CHAPTER 1

Logic and Proofs

We recommend that you read the *Preface to the Student* before beginning this first chapter. Most of the terms and concepts in that *Preface* should be familiar to you, but it is well worth making sure you know the terminology and notations we will use throughout the book. It is especially important that you know precisely the definitions of such terms as: "divides," "prime," "rational," and "even" and "odd."

As described in the *Preface*, mathematics is concerned with the formation of a **theory** (collection of true statements) that describes patterns or relationships among quantities and structures. It is characterized by **deductive reasoning**, in which one uses logic to develop and extend a theory by drawing conclusions based on statements accepted as true. We give **proofs** to demonstrate that our conclusions are true. This chapter will provide a working knowledge of the basics of logic and how to construct a proof.

1.1 Propositions and Connectives

Our goal in this section is to understand truth values of propositions and how propositions can be combined using logical connectives.

Most sentences, such as "$\pi > 3$" and "Earth is the closest planet to the sun," have a truth value. That is, they are either true or false. We call these sentences propositions. Other sentences, such as "What time is it?" and "Look out!" are interrogatory or exclamatory; they express complete thoughts but have no truth value.

DEFINITION A **proposition** is a sentence that has exactly one truth value: true, which we denote by T, or false, which we denote by F.

Some propositions, such as "$7^2 = 60$," have easily determined truth values. It will take years to determine the truth value of the proposition "The North Pacific right whale will be an extinct species before the year 2525." Other statements, such as "Euclid was left-handed," are propositions whose truth values may never be known.

Sentences like "She lives in New York City" and "$x^2 = 36$" are not propositions because each could be true or false depending upon the person to whom "she" refers and what numerical value is assigned to x. We will deal with sentences like these in Section 1.3.

The statement "This sentence is false" is not a proposition because it is neither true nor false. It is an example of a **paradox**—a situation in which, from premises that look reasonable, one uses apparently acceptable reasoning to derive a conclusion that seems to be contradictory. If the statement "This sentence is false" is true, then by its meaning it must be false. On the other hand, if the given statement is false, then what it claims is false, so it must be true. The study of paradoxes such as this has played a key role in the development of modern mathematical logic. A famous example of a paradox formulated in 1901 by Bertand Russell* is discussed in Section 2.1.

By applying logical connectives to propositions, we can form new propositions.

DEFINITION The **negation** of a proposition P, denoted $\sim P$, is the proposition "not P." The proposition $\sim P$ is true exactly when P is false.

The truth value of the negation of a proposition is the opposite of the truth value of the proposition. For example, the negation of the false proposition "7 is divisible by 2" is the true statement "It is not the case that 7 is divisible by 2," or "7 is not divisible by 2."

DEFINITIONS Given propositions P and Q, the **conjunction** of P and Q, denoted $P \wedge Q$, is the proposition "P and Q." $P \wedge Q$ is true exactly when *both* P and Q are true.

The **disjunction** of P and Q, denoted $P \vee Q$, is the proposition "P or Q." $P \vee Q$ is true exactly when *at least one* of P or Q is true.

Examples. If C is the proposition "19 is composite" and M is "45 is a multiple of 3," we know C is false and M is true. Thus "19 is composite and 45 is a multiple of 3," written using logical connectives as $C \wedge M$, is a false proposition, while "19 is composite or 45 is a multiple of 3," which has form $C \vee M$, is true. The false proposition "Either 19 is composite or 45 is not a multiple of 3" has the form $C \vee \sim M$.

The English words *but*, *while*, and *although* are usually translated symbolically with the conjunction connective, because they have the same meaning as *and*. For

* Bertrand Russell (1872–1970) was a British philosopher, mathematician, and advocate for social reform. He was a strong voice for precision and clarity of arguments in mathematics and logic. He coauthored *Principia Mathematica* (1910–1913), a monumental effort to derive all of mathematics from a specific set of axioms and well-defined rules of inference.

example, we would write "19 is not composite, but 45 is a multiple of 3" in symbolic form as: $(\sim C) \wedge M$.

An important distinction must be made between a statement and the *form* of a statement. In the previous example "19 is composite and 45 is a multiple of 3" is a proposition with truth value F. We used the form $C \wedge M$ to represent this proposition, but *the form* $C \wedge M$ *itself has no truth value* unless C and M are assigned to be specific propositions. If we let C be "Copenhagen is the capital of Denmark" and M be "Madrid is the capital of Spain," then $C \wedge M$ would have the value T.

To repeat: a propositional form does not have *a* truth value. Instead, each form has a *list* of truth values that depend on the values assigned to its components. This list is displayed by presenting all possible combinations for the truth values of its components in a truth table. Since the connectives $\wedge$ and $\vee$ involve two components, their truth tables must list the four possible combinations of the truth values of those components:

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

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

Since the value of $\sim P$ depends only on the two possible values for P, its truth table is

P	$\sim P$
T	F
F	T

Frequently you will encounter compound propositions formed from more than two propositional variables. The propositional form $(P \wedge Q) \vee \sim R$ has three variables P, Q, and R; it follows that there are $2^3 = 8$ possible combinations of truth values. The two main components are $P \wedge Q$ and $\sim R$. We make truth tables for these and combine them by using the truth table for $\vee$.

