truth of a mathematical statement. A proof can use the hypotheses of the theorem, if any, axioms assumed to be true, and previously proven
theorems. Using these ingredients and rules of inference, the final step of the proof establishes the truth of the statement being proved.

In our discussion we move from formal proofs of theorems toward more informal proofs. The arguments we introduced in Section 1.6 to show that statements involving propositions and quantified statements are true were formal proofs, where all steps were supplied, and the rules for each step in the argument were given. However, formal proofs of useful theorems can be extremely long and hard to follow. In practice, the proofs of theorems designed for human consumption are almost always informal proofs, where more than one rule of inference may be used in each step, where steps may be skipped, where the axioms being assumed and the rules of inference used are not explicitly stated. Informal proofs can often explain to humans why theorems are true, while computers are perfectly happy producing formal proofs using automated reasoning systems.

The methods of proof discussed in this chapter are important not only because they are used to prove mathematical theorems, but also for their many applications to computer science. These applications include verifying that computer programs are correct, establishing that operating systems are secure, making inferences in artificial intelligence, showing that system specifications are consistent, and so on. Consequently, understanding the techniques used in proofs is essential both in mathematics and in computer science.

Some Terminology

Formally, a theorem is a statement that can be shown to be true. In mathematical writing, the term theorem is usually reserved for a statement that is considered at least somewhat important. Less important theorems sometimes are called propositions. (Theorems can also be referred to as facts or results.) A theorem may be the universal quantification of a conditional statement with one or more premises and a conclusion. However, it may be some other type of logical statement, as the examples later in this chapter will show. We demonstrate that a theorem is true with a proof. A proof is a valid argument that establishes the truth of a theorem. The statements used in a proof can include axioms (or postulates), which are statements we assume to be true (for example, the axioms for the real numbers, given in Appendix 1, and the axioms of plane geometry), the premises, if any, of the theorem, and previously proven theorems. Axioms may be stated using primitive terms that do not require definition, but all other terms used in theorems and their proofs must be defined. Rules of inference, together with definitions of terms, are used to draw conclusions from other assertions, tying together the steps of a proof. In practice, the final step of a proof is usually just the conclusion of the theorem. However, for clarity, we will often recap the statement of the theorem as the final step of a proof.

A less important theorem that is helpful in the proof of other results is called a lemma (plural lemmas or lemmata). Complicated proofs are usually easier to understand when they are proved using a series of lemmas, where each lemma is proved individually. A corollary is a theorem that can be established directly from a theorem that has been proved. A conjecture is a statement that is being proposed to be a true statement, usually on the basis of some partial evidence, a heuristic argument, or the intuition of an expert. When a proof of a conjecture is found, the conjecture becomes a theorem. Many times conjectures are shown to be false, so they are not theorems.

Understanding How Theorems Are Stated

Before we introduce methods for proving theorems, we need to understand how many mathematical theorems are stated. Many theorems assert that a property holds for all elements in a domain, such as the integers or the real numbers. Although the precise statement of such
theorems needs to include a universal quantifier, the standard convention in mathematics is to omit it. For example, the statement

“If \( x > y \), where \( x \) and \( y \) are positive real numbers, then \( x^2 > y^2 \).”

really means

“For all positive real numbers \( x \) and \( y \), if \( x > y \), then \( x^2 > y^2 \).”

Furthermore, when theorems of this type are proved, the first step of the proof usually involves selecting a general element of the domain. Subsequent steps show that this element has the property in question. Finally, universal generalization implies that the theorem holds for all members of the domain.

Methods of Proving Theorems

Proving mathematical theorems can be difficult. To construct proofs we need all available ammunition, including a powerful battery of different proof methods. These methods provide the overall approach and strategy of proofs. Understanding these methods is a key component of learning how to read and construct mathematical proofs. One we have chosen a proof method, we use axioms, definitions of terms, previously proved results, and rules of inference to complete the proof. Note that in this book we will always assume the axioms for real numbers found in Appendix 1. We will also assume the usual axioms whenever we prove a result about geometry. When you construct your own proofs, be careful not to use anything but these axioms, definitions, and previously proved results as facts!

To prove a theorem of the form \( \forall x (P(x) \rightarrow Q(x)) \), our goal is to show that \( P(c) \rightarrow Q(c) \) is true, where \( c \) is an arbitrary element of the domain, and then apply universal generalization. In this proof, we need to show that a conditional statement is true. Because of this, we now focus on methods that show that conditional statements are true. Recall that \( p \rightarrow q \) is true unless \( p \) is true but \( q \) is false. Note that to prove the statement \( p \rightarrow q \), we need only show that \( q \) is true if \( p \) is true. The following discussion will give the most common techniques for proving conditional statements. Later we will discuss methods for proving other types of statements. In this section, and in Section 1.8, we will develop a large arsenal of proof techniques that can be used to prove a wide variety of theorems.

When you read proofs, you will often find the words “obviously” or “clearly.” These words indicate that steps have been omitted that the author expects the reader to be able to fill in. Unfortunately, this assumption is often not warranted and readers are not at all sure how to fill in the gaps. We will assiduously try to avoid using these words and try not to omit too many steps. However, if we included all steps in proofs, our proofs would often be excruciatingly long.

Direct Proofs

A direct proof of a conditional statement \( p \rightarrow q \) is constructed when the first step is the assumption that \( p \) is true; subsequent steps are constructed using rules of inference, with the final step showing that \( q \) must also be true. A direct proof shows that a conditional statement \( p \rightarrow q \) is true by showing that if \( p \) is true, then \( q \) must also be true, so that the combination \( p \) true and \( q \) false never occurs. In a direct proof, we assume that \( p \) is true and use axioms, definitions, and previously proven theorems, together with rules of inference, to show that \( q \) must also be true. You will find that direct proofs of many results are quite straightforward, with a fairly obvious sequence of steps leading from the hypothesis to the conclusion. However, direct proofs sometimes require particular insights and can be quite tricky. The first direct proofs we present here are quite straightforward; later in the text you will see some that are less obvious.

We will provide examples of several different direct proofs. Before we give the first example, we need to define some terminology.
DEFINITION 1

The integer \( n \) is even if there exists an integer \( k \) such that \( n = 2k \), and \( n \) is odd if there exists an integer \( k \) such that \( n = 2k + 1 \). (Note that every integer is either even or odd, and no integer is both even and odd.) Two integers have the same parity when both are even or both are odd; they have opposite parity when one is even and the other is odd.

EXAMPLE 1

Give a direct proof of the theorem "If \( n \) is an odd integer, then \( n^2 \) is odd."

Solution: Note that this theorem states \( \forall n \left( P(n) \rightarrow Q(n) \right) \), where \( P(n) \) is "\( n \) is an odd integer" and \( Q(n) \) is "\( n^2 \) is odd." As we have said, we will follow the usual convention in mathematical proofs by showing that \( P(n) \) implies \( Q(n) \), and not explicitly using universal instantiation. To begin a direct proof of this theorem, we assume that the hypothesis of this conditional statement is true, namely, we assume that \( n \) is odd. By the definition of an odd integer, it follows that \( n = 2k + 1 \), where \( k \) is some integer. We want to show that \( n^2 \) is also odd. We can square both sides of the equation \( n = 2k + 1 \) to obtain a new equation that expresses \( n^2 \). When we do this, we find that \( n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 \). By the definition of an odd integer, we can conclude that \( n^2 \) is an odd integer (it is one more than twice an integer). Consequently, we have proved that if \( n \) is an odd integer, then \( n^2 \) is an odd integer.

EXAMPLE 2

Give a direct proof that if \( m \) and \( n \) are both perfect squares, then \( mn \) is also a perfect square. (An integer \( a \) is a perfect square if there is an integer \( b \) such that \( a = b^2 \).)

Solution: To produce a direct proof of this theorem, we assume that the hypothesis of this conditional statement is true, namely, we assume that \( m \) and \( n \) are both perfect squares. By the definition of a perfect square, it follows that there are integers \( s \) and \( t \) such that \( m = s^2 \) and \( n = t^2 \). The goal of the proof is to show that \( mn \) must also be a perfect square when \( m \) and \( n \) are; looking ahead we see how we can show this by substituting \( s^2 \) for \( m \) and \( t^2 \) for \( n \) into \( mn \). This tells us that \( mn = s^2t^2 \). Hence, \( mn = s^2t^2 = (st)(st) = (st)(st) = (st)^2 \), using commutativity and associativity of multiplication. By the definition of perfect square, it follows that \( mn \) is also a perfect square, because it is the square of \( st \), which is an integer. We have proved that if \( m \) and \( n \) are both perfect squares, then \( mn \) is also a perfect square.

Proof by Contraposition

Direct proofs lead from the premises of a theorem to the conclusion. They begin with the premises, continue with a sequence of deductions, and end with the conclusion. However, we will see that attempts at direct proofs often reach dead ends. We need other methods of proving theorems of the form \( \forall x \left( P(x) \rightarrow Q(x) \right) \). Proofs of theorems of this type that are not direct proofs, that is, that do not start with the premises and end with the conclusion, are called indirect proofs.

An extremely useful type of indirect proof is known as proof by contraposition. Proofs by contraposition make use of the fact that the conditional statement \( p \rightarrow q \) is equivalent to its contrapositive, \( \neg q \rightarrow \neg p \). This means that the conditional statement \( p \rightarrow q \) can be proved by showing that its contrapositive, \( \neg q \rightarrow \neg p \), is true. In a proof by contraposition of \( p \rightarrow q \), we take \( \neg q \) as a premise, and using axioms, definitions, and previously proven theorems, together with rules of inference, we show that \( \neg p \) must follow. We will illustrate proof by contraposition with two examples. These examples show that proof by contraposition can succeed when we cannot easily find a direct proof.

EXAMPLE 3

Prove that if \( n \) is an integer and \( 3n + 2 \) is odd, then \( n \) is odd.

Solution: We first attempt a direct proof. To construct a direct proof, we first assume that \( 3n + 2 \) is an odd integer. This means that \( 3n + 2 = 2k + 1 \) for some integer \( k \). Can we use this fact
to show that \( n \) is odd? We see that \( 3n + 1 = 2k \), but there does not seem to be any direct way to conclude that \( n \) is odd. Because our attempt at a direct proof failed, we next try a proof by contraposition.

The first step in a proof by contraposition is to assume that the conclusion of the conditional statement "If \( 3n + 2 \) is even, then \( n \) is odd" is false; namely, assume that \( n \) is even. Then, by the definition of an even integer, \( n = 2k \) for some integer \( k \). Substituting \( 2k \) for \( n \), we find that \( 3n + 2 = 3(2k) + 2 = 6k + 2 = (3k + 1) \). This tells us that \( 3n + 2 \) is even (because it is a multiple of 2), and therefore not odd. This is the negation of the premise of the theorem. Because the negation of the conclusion of the conditional statement implies that the hypothesis is false, the original conditional statement is true. Our proof by contraposition succeeded; we have proved the theorem "If \( 3n + 2 \) is odd, then \( n \) is odd."

**EXAMPLE 4**

Prove that if \( n = ab \), where \( a \) and \( b \) are positive integers, then \( a \leq \sqrt{n} \) or \( b \leq \sqrt{n} \).

**Solution:** Because there is no obvious way of showing that \( a \leq \sqrt{n} \) or \( b \leq \sqrt{n} \) directly from the equation \( n = ab \), where \( a \) and \( b \) are positive integers, we attempt a proof by contraposition.

The first step in a proof by contraposition is to assume that the conclusion of the conditional statement "If \( n = ab \), where \( a \) and \( b \) are positive integers, then \( a \leq \sqrt{n} \) or \( b \leq \sqrt{n} \)" is false. That is, we assume that the statement \( (a > \sqrt{n}) \lor (b > \sqrt{n}) \) is false. Using the meaning of disjunction together with De Morgan's law, we see that this implies that both \( a \leq \sqrt{n} \) and \( b \leq \sqrt{n} \) are false. This implies that \( a > \sqrt{n} \) and \( b > \sqrt{n} \). We can multiply these inequalities together (using the fact that if \( 0 < x < 1 \) and \( 0 < u < v \), then \( su < tv \)) to obtain \( ab > \sqrt{n} \cdot \sqrt{n} = n \). This shows that \( ab \neq n \), which contradicts the statement \( n = ab \).

Because the negation of the conclusion of the conditional statement implies that the hypothesis is false, the original conditional statement is true. Our proof by contraposition succeeded; we have proved that if \( n = ab \), where \( a \) and \( b \) are positive integers, then \( a \leq \sqrt{n} \) or \( b \leq \sqrt{n} \).

**VACUOUS AND TRIVIAL PROOFS**

We can quickly prove that a conditional statement \( p \rightarrow q \) is true when we know that \( p \) is false, because \( p \rightarrow q \) must be true when \( p \) is false. Consequently, if we can show that \( p \) is false, then we have a proof, called a vacuous proof, of the conditional statement \( p \rightarrow q \). Vacuous proofs are often used to establish special cases of theorems that state that a conditional statement is true for all positive integers [i.e., a theorem of the kind \( \forall n \, P(n) \), where \( P(n) \) is a propositional function]. Proof techniques for theorems of this kind will be discussed in Section 5.1.

**EXAMPLE 5**

Show that the proposition \( P(0) \) is true, where \( P(n) \) is "If \( n > 1 \), then \( n^2 > n \)" and the domain consists of all integers.

**Solution:** Note that \( P(0) \) is "If \( 0 > 1 \), then \( 0^2 > 0 \)." We can show \( P(0) \) using a vacuous proof. Indeed, the hypothesis \( 0 > 1 \) is false. This tells us that \( P(0) \) is automatically true.

**Remark:** The fact that the conclusion of this conditional statement, \( 0^2 > 0 \), is false is irrelevant to the truth value of the conditional statement, because a conditional statement with a false hypothesis is guaranteed to be true.

We can also quickly prove a conditional statement \( p \rightarrow q \) if we know that the conclusion \( q \) is true. By showing that \( p \) is true, it follows that \( p \rightarrow q \) must also be true. A proof of \( p \rightarrow q \) that uses the fact that \( q \) is true is called a trivial proof. Trivial proofs are often important when special cases of theorems are proved (see the discussion of proof by cases in Section 1.8) and in mathematical induction, which is a proof technique discussed in Section 5.1.
EXAMPLE 6 Let \( P(n) \) be "If \( a \) and \( b \) are positive integers with \( a \geq b \), then \( a^n \geq b^n \)." where the domain consists of all nonnegative integers. Show that \( P(0) \) is true.

**Solution:** The proposition \( P(0) \) is "If \( a \geq b \), then \( a^0 \geq b^0 \)." Because \( a^0 = b^0 = 1 \), the conclusion of the conditional statement "If \( a \geq b \), then \( a^0 \geq b^0 \)" is true. Hence, this conditional statement, which is \( P(0) \), is true. This is an example of a trivial proof. Note that the hypothesis, which is the statement "\( a \geq b \)" was not needed in this proof.