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

The statement "Either 7 is prime and 9 is even or else 11 is not less than 3" may be symbolized by $(P \wedge Q) \vee \sim R$, where P is "7 is prime," Q is "9 is even," and R

is "11 is less than 3." We know P is true, Q is false and R is false. Therefore, $(P \wedge Q)$ is false and $\sim R$ is true. Thus $(P \wedge Q) \vee \sim R$ is true, in agreement with line 7 of the table. Thus the proposition "Either 7 is prime and 9 is even or else 11 is not less than 3" is a true statement.

Some compound forms always yield the value true just because of the way they are formed; others are always false.

DEFINITIONS A **tautology** is a propositional form that is true for every assignment of truth values to its components.

A **contradiction** is a propositional form that is false for every assignment of truth values to its components.

For example, the *Law of Excluded Middle*, $P \vee \sim P$, is a tautology because $P \vee \sim P$ is true when P is true and true when P is false. We know that a statement like "The absolute value function is continuous or it is not continuous" must be true because it has the form of the Law of Excluded Middle.

Example. Show that $(P \vee Q) \vee (\sim P \wedge \sim Q)$ is a tautology.

The truth table for this propositional form is

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

Since the last column is all true, $(P \vee Q) \vee (\sim P \wedge \sim Q)$ is a tautology.

Both $\sim(P \vee \sim P)$ and $Q \wedge \sim Q$ are examples of contradictions. The negation of a contradiction is, of course, a tautology.

Writing a proof requires the ability to connect statements so that the truth of any given statement in the proof follows logically from previous statements in the proof, from known results, or from basic assumptions. Particularly important is the ability to recognize or write a statement equivalent to another. Sometimes, it is the *form* of a compound statement that may be used to find a useful equivalent.

DEFINITION Two propositional forms are **equivalent** if and only if they have the same truth tables.

Example. The propositional forms P and $\sim(\sim P)$ are equivalent. The truth tables for these forms may be combined in one table to show that they are the same:

P	$\sim P$	$\sim(\sim P)$
T	F	T
F	T	F

The fact that P and $\sim(\sim P)$ have the same truth value for each line of the truth table means that whatever proposition we choose for P, the truth value of P and $\sim(\sim P)$ are identical.

Some of the most commonly used equivalent forms are presented in the following theorem.

Theorem 1.1.1 For propositions P, Q, and R, the following are equivalent:

(a)	P	and	$\sim(\sim P)$	Double Negation Law
(b)	$P \vee Q$	and	$Q \vee P$	Commutative Laws
(c)	$P \wedge Q$	and	$Q \wedge P$	
(d)	$P \vee (Q \vee R)$	and	$(P \vee Q) \vee R$	Associative Laws
(e)	$P \wedge (Q \wedge R)$	and	$(P \wedge Q) \wedge R$	
(f)	$P \wedge (Q \vee R)$	and	$(P \wedge Q) \vee (P \wedge R)$	Distributive Laws
(g)	$P \vee (Q \wedge R)$	and	$(P \vee Q) \wedge (P \vee R)$	
(h)	$\sim(P \wedge Q)$	and	$\sim P \vee \sim Q$	DeMorgan's* Laws
(i)	$\sim(P \vee Q)$	and	$\sim P \wedge \sim Q$	

Proof.

(a) See the discussion above.

(h) By examining the fourth and seventh columns of their combined truth tables as shown here,

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

we see that the truth tables for $\sim(P \wedge Q)$ and $\sim P \vee \sim Q$ are identical. Thus $\sim(P \wedge Q)$ and $\sim P \vee \sim Q$ are equivalent propositional forms.

Proofs of the remaining parts are left as exercises. ■

In addition to making tables to verify the remaining parts of Theorem 1.1.1, you should also think about why two propositional forms are equivalent by looking

* Augustus DeMorgan (1806–1871) was an English logician and mathematician whose contributions include his notational system for symbolic logic. He also introduced the term "mathematical induction" (see Section 2.4) and developed a rigorous foundation for that proof technique.

at their meanings. For part (h), negation is applied to a conjunction. The form $\sim(P \wedge Q)$ is true precisely when $P \wedge Q$ is false. This happens when one of P or Q is false, or in other words, when one of $\sim P$ or $\sim Q$ is true. Thus, $\sim(P \wedge Q)$ is equivalent to $\sim P \vee \sim Q$. That is, to say "You don't have both P and Q" is the same as saying "You don't have P or you don't have Q."

As an example of how this theorem might be useful in dealing with statements, suppose we are told that the statement "The function f is increasing and concave upward" is false. The statement has the form $P \wedge Q$, where P is the statement "f is increasing" and Q is the statement "f is concave upward." The negation $\sim(P \wedge Q)$ is "It is not the case that f is increasing and f is concave upward." By part (h) above, this is equivalent to $\sim P \vee \sim Q$, which is

> "It is not the case that f is increasing or it is not the case that f is concave upward."

An easier way to say this is

> "f is not increasing or f is not concave upward."

A **denial** of a proposition P is any proposition equivalent to $\sim P$. A proposition has only one negation, $\sim P$, but always has many denials, including $\sim P$, $\sim\sim\sim P$, $\sim\sim\sim\sim\sim P$, etc. DeMorgan's Laws provide others ways to construct useful denials.

Example. A denial of "Either Miss Scarlet is not guilty or the crime did not take place in the ballroom" is "The crime took place in the ballroom and Miss Scarlet is guilty." This can be verified by writing the two propositions symbolically as $(\sim S) \vee (\sim B)$ and $B \wedge S$, respectively, and checking that their truth tables have exactly opposite values. We could also observe that $B \wedge S$ is equivalent to $S \wedge B$ so a denial of $B \wedge S$ is equivalent to $\sim(S \wedge B)$, which we know by DeMorgan's Laws is equivalent to $(\sim S) \vee (\sim B)$.

Example. The statement "Line L_1 has slope 3/5 or line L_2 does not have slope -4" may be symbolized using the form $P \vee \sim Q$, so its negation is $\sim(P \vee \sim Q)$. We can write a simpler denial $(\sim P) \wedge Q$ by applying DeMorgan's Laws and the Double Negation Law. The simplified denial says "Line L_1 does not have slope $3/5$ and line L_2 has slope -4."

Notice that someone might read the negation $\sim(P \vee \sim Q)$ as "It is not the case that L_1 has slope $3/5$ or line L_2 does not have slope -4." This sentence is ambiguous because without some further explanation, it is not clear if the phrase "It is not the case" refers to the entire remainder of the sentence or to just "L_1 has slope $3/5$."

Ambiguities like the one above are sometimes allowable in English but can cause trouble in mathematics. To avoid ambiguities, you should use delimiters, such as parentheses ( ), square brackets [ ], and braces { }.

To avoid writing large numbers of delimiters, we use the following rules, which we refer to as the *hierarchy of connectives*.

> First, $\sim$ always is applied to the smallest proposition following it.
> Then, $\wedge$ always connects the smallest propositions surrounding it.
> Finally, $\vee$ connects the smallest propositions surrounding it.

Thus, $\sim P \vee Q$ is an abbreviation for $(\sim P) \vee Q$, but $\sim(P \vee Q)$ is the only way to write the negation of $P \vee Q$. Here are some other examples:

$P \vee Q \wedge R$ abbreviates $P \vee (Q \wedge R)$.
$P \wedge \sim Q \vee \sim R$ abbreviates $[P \wedge (\sim Q)] \vee (\sim R)$.
$\sim P \vee \sim Q$ abbreviates $(\sim P) \vee (\sim Q)$.
$\sim P \wedge \sim R \vee \sim P \wedge R$ abbreviates $[(\sim P) \wedge (\sim R)] \vee [(\sim P) \wedge R]$.

When the same connective is used several times in succession, parentheses may be omitted. We reinsert parentheses from the left, so that $P \vee Q \vee R$ is really $(P \vee Q) \vee R$. For example, $R \wedge P \wedge \sim P \wedge Q$ abbreviates $[(R \wedge P) \wedge (\sim P)] \wedge Q$, whereas $R \vee P \wedge \sim P \vee Q$, which does not use the same connective consecutively, abbreviates $(R \vee [P \wedge (\sim P)]) \vee Q$. Leaving out parentheses is not required; some propositional forms are much easier to read with a few well-chosen "unnecessary" parentheses.

Exercises 1.1

1. Use your knowledge of number systems to determine whether each is true or false.
- **(a)** 11 is a rational number.
- ★ **(b)** 5π is a rational number.
- **(c)** There are exactly 3 prime numbers between 40 and 50.
- **(d)** There are exactly 5 prime numbers less than 10.
- **(e)** 29 is a composite number.
- **(f)** 0 is a natural number.
- ★ **(g)** $(5 + 2i)(5 - 2i)$ is a real number.
- **(h)** 18 is a multiple of 12.

2. Which of the following are propositions? Give the truth value of each proposition.
- **(a)** What time is dinner?
- **(b)** It is not the case that $5 + \pi$ is not a rational number.
- ★ **(c)** $x/2$ is a rational number.
- **(d)** $2x + 3y$ is a real number.
- **(e)** Either $3 + \pi$ is rational or $3 - \pi$ is rational.
- ★ **(f)** Either 2 is rational and π is irrational, or 2π is rational.
- **(g)** Either 5π is rational and 4.9 is rational, or 3π is rational.
- **(h)** $-\frac{1}{2}$ is rational, and either $3\pi < 10$ or $3\pi > 15$.
- **(i)** It is not the case that 39 is prime, or that 64 is a power of 2.
- **(j)** There are more than three false statements in this book and this statement is one of them.

3. Make truth tables for each of the following propositional forms.
- ★ **(a)** $P \wedge \sim P$.
- **(b)** $P \vee \sim P$.
- ★ **(c)** $P \wedge \sim Q$.
- **(d)** $P \wedge (Q \vee \sim Q)$.
- ★ **(e)** $(P \wedge Q) \vee \sim Q$.
- **(f)** $\sim(P \wedge Q)$.
- **(g)** $(P \vee \sim Q) \wedge R$.
- **(h)** $\sim P \wedge \sim Q$.

★ **(i)** $P \wedge (Q \vee R)$.
(j) $(P \wedge Q) \vee (P \wedge R)$.
(k) $P \wedge P$.
(l) $(P \wedge Q) \vee (R \wedge \sim S)$.

4. If P, Q, and R are true while S and T are false, which of the following are true?
★ **(a)** $Q \wedge (R \wedge S)$.
(b) $Q \vee (R \wedge S)$.
★ **(c)** $(P \vee Q) \wedge (R \vee S)$.
(d) $(\sim P \vee \sim Q) \vee (\sim R \vee \sim S)$.
(e) $\sim P \vee \sim Q$.
★ **(f)** $(\sim Q \vee S) \wedge (Q \vee S)$.
★ **(g)** $(P \vee S) \wedge (P \vee T)$.