A LITTLE PROOF STRATEGY We have described two important approaches for proving theorems of the form \( \forall x \, (P(x) \rightarrow Q(x)) \): direct proof and proof by contraposition. We have also given examples that show how each is used. However, when you are presented with a theorem of the form \( \forall x \, (P(x) \rightarrow Q(x)) \), which method should you use to attempt to prove it? We will provide a few rules of thumb here; in Section 1.8 we will discuss proof strategy at greater length. When you want to prove a statement of the form \( \forall x \, (P(x) \rightarrow Q(x)) \), first evaluate whether a direct proof looks promising. Begin by expanding the definitions in the hypotheses. Start to reason using these hypotheses, together with axioms and available theorems. If a direct proof does not seem to go anywhere, try the same thing with a proof by contraposition. Recall that in a proof by contraposition you assume that the conclusion of the conditional statement is false and use a direct proof to show this implies that the hypothesis must be false. We illustrate this strategy in Examples 7 and 8. Before we present our next example, we need a definition.

**DEFINITION 2** The real number \( r \) is rational if there exist integers \( p \) and \( q \) with \( q \neq 0 \) such that \( r = p/q \). A real number that is not rational is called irrational.

**EXAMPLE 7** Prove that the sum of two rational numbers is rational. (Note that if we include the implicit quantifiers here, the theorem we want to prove is "For every real number \( r \) and every real number \( s \), if \( r \) and \( s \) are rational numbers, then \( r + s \) is rational."

**Solution:** We first attempt a direct proof. To begin, suppose that \( r \) and \( s \) are rational numbers. From the definition of a rational number, it follows that there are integers \( p \) and \( q \), with \( q \neq 0 \), such that \( r = p/q \), and integers \( t \) and \( u \), with \( u \neq 0 \), such that \( s = t/u \). We can use this information to show that \( r + s \) is rational? The obvious next step is to add \( r = p/q \) and \( s = t/u \), to obtain
\[
\frac{r + s}{q} = \frac{pu + qt}{qu}
\]
Because \( q \neq 0 \) and \( u \neq 0 \), it follows that \( qu \neq 0 \). Consequently, we have expressed \( r + s \) as the ratio of two integers, \( pu + qt \) and \( qu \), where \( qu \neq 0 \). This means that \( r + s \) is rational. We have proved that the sum of two rational numbers is rational; our attempt to find a direct proof succeeded.

**EXAMPLE 8** Prove that if \( n \) is an integer and \( n^2 \) is odd, then \( n \) is odd.

**Solution:** We first attempt a direct proof. Suppose that \( n \) is an integer and \( n^2 \) is odd. Then, there exists an integer \( k \) such that \( n^2 = 2k + 1 \). Can we use this information to show that \( n \) is odd? There seems to be no obvious approach to show that \( n \) is odd because solving for \( n \) produces the equation \( n = \pm \sqrt{2k + 1} \), which is not terribly useful.

Because this attempt to use a direct proof did not bear fruit, we next attempt a proof by contraposition. We take as our hypothesis the statement that \( n \) is not odd. Because every integer is odd or even, this means that \( n \) is even. This implies that there exists an integer \( k \) such that \( n = 2k \). To prove the theorem, we need to show that this hypothesis implies the conclusion that \( n^2 \) is not odd, that is, that \( n^2 \) is even. Can we use the equation \( n = 2k \) to achieve this? By
squaring both sides of this equation, we obtain \( n^2 = 4k^2 = 2(2k^2) \), which implies that \( n^2 \) is also even because \( n^2 = 2t \), where \( t = 2k^2 \). We have proved that if \( n \) is an integer and \( n^2 \) is odd, then \( n \) is odd. Our attempt to find a proof by contraposition succeeded.

**Proofs by Contradiction**

Suppose we want to prove that a statement \( p \) is true. Furthermore, suppose that we can find a contradiction \( q \) such that \( \neg p \rightarrow q \) is true. Because \( q \) is false, but \( \neg p \rightarrow q \) is true, we can conclude that \( \neg p \) is false, which means that \( p \) is true. How can we find a contradiction \( q \) that might help us prove that \( p \) is true in this way?

Because the statement \( r \land \neg r \) is a contradiction whenever \( r \) is a proposition, we can prove that \( p \) is true if we can show that \( \neg p \rightarrow (r \land \neg r) \) is true for some proposition \( r \). Proofs of this type are called **proofs by contradiction**. Because a proof by contradiction does not prove a result directly, it is another type of indirect proof. We provide three examples of proof by contradiction.

**EXAMPLE 9** Show that at least four of any 22 days must fall on the same day of the week.

**Solution:** Let \( p \) be the proposition “At least four of 22 chosen days fall on the same day of the week.” Suppose that \( \neg p \) is true. This means that at most three of the 22 days fall on the same day of the week. Because there are seven days of the week, this implies that at most 21 days could have been chosen, as for each of the days of the week, at most three of the chosen days could fall on that day. This contradicts the premise that we have 22 days under consideration. That is, if \( r \) is the statement that 22 days are chosen, then we have shown that \( \neg p \rightarrow (r \land \neg r) \). Consequently, we know that \( p \) is true. We have proved that at least four of 22 chosen days fall on the same day of the week.

**EXAMPLE 10** Prove that \( \sqrt{2} \) is irrational by giving a proof by contradiction.

**Solution:** Let \( p \) be the proposition “\( \sqrt{2} \) is irrational.” To start a proof by contradiction, we suppose that \( \neg p \) is true. Note that \( \neg p \) is the statement “It is not the case that \( \sqrt{2} \) is rational,” which says that \( \sqrt{2} \) is rational. We will show that assuming that \( \neg p \) is true leads to a contradiction.

If \( \sqrt{2} \) is rational, there exist integers \( a \) and \( b \) with \( \sqrt{2} = a/b \), where \( b \neq 0 \) and \( a \) and \( b \) have no common factors (so that the fraction \( a/b \) is in lowest terms.) (Here, we are using the fact that every rational number can be written in lowest terms.) Because \( \sqrt{2} = a/b \), when both sides of this equation are squared, it follows that

\[
2 = \frac{a^2}{b^2}
\]

Hence,

\[
2b^2 = a^2.
\]

By the definition of an even integer it follows that \( a^2 \) is even. We next use the fact that if \( a^2 \) is even, \( a \) must also be even, which follows by Exercise 16. Furthermore, because \( a \) is even, by the definition of an even integer, \( a = 2c \) for some integer \( c \). Thus,

\[
2b^2 = 4c^2.
\]

Dividing both sides of this equation by 2 gives

\[
b^2 = 2c^2.
\]

By the definition of even, this means that \( b^2 \) is even. Again using the fact that if the square of an integer is even, then the integer itself must be even, we conclude that \( b \) must be even as well.
EXAMPLE 12

Prove the theorem "If $3n + 2$ is odd, then $n$ is odd."

Solution: Let $p$ be "$3n + 2$ is odd" and $q$ be "$n$ is odd." To construct a proof by contradiction, assume that both $p$ and $\neg q$ are true. That is, assume that $3n + 2$ is odd and that $n$ is odd. Because $n$ is not odd, we know that it is even. Because $n$ is even, there is an integer $k$ such that $n = 2k$. This implies that $3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$. Because $3n + 2$ is $2\cdot$, where $t = 3k + 1$, $3n + 2$ is even. Note that the statement "$3n + 2$ is even" is equivalent to the statement $\neg p$, because an integer is even if and only if it is not odd. Because both $p$ and $\neg p$ are true, we have a contradiction. This completes the proof by contradiction, proving that $3n + 2$ is odd, then $n$ is odd.

Note that we can also prove by contradiction that $p \rightarrow q$ is true by assuming that $p$ and $\neg q$ are true, and showing that $q$ must be also be true. This implies that $\neg q$ and $q$ are both true, a contradiction. This observation tells us that we can turn a direct proof into a proof by contradiction.

PROOFS OF EQUIVALENCE

To prove a theorem that is a biconditional statement, that is, a statement of the form $p \leftrightarrow q$, we show that $p \rightarrow q$ and $q \rightarrow p$ are both true. The validity of this approach is based on the tautology

$$(p \leftrightarrow q) \leftrightarrow ((p \rightarrow q) \land (q \rightarrow p)).$$

EXAMPLE 12

Prove the theorem "If $n$ is an integer, then $n$ is odd if and only if $n^2$ is odd."

Solution: This theorem has the form "$p$ if and only if $q$," where $p$ is "$n$ is odd" and $q$ is "$n^2$ is odd." (As usual, we do not explicitly deal with the universal quantification.) To prove this theorem, we need to show that $p \rightarrow q$ and $q \rightarrow p$ are true.

We have already shown (in Example 1) that $p \rightarrow q$ is true and (in Example 8) that $q \rightarrow p$ is true.

Because we have shown that both $p \rightarrow q$ and $q \rightarrow p$ are true, we have shown that the theorem is true.
Sometimes a theorem states that several propositions are equivalent. Such a theorem states that propositions \( p_1, p_2, p_3, \ldots, p_n \) are equivalent. This can be written as

\[ p_1 \leftrightarrow p_2 \leftrightarrow \cdots \leftrightarrow p_n, \]

which states that all \( n \) propositions have the same truth values, and consequently, that for all \( i \) and \( j \) with \( 1 \leq i \leq n \) and \( 1 \leq j \leq n \), \( p_i \) and \( p_j \) are equivalent. One way to prove these mutually equivalent is to use the tautology

\[ p_1 \leftrightarrow p_2 \leftrightarrow \cdots \leftrightarrow p_n \leftrightarrow (p_1 \rightarrow p_2) \land (p_2 \rightarrow p_3) \land \cdots \land (p_n \rightarrow p_1). \]

This shows that if the \( n \) conditional statements \( p_1 \rightarrow p_2, p_2 \rightarrow p_3, \ldots, p_n \rightarrow p_1 \) can be shown to be true, then the propositions \( p_1, p_2, \ldots, p_n \) are all equivalent.

This is much more efficient than proving that \( p_i \rightarrow p_j \) for all \( i \neq j \) with \( 1 \leq i \leq n \) and \( 1 \leq j \leq n \). (Note that there are \( n^2 - n \) such conditional statements.)

When we prove that a group of statements are equivalent, we can establish any chain of conditional statements we choose as long as it is possible to work through the chain to go from any one of these statements to any other statement. For example, we can show that \( p_1, p_2, \) and \( p_3 \) are equivalent by showing that \( p_1 \rightarrow p_2, p_2 \rightarrow p_3, \) and \( p_3 \rightarrow p_1 \).

**Example 13**

Show that these statements about the integer \( n \) are equivalent:

\[
\begin{align*}
p_1 & : n \text{ is even.} \\
p_2 & : n - 1 \text{ is odd.} \\
p_3 & : n^2 \text{ is even.}
\end{align*}
\]

**Solution:** We will show that these three statements are equivalent by showing that the conditional statements \( p_1 \rightarrow p_2, p_2 \rightarrow p_3, \) and \( p_3 \rightarrow p_1 \) are true.

We use a direct proof to show that \( p_1 \rightarrow p_2 \). Suppose that \( n \) is even. Then \( n = 2k \) for some integer \( k \). Consequently, \( n - 1 = 2k - 1 = 2(k - 1) + 1 \). This means that \( n - 1 \) is odd because it is of the form \( 2m + 1 \), where \( m \) is the integer \( k - 1 \).

We also use a direct proof to show that \( p_2 \rightarrow p_3 \). Now suppose \( n - 1 \) is odd. Then \( n - 1 = 2k + 1 \) for some integer \( k \). Hence, \( n = 2k + 2 \) so that \( n^2 = (2k + 2)^2 = 4k^2 + 8k + 4 = 2(2k^2 + 4k + 2) \). This means that \( n^2 \) is twice the integer \( 2k^2 + 4k + 2 \), and hence is even.

To prove \( p_3 \rightarrow p_1 \), we use a proof by contraposition. That is, we prove that if \( n \) is not even, then \( n^2 \) is not even. This is the same as proving that if \( n \) is odd, then \( n^2 \) is odd, which we have already done in Example 1. This completes the proof.

**Counterexamples**

In Section 1.4 we stated that to show that a statement of the form \( \forall x P(x) \) is false, we need only find a counterexample, that is, an example \( x \) for which \( P(x) \) is false. When presented with a statement of the form \( \forall x P(x) \), which we believe to be false or which has resisted all proof attempts, we look for a counterexample. We illustrate the use of counterexamples in Example 14.

**Example 14**

Show that the statement “Every positive integer is the sum of the squares of two integers” is false.

**Solution:** To show that this statement is false, we look for a counterexample, which is a particular integer that is not the sum of the squares of two integers. It does not take long to find a counterexample, because 3 cannot be written as the sum of the squares of two integers. To show this is the case, note that the only perfect squares not exceeding 3 are \( 0^2 = 0 \) and \( 1^2 = 1 \). Furthermore, there is no way to get 3 as the sum of two terms each of which is 0 or 1. Consequently, we have shown that “Every positive integer is the sum of the squares of two integers” is false.
Mistakes in Proofs

There are many common errors made in constructing mathematical proofs. We will briefly describe some of these here. Among the most common errors are mistakes in arithmetic and basic algebra. Even professional mathematicians make such errors, especially when working with complicated formulae. Whenever you use such computations you should check them as carefully as possible. (You should also review any troublesome aspects of basic algebra, especially before you study Section 5.1.)

Each step of a mathematical proof needs to be correct and the conclusion needs to follow logically from the steps that precede it. Many mistakes result from the introduction of steps that do not logically follow from those that precede it. This is illustrated in Examples 15–17.

EXAMPLE 15

What is wrong with this famous supposed “proof” that 1 = 2?

"Proof:" We use these steps, where a and b are two equal positive integers.

<table>
<thead>
<tr>
<th>Step</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. a = b</td>
<td>Given</td>
</tr>
<tr>
<td>2. a² = ab</td>
<td>Multiply both sides of (1) by a</td>
</tr>
<tr>
<td>3. a² – b² = ab – b²</td>
<td>Subtract b² from both sides of (2)</td>
</tr>
<tr>
<td>4. (a – b)(a + b) = b(a – b)</td>
<td>Factor both sides of (3)</td>
</tr>
<tr>
<td>5. a + b = b</td>
<td>Divide both sides of (4) by a – b</td>
</tr>
<tr>
<td>6. 2b = b</td>
<td>Replace a by b in (5) because a = b and simplify</td>
</tr>
<tr>
<td>7. 2 = 1</td>
<td>Divide both sides of (6) by b</td>
</tr>
</tbody>
</table>

Solution: Every step is valid except for one, step 5 where we divided both sides by a – b. The error is that a – b equals zero; division of both sides of an equation by the same quantity is valid as long as this quantity is not zero.