5. Use truth tables to prove the remaining parts of Theorem 1.1.1.

6. Which of the following pairs of propositional forms are equivalent?
★ **(a)** $P \wedge P, P$.
(b) $P \vee P, P$.
★ **(c)** $P \wedge Q, Q \wedge P$.
(d) $(\sim P) \vee (\sim Q), \sim(P \vee \sim Q)$.
★ **(e)** $\sim P \wedge \sim Q, \sim(P \wedge \sim Q)$.
(f) $\sim(P \wedge Q), \sim P \wedge \sim Q$.
★ **(g)** $(P \wedge Q) \vee R, P \wedge (Q \vee R)$.
(h) $(P \wedge Q) \vee R, P \vee (Q \wedge R)$.

7. Determine the propositional form and truth value for each of the following:
(a) It is not the case that 2 is odd.
(b) $f(x) = e^x$ is increasing and concave up.
(c) Both 7 and 5 are factors of 70.
(d) Perth or Panama City or Pisa is located in Europe.

8. P, Q, and R are propositional forms, and P is equivalent to Q, and Q is equivalent to R. Prove that
★ **(a)** Q is equivalent to P.
(b) P is equivalent to R.
(c) $\sim Q$ is equivalent to $\sim P$.

9. Use a truth table to determine whether each of the following is a tautology, a contradiction, or neither.
(a) $(P \wedge Q) \vee (\sim P \wedge \sim Q)$.
(b) $\sim(P \wedge \sim P)$.
★ **(c)** $(P \wedge Q) \vee (\sim P \vee \sim Q)$.
(d) $(A \wedge B) \vee (A \wedge \sim B) \vee (\sim A \wedge B) \vee (\sim A \wedge \sim B)$.
(e) $(Q \wedge \sim P) \wedge \sim(P \wedge R)$.
(f) $P \vee [(\sim Q \wedge P) \wedge (R \vee Q)]$.

10. Suppose A is a tautology and B is a contradiction. Are the following tautologies, contradictions, or neither?
★ **(a)** $A \wedge B$.
(b) $A \wedge \sim B$.
★ **(c)** $A \vee B$.
(d) $\sim(\sim A \wedge B)$.

11. Give a useful denial of each statement.
★ **(a)** x is a positive integer. (Assume that x is some fixed integer.)
(b) Cleveland will win the first game or the second game.
★ **(c)** $5 \geq 3$.
(d) 641,371 is a composite integer.
★ **(e)** Roses are red and violets are blue.
(f) T is not bounded or T is compact. (Assume that T is a fixed object.)
(g) M is odd and one-to-one. (Assume that M is some fixed function.)

(h) The function f has positive first and second derivatives at x_0. (Assume that f is a fixed function and x_0 is a fixed real number.)

(i) The function g has a relative maximum at $x = 2$ or $x = 4$ and a relative minimum at $x = 3$. (Assume that g is a fixed function.)

(j) Neither $z < s$ nor $z \leq t$ is true. (Assume that z, s, and t are fixed real numbers.)

(k) R is transitive but not reflexive. (Assume that R is a fixed object.)

12. Restore parentheses to these abbreviated propositional forms.

(a) $\sim\sim P \vee \sim Q \wedge \sim S$.

(b) $Q \wedge \sim S \vee \sim(\sim P \wedge Q)$.

(c) $P \wedge \sim Q \vee \sim P \wedge \sim R \vee \sim P \wedge S$.

(d) $\sim P \vee Q \wedge \sim\sim P \wedge Q \vee R$.

13. Other logical connectives between two propositions P and Q are possible.

(a) The word *or* is used in two different ways in English. We have presented the truth table for $\vee$, the **inclusive or,** whose meaning is "one or the other or both." The **exclusive or,** meaning "one or the other but not both" and denoted $\veebar$, has its uses in English, as in "She will marry Heckle or she will marry Jeckle." The "inclusive or" is much more useful in mathematics and is the accepted meaning unless there is a statement to the contrary.

★ **(i)** Make a truth table for the "exclusive or" connective $\veebar$.

(ii) Show that $A \veebar B$ is equivalent to $(A \vee B) \wedge \sim(A \wedge B)$.

(b) "NAND" and "NOR" circuits are commonly used as a basis for flash memory chips. A NAND B is defined to be the negation of "A and B." A NOR B is defined to be the negation of "A or B."

(i) Write truth tables for NAND and NOR connectives.

(ii) Show that (A NAND B) $\vee$ (A NOR B) is equivalent to (A NAND B).

(iii) Show that (A NAND B) $\wedge$ (A NOR B) is equivalent to (A NOR B).

1.2 Conditionals and Biconditionals

Sentences of the form "If P, then Q" are the most important kind of propositions in mathematics. You have seen many examples of such statements in mathematics courses: from precalculus, "If two lines in a plane have the same slope, then the lines are parallel"; from trigonometry, "If $\sec\theta = \frac{5}{3}$, then $\sin\theta = \frac{4}{5}$."; from calculus, "If f is differentiable at x_0 and $f(x_0)$ is a relative minimum for f, then $f'(x_0) = 0$."

DEFINITIONS For propositions P and Q, the **conditional sentence** $P \Rightarrow Q$ is the proposition "If P, then Q." Proposition P is called the **antecedent** and Q is the **consequent.** The conditional sentence $P \Rightarrow Q$ is true if and only if P is false or Q is true.

The truth table for $P \Rightarrow Q$ is

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

According to this table, there is only one way that $P \Rightarrow Q$ can be false: when P is true and Q is false. Thus, this truth table agrees with the way we understand promises: the only situation where a promise is broken is when the antecedent is true but the person making the promise fails to make the consequent true.

Example. Suppose someone says to a friend "If the concert is sold out, I'll take you sailing." This promise is broken (the conditional sentence is false) only when the concert was sold out (the antecedent is true) and the person who made the promise did not take the other person sailing (the consequent is false). This is line 3 of the truth table. In all other situations, the promise is true. If there were tickets left (lines 2 and 4 of the table), we don't say the promise was broken, regardless of whether the friends decided to go sailing. The promise is also kept in the situation where the concert is sold out and the friends went sailing, which is line 1 of the table.

One curious consequence of the truth table for $P \Rightarrow Q$ is that a conditional sentence may be true even when there is no connection between the antecedent and the consequent. The reason for this is that the truth value of $P \Rightarrow Q$ depends *only* on the truth value of components P and Q, not on their interpretation. For this reason all of the following are true:

"If $\sin \pi = 1$, then 6 is prime." (line 4 of the truth table)
"$13 > 7 \Rightarrow 2 + 3 = 5$." (line 1 of the truth table)
"$\pi = 3 \Rightarrow$ Paris is the capital of France." (line 2 of the truth table)

and both of these are false by line 3 of the truth table:

"If Saturn has rings, then $(2 + 3)^2 = 2^2 + 3^2$."
"If $4\pi > 10$, then 1 is a prime number."

Other consequences of the truth table for $P \Rightarrow Q$ are worth noting. When P is false, it doesn't matter what truth value Q has: $P \Rightarrow Q$ will be true by lines 2 and 4. When Q is true, it doesn't matter what truth value P has: $P \Rightarrow Q$ will be true by lines 1 and 2. Finally, when P and $P \Rightarrow Q$ are both true (on line 1), Q must also be true.

Example. Both propositions

"If Isaac Newton was born in 1642, then $3 \cdot 5 = 15$"
"If Isaac Newton was born in 1643, then $3 \cdot 5 = 15$"

are true because the consequent "$3 \cdot 5 = 15$" is true.

Our truth table definition for $P \Rightarrow Q$ captures the same meaning for "If ..., then ..." that you have always used in mathematics. For example, if we think of x as some fixed real number, we all know that

"If $x > 8$, then $x > 5$"

is a true statement, no matter what number x we have in mind. Let's examine why we say this sentence is true for some specific values of x, where the antecedent P is "$x > 8$" and the consequent Q is "$x > 5$."

In the case $x = 11$, both P and Q are true, as in line 1 of the truth table. The case $x = 7$ corresponds to the second line of the table, and for $x = 3$ we have the situation in line 4. There is no case corresponding to line 3 because $P \Rightarrow Q$ is true. Note that when we say "If P, then Q" is true, we don't claim that either P or Q is true. What we do say is that no matter what number we think of, *if* it's larger than 8, it's also larger than 5.

Two propositions closely related to $P \Rightarrow Q$ are its converse and contrapositive.

DEFINITION Let P and Q be propositions.

The **converse** of $P \Rightarrow Q$ is $Q \Rightarrow P$.
The **contrapositive** of $P \Rightarrow Q$ is $(\sim Q) \Rightarrow (\sim P)$.

For the conditional sentence "If π is an integer, then 14 is even," the converse of the sentence is "If 14 is even, then π is an integer" and the contrapositive is "If 14 is not even, then π is not an integer." The converse is false, but the sentence and its contrapositive are true.

For the sentence "If $1 + 1 = 2$, then $\sqrt{10} > 3$," the converse and contrapositive are, respectively, "If $\sqrt{10} > 3$, then $1 + 1 = 2$" and "If $\sqrt{10}$ is not greater than 3, then $1 + 1$ is not equal to 2." In this example, all three sentences are true.

The previous two examples suggest that the truth values of a conditional sentence and its contrapositive are related, but there seems to be little connection between the truth values of $P \Rightarrow Q$ and its converse. We describe the relationships in the following theorem.

Theorem 1.2.1 For propositions P and Q,

(a) $P \Rightarrow Q$ is equivalent to its contrapositive $(\sim Q) \Rightarrow (\sim P)$.
(b) $P \Rightarrow Q$ is *not* equivalent to its converse $Q \Rightarrow P$.

Proof. The proofs are carried out by examination of the truth tables.

P	Q	$P \Rightarrow Q$	$\sim P$	$\sim Q$	$(\sim Q) \Rightarrow (\sim P)$	$Q \Rightarrow P$
T	T	T	F	F	T	T
F	T	T	T	F	T	F
T	F	F	F	T	F	T
F	F	T	T	T	T	T

(a) $P \Rightarrow Q$ is equivalent to $(\sim Q) \Rightarrow (\sim P)$ because the third column in the truth table is identical to the sixth column in the table.

(b) $P \Rightarrow Q$ is not equivalent to $Q \Rightarrow P$ because column 3 in the truth table differs from column 7 in rows 2 and 3. ■

We have seen cases where a conditional sentence and its converse have the same truth value. Theorem 1.2.1(b) simply says that this need not always be the case—the truth values of $P \Rightarrow Q$ cannot be inferred from its converse $Q \Rightarrow P$.