EXAMPLE 16

What is wrong with this "proof?"

"Theorem:" If n² is positive, then n is positive.

"Proof:" Suppose that n² is positive. Because the conditional statement “If n is positive, then n² is positive” is true, we can conclude that n is positive.

Solution: Let P(n) be “n is positive” and Q(n) be “n² is positive.” Then our hypothesis is Q(n). The statement “If n is positive, then n² is positive” is the statement ∀n(P(n) → Q(n)). From the hypothesis Q(n) and the statement ∀n(P(n) → Q(n)) we cannot conclude P(n), because we are not using a valid rule of inference. Instead, this is an example of the fallacy of affirming the conclusion. A counterexample is supplied by n = −1 for which n² = 1 is positive, but n is negative.

EXAMPLE 17

What is wrong with this “proof?”

"Theorem:" If n is not positive, then n² is not positive. (This is the contrapositive of the "theorem" in Example 16.)
“Proof.” Suppose that \( n \) is not positive. Because the conditional statement “If \( n \) is positive, then \( n^2 \) is positive” is true, we can conclude that \( n^2 \) is not positive.

**Solution:** Let \( P(n) \) and \( Q(n) \) be as in the solution of Example 16. Then our hypothesis is \( \neg P(n) \) and the statement “If \( n \) is positive, then \( n^2 \) is positive” is the statement \( \forall n (P(n) \rightarrow Q(n)) \), because we are not using a valid rule of inference. Instead, this is an example of the fallacy of denying the hypothesis. A counterexample is supplied by \( n = -1 \), as in Example 16.

Finally, we briefly discuss a particularly nasty type of error. Many incorrect arguments are based on a fallacy called **begging the question**. This fallacy occurs when one or more steps of a proof are based on the truth of the statement being proved. In other words, this fallacy arises when a statement is proved using itself, or a statement equivalent to it. That is why this fallacy is also called **circular reasoning**.

**EXAMPLE 18**

Is the following argument correct? It supposedly shows that \( n \) is an even integer whenever \( n^2 \) is an even integer.

Suppose that \( n^2 \) is even. Then \( n^2 = 2k \) for some integer \( k \). Let \( n = 2l \) for some integer \( l \). This shows that \( n \) is even.

**Solution:** This argument is incorrect. The statement “let \( n = 2l \) for some integer \( l \)” occurs in the proof. No argument has been given to show that \( n \) can be written as \( 2l \) for some integer \( l \). This is circular reasoning because this statement is equivalent to the statement being proved, namely, “\( n \) is even.” Of course, the result itself is correct; only the method of proof is wrong.

Making mistakes in proofs is part of the learning process. When you make a mistake that someone else finds, you should carefully analyze where you went wrong and make sure that you do not make the same mistake again. Even professional mathematicians make mistakes in proofs. More than a few incorrect proofs of important results have fooled people for many years before subtle errors in them were found.

**Just a Beginning**

We have now developed a basic arsenal of proof methods. In the next section we will introduce other important proof methods. We will also introduce several important proof techniques in Chapter 5, including mathematical induction, which can be used to prove results that hold for all positive integers. In Chapter 6 we will introduce the notion of combinatorial proofs.

In this section we introduced several methods for proving theorems of the form \( \forall x (P(x) \rightarrow Q(x)) \), including direct proofs and proofs by contraposition. There are many theorems of this type whose proofs are easy to construct by directly working through the hypotheses and definitions of the terms of the theorem. However, it is often difficult to prove a theorem without resorting to a clever use of a proof by contraposition or a proof by contradiction, or some other proof technique. In Section 1.8 we will address proof strategy. We will describe various approaches that can be used to find proofs when straightforward approaches do not work. Constructing proofs is an art that can be learned only through experience, including writing proofs, having your proofs critiqued, and reading and analyzing other proofs.
Exercises

1. Use a direct proof to show that the sum of two odd integers is even.
2. Use a direct proof to show that the sum of two even integers is even.
3. Show that the square of an even number is an even number using a direct proof.
4. Show that the square of an odd number is an odd number.
5. Prove that if \( m + n \) and \( n + p \) are even integers, where \( m, n, \) and \( p \) are integers, then \( m + p \) is even. What kind of proof did you use?
6. Use a direct proof to show that the product of two odd numbers is odd.
7. Use a direct proof to show that every odd integer is the difference of two squares.
8. Prove that if \( n \) is a perfect square, then \( n + 2 \) is not a perfect square.
9. Use the direct proof to prove that the product of an irrational number and a rational number is irrational.
10. Use a direct proof to prove that the product of two rational numbers is rational.
11. Prove or disprove that the product of two irrational numbers is irrational.
12. Prove or disprove that the product of two rational numbers and an irrational number is irrational.
13. Prove that if \( x \) is irrational, then \( 1/x \) is irrational.
14. Prove that if \( x \) is rational and \( x \neq 0 \), then \( 1/x \) is rational.
15. Use a proof by contradiction to prove that if \( x + y \geq 2 \), where \( x \) and \( y \) are real numbers, then \( x \geq 1 \) or \( y \geq 1 \).
16. Prove that if \( m \) and \( n \) are integers and \( mn = 1 \), then \( m \) is even or \( n \) is even.
17. Show that if \( x \) is an integer and \( x^3 + 5 \) is odd, then \( n \) is even using
   a) a proof by contradiction.
   b) a proof by direct proof.
18. Prove that if \( n \) is an integer and \( 3n + 2 \) is even, then \( n \) is even using
   a) a proof by contradiction.
   b) a proof by contradiction.
19. Prove the proposition \( P(0) \), where \( P(n) \) is the proposition “If \( n \) is a positive integer greater than 1, then \( n^2 > n^2 \).” What kind of proof did you use?
20. Prove the proposition \( P(1) \), where \( P(n) \) is the proposition “If \( n \) is a positive integer, then \( n^2 \geq n^2 \).” What kind of proof did you use?
21. Let \( P(n) \) be the proposition “If \( a \) and \( b \) are positive real numbers, then \( (a + b) \geq a^n + b^n \).” Prove that \( P(1) \) is true. What kind of proof did you use?
22. Show that if you pick three socks from a drawer containing just blue socks and black socks, you must get either a pair of blue socks or a pair of black socks.
23. Show that at least ten of any 64 days chosen must fall on the same day of the week.
24. Show that at least three of any 25 days chosen must fall in the same month of the year.
25. Use a proof by contradiction to prove that there is no rational number \( x \) for which \( r^2 + r + 1 = 0 \). [Hint: Assume that \( r = a/b \) is a root, where \( a \) and \( b \) are integers and \( a/b \) is in lowest terms. Obtain an equation involving integers by multiplying by \( b^3 \). Then look at whether \( a \) and \( b \) are each odd or even.]
38. Find a counterexample to the statement that every positive integer can be written as the sum of the squares of three integers.

39. Prove that at least one of the real numbers \(a_1, a_2, \ldots, a_n\) is greater than or equal to the average of these numbers. What kind of proof did you use?

40. Use Exercise 39 to show that if the first 10 positive integers are placed around a circle, in any order, there exist three integers in consecutive locations around the circle that have a sum greater than or equal to 17.

41. Prove that if \(n\) is an integer, these four statements are equivalent: (i) \(n\) is even, (ii) \(n + 1\) is odd, (iii) \(3n + 1\) is odd, (iv) \(3n\) is even.

42. Prove that these four statements about the integer \(n\) are equivalent: (i) \(n^2\) is odd, (ii) \(1 - n^3\) is even, (iii) \(n^2\) is odd, (iv) \(n^2 + 1\) is even.

1.8 Proof Methods and Strategy

Introduction

In Section 1.7 we introduced many methods of proof and illustrated how each method can be used. In this section we continue this effort. We will introduce several other commonly used proof methods, including the method of proving a theorem by considering different cases separately. We will also discuss proofs where we prove the existence of objects with desired properties.

In Section 1.7 we briefly discussed the strategy behind constructing proofs. This strategy includes selecting a proof method and then successfully constructing an argument step by step, based on this method. In this section, after we have developed a versatile arsenal of proof methods, we will study some aspects of the art and science of proofs. We will provide advice on how to find a proof of a theorem. We will describe some tricks of the trade, including how proofs can be found by working backward and by adapting existing proofs.

When mathematicians work, they formulate conjectures and attempt to prove or disprove them. We will briefly describe this process here by proving results about tiling checkerboards with dominoes and other types of pieces. Looking at tilings of this kind, we will be able to quickly formulate conjectures and prove theorems without first developing a theory.

We will conclude the section by discussing the role of open questions. In particular, we will discuss some interesting problems either that have been solved after remaining open for hundreds of years or that still remain open.

Exhaustive Proof and Proof by Cases

Sometimes we cannot prove a theorem using a single argument that holds for all possible cases. We now introduce a method that can be used to prove a theorem, by considering different cases separately. This method is based on a rule of inference that we will now introduce. To prove a conditional statement of the form

\[(p_1 \lor p_2 \lor \cdots \lor p_n) \rightarrow q\]

the tautology

\[\left[ (p_1 \lor p_2 \lor \cdots \lor p_n) \rightarrow q \right] \leftrightarrow \left[ (p_1 \rightarrow q) \land (p_2 \rightarrow q) \land \cdots \land (p_n \rightarrow q) \right]\]

can be used as a rule of inference. This shows that the original conditional statement with a hypothesis made up of a disjunction of the propositions \(p_1, p_2, \ldots, p_n\) can be proved by proving each of the \(n\) conditional statements \(p_i \rightarrow q\), \(i = 1, 2, \ldots, n\), individually. Such an argument is called a proof by cases. Sometimes to prove that a conditional statement \(p \rightarrow q\) is true, it is convenient to use a disjunction \(p_1 \lor p_2 \lor \cdots \lor p_n\) instead of \(p\) as the hypothesis of the conditional statement, where \(p\) and \(p_1 \lor p_2 \lor \cdots \lor p_n\) are equivalent.
EXHAUSTIVE PROOF  Some theorems can be proved by examining a relatively small number of examples. Such proofs are called exhaustive proofs, or proofs by exhaustion, because these proofs proceed by exhausting all possibilities. An exhaustive proof is a special type of proof by cases where each case involves checking a single example. We now provide some illustrations of exhaustive proofs.

EXAMPLE 1  Prove that \((n+1)^3 \geq 3^6\) if \(n\) is a positive integer with \(n \leq 4\).

Solution: We use a proof by exhaustion. We only need verify the inequality \((n+1)^3 \geq 3^6\) when \(n = 1, 2, 3,\) and 4. For \(n = 1\), we have \((n+1)^3 = 2^3 = 8\) and \(3^6 = 3^3 = 27\); for \(n = 2\), we have \((n+1)^3 = 3^3 = 27\) and \(3^6 = 3^3 = 27\); for \(n = 3\), we have \((n+1)^3 = 4^3 = 64\) and \(3^6 = 3^3 = 27\); and for \(n = 4\), we have \((n+1)^3 = 5^3 = 125\) and \(3^6 = 3^3 = 27\). In each of these four cases, we see that \((n+1)^3 \geq 3^6\). We have used the method of exhaustion to prove that \((n+1)^3 \geq 3^6\) if \(n\) is a positive integer with \(n \leq 4\).

EXAMPLE 2  Prove that the only consecutive positive integers not exceeding 100 that are perfect powers are 8 and 9. (An integer is a perfect power if it equals \(a^n\), where \(a\) is an integer greater than 1.)

Solution: We use a proof by exhaustion. In particular, we can prove this fact by examining perfect integers \(n\) not exceeding 100, first checking whether \(n\) is a perfect power, and if it is, checking whether \(n + 1\) is also a perfect power. A quick way to do this is simply to look at all perfect powers not exceeding 100 and checking whether the next largest integer is also a perfect power. The squares of positive integers not exceeding 100 are 1, 4, 9, 16, 25, 36, 49, 64, 81, and 100. The cubes of positive integers not exceeding 100 are 1, 8, 27, and 64. The fourth powers of positive integers not exceeding 100 are 1, 16, and 81. The fifth powers of positive integers not exceeding 100 are 1 and 32. The sixth powers of positive integers not exceeding 100 are 1 and 64. There are no powers of perfect integers greater than the sixth power not exceeding 100, other than 1. Looking at this list of perfect powers not exceeding 100, we see that \(n = 8\) is the only perfect power \(n\) for which \(n + 1\) is also a perfect power. That is, \(3^3 = 8\) and \(3^2 = 9\) are the only two consecutive perfect powers not exceeding 100.

People can carry out exhaustive proofs when it is necessary to check only a relatively small number of instances of a statement. Computers do not complain when they are asked to check a much larger number of instances of a statement, but they still have limitations. Note that not even a computer can check all instances when it is impossible to list all instances to check.

PROOF BY CASES  A proof by cases must cover all possible cases that arise in a theorem. We illustrate proof by cases with a couple of examples. In each example, you should check that all possible cases are covered.

EXAMPLE 3  Prove that if \(n\) is an integer, then \(n^2 \geq n\).

Solution: We can prove that \(n^2 \geq n\) for every integer by considering three cases, when \(n = 0\), when \(n \geq 1\), and when \(n \leq -1\). We split the proof into three cases because it is straightforward to prove the result by considering zero, positive integers, and negative integers separately.

Case (i): When \(n = 0\), because \(0^2 = 0\), we see that \(0^2 \geq 0\). It follows that \(n^2 \geq n\) is true in this case.

Case (ii): When \(n \geq 1\), when we multiply both sides of the inequality \(n \geq 1\) by the positive integer \(n\), we obtain \(n \cdot n \geq n \cdot 1\). This implies that \(n^2 \geq n\) for \(n \geq 1\).

Case (iii): In this case \(n \leq -1\). However, \(n^2 \geq 0\). It follows that \(n^2 \geq n\).

Because the inequality \(n^2 \geq n\) holds in all three cases, we can conclude that if \(n\) is an integer, then \(n^2 \geq n\).
EXAMPLE 4

Use a proof by cases to show that $|xy| = |x||y|$, where $x$ and $y$ are real numbers. (Recall that $|a|$, the absolute value of $a$, equals $a$ when $a \geq 0$ and equals $-a$ when $a \leq 0$.)

Solution: In our proof of this theorem, we remove absolute values using the fact that $|a| = a$ when $a \geq 0$ and $|a| = -a$ when $a < 0$. Because both $|x|$ and $|y|$ occur in our formula, we will need four cases: (i) $x$ and $y$ both nonnegative; (ii) $x$ nonnegative and $y$ is negative; (iii) $x$ negative and $y$ nonnegative; and (iv) $x$ negative and $y$ negative. We denote by $p_1$, $p_2$, $p_3$, and $p_4$ the proposition stating the assumption for each of these four cases, respectively.

(Note that we can remove the absolute value signs by making the appropriate choice of signs within each case.)