The next connective we need is the biconditional connective $\Leftrightarrow$. The double arrow $\Leftrightarrow$ reminds one of both $\Leftarrow$ and $\Rightarrow$, and this is no accident, because $P \Leftrightarrow Q$ is equivalent to $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$.

DEFINITION For propositions P and Q, the **biconditional sentence** $P \Leftrightarrow Q$ is the proposition "P if and only if Q." $P \Leftrightarrow Q$ is true exactly when P and Q have the same truth values. We also write P iff Q to abbreviate P if and only if Q.

The truth table for $P \Leftrightarrow Q$ is

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

Examples. The proposition "$2^3 = 8$ iff 49 is a perfect square" is true because both components are true. The proposition "$\pi = 22/7$ iff $\sqrt{2}$ is a rational number" is true because both components are false. The proposition "$6 + 1 = 7$ iff Lake Michigan is in Kansas" is false because the truth values of the components differ.

Definitions, fully stated with the "if and only if" connective, are important examples of biconditional sentences because they describe exactly the condition(s) to meet the definition. Although sometimes a definition does not explicitly use the iff wording, biconditionality does provide a good test of whether a statement could serve as a definition or just a description.

Example. The statement "Vertical lines have undefined slope" could be used as a definition because a line is vertical iff its slope is undefined. However, "A zebra is a striped animal" is not a definition, because the sentence "An animal is a zebra iff the animal is striped" is false.

Because the biconditional sentence $P \Leftrightarrow Q$ is true exactly when the truth values of P and Q agree, we can use the biconditional connective to restate the meaning of equivalent propositional forms:

The propositional forms P and Q are equivalent precisely when $P \Leftrightarrow Q$ is a tautology.

Thus each statement in Theorem 1.1.1 may be restated using the $\Leftrightarrow$ connective. For example, DeMorgan's Laws are:

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

All of the statements in Theorem 1.1.1 are used regularly in proofs. The next theorem contains several additional important pairs of equivalent propositional forms that involve implication. They, too, will be used often.

Theorem 1.2.2 For propositions P, Q, and R,

(a) $P \Rightarrow Q$ is equivalent to $\sim P \vee Q$.
(b) $P \Leftrightarrow Q$ is equivalent to $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$.
(c) $\sim(P \Rightarrow Q)$ is equivalent to $P \wedge \sim Q$.
(d) $\sim(P \wedge Q)$ is equivalent to $P \Rightarrow \sim Q$ and to $Q \Rightarrow \sim P$.
(e) $P \Rightarrow (Q \Rightarrow R)$ is equivalent to $(P \wedge Q) \Rightarrow R$.
(f) $P \Rightarrow (Q \wedge R)$ is equivalent to $(P \Rightarrow Q) \wedge (P \Rightarrow R)$.
(g) $(P \vee Q) \Rightarrow R$ is equivalent to $(P \Rightarrow R) \wedge (Q \Rightarrow R)$.

Exercise 8 asks you to prove each part of Theorem 1.2.2. The natural way to proceed is by constructing and then comparing truth tables, but you should also think about the meaning of both sides of each statement of equivalence. With part (a), for example, we reason as follows: $P \Rightarrow Q$ is false exactly when P is true and Q is false, which happens exactly when both $\sim P$ and Q are false. Since this happens exactly when $\sim P \vee Q$ is false, the truth tables for $P \Rightarrow Q$ and $\sim P \vee Q$ are identical.

Note that many of the statements in Theorems 1.1.1 and 1.2.2 are related. For example, once we have established Theorem 1.1.1 and 1.2.2(a), we reason that part (c) is correct as follows:

$\sim(P \Rightarrow Q)$ is equivalent, by part (a), to
$\sim(\sim P \vee Q)$, which is equivalent, by Theorem 1.1.1(i), to
$\sim(\sim P) \wedge \sim Q$, which is equivalent, by Theorem 1.1.1(a), to
$P \wedge \sim Q$.

Recognizing the structure of a sentence and translating the sentence into symbolic form using logical connectives are aids in determining its truth or falsity. The translation of sentences into propositional symbols is sometimes very complicated because some natural languages such as English are rich and powerful with many nuances. The ambiguities that we tolerate in English would destroy structure and usefulness if we allowed them in mathematics.

Even the translations of simple sentences can present special problems. Suppose a teacher says to a student

"If you score 74% or higher on the next test, you will pass this course."

This sentence clearly has the form of a conditional sentence, although almost everyone will interpret the meaning as a biconditional.

Contrast this with the situation in mathematics where "If $x = 2$, then x is a solution to $x^2 = 2x$" must have only the meaning of the connective $\Rightarrow$, because $x^2 = 2x$ does not imply $x = 2$.

Shown below are some phrases in English that are ordinarily translated by using the connectives $\Rightarrow$ or $\Leftrightarrow$. In the accompanying examples, think of a and t as fixed real numbers.

Use $P \Rightarrow Q$ to translate:	Examples:
If P, then Q.	If $a > 5$, then $a > 3$.
P implies Q.	$a > 5$ implies $a > 3$.
P is sufficient for Q.	$a > 5$ is sufficient for $a > 3$.
P only if Q.	$a > 5$ only if $a > 3$.
Q, if P.	$a > 3$, if $a > 5$.
Q whenever P.	$a > 3$ whenever $a > 5$.
Q is necessary for P.	$a > 3$ is necessary for $a > 5$.
Q, when P.	$a > 3$, when $a > 5$.