Case (i): We see that $p_1 \rightarrow q$ because $xy \geq 0$ when $x \geq 0$ and $y \geq 0$, so that $|xy| = xy = |x||y|$.  

Case (ii): To see that $p_2 \rightarrow q$, note that if $x \geq 0$ and $y < 0$, then $xy \leq 0$, so that $|xy| = -xy = x(-y) = |x||y|$. (Here, because $y < 0$, we have $|y| = -y$.)

Case (iii): To see that $p_3 \rightarrow q$, we follow the same reasoning as the previous case with the roles of $x$ and $y$ reversed.

Case (iv): To see that $p_4 \rightarrow q$, note that when $x < 0$ and $y < 0$, it follows that $xy > 0$. Hence, $|xy| = xy = (-x)(-y) = |x||y|$. Because $|xy| = |x||y|$ holds in each of the four cases and these cases exhaust all possibilities, we can conclude that $|xy| = |x||y|$, whenever $x$ and $y$ are real numbers.

LEVERAGING PROOF BY CASES

The examples we have presented illustrating proof by cases provide some insight into when to use this method of proof. In particular, when it is not possible to reduce our proof to the consideration of six cases.

EXAMPLE 5

Formulate a conjecture about the final decimal digit of the square of an integer and prove your result.

Solution: The smallest perfect squares are $1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, 169, 196, 225$, and so on. We notice that the digits that occur as the final digit of a square are $0, 1, 4, 5, 6$, and $9$, with $2, 3, 7$, and $8$ never appearing as the final digit of a square. We conjecture this theorem: The final decimal digit of a perfect square is $0, 1, 4, 5, 6$, or $9$. How can we prove this theorem?

We first note that we can express an integer $n$ as $10a + b$, where $a$ and $b$ are positive integers and $b$ is $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$. Here $a$ is the integer obtained by subtracting the final decimal digit of $n$ from $n$ and dividing by 10. Next, note that $(10a + b)^2 = 100a^2 + 20ab + b^2 = 10(10a^2 + 2b) + b^2$, so that the final decimal digit of $n^2$ is the same as the final decimal digit of $b^2$. Furthermore, note that the final decimal digit of $b^2$ is the same as the final decimal digit of $(10 - b)^2 = 100 - 20b + b^2$. Consequently, we can reduce our proof to the consideration of six cases.

Case (i): The final digit of $n$ is $1$ or $9$. Then the final decimal digit of $n^2$ is the final decimal digit of $1^2 = 1$ or $9^2 = 81$, namely $1$.

Case (ii): The final digit of $n$ is $2$ or $8$. Then the final decimal digit of $n^2$ is the final decimal digit of $2^2 = 4$ or $8^2 = 64$, namely $4$.

Case (iii): The final digit of $n$ is $3$ or $7$. Then the final decimal digit of $n^2$ is the final decimal digit of $3^2 = 9$ or $7^2 = 49$, namely $9$.

Case (iv): The final digit of $n$ is $4$ or $6$. Then the final decimal digit of $n^2$ is the final decimal digit of $4^2 = 16$ or $6^2 = 36$, namely $6$.

Case (v): The final decimal digit of $n$ is $5$. Then the final decimal digit of $n^2$ is the final decimal digit of $5^2 = 25$, namely $5$.
EXAMPLE 6
Show that there are no solutions in integers $x$ and $y$ of $x^2 + 3y^2 = 8$.

**Solution:** We can quickly reduce a proof to checking just a few simple cases because $x^2 > 8$ when $|x| \geq 3$ and $3y^2 > 8$ when $|y| \geq 2$. This leaves the cases when $x$ equals $-2$, $-1$, $0$, $1$, $2$ and $y$ equals $-1$, $0$, $1$, $2$. We can finish using an exhaustive proof. To dispense with the remaining cases, we note that possible values for $x^2$ are $0$, $1$, and $4$, and possible values for $3y^2$ are $0$ and $3$, and the largest sum of possible values for $x^2 + 3y^2$ is $7$. Consequently, it is impossible for $x^2 + 3y^2 = 8$ to hold when $x$ and $y$ are integers.

**WITHOUT LOSS OF GENERALITY** In the proof in Example 4, we dismissed case (iii), where $x < 0$ and $y \geq 0$, because it is the same as case (ii), where $x \geq 0$ and $y < 0$, with the roles of $x$ and $y$ reversed. To shorten the proof, we could have proved cases (ii) and (iii) together by assuming, without loss of generality, that $x \geq 0$ and $y < 0$. Implicit in this statement is that we can complete the case with $x < 0$ and $y \geq 0$ using the same argument as we used for the case with $x \geq 0$ and $y < 0$, but with the obvious changes.

In general, when the phrase ‘without loss of generality’ is used in a proof (often abbreviated as WLOG), we assert that by proving one case of a theorem, no additional argument is required to prove other specified cases. That is, other cases follow by making straightforward changes to the argument, or by filling in some straightforward initial step. Proofs by cases can often be made much more efficient when the notion of without loss of generality is employed. Of course, incorrect use of this principle can lead to unfortunate errors. Sometimes assumptions are made that lead to a loss in generality. Such assumptions can be made that do not take into account that one case may be substantially different from others. This can lead to an incomplete, and possibly unavailing, proof. In fact, many incorrect proofs of famous theorems turned out to rely on arguments that used the idea of “without loss of generality” to establish cases that could not be quickly proved from simpler cases.

We now illustrate a proof where without loss of generality is used effecttively together with other proof techniques.

EXAMPLE 7
Show that if $x$ and $y$ are integers and both $xy$ and $x+y$ are even, then both $x$ and $y$ are even.

**Solution:** We will use proof by contraposition, the notion of without loss of generality, and proof by cases. First, suppose that $x$ and $y$ are not both even. That is, assume that $x$ is odd or that $y$ is odd (or both). Without loss of generality, we assume that $x$ is odd, so that $x = 2m + 1$ for some integer $k$.

To complete the proof, we need to show that $xy$ is odd or $x+y$ is odd. Consider two cases: (i) $y$ even, and (ii) $y$ odd. In (i), $y = 2n$ for some integer $n$, so that $x+y = (2m+1) + 2n = 2(m+n) + 1$ is odd. In (ii), $y = 2n+1$ for some integer $n$, so that $xy = (2m+1)(2n+1) = 4mn + 2m + 2n + 1 = 2(2mn + m + n) + 1$ is odd. This completes the proof by contraposition. (Note that our use of without loss of generality within the proof is justified because the proof when $y$ is odd can be obtained by simply interchanging the roles of $x$ and $y$ in the proof we have given.)

**COMMON ERRORS WITH EXHAUSTIVE PROOF AND PROOF BY CASES** A common error of reasoning is to draw incorrect conclusions from examples. No matter how many separate examples are considered, a theorem is not proved by considering examples unless every possible...
case is covered. The problem of proving a theorem is analogous to showing that a computer
program always produces the output desired. No matter how many input values are tested, unless
all input values are tested, we cannot conclude that the program always produces the correct
output.

**EXAMPLE 8**
Is it true that every positive integer is the sum of 18 fourth powers of integers?

**Solution:** To determine whether a positive integer \( n \) can be written as the sum of 18 fourth powers of integers, we might begin by examining whether \( n \) is the sum of 18 fourth powers of the smallest positive integers. Because the fourth powers of integers are 0, 1, 16, 81, ..., if we can select 18 terms from these numbers that add up to \( n \), then \( n \) is the sum of 18 fourth powers. We can show that all positive integers up to 78 can be written as the sum of 18 fourth powers. (The details are left to the reader.) However, if we decided this was enough checking, we would come to the wrong conclusion. It is not true that every positive integer is the sum of 18 fourth powers because 79 is not the sum of 18 fourth powers (as the reader can verify). ▲

Another common error involves making unwarranted assumptions that lead to incorrect
proofs by cases where not all cases are considered. This is illustrated in Example 9.

**EXAMPLE 9**
What is wrong with this “proof”?

“Theorem:” If \( x \) is a real number, then \( x^2 \) is a positive real number.

“Proof:” Let \( p_1 \) be “\( x \) is positive,” let \( p_2 \) be “\( x \) is negative,” and let \( q \) be “\( x^2 \) is positive.” To show that \( p_1 \rightarrow q \) is true, note that when \( x \) is positive, \( x^2 \) is positive because it is the product of two positive numbers, \( x \) and \( x \). To show that \( p_2 \rightarrow q \), note that when \( x \) is negative, \( x^2 \) is positive because it is the product of two negative numbers, \( x \) and \( x \). This completes the proof.

**Solution:** The problem with this “proof” is that we missed the case of \( x = 0 \). When \( x = 0 \), \( x^2 = 0 \) is not positive, so the supposed theorem is false. If \( p \) is “\( x \) is a real number,” then we can prove results where \( p \) is the hypothesis with three cases, \( p_1 \), \( p_2 \), and \( p_3 \), where \( p_1 \) is “\( x \) is positive,” \( p_2 \) is “\( x \) is negative,” and \( p_3 \) is “\( x = 0 \)” because of the equivalence \( p \leftrightarrow p_1 \lor p_2 \lor p_3 \). ▲

**Existence Proofs**
Many theorems are assertions that objects of a particular type exist. A theorem of this type is a
proposition of the form \( \exists x \, P(x) \), where \( P \) is a predicate. A proof of a proposition of the form \( \exists x \, P(x) \) is called an existence proof. There are several ways to prove a theorem of this type. Sometimes an existence proof of \( \exists x \, P(x) \) can be given by finding an element \( a \), called a witness, such that \( P(a) \) is true. This type of existence proof is called constructive. It is also possible to give an existence proof that is nonconstructive; that is, we do not find an element \( a \) such that \( P(a) \) is true, but rather prove that \( \exists x \, P(x) \) is true in some other way. One common method of giving a nonconstructive existence proof is to use proof by contradiction and show that the negation of the existential quantification implies a contradiction. The concept of a constructive existence proof is illustrated by Example 10 and the concept of a nonconstructive existence proof is illustrated by Example 11.

**EXAMPLE 10**
A Constructive Existence Proof  Show that there is a positive integer that can be written as the sum of cubes of positive integers in two different ways.

**Solution:** After considerable computation (such as a computer search) we find that
\[
1729 = 10^3 + 9^3 = 12^3 + 1^3.
\]
By Example 10 in Section 1.7 we know that \( \sqrt{2} \) and \( \sqrt{2} \) are irrational numbers.

Show that there exist irrational numbers \( x \) and \( y \) such that

\[
\sqrt{2} = y \quad \text{and} \quad 2 = x\sqrt{2}.
\]

This is an example of a nonconstructive existence proof because we have not found irrational numbers \( x \) and \( y \) such that \( x^2 \) is rational. Rather, we have shown that either the pair \( x = \sqrt{2} \) or the pair \( x = \sqrt{2} \cdot \sqrt{2} \) have the desired property, but we do not know which of these two pairs works!

EXAMPLE 11

A Nonconstructive Existence Proof

Show that there exist irrational numbers \( x \) and \( y \) such that \( x^2 = 2 \). If it is rational, we have two irrational numbers \( x \) and \( y \) with \( x^2 \) rational, namely, \( x = \sqrt{2} \) and \( y = \sqrt{2} \). On the other hand if \( \sqrt{2} \) is irrational, then we can let \( x = \sqrt{2} \) and \( y = \sqrt{2} \) so that \( x^2 = y \sqrt{2} \). Consider the number \( \sqrt{2} \), \( y \) or the pair \( x = \sqrt{2} \) and \( y = \sqrt{2} \) have the desired property, but we do not know which of these two pairs works!

Because we have displayed a positive integer that can be written as the sum of cubes in two different ways, we are done.

There is an interesting story pertaining to this example. The English mathematician G. H. Hardy, when visiting the ailing Indian prodigy Ramanujan in the hospital, remarked that 1729, the number of the cab he took, was rather dull. Ramanujan replied “No, it is a very interesting number; it is the smallest number expressible as the sum of cubes in two different ways.”

There is an interesting story pertaining to this example. The English mathematician G. H. Hardy, when visiting the ailing Indian prodigy Ramanujan in the hospital, remarked that 1729, the number of the cab he took, was rather dull. Ramanujan replied “No, it is a very interesting number; it is the smallest number expressible as the sum of cubes in two different ways.”

EXAMPLE 11

A Nonconstructive Existence Proof

Show that there exist irrational numbers \( x \) and \( y \) such that

\[
x^2 = 2.
\]

If it is rational, we have two irrational numbers \( x \) and \( y \) with \( x^2 \) rational, namely, \( x = \sqrt{2} \) and \( y = \sqrt{2} \). On the other hand if \( \sqrt{2} \) is irrational, then we can let \( x = \sqrt{2} \) and \( y = \sqrt{2} \) so that \( x^2 = \sqrt{2} \). Consider the number \( \sqrt{2} \), \( y \) or the pair \( x = \sqrt{2} \) and \( y = \sqrt{2} \) have the desired property, but we do not know which of these two pairs works!

Because we have displayed a positive integer that can be written as the sum of cubes in two different ways, we are done.

There is an interesting story pertaining to this example. The English mathematician G. H. Hardy, when visiting the ailing Indian prodigy Ramanujan in the hospital, remarked that 1729, the number of the cab he took, was rather dull. Ramanujan replied “No, it is a very interesting number; it is the smallest number expressible as the sum of cubes in two different ways.”

There is an interesting story pertaining to this example. The English mathematician G. H. Hardy, when visiting the ailing Indian prodigy Ramanujan in the hospital, remarked that 1729, the number of the cab he took, was rather dull. Ramanujan replied “No, it is a very interesting number; it is the smallest number expressible as the sum of cubes in two different ways.”

Because we have displayed a positive integer that can be written as the sum of cubes in two different ways, we are done.

There is an interesting story pertaining to this example. The English mathematician G. H. Hardy, when visiting the ailing Indian prodigy Ramanujan in the hospital, remarked that 1729, the number of the cab he took, was rather dull. Ramanujan replied “No, it is a very interesting number; it is the smallest number expressible as the sum of cubes in two different ways.”

There is an interesting story pertaining to this example. The English mathematician G. H. Hardy, when visiting the ailing Indian prodigy Ramanujan in the hospital, remarked that 1729, the number of the cab he took, was rather dull. Ramanujan replied “No, it is a very interesting number; it is the smallest number expressible as the sum of cubes in two different ways.”

Because we have displayed a positive integer that can be written as the sum of cubes in two different ways, we are done.

There is an interesting story pertaining to this example. The English mathematician G. H. Hardy, when visiting the ailing Indian prodigy Ramanujan in the hospital, remarked that 1729, the number of the cab he took, was rather dull. Ramanujan replied “No, it is a very interesting number; it is the smallest number expressible as the sum of cubes in two different ways.”

There is an interesting story pertaining to this example. The English mathematician G. H. Hardy, when visiting the ailing Indian prodigy Ramanujan in the hospital, remarked that 1729, the number of the cab he took, was rather dull. Ramanujan replied “No, it is a very interesting number; it is the smallest number expressible as the sum of cubes in two different ways.”

Because we have displayed a positive integer that can be written as the sum of cubes in two different ways, we are done.

There is an interesting story pertaining to this example. The English mathematician G. H. Hardy, when visiting the ailing Indian prodigy Ramanujan in the hospital, remarked that 1729, the number of the cab he took, was rather dull. Ramanujan replied “No, it is a very interesting number; it is the smallest number expressible as the sum of cubes in two different ways.”

Because we have displayed a positive integer that can be written as the sum of cubes in two different ways, we are done.

There is an interesting story pertaining to this example. The English mathematician G. H. Hardy, when visiting the ailing Indian prodigy Ramanujan in the hospital, remarked that 1729, the number of the cab he took, was rather dull. Ramanujan replied “No, it is a very interesting number; it is the smallest number expressible as the sum of cubes in two different ways.”

Because we have displayed a positive integer that can be written as the sum of cubes in two different ways, we are done.

There is an interesting story pertaining to this example. The English mathematician G. H. Hardy, when visiting the ailing Indian prodigy Ramanujan in the hospital, remarked that 1729, the number of the cab he took, was rather dull. Ramanujan replied “No, it is a very interesting number; it is the smallest number expressible as the sum of cubes in two different ways.”

Because we have displayed a positive integer that can be written as the sum of cubes in two different ways, we are done.

There is an interesting story pertaining to this example. The English mathematician G. H. Hardy, when visiting the ailing Indian prodigy Ramanujan in the hospital, remarked that 1729, the number of the cab he took, was rather dull. Ramanujan replied “No, it is a very interesting number; it is the smallest number expressible as the sum of cubes in two different ways.”

Because we have displayed a positive integer that can be written as the sum of cubes in two different ways, we are done.

There is an interesting story pertaining to this example. The English mathematician G. H. Hardy, when visiting the ailing Indian prodigy Ramanujan in the hospital, remarked that 1729, the number of the cab he took, was rather dull. Ramanujan replied “No, it is a very interesting number; it is the smallest number expressible as the sum of cubes in two different ways.”

Because we have displayed a positive integer that can be written as the sum of cubes in two different ways, we are done.

There is an interesting story pertaining to this example. The English mathematician G. H. Hardy, when visiting the ailing Indian prodigy Ramanujan in the hospital, remarked that 1729, the number of the cab he took, was rather dull. Ramanujan replied “No, it is a very interesting number; it is the smallest number expressible as the sum of cubes in two different ways.”

Because we have displayed a positive integer that can be written as the sum of cubes in two different ways, we are done.

There is an interesting story pertaining to this example. The English mathematician G. H. Hardy, when visiting the ailing Indian prodigy Ramanujan in the hospital, remarked that 1729, the number of the cab he took, was rather dull. Ramanujan replied “No, it is a very interesting number; it is the smallest number expressible as the sum of cubes in two different ways.”

Because we have displayed a positive integer that can be written as the sum of cubes in two different ways, we are done.

There is an interesting story pertaining to this example. The English mathematician G. H. Hardy, when visiting the ailing Indian prodigy Ramanujan in the hospital, remarked that 1729, the number of the cab he took, was rather dull. Ramanujan replied “No, it is a very interesting number; it is the smallest number expressible as the sum of cubes in two different ways.”

Because we have displayed a positive integer that can be written as the sum of cubes in two different ways, we are done.
Nonconstructive existence proofs often are quite subtle, as Example 12 illustrates.

**EXAMPLE 12** Chomp is a game played by two players. In this game, cookies are laid out on a rectangular grid. The cookie in the top left position is poisoned, as shown in Figure 1(a). The two players take turns making moves; at each move, a player is required to eat a remaining cookie, together with all cookies to the right and/or below it (see Figure 1(b), for example). The loser is the player who has no choice but to eat the poisoned cookie. We ask whether one of the two players has a winning strategy. That is, can one of the players always make moves that are guaranteed to lead to a win?

**Solution:** We will give a nonconstructive existence proof of a winning strategy for the first player. That is, we will show that the first player always has a winning strategy without explicitly describing the moves this player must follow.

First, note that the game ends and cannot finish in a draw because with each move at least one cookie is eaten, so after no more than \( m \times n \) moves the game ends, where the initial grid is \( m \times n \). Now, suppose that the first player begins the game by eating just the cookie in the bottom right corner. There are two possibilities, this is the first move of a winning strategy for the first player, or the second player can make a move that is the first move of a winning strategy for the second player. In this second case, instead of eating just the cookie in the bottom right corner, the first player could have made the same move that the second player made as the first move of a winning strategy for the second player.
proof method and strategy

(a) Chomp (Top Left Cookie Poisoned). (b) Three Possible Moves.

move of a winning strategy (and then continued to follow that winning strategy). This would guarantee a win for the first player.

Note that we showed that a winning strategy exists, but we did not specify an actual winning strategy. Consequently, the proof is a nonconstructive existence proof. In fact, no one has been able to describe a winning strategy for that Chomp that applies for all rectangular grids by describing the moves that the first player should follow. However, winning strategies can be described for certain special cases, such as when the grid is square and when the grid only has two rows of cookies (see Exercises 15 and 16 in Section 5.2).

Uniqueness Proofs

Some theorems assert the existence of a unique element with a particular property. In other words, these theorems assert that there is exactly one element with this property. To prove a statement of this type we need to show that an element with this property exists and that no other element has this property. The two parts of a uniqueness proof are:

Existence: We show that an element \( x \) with the desired property exists.

Uniqueness: We show that if \( y \neq x \), then \( y \) does not have the desired property.

Equivalently, we can show that if \( x \) and \( y \) both have the desired property, then \( x = y \).

Remark: Showing that there is a unique element \( x \) such that \( P(x) \) is the same as proving the statement \( \exists x \left( P(x) \land \forall y (y \neq x \rightarrow \neg P(y)) \right) \).

We illustrate the elements of a uniqueness proof in Example 13.

**Example 13**

Show that if \( a \) and \( b \) are real numbers and \( a \neq 0 \), then there is a unique real number \( r \) such that \( ar + b = 0 \).

**Solution:** First, note that the real number \( r = -b/a \) is a solution of \( ar + b = 0 \) because \( a(-b/a) + b = -b + b = 0 \). Consequently, a real number \( r \) exists for which \( ar + b = 0 \). This is the existence part of the proof.

Second, suppose that \( s \) is a real number such that \( as + b = 0 \). Then \( ar + b = as + b \), where \( r = -b/a \). Subtracting \( b \) from both sides, we find that \( ar = as \). Dividing both sides of this last equation by \( a \), which is nonzero, we see that \( r = s \). This means that if \( s \neq r \), then \( as + b \neq 0 \). This establishes the uniqueness part of the proof.
Proof Strategies

Finding proofs can be a challenging business. When you are confronted with a statement to prove, you should first replace terms by their definitions and then carefully analyze what the hypotheses and the conclusion mean. After doing so, you can attempt to prove the result using one of the available methods of proof. Generally, if the statement is a conditional statement, you should first try a direct proof; if this fails, you can try an indirect proof. If neither of these approaches works, you might try a proof by contradiction.

FORWARD AND BACKWARD REASONING

Whichever method you choose, you need a starting point for your proof. To begin a direct proof of a conditional statement, you start with the premises. Using these premises, together with axioms and known theorems, you can construct a proof using a sequence of steps that leads to the conclusion. This type of reasoning, called forward reasoning, is the most common type of reasoning used to prove relatively simple results. Similarly, with indirect reasoning you can start with the negation of the conclusion and, using a sequence of steps, obtain the negation of the premises.

Unfortunately, forward reasoning is often difficult to use to prove more complicated results, because the reasoning needed to reach the desired conclusion may be far from obvious. In such cases it may be helpful to use backward reasoning. To reason backward to prove a statement \( q \), we find a statement \( p \) that we can prove with the property that \( p \rightarrow q \). (Note that it is not helpful to find a statement \( r \) that you can prove such that \( q \rightarrow r \), because it is the fallacy of begging the question to conclude from \( q \rightarrow r \) and \( r \) that \( q \) is true.) Backward reasoning is illustrated in Examples 14 and 15.

**EXAMPLE 14**

Given two positive real numbers \( x \) and \( y \), their arithmetic mean is \((x + y)/2\) and their geometric mean is \(\sqrt{xy}\). When we compare the arithmetic and geometric means of pairs of distinct positive real numbers, we find that the arithmetic mean is always greater than the geometric mean. (For example, when \( x = 4 \) and \( y = 6 \), we have \( 5 = (4 + 6)/2 > \sqrt{4 \cdot 6} = \sqrt{24} \).) Can we prove that this inequality is always true?

**Solution:** To prove that \((x + y)/2 > \sqrt{xy}\) when \( x \) and \( y \) are distinct positive real numbers, we can work backward. We construct a sequence of equivalent inequalities. The equivalent inequalities are

\[
\begin{align*}
(x + y)/2 &= \sqrt{xy}, \\
(x + y)^2/4 &> xy, \\
(x + y)^2 &> 4xy, \\
x^2 + 2xy + y^2 &> 4xy, \\
x^2 - 2xy + y^2 &> 0, \\
(x - y)^2 &> 0.
\end{align*}
\]

Because \((x - y)^2 > 0\) when \( x \neq y \), it follows that the final inequality is true. Because all these inequalities are equivalent, it follows that \((x + y)/2 > \sqrt{xy}\) when \( x \neq y \). Once we have carried out this backward reasoning, we can easily reverse the steps to construct a proof using forward reasoning. We now give this proof.

Suppose that \( x \) and \( y \) are distinct positive real numbers. Then \((x - y)^2 > 0\) because the square of a nonzero real number is positive (see Appendix 1). Because \((x - y)^2 = x^2 - 2xy + y^2\), this implies that \(x^2 - 2xy + y^2 > 0\). Adding \(4xy\) to both sides, we obtain \(x^2 + 2xy + y^2 > 4xy\). Because \(x^2 + 2xy + y^2 = (x + y)^2\), this means that \((x + y)^2 > 4xy\). Dividing both sides of this equation by \(4\), we see that \((x + y)^2/4 > xy\). Finally, taking square roots of both sides (which preserves the inequality because both sides are positive) yields...
We conclude that if $x$ and $y$ are distinct positive real numbers, then their arithmetic mean $(x + y)/2$ is greater than their geometric mean $\sqrt{xy}$.

**EXAMPLE 15**

Suppose that two people play a game taking turns removing one, two, or three stones at a time from a pile that begins with 15 stones. The person who removes the last stone wins the game. Show that the first player can win the game no matter what the second player does.

**Solution:** To prove that the first player can always win the game, we work backward. At the last step, the first player can win if this player is left with a pile containing one, two, or three stones. The second player will be forced to leave one, two, or three stones if this player has to remove stones from a pile containing four stones. Consequently, one way for the first person to win is to leave four stones for the second player on the next-to-last move. The first person can leave four stones when there are five, six, or seven stones left at the beginning of this player’s move, which happens when the second player has to remove stones from a pile with eight stones. Consequently, to force the second player to leave five, six, or seven stones, the first player should leave eight stones for the second player at the second-to-last move for the first player. This means that there are nine, ten, or eleven stones when the first player makes this move. Similarly, the first person should leave twelve stones when this player makes the first move. We can reverse this argument to show that the first player can always make moves so that this player wins the game no matter what the second player does. These moves successively leave twelve, eight, and four stones for the second player.

**ADAPTING EXISTING PROOFS** An excellent way to look for possible approaches that can be used to prove a statement is to take advantage of existing proofs of similar results. Often an existing proof can be adapted to prove other facts. Even when this is not the case, some of the ideas used in existing proofs may be helpful. Because existing proofs provide clues for new proofs, you should read and understand the proofs you encounter in your studies. This process is illustrated in Example 16.

**EXAMPLE 16**

In Example 10 of Section 1.7 we proved that $\sqrt{2}$ is irrational. We now conjecture that $\sqrt{3}$ is irrational. Can we adapt the proof in Example 10 in Section 1.7 to show that $\sqrt{3}$ is irrational?

**Solution:** To adapt the proof in Example 10 in Section 1.7, we begin by mimicking the steps in that proof, but with $\sqrt{2}$ replaced with $\sqrt{3}$. First, we suppose that $\sqrt{3} = \frac{d}{c}$ where the fraction $\frac{c}{d}$ is in lowest terms. Squaring both sides tells us that $3 = \frac{c^2}{d^2}$, so that $3d^2 = c^2$. Can we use this equation to show that 3 must be a factor of both $c$ and $d$, similar to how we used the equation $2b^2 = a^2$ in Example 10 in Section 1.7 to show that 2 must be a factor of both $a$ and $b$? (Recall that an integer $n$ is a factor of the integer $t$ if $t/n$ is an integer. An integer $n$ is even if and only if 2 is a factor of $n$.) In turns out that we can, but we need some ammunition from number theory, which we will develop in Chapter 4. We sketch out the remainder of the proof, but leave the justification of these steps until Chapter 4. Because 3 is a factor of $c^2$, it must also be a factor of $c$. Furthermore, because 3 is a factor of $c$, 9 is a factor of $c^2$, which means that 9 is a factor of $3d^2$. This implies that 3 is a factor of $d^2$, which means that 3 is a factor of that $d$. This makes 3 a factor of both $c$ and $d$, which contradicts the assumption that $c/d$ is in lowest terms. After we have filled in the justification for these steps, we will have shown that $\sqrt{3}$ is irrational by adapting the proof that $\sqrt{2}$ is irrational. Note that this proof can be extended to show that $\sqrt{n}$ is irrational whenever $n$ is a positive integer that is not a perfect square. We leave the details of this to Chapter 4.

A good tip is to look for existing proofs that you might adapt when you are confronted with proving a new theorem, particularly when the new theorem seems similar to one you have already proved.
Looking for Counterexamples

In Section 1.7 we introduced the use of counterexamples to show that certain statements are false. When confronted with a conjecture, you might first try to prove this conjecture, and if your attempts are unsuccessful, you might try to find a counterexample, first by looking at the simplest, smallest examples. If you cannot find a counterexample, you might again try to prove the statement. In any case, looking for counterexamples is an extremely important pursuit, which often provides insights into problems. We will illustrate the role of counterexamples in Example 17.

**Example 17**

In Example 14 in Section 1.7 we showed that the statement “Every positive integer is the sum of two squares of integers” is false by finding a counterexample. That is, there are positive integers that cannot be written as the sum of the squares of two integers. Although we cannot write every positive integer as the sum of the squares of two integers, maybe we can write every positive integer as the sum of the squares of three integers. That is, is the statement “Every positive integer is the sum of the squares of three integers” true or false?