Use $P \Leftrightarrow Q$ to translate:	Examples:
P if and only if Q.	$\lvert t \rvert = 2$ if and only if $t^2 = 4$.
P if, but only if, Q.	$\lvert t \rvert = 2$ if, but only if, $t^2 = 4$.
P is equivalent to Q.	$\lvert t \rvert = 2$ is equivalent to $t^2 = 4$.
P is necessary and sufficient for Q.	$\lvert t \rvert = 2$ is necessary and sufficient for $t^2 = 4$.

The word *unless* is one of those connective words in English that poses special problems because it has so many different interpretations. See Exercise 11.

Examples. In these sentence translations, we assume that S, G, and e have been specified. It is not necessary to know the meanings of all the words because the form of the sentence is sufficient to determine the correct translation.

"S is compact is sufficient for S to be bounded" is translated

$$S \text{ is compact} \Rightarrow S \text{ is bounded.}$$

"A necessary condition for a group G to be cyclic is that G is abelian" is translated

$$G \text{ is cyclic} \Rightarrow G \text{ is abelian.}$$

"A set S is infinite if S has an uncountable subset" is translated

$$S \text{ has an uncountable subset} \Rightarrow S \text{ is infinite.}$$

"A necessary and sufficient condition for the graph G to be a tree is that G is connected and every edge of G is a bridge" is translated

$$G \text{ is a tree} \Leftrightarrow (G \text{ is connected} \wedge \text{every edge of } G \text{ is a bridge}).$$

Example. If we let P denote the proposition "Roses are red" and Q denote the proposition "Violets are blue," we can translate the sentence "It is not the case that roses are red, nor that violets are blue" in at least two ways: $\sim(P \vee Q)$ or $(\sim P) \wedge (\sim Q)$. Fortunately, these are equivalent by Theorem 1.1.1(h). Note that the proposition "Violets are purple" requires a new symbol, say R, since it expresses a new idea that cannot be formed from the components P and Q.

The sentence "17 and 35 have no common divisors" shows that the meaning, and not just the form of the sentence, must be considered in translating; it cannot be broken up into the two propositions: "17 has no common divisors" and "35 has no common divisors." Compare this with the proposition "17 and 35 have digits totaling 8," which can be written as a conjunction.

Example. Suppose b is a fixed real number. The form of the sentence "If b is an integer, then b is either even or odd" is $P \Rightarrow (Q \vee R)$, where P is "b is an integer," Q is "b is even," and R is "b is odd."

Example. Suppose a, b, and p are fixed integers. "If p is a prime number that divides ab, then p divides a or b" has the form $(P \wedge Q) \Rightarrow (R \vee S)$, where P is "p is a prime," Q is "p divides ab," R is "p divides a," and S is "p divides b."

The hierarchy of connectives in Section 1.1 that governs the use of parentheses for propositional forms can be extended to the connectives $\Rightarrow$ and $\Leftrightarrow$:

The connectives $\sim$, $\wedge$, $\vee$, $\Rightarrow$, and $\Leftrightarrow$ are always applied in the order listed.

Thus, $\sim$ applies to the smallest possible proposition, then $\wedge$ is applied with the next smallest scope, and so forth. For example,

$$P \Rightarrow \sim Q \vee R \Leftrightarrow S \text{ is an abbreviation for } (P \Rightarrow [(\sim Q) \vee R]) \Leftrightarrow S,$$
$$P \vee \sim Q \Leftrightarrow R \Rightarrow S \text{ is an abbreviation for } [P \vee (\sim Q)] \Leftrightarrow (R \Rightarrow S),$$

and

$$P \Rightarrow Q \Rightarrow R \text{ is an abbreviation for } (P \Rightarrow Q) \Rightarrow R.$$

Exercises 1.2

1. Identify the antecedent and the consequent for each of the following conditional sentences. Assume that a, b, and f represent some fixed sequence, integer, or function, respectively.
   - ★ **(a)** If squares have three sides, then triangles have four sides.
   - **(b)** If the moon is made of cheese, then 8 is an irrational number.
   - **(c)** b divides 3 only if b divides 9.
   - ★ **(d)** The differentiability of f is sufficient for f to be continuous.
   - **(e)** A sequence a is bounded whenever a is convergent.
   - ★ **(f)** A function f is bounded if f is integrable.
   - **(g)** $1 + 2 = 3$ is necessary for $1 + 1 = 2$.

(h) The fish bite only when the moon is full.

★ **(i)** A time of 3 minutes, 48 seconds or less is necessary to qualify for the Olympic team.

☆ **2.** Write the converse and contrapositive of each conditional sentence in Exercise 1.

3. What can be said about the truth value of Q when

(a) P is false and $P \Rightarrow Q$ is true? **(b)** P is true and $P \Rightarrow Q$ is true?
(c) P is true and $P \Rightarrow Q$ is false? **(d)** P is false and $P \Leftrightarrow Q$ is true?
(e) P is true and $P \Leftrightarrow Q$ is false?