**Solution:**

Because we know that not every positive integer can be written as the sum of two squares of integers, we might initially be skeptical that every positive integer can be written as the sum of three squares of integers. So, we first look for a counterexample. That is, we can show that the statement “Every positive integer is the sum of three squares of integers” is false if we can find a particular integer that is not the sum of the squares of three integers. To look for a counterexample, we try to write successive positive integers as a sum of three squares. We find that $\text{1} = 0^2 + 0^2 + 1^2$, $\text{2} = 0^2 + 1^2 + 1^2$, $\text{3} = 1^2 + 1^2 + 1^2$, $\text{4} = 0^2 + 0^2 + 2^2$, $\text{5} = 0^2 + 1^2 + 2^2$, $\text{6} = 1^2 + 1^2 + 2^2$, $\text{7}$, but we cannot find a way to write 7 as the sum of three squares. To show that there are not three squares that add up to 7, we note that the only possible squares we can use are those not exceeding 7, namely, 0, 1, and 4. Because no three terms where each term is 0, 1, or 4 add up to 7, it follows that 7 is a counterexample. We conclude that the statement “Every positive integer is the sum of the squares of three integers” is false.

We have shown that not every positive integer is the sum of the squares of three integers. The next question to ask is whether every positive integer is the sum of the squares of four positive integers. Some experimentation provides evidence that the answer is yes. For example, $\text{7} = 1^2 + 1^2 + 1^2 + 2^2$, $\text{25} = 4^2 + 2^2 + 2^2 + 1^2$, and $\text{87} = 9^2 + 2^2 + 2^2 + 1^2$. It turns out the conjecture “Every positive integer is the sum of the squares of four integers” is true. For a proof, see [Ro10].

**Proof Strategy in Action**

Mathematics is generally taught as if mathematical facts were carved in stone. Mathematics texts (including the bulk of this book) formally present theorems and their proofs. Such presentations do not convey the discovery process in mathematics. This process begins with exploring concepts and examples, asking questions, formulating conjectures, and attempting to settle these conjectures either by proof or by counterexample. These are the day-to-day activities of mathematicians. Believe it or not, the material taught in textbooks was originally developed in this way.

People formulate conjectures on the basis of many types of possible evidence. The examination of special cases can lead to a conjecture, as can the identification of possible patterns. Altering the hypotheses and conclusions of known theorems also can lead to plausible conjectures. At other times, conjectures are made based on intuition or a belief that a result holds. No matter how a conjecture was made, once it has been formulated, the goal is to prove or disprove it. When mathematicians believe that a conjecture may be true, they try to find a proof. If they cannot find a proof, they may look for a counterexample. When they cannot find a counterexample, they may switch gears and once again try to prove the conjecture. Although many conjectures are quickly settled, a few conjectures resist attack for hundreds of years and lead to...
1.8 Proof Methods and Strategy

The development of new parts of mathematics. We will mention a few famous conjectures later in this section.

Tilings

We can illustrate aspects of proof strategy through a brief study of tilings of checkerboards. Looking at tilings of checkerboards is a fruitful way to quickly discover many different results and construct their proofs using a variety of proof methods. There are almost an endless number of conjectures that can be made and studied in this area too. To begin, we need to define some terms. A checkerboard is a rectangle divided into squares of the same size by horizontal and vertical lines. The game of checkers is played on a board with 8 rows and 8 columns; this board is called the standard checkerboard and is shown in Figure 2. In this section we use the term board to refer to a checkerboard of any rectangular size as well as parts of checkerboards obtained by removing one or more squares. A domino is a rectangular piece that is one square by two squares, as shown in Figure 3. We say that a board is tiled by dominoes when all its squares are covered with no overlapping dominoes and no dominoes overhanging the board. We now develop some results about tiling boards using dominoes.

EXAMPLE 18

Can we tile the standard checkerboard using dominoes?

Solution: We can find many ways to tile the standard checkerboard using dominoes. For example, we can tile it by placing 32 dominoes horizontally, as shown in Figure 4. The existence of one such tiling completes a constructive existence proof. Of course, there are a large number of other ways to do this tiling. We can place 32 dominoes vertically on the board or we can place some tiles vertically and some horizontally. But for a constructive existence proof we needed to find just one such tiling.

EXAMPLE 19

Can we tile a board obtained by removing one of the four corner squares of a standard checkerboard?

Solution: To answer this question, note that a standard checkerboard has 64 squares, so removing a square produces a board with 63 squares. Now suppose that we could tile a board obtained from the standard checkerboard by removing a corner square. The board has an even number of
sure, we can prove by contradiction that a standard checkerboard with one square removed cannot be tiled using dominoes because such a board has an odd number of squares.

We now consider a trickier situation.

EXAMPLE 20 Can we tile the board obtained by deleting the upper left and lower right corner squares of a standard checkerboard, shown in Figure 5?

Solution: A board obtained by deleting two squares of a standard checkerboard contains \(64 - 2 = 62\) squares. Because 62 is even, we cannot quickly rule out the existence of a tiling of the standard checkerboard with its upper left and lower right squares removed, unlike Example 19, where we ruled out the existence of a tiling of the standard checkerboard with one corner square removed. Trying to construct a tiling of this board by successively placing dominoes might be a first approach, as the reader should attempt. However, no matter how much we try, we cannot find such a tiling. Because our efforts do not produce a tiling, we are led to conjecture that no tiling exists.

We might try to prove that no tiling exists by showing that we reach a dead end however we successively place dominoes on the board. To construct such a proof, we would have to consider all possible cases that arise as we run through all possible choices of successively placing dominoes. For example, we have two choices for covering the square in the second column of the first row, next to the removed top left corner. We could cover it with a horizontally placed tile or a vertically placed tile. Each of these two choices leads to further choices, and so on. It does not take long to see that this is not a fruitful plan of attack for a person, although a computer could be used to complete such a proof by exhaustion. (Exercise 45 asks you to supply such a proof to show that a \(4 \times 4\) checkerboard with opposite corners removed cannot be tiled.)

We need another approach. Perhaps there is an easier way to prove there is no tiling of a standard checkerboard with two opposite corners removed. As with many proofs, a key observation can help. We color the squares of this checkerboard using alternating white and black squares, as in Figure 2. Observe that a domino in a tiling of such a board covers one white square and one black square. Next, note that this board has unequal numbers of white square and black...
Proof Methods and Strategy

1.8 Proof Methods and Strategy

105

squares. We can use these observations to prove by contradiction that a standard checkerboard
with opposite corners removed cannot be tiled using dominoes. We now present such a proof.

Proof: Suppose we can use dominoes to tile a standard checkerboard with opposite corners
removed. Note that the standard checkerboard with opposite corners removed contains \(64 - 2 = 62\) squares. The tiling would use \(62/2 = 31\) dominoes. Note that each domino in this tiling covers
one white and one black square. Consequently, the tiling covers 31 white squares and 31 black
squares. However, when we remove two opposite corner squares, either 32 of the remaining
squares are white and 30 are black or else 30 are white and 32 are black. This contradicts the
assumption that we can use dominoes to cover a standard checkerboard with opposite corners
removed, completing the proof.

\[\Box\]

We can use other types of pieces besides dominoes in tilings. Instead of dominoes we can
study tilings that use identically shaped pieces constructed from congruent squares that are
connected along their edges. Such pieces are called polyominoes, a term coined in 1953 by the
mathematician Solomon Golomb, the author of an entertaining book about them \[Go94\]. We
will consider two polyominoes with the same number of squares the same if we can rotate and/or
flip one of the polyominoes to get the other one. For example, there are two types of triominoes
(see Figure 6), which are polyominoes made up of three squares connected by their sides. One
type of triomino, the straight triomino, has three horizontally connected squares; the other
type, right triominoes, resembles the letter L in shape, flipped and/or rotated, if necessary. We
will study the tilings of a checkerboard by straight triominoes here; we will study tilings by
right triominoes in Section 5.1.

EXAMPLE 21
Can you use straight triominoes to tile a standard checkerboard?

Solution: The standard checkerboard contains 64 squares and each triomino covers three
squares. Consequently, if triominoes tile a board, the number of squares of the board must be
a multiple of 3. Because 64 is not a multiple of 3, triominoes cannot be used to cover an \(8 \times 8\)
checkerboard.

\[\Box\]

In Example 22, we consider the problem of using straight triominoes to tile a standard
checkerboard with one corner missing.

EXAMPLE 22
Can we use straight triominoes to tile a standard checkerboard with one of its four corners
removed? An \(8 \times 8\) checkerboard with one corner removed contains \(64 - 1 = 63\) squares. Any
tiling by straight triominoes of one of these four boards uses \(63/3 = 21\) triominoes. However,
when we experiment, we cannot find a tiling of one of these boards using straight triominoes.
A proof by exhaustion does not appear promising. Can we adapt our proof from Example 20 to
prove that no such tiling exists?

Solution: We will color the squares of the checkerboard in an attempt to adapt the proof by
contradiction we gave in Example 20 of the impossibility of using dominoes to tile a standard
checkerboard with opposite corners removed. Because we are using straight triominoes rather
than dominoes, we color the squares using three colors rather than two colors, as shown in
Figure 7. Note that there are 21 blue squares, 21 black squares, and 22 white squares in this
coloring. Next, we make the crucial observation that when a straight triomino covers three
squares of the checkerboard, it covers one blue square, one black square, and one white square.
Next, note that each of the three colors appears in a corner square. Thus without loss of generality,
we may assume that we have rotated the coloring so that the missing square is colored blue.
Therefore, we assume that the remaining board contains 20 blue squares, 21 black squares, and
22 white squares.

If we could tile this board using straight triominoes, then we would use \(63/3 = 21\) straight
triominoes. These triominoes would cover 21 blue squares, 21 black squares, and 21 white
FIGURE 7 Coloring the Squares of the Standard Checkerboard with Three Colors.

squares. This contradicts the fact that this board contains 20 blue squares, 21 black squares, and 22 white squares. Therefore we cannot tile this board using straight triominoes.

The Role of Open Problems

Many advances in mathematics have been made by people trying to solve famous unsolved problems. In the past 20 years, many unsolved problems have finally been resolved, such as the proof of a conjecture in number theory made more than 300 years ago. This conjecture asserts the truth of the statement known as Fermat’s last theorem.

THEOREM 1 FERMAT’S LAST THEOREM

The equation

\[ x^n + y^n = z^n \]

has no solutions in integers \( x, y, \) and \( z \) with \( xyz \neq 0 \) whenever \( n \) is an integer with \( n > 2 \).

Remark: The equation \( x^2 + y^2 = z^2 \) has infinitely many solutions in integers \( x, y, \) and \( z \); these solutions are called Pythagorean triples and correspond to the lengths of the sides of right triangles with integer lengths. See Exercise 32.

This problem has a fascinating history. In the seventeenth century, Fermat jotted in the margin of his copy of the works of Diophantus that he had a “wondrous proof” that there are no integer solutions of \( x^n + y^n = z^n \) when \( n \) is an integer greater than 2 with \( xyz \neq 0 \). However, he never published a proof (Fermat published almost nothing), and no proof could be found in the papers he left when he died. Mathematicians looked for a proof for three centuries without success, although many people were convinced that a relatively simple proof could be found. (Proofs of special cases were found, such as the proof of the case when \( n = 3 \) by Euler and the proof of the \( n = 4 \) case by Fermat himself.) Over the years, several established mathematicians thought that they had proved this theorem. In the nineteenth century, one of these failed attempts led to the development of the part of number theory called algebraic number theory. A correct
proof, requiring hundreds of pages of advanced mathematics, was not found until the 1990s, when Andrew Wiles used recently developed ideas from a sophisticated area of number theory called the theory of elliptic curves to prove Fermat’s last theorem. Wiles’s quest to find a proof of Fermat’s last theorem using this powerful theory, described in a program in the *Nova* series on public television, took close to ten years! Moreover, his proof was based on major contributions of many mathematicians. (The interested reader should consult [Ro10] for more information about Fermat’s last theorem and for additional references concerning this problem and its resolution.)

We now state an open problem that is simple to describe, but that seems quite difficult to resolve.

**EXAMPLE 23 The 3x + 1 Conjecture** Let $T$ be the transformation that sends an even integer $x$ to $x/2$ and an odd integer $x$ to $3x + 1$. A famous conjecture, sometimes known as the 3x + 1 conjecture, states that for all positive integers $x$, when we repeatedly apply the transformation $T$, we will eventually reach the integer 1. For example, starting with $x = 13$, we find $T(13) = 3 \cdot 13 + 1 = 40$, $T(40) = 40/2 = 20$, $T(20) = 20/2 = 10$, $T(10) = 10/2 = 5$, $T(5) = 3 \cdot 5 + 1 = 16$, $T(16) = 8$, $T(8) = 4$, $T(4) = 2$, and $T(2) = 1$. The 3x + 1 conjecture has been verified using computers for all integers $x$ up to $5 \cdot 10^{13}$.

The 3x + 1 conjecture has an interesting history and has attracted the attention of mathematicians since the 1950s. The conjecture has been raised many times and goes by many other names, including the Collatz problem, Hasse’s algorithm, Ulam’s problem, the Syracuse problem, and Kakutani’s problem. Many mathematicians have been diverted from their work to spend time attacking this conjecture. This led to the joke that this problem was part of a conspiracy to slow down American mathematical research. See the article by Jeffrey Lagarias [La10] for a fascinating discussion of this problem and the results that have been found by mathematicians attacking it.

In Chapter 4 we will describe additional open questions about prime numbers. Students already familiar with the basic notions about primes might want to explore Section 4.3, where these open questions are discussed. We will mention other important open questions throughout the book.

**Additional Proof Methods**

In this chapter we introduced the basic methods used in proofs. We also described how to leverage these methods to prove a variety of results. We will use these proof methods in all subsequent chapters. In particular, we will use them in Chapters 2, 3, and 4 to prove results about sets, functions, algorithms, and number theory and in Chapters 9, 10, and 11 to prove results in graph theory. Among the theorems we will prove is the famous halting theorem which states that there is a problem that cannot be solved using any procedure. However, there are many important proof methods besides those we have covered. We will introduce some of these methods later in this book. In particular, in Section 5.1 we will discuss mathematical induction, which is an extremely useful method for proving statements of the form $\forall n \in \mathbb{N}, P(n)$, where the domain consists of all positive integers. In Section 5.3 we will introduce structural induction, which can be used to prove results about recursively defined sets. We will use the Cantor diagonalization method, which can be used to prove results about the size of infinite sets, in Section 2.5. In Chapter 6 we will introduce the notion of combinatorial proofs, which can be used to prove results by counting arguments. The reader should note that entire books have been devoted to the activities discussed in this section, including many excellent works by George Pólya ([Po61], [Po71], [Po90]).

Finally, note that we have not given a procedure that can be used for proving theorems in mathematics. It is a deep theorem of mathematical logic that there is no such procedure.
Exercises

1. Prove that \( n^2 + 1 \geq 2^n \) when \( n \) is a positive integer with \( 1 \leq n \leq 4. \)

2. Prove that there are no positive perfect cubes less than 1000 that are the sum of the cubes of two positive integers.

3. Prove that if \( x \) and \( y \) are real numbers, then \( \max(x, y) + \min(x, y) = x + y \). \[ \text{Hint: Use a proof by cases, with the two cases corresponding to } x \geq y \text{ and } x < y, \text{ respectively}. \]

4. Use a proof by cases to show that \( \min(a, \min(b, c)) = \min(\min(a, b), c) \) whenever \( a, b, \) and \( c \) are real numbers.

5. Prove using the notion of without loss of generality that \( \min(x, y) = (x + y - |x - y|)/2 \) whenever \( x \) and \( y \) are real numbers.

6. Prove using the notion of without loss of generality that \( 5x + 5y \) is an odd integer when \( x \) and \( y \) are integers of opposite parity.

7. Prove the triangle inequality, which states that if \( x \) and \( y \) are real numbers, then \( |x| + |y| \geq |x + y| \) (where \(|x|\) represents the absolute value of \( x \)), which equals \( s \) if \( s \geq 0 \) and equals \(-s\) if \( s < 0 \).

8. Prove that there is a positive integer that equals the sum of the positive integers not exceeding it. Is your proof constructive or nonconstructive?

9. Prove that there are 100 consecutive positive integers that are not perfect squares. Is your proof constructive or nonconstructive?

10. Prove that either \( 2 \cdot 10^{991} + 15 \) or \( 2 \cdot 10^{991} + 16 \) is not a perfect square. Is your proof constructive or nonconstructive?

11. Prove that there exists a pair of consecutive integers such that one of these integers is a perfect square and the other is a perfect cube.

12. Show that the product of two of the numbers 65, 100, 001 \( \cdot 3^2 \), \( \sqrt[3]{27} \), \( \sqrt[3]{121} \), \( \sqrt[3]{121} \), \( \sqrt[3]{2000} \), and \( 24493 = 5^1 \cdot 7^2 \cdot 17^2 \) is nonnegative. Is your proof constructive or nonconstructive?

13. Prove or disprove that there is a rational number \( x \) and an irrational number \( y \) such that \( x^y \) is irrational.

14. Prove or disprove that if \( a \) and \( b \) are rational numbers, then \( a^b \) is also rational.

15. Show that each of these statements can be used to express the fact that there is a unique element \( s \) such that \( P(s) \) is true. \[ \text{[Note that we can also write this statement as } \exists!x P(x) \text{.]} \]

a) \( \exists!y (P(y) \iff y = y) \)

b) \( \exists!x \forall y P(x) \land P(y) \iff x = y) \)

c) \( \exists!(x, y) (x \land y \iff y = x) \)

16. Show that if \( a, b, \) and \( c \) are real numbers and \( a \neq 0 \), then there is a unique solution of the equation \( ax + b = c \).

17. Suppose that \( a \) and \( b \) are odd integers with \( a \neq b \). Show that there is an unique integer \( c \) such that \( a - c = b - c \).

18. Show that if \( r \) is an irrational number, there is a unique integer \( n \) such that the distance between \( r \) and \( n \) is less than \( 1/2. \)

19. Show that if \( n \) is an odd integer, then there is a unique integer \( k \) such that \( n = k - 2 \) and \( k + 3 \) or \( k + 3 \).

20. Prove that if \( x \) and \( y \) are rational numbers and \( a \) and \( b \) are integers, then \( a = b \).

21. Prove that there are infinitely many solutions in positive integers \( n \) and \( k \) such that \( n = n - k \), \( n \) is an integer, and \( 0 \leq k \leq 1 \).

22. Use forward reasoning to show that if \( x \) is a nonzero real number, then \( x^2 + 1/x^2 \geq 2 \). \[ \text{[Hint: Start with the inequality } (x - 1/x^2)^2 \geq 0 \text{ which holds for all nonzero real numbers } x. \]

23. The harmonic mean of two real numbers \( x \) and \( y \) equals \( 2xy/(x + y) \). By computing the arithmetic and geometric means of different pairs of positive real numbers, formulate a conjecture about their relative sizes and prove your conjecture.

24. The quadratic mean of two real numbers \( x \) and \( y \) equals \( \sqrt{(x^2 + y^2)/2} \). By computing the arithmetic and quadratic means of different pairs of positive real numbers, formulate a conjecture about their relative sizes and prove your conjecture.

25. Write the numbers 1, 2, ..., 20 on a blackboard, where \( n \) is an odd integer. Pick any two of the numbers, \( a \) and \( b \), write \( |a - b| \) on the board and erase \( a \) and \( b \). Continue this process until only one integer is written on the board. Prove that this integer must be odd.

26. Suppose that five ones and four zeros are arranged around a circle. Between any two equal bits you insert a 1 and between any two unequal bits you insert a 1 to produce nine new bits. Then you erase the original bits. Show that when you iterate this procedure, you can never get nine zeros. \[ \text{[Hint: Work backward, assuming that you did end up with nine zeros.]} \]

27. Formulate a conjecture about the decimal digits that appear as the final decimal digit of the fourth power of an integer. Prove your conjecture using a proof by cases.

28. Formulate a conjecture about the final two decimal digits of the square of an integer. Prove your conjecture using a proof by cases.

29. Prove that there is no positive integer \( n \) such that \( n^2 + n^2 = 100 \).

30. Prove that there are no solutions in integers \( a \) and \( b \) to the equation \( 2a^2 + 3b^2 = 14 \).

31. Prove that there are no solutions in positive integers \( x \) and \( y \) to the equation \( x^2 + y^2 = 625 \).

32. Prove that there are infinitely many solutions in positive integers \( x \), \( y \), and \( z \) to the equation \( x^2 + y^2 = z^2 \). \[ \text{[Hint: Let } x = m^2 - n^2, \ y = 2mn, \text{ and } z = m^2 + n^2, \text{ where } m \text{ and } n \text{ are integers.]} \]
33. Adapt the proof in Example 4 in Section 1.7 to prove that if \( a > b \), then \( a + c > b + c \).
34. Prove that \( \sqrt{2} \) is irrational.
35. Prove that between every two rational numbers there is an irrational number.
36. Prove that every rational number and every irrational number there is a rational number.

\[ \neg p \text{ truth value: } \neg \text{proposition variable: } \neg \text{a variable that represents a proposition.} \]

37. Let \( S = \sum_{i=1}^{n} a_i \), where \( a_1, a_2, \ldots, a_n \) are elements of two different sequences of positive real numbers, each containing \( n \) elements.
   a) Show that \( S \) takes its maximum value over all orderings of the two sequences when both sequences are sorted (so that the elements in each sequence are in nondecreasing order).
   b) Show that \( S \) takes its minimum value over all orderings of the two sequences when one sequence is sorted into nondecreasing order and the other is sorted into nonincreasing order.

38. Prove or disprove that if you have an 8-gallon jug of water and two empty jugs with capacities of 5 gallons and 3 gallons, respectively, then you can measure 4 gallons by successively pouring some of or all of the water in a jug into another jug.

39. Verify the 3 \( x + 1 \) conjecture for these integers.
   a) 6  b) 7  c) 17  d) 21

40. Verify the 3 \( x + 1 \) conjecture for these integers.
   a) 16  b) 11  c) 35  d) 113

41. Prove or disprove that you can use dominoes to tile a standard checkerboard with two adjacent corners removed (that is, corners that are not opposite).

42. Prove or disprove that you can use dominoes to tile a standard checkerboard with all four corners removed.

43. Prove that you can use dominoes to tile a rectangular checkerboard with an even number of squares.

44. Prove or disprove that you can use dominoes to tile a 5 \( \times \) 5 checkerboard with three corners removed.

45. Use a proof by exhaustion to show that a tiling using dominoes of a 4 \( \times \) 4 checkerboard with opposite corners removed does not exist. [Hint: First show that you can assume that the squares in the upper left and lower right corners are removed. Number the squares of the original checkerboard from 1 to 16, starting in the first row, moving right in this row, then starting in the leftmost square in the second row and moving right, and so on. Remove squares 1 and 16. To begin the proof, note that square 2 is covered either by a domino laid horizontally, which covers squares 2 and 3, or vertically, which covers squares 2 and 6. Consider each of these cases separately, and work through all the subcases that arise.]

46. Prove that when a white square and a black square are removed from an 8 \( \times \) 8 checkerboard (colored as in the text) you can tile the remaining squares of the checkerboard using dominoes. [Hint: Show that when one black and one white square are removed, each part of the partition of the remaining cells formed by inserting the barriers shown in the figure can be covered by dominoes.]

47. Show that by removing two white squares and two black squares from an 8 \( \times \) 8 checkerboard (colored as in the text) you can make it impossible to tile the remaining squares using dominoes.

48. Find all squares, if they exist, on an 8 \( \times \) 8 checkerboard such that the board obtained by removing one of these squares can be tiled using straight triominoes. [Hint: First use arguments based on coloring and rotations to eliminate as many squares as possible from consideration.]

49. a) Draw each of the five different tetrominoes, where a tetromino is a polyomino consisting of four squares.
   b) For each of the five different tetrominoes, prove or disprove that you can tile a standard checkerboard using these tetrominoes.

50. Prove or disprove that you can tile a 10 \( \times \) 10 checkerboard using straight tetrominoes.

---

**Key Terms and Results**

**TERMS**

proposition: a statement that is true or false
propositional variable: a variable that represents a proposition
truth value: true or false
\( \neg p \) (negation of \( p \)): the proposition with truth value opposite to the truth value of \( p \)

**logical operators: operators used to combine propositions**
compound proposition: a proposition constructed by combining propositions using logical operators
truth table: a table displaying all possible truth values of propositions
\( p \lor q \) (disjunction of \( p \) and \( q \)): the proposition \( "p \lor q\), which is true if and only if at least one of \( p \) and \( q \) is true.
argument: a sequence of statements

p → q (conjunction of p and q): the proposition "p and q," which is true if and only if both p and q are true
p ⊕ q (exclusive or of p and q): the proposition "p XOR q," which is false if and only if both p and q are true
p → q (implies): the proposition "if p, then q," which is false if and only if p is true and q is false
converse of p → q: the conditional statement q → p
contrapositive of p → q: the conditional statement ¬q → ¬p

bit: either a 0 or a 1
Boolean variable: a variable that has a value of 0 or 1

predicate: a part of a sentence that attributes a property to the subject

propositional function: a statement containing one or more variables that becomes a proposition when each of its variables is assigned a value or is bound by a quantifier

domain (or universe) of discourse: the values a variable in a propositional function may take

∃x P(x): (existential quantification of P(x)): the proposition that is true if and only if there exists an x in the domain such that P(x) is true
∀x P(x): (universal quantification of P(x)): the proposition that is true if and only if P(x) is true for every x in the domain

logically equivalent expressions: expressions that have the same truth value no matter which propositional functions and domains are used

free variable: a variable not bound in a propositional function

bound variable: a variable that is quantified

scope of a quantifier: portion of a statement where the quantifier binds its variable

argument: a sequence of statements involving propositional variables

premise: a statement, in an argument, or argument form, other than the final one

conclusion: the final statement in an argument or argument form

valid argument form: a sequence of compound propositions involving propositional variables where the truth of all the premises implies the truth of the conclusion
valid argument: an argument with a valid argument form

rule of inference: a valid argument form that can be used in the demonstration that arguments are valid

fallacy: an invalid argument form often used incorrectly as a rule of inference (or sometimes, more generally, an incorrect argument)


theorem: a mathematical assertion that can be shown to be true

conjecture: a mathematical assertion proposed to be true, but that has not been proved

proof: a demonstration that a theorem is true

axiom: a statement that is assumed to be true and that can be used as a basis for proving theorems


lemma: a theorem used to prove other theorems
corollary: a proposition that can be proved as a consequence of a theorem that has just been proved

vacuous proof: a proof that p → q is true based on the fact that p is false

trivial proof: a proof that p → q is true based on the fact that q is true
direct proof: a proof that p → q is true that proceeds by showing that q must be true when p is true

proof by contraposition: a proof that p → q is true that proceeds by showing that q must be false when p is false

proof by contradiction: a proof that p is true based on the fact that the conditional statement ¬p → q, where q is a contradiction

exhaustive proof: a proof that establishes a result by checking a list of all possible cases

proof by cases: a proof broken into separate cases, where these cases cover all possibilities

without loss of generality: an assumption in a proof that makes it possible to prove a theorem by reducing the number of cases to consider in the proof

counterexample: an element x such that P(x) is false
constructive existence proof: a proof that an element with a specified property exists that explicitly finds such an element

nonconstructive existence proof: a proof that an element with a specified property exists that does not explicitly find such an element

rational number: a number that can be expressed as the ratio of two integers p and q such that q ≠ 0

uniqueness proof: a proof that there is exactly one element satisfying a specified property
RESULTS

The logical equivalences given in Tables 6, 7, and 8 in Section 1.3.

Review Questions

1. a) Define the negation of a proposition.
   b) Give an example of a predicate $P(x, y)$ such that $\exists y P(x, y)$ and $\forall y P(x, y)$ have different truth values.

2. a) Define using truth tables the conjunction, exclusive or, or, and biconditional of the propositions $p$ and $q$.
   b) Describe at least five different ways to write the conditional statement $p \rightarrow q$ in English.

3. a) State the converse and contrapositive of a conditional statement.
   b) State the converse and the contrapositive of the conditional statement “If it is sunny tomorrow, then I will go for a walk in the woods.”

4. a) What does it mean for two propositions to be logically equivalent?
   b) Describe the different ways to show that two compound propositions are logically equivalent.

5. (Depends on the Exercise Set in Section 1.3)
   a) Given a truth table, explain how to use disjunctive normal form to construct a compound proposition with this truth table.
   b) Explain why part (a) shows that the operators $\land$, $\lor$, and $\neg$ are functionally complete.
   c) Is there an operator such that the set containing just this operator is functionally complete?

6. a) What is the difference between the quantification $\exists x P(x, y)$ and $\forall x P(x, y)$, where $P(x, y)$ is a predicate?
   b) Give a direct proof, a proof by contraposition and a proof by contradiction of a conditional statement.
   c) Prove the statement: “If the earth is flat, then you can sail off the edge of the earth,” “You cannot sail off the edge of the earth,” “The earth is not flat” is a valid argument.

7. a) What is the difference between the quantification $\exists x \forall y P(x, y)$ and $\forall x \exists y P(x, y)$? What are their negations?
   b) Use rules of inference to show that if the premises “All zebras have stripes” and “Mark is a zebra” are true, then the conclusion “Mark has stripes” is true.

8. Describe what is meant by a valid argument in propositional logic and show that the argument “If the earth is flat, then you can sail off the edge of the earth,” “You cannot sail off the edge of the earth,” “The earth is not flat” is a valid argument.

9. Use rules of inference to show that if the premises “All zebras have stripes” and “Mark is a zebra” are true, then the conclusion “Mark has stripes” is true.

10. a) What is the difference between a constructive and non-constructive existence proof? Give an example of each.
    b) Show that the statement “For every positive integer $n$, $n^2 \geq 2^n$” is false.

11. a) Describe a way to prove the biconditional $p \leftrightarrow q$.
    b) Prove the statement: “The integer $3n + 2$ is odd if and only if the integer $9n + 5$ is even, where $n$ is an integer.”

12. To prove that the statements $p_1, p_2, p_3,$ and $p_4$ are equivalent, is it sufficient to show that the conditional statements $p_4 \rightarrow p_3, p_3 \rightarrow p_1,$ and $p_1 \rightarrow p_2$ are valid? If not, provide another collection of conditional statements that can be used to show that the four statements are equivalent.

13. a) Suppose that a statement of the form $\forall x P(x)$ is false. How can this be proved?
    b) Suppose that a statement of the form $\exists x P(x)$ is false. How can this be proved?

14. What is the difference between a constructive and non-constructive existence proof? Give an example of each.

15. What are the elements of a proof that there is a unique element $x$ such that $P(x)$, where $P(x)$ is a propositional function?

16. Explain how a proof by cases can be used to prove a result about absolute values, such as the fact that $|xy| = |x||y|$ for all real numbers $x$ and $y$.

Supplementary Exercises

1. Let $p$ be the proposition “I will do every exercise in this book” and $q$ be the proposition “I will get an “A” in this course.” Express each of these as a combination of $p$ and $q$.
   a) I will get an “A” in this course only if I do every exercise in this book.
   b) I will get an “A” in this course and I will do every exercise in this book.
   c) Either I will not get an “A” in this course or I will not do every exercise in this book.
   d) For me to get an “A” in this course it is necessary and sufficient that I do every exercise in this book.

Rules of inference for propositional calculus.

De Morgan’s laws for quantifiers.

Rules of inference for quantified statements.
2. Find the truth table of the compound proposition \((p \vee q) \implies (p \land q)\).

3. Show that these compound propositions are tautologies.
   a) \((\neg q \land (p \implies q)) \implies p\)
   b) \((p \lor q) \land (p \implies q) \implies q\)

4. Give the converse, the contrapositive, and the inverse of these conditional statements.
   a) If it rains today, then I will drive to work.
   b) If \(x = x\), then \(x \geq 0\).
   c) If \(r\) is greater than 3, then \(n^2\) is greater than 9.

5. Give the converse, the contrapositive, and the inverse of these compound propositions.
   a) If the consistency of all commitments is maintained, then the student passes the test.
   b) When the student rejects an assertion, its negation is added as a commitment.
   c) In each round the teacher gives the student successive assertions that the student must either accept or reject as they are given. When the student accepts an assertion, it is added as a commitment; when the student rejects an assertion its negation is added as a commitment.

6. Show that these statements are inconsistent: "If Sergei takes the job offer then he will get a signing bonus." "If Sergei takes the job offer, then he will receive a higher salary." "If Sergei gets a signing bonus, then he will not receive a higher salary." "Sergei takes the job offer." Give this book.

7. Teachers in the Middle Ages supposedly tested the real-time propositional logic ability of a student via a technique known as an obligato game. In an obligato game, a number of rounds is set and in each round the teacher gives the student successive assertions that the student must either accept or reject as they are given. When the student accepts an assertion, it is added as a commitment; when the student rejects an assertion its negation is added as a commitment. The student passes the test if the consistency of all commitments is maintained throughout the test.

8. Suppose that in a three-round obligato game, the teacher first gives the student the proposition \(p \implies q\), then the proposition \((p \lor q) \lor q\), and finally the proposition \(q\). For which of the eight possible sequences of three answers will the student pass the test?

9. Suppose that in a four-round obligato game, the teacher first gives the student the proposition \(\neg (p \implies q)\), then the proposition \((p \lor q) \lor (q \lor r)\), and finally the proposition \((p \land q) \lor (q \implies p)\). For which of the sixteen possible sequences of four answers will the student pass the test?

10. Explain why every obligato game has a winning strategy. Exercises 13 and 14 are set on the island of knights and knaves described in Example 7 in Section 1.2.

11. Suppose that you meet three people Aaron, Bohan, and Crystal. Can you determine what Aaron, Bohan, and Crystal are if Aaron says "All of us are knaves" and Bohan says "Exactly one of us is a knave."?

12. Suppose that you meet three people, Anita, Boris, and Carmen. What are Anita, Boris, and Carmen if Anita says "I am a knave and Boris is a knight" and Boris says "Exactly one of us is a knight"?

13. Suppose that you meet three people Aaron, Bohan, and Crystal. Can you determine what Aaron, Bohan, and Crystal are if Aaron says "All of us are knaves" and Bohan says "Exactly one of us is a knave."?

14. Suppose that you meet three people, Anita, Boris, and Carmen. What are Anita, Boris, and Carmen if Anita says "I am a knave and Boris is a knight" and Boris says "Exactly one of the three of us is a knight"?

15. (Adapted from [Smi78]) Suppose that on an island there are three types of people, knights, knaves, and normals (also known as spies). Knights always tell the truth, knaves always lie, and normals sometimes lie and sometimes tell the truth. Detectives questioned three inhabitants of the island—Amy, Brenda, and Claire—as part of the investigation of a crime. The detectives know that one of the three committed the crime, but not which one. They also knew that the criminal was a knight, and that the other two were not. Additionally, the detectives recorded these statements: Amy: "I am an innocent." Brenda: "What Amy says is true." Claire: "Brenda is not a normal." After analyzing their information, the detectives positively identified the guilty party. Who was it?

16. Show that if \(S\) is a proposition, where \(S\) is the conditional statement "If \(S\) is true, then unicorns live," then "Unicorns live" is true. Show that it follows that \(S\) cannot be a proposition. (This paradox is known as Lobo's paradox.)

17. Model 16 Sudoku puzzles (with 4 × 4 blocks) as satisfiability problems.

18. Suppose that the truth value of the proposition \(p_i\) is \(T\) whenever \(i\) is an odd positive integer and is \(F\) whenever \(i\) is an even positive integer. Find the truth values of \(\exists_i^1 p_i\lor p_{i+2}\) and \(\forall_i^1 p_i\lor p_{i+2}\).

19. Model 16 × 16 Sudoku puzzles (with 4 × 4 blocks) as satisfiability problems.

20. Let \(P(x)\) be the statement "Student \(x\) knows calculus" and let \(Q(y)\) be the statement "Class \(y\) contains a student who knows calculus." Express each of these as quantifications of \(P(x)\) and \(Q(y)\):
   a) Some students know calculus.
   b) Not every student knows calculus.
   c) Every class has a student in it who knows calculus.
   d) Every student in every class knows calculus.
   e) There is at least one class with no students who know calculus.

21. Let \(P(m, n)\) be the statement "\(m\) divides \(n\)," where the domain for both variables consists of all positive integers. (By "\(m\) divides \(n\)" we mean that \(n = km\) for some integer \(k\).) Determine the truth values of each of these statements:
   a) \(P(4, 5)\)
   b) \(P(2, 4)\)
   c) \(\exists n \forall m P(m, n)\)
   d) \(\exists m \forall n P(m, n)\)
   e) \(\forall m \exists n P(m, n)\)
   f) \(\exists n \forall m P(m, n)\)

22. Find a domain for the quantifiers in \(\exists x \exists y (x \neq y \land \forall z ((z = x) \lor (z = y)))\) such that this statement is true.
23. Find a domain for the quantifiers in \( \exists x \forall y (x \neq y \land y \in \{x \mid x \neq y\}) \) such that this statement is false.

24. Use existential and universal quantifiers to express the statement “No one has more than three grandmothers” using the propositional function \( G(x, y) \), which represents “x is the grandmother of y.”

25. Use existential and universal quantifiers to express the statement “Everyone has exactly two biological parents” using the propositional function \( P(x, y) \), which represents “x is the biological parent of y.”

26. The quantifier \( \exists x \) denotes “there exists exactly one,” so that \( \exists x P(x) \) means there exist exactly \( n \) values in the domain such that \( P(x) \) is true. Determine the true value of these statements where the domain consists of all real numbers.
   a) \( \exists x (x^2 = -1) \)
   b) \( \exists x (x = 0) \)
   c) \( \exists x (x = 2) \)
   d) \( \exists x (x = |x|) \)

27. Express each of these statements using existential and universal quantifiers and propositional logic where \( \exists x \) is defined in Exercise 26.
   a) \( \exists x P(x) \)
   b) \( \exists x P(x) \)
   c) \( \exists x P(x) \)
   d) \( \exists x P(x) \)

28. Let \( P(x,y) \) be a propositional function. Show that \( \exists x \forall y P(x,y) \) is a tautology.

29. Let \( P(x) \) and \( Q(x) \) be propositional functions. Show that \( \exists x (P(x) \land Q(x)) \) and \( \forall x (P(x) \to Q(x)) \) always have the same truth value.

30. If \( \forall x \exists y P(x,y) \) is true, does it necessarily follow that \( \exists x \forall y P(x,y) \) is true?

31. If \( \forall x \exists y P(x,y) \) is true, does it necessarily follow that \( \exists x \forall y P(x,y) \) is true?

32. Find the negations of these statements.
   a) If it snows today, then I will go skiing tomorrow.
   b) Everyone in this class understands mathematical induction.
   c) Some students in this class do not like discrete mathematics.
   d) In every mathematics class there is some student who falls asleep during lectures.

33. Express this statement using quantifiers: “Every student in this class has taken some course in every department in the school of mathematical sciences.”

34. Express this statement using quantifiers: “There is a building on the campus of some college in the United States in which every room is painted white.”

35. Express the statement “There is exactly one student in this class who has taken exactly one mathematics class at this school” using the uniqueness quantifier. Then express this statement using quantifiers, without using the uniqueness quantifier.

36. Describe a rule of inference that can be used to prove that there are exactly two elements \( x \) and \( y \) in a domain such that \( P(x) \) and \( P(y) \) are true. Express this rule of inference as a statement in English.

37. Use rules of inference to show that if the premises \( \forall x (P(x) \to Q(x)) \) and \( \forall x (Q(x) \to R(x)) \) and \( \neg R(a) \), where \( a \) is in the domain, are true, then the conclusion \( \neg P(a) \) is true.

38. Prove that if \( x \) is irrational, then \( x \) is irrational.

39. Prove that if \( x \) is irrational and \( x \geq 0 \), then \( \sqrt{x} \) is irrational.

40. Prove that given a nonnegative integer \( n \), there is a unique nonnegative integer \( m \) such that \( m^2 \leq n < (m+1)^2 \).

41. Prove that there exists an integer \( m \) such that \( m^2 < 10^{100} \). Is your proof constructive or nonconstructive?

42. Prove that there is a positive integer that can be written as the sum of squares of positive integers in two different ways. (Use a computer or calculator to speed up your work.)

43. Disprove the statement that every positive integer is the sum of the cubes of eight nonnegative integers.

44. Disprove the statement that every positive integer is the sum of at most two squares and a cube of nonnegative integers.

45. Disprove the statement that every positive integer is the sum of 36 fifth powers of nonnegative integers.

46. Assuming the truth of the theorem that states that \( \sqrt{2} \) is irrational whenever \( n \) is a positive integer that is not a perfect square, prove that \( \sqrt[3]{2} + \sqrt{3} \) is irrational.

Computer Projects

Write programs with the specified input and output.

1. Given the truth values of the propositions \( p \) and \( q \), find the truth values of the conjunction, disjunction, exclusive or, conditional statement, and biconditional of these propositions.

2. Given two bit strings of length \( n \), find the bitwise AND, OR, and bitwise XOR of these strings.

3. Given a compound proposition, determine whether it is satisfiable by checking its truth value for all positive assignments of truth values to its propositional variables.

4. Given the truth values of the propositions \( p \) and \( q \) in fuzzy logic, find the truth value of the conjunction and the disjunction and \( q \) (see Exercises 46 and 47 of Section 1.1).

5. Given positive integers \( m \) and \( n \), interactively play the game of Chomp.

6. Given a portion of a checkerboard, look for tilings of this checkerboard with various types of polyominoes, including dominoes, the two types of trominoes, and larger polyominoes.
Computations and Explorations

Use a computational program or programs you have written to do these exercises.

1. Look for positive integers that are not the sum of the cubes of nine different positive integers.
2. Look for positive integers greater than 79 that are not the sum of the fourth powers of 18 positive integers.
3. Find as many positive integers as you can that can be written as the sum of cubes of positive integers, in two different ways, sharing this property with 1729.
4. Try to find winning strategies for the game of Chomp for different initial configurations of cookies.
5. Construct the 12 different pentominoes, where a pentomino is a polyomino consisting of five squares.
6. Find all the rectangles of 60 squares that can be tiled using every one of the 12 different pentominoes.

Writing Projects

Respond to these with essays using outside sources.

1. Discuss logical paradoxes, including the paradox of Epimenides the Cretan, Jourdain’s card paradox, and the barber paradox, and how they are resolved.
2. Describe how fuzzy logic is being applied to practical applications. Consult one or more of the recent books on fuzzy logic written for general audiences.
3. Describe some of the practical problems that can be modeled as satisfiability problems.
4. Describe some of the techniques that have been devised to help people solve Sudoku puzzles without the use of a computer.
5. Describe the basic rules of WFF’N PROOF, The Game of Modern Logic, developed by Layman Allen. Give examples of some of the games included in WFF’N PROOF.
6. Read some of the writings of Lewis Carroll on symbolic logic. Describe in detail some of the models he used to represent logical arguments and the rules of inference he used in these arguments.
7. Extend the discussion of Prolog given in Section 1.4, explaining in more depth how Prolog employs resolution.
8. Discuss some of the techniques used in computational logic, including Skolem’s rule.
9. “Automated theorem proving” is the task of using computers to mechanically prove theorems. Discuss the goals and applications of automated theorem proving and the progress made in developing automated theorem provers.
10. Describe how DNA computing has been used to solve instances of the satisfiability problem.
11. Look up some of the incorrect proofs of famous open questions and open questions that were solved since 1970 and describe the type of error made in each proof.
12. Discuss what is known about winning strategies in the game of Chomp.
13. Describe various aspects of proof strategy discussed by George Pólya in his writings on reasoning, including [Po62], [Po71], and [Po90].
14. Describe a few problems and results about tilings with polyominoes, as described in [Go94] and [Ma91], for example.