4. Identify the antecedent and consequent for each conditional sentence in the following statements from this book.

(a) Theorem 1.3.1(a) **(b)** Exercise 3 of Section 1.6
(c) Theorem 2.1.4 **(d)** The PMI, Section 2.4
(e) Theorem 2.6.4 **(f)** Theorem 3.4.2
(g) Theorem 4.2.2 **(h)** Theorem 5.1.7(a)

5. Which of the following conditional sentences are true?

★ **(a)** If triangles have three sides, then squares have four sides.
(b) If a hexagon has six sides, then the moon is made of cheese.
★ **(c)** If $7 + 6 = 14$, then $5 + 5 = 10$.
(d) If $5 < 2$, then $10 < 7$.
★ **(e)** If one interior angle of a right triangle is 92°, then the other interior angle is 88°.
(f) If Euclid's birthday was April 2, then rectangles have four sides.
(g) 5 is prime if $\sqrt{2}$ is not irrational.
(h) $1 + 1 = 2$ is sufficient for $3 > 6$.

6. Which of the following are true?

★ **(a)** Triangles have three sides iff squares have four sides.
(b) $7 + 5 = 12$ iff $1 + 1 = 2$.
★ **(c)** b is even iff $b + 1$ is odd. (Assume that b is some fixed integer.)
(d) m is odd iff m^2 is odd. (Assume that m is some fixed integer.)
(e) $5 + 6 = 6 + 5$ iff $7 + 1 = 10$.
(f) A parallelogram has three sides iff 27 is prime.
(g) The Eiffel Tower is in Paris if and only if the chemical symbol for helium is H.
(h) $\sqrt{10} + \sqrt{13} < \sqrt{11} + \sqrt{12}$ iff $\sqrt{13} - \sqrt{12} < \sqrt{11} - \sqrt{10}$.
(i) $x^2 \geq 0$ iff $x \geq 0$. (Assume that x is a fixed real number.)
(j) $x^2 - y^2 = 0$ iff $(x - y)(x + y) = 0$. (Assume that x and y are fixed real numbers.)
(k) $x^2 + y^2 = 50$ iff $(x + y)^2 = 50$. (Assume that x and y are fixed real numbers.)

7. Make truth tables for these propositional forms.

(a) $P \Rightarrow (Q \wedge P)$. ★ **(b)** $({\sim}P \Rightarrow Q) \vee (Q \Leftrightarrow P)$.
★ **(c)** ${\sim}Q \Rightarrow (Q \Leftrightarrow P)$. **(d)** $(P \vee Q) \Rightarrow (P \wedge Q)$.
(e) $(P \wedge Q) \vee (Q \wedge R) \Rightarrow P \vee R$.
(f) $[(Q \Rightarrow S) \wedge (Q \Rightarrow R)] \Rightarrow [(P \vee Q) \Rightarrow (S \vee R)]$.

8. Prove Theorem 1.2.2 by constructing truth tables for each equivalence.

9. Determine whether each statement qualifies as a definition.

(a) $y = f(x)$ is a linear function when its graph is a straight line.
(b) $y = f(x)$ is a quadratic function when it contains an x^2 term.
(c) m is a perfect square when $m = n^2$ for some integer n.
(d) A triangle is a right triangle when the sum of two of its interior angles is 90°.
(e) Two lines are parallel when their slopes are the same number.
(f) A sundial is an instrument for measuring time.

10. Rewrite each of the following sentences using logical connectives. Assume that each symbol $f, x_0, n, x, S, \mathbf{B}$ represents some fixed object.

★ **(a)** If f has a relative minimum at x_0 and if f is differentiable at x_0, then $f'(x_0) = 0$.
(b) If n is prime, then $n = 2$ or n is odd.
(c) A number x is real and not rational whenever x is irrational.
★ **(d)** If $x = 1$ or $x = -1$, then $|x| = 1$.
★ **(e)** f has a critical point at x_0 iff $f'(x_0) = 0$ or $f'(x_0)$ does not exist.
(f) S is compact iff S is closed and bounded.
(g) $\mathbf{B}$ is invertible is a necessary and sufficient condition for det $\mathbf{B} \neq 0$.
(h) $6 \geq n - 3$ only if $n > 4$ or $n > 10$.
(i) x is Cauchy implies x is convergent.
(j) f is continuous at x_0 whenever $\lim_{x \to x_0} f(x) = f(x_0)$.
(k) If f is differentiable at x_0 and f is strictly increasing at x_0, then $f'(x_0) > 0$.

11. Dictionaries indicate that the conditional meaning of *unless* is preferred, but there are other interpretations as a converse or a biconditional. Discuss the translation of each sentence.

(a) I will go to the store unless it is raining.
★ **(b)** The Dolphins will not make the playoffs unless the Bears win all the rest of their games.
(c) You cannot go to the game unless you do your homework first.
(d) You won't win the lottery unless you buy a ticket.

12. Show that the following pairs of statements are equivalent.

(a) $(P \vee Q) \Rightarrow R$ and $\sim R \Rightarrow (\sim P \wedge \sim Q)$.
★ **(b)** $(P \wedge Q) \Rightarrow R$ and $(P \wedge \sim R) \Rightarrow \sim Q$.
(c) $P \Rightarrow (Q \wedge R)$ and $(\sim Q \vee \sim R) \Rightarrow \sim P$.
(d) $P \Rightarrow (Q \vee R)$ and $(P \wedge \sim R) \Rightarrow Q$.
(e) $(P \Rightarrow Q) \Rightarrow R$ and $(P \wedge \sim Q) \vee R$.
(f) $P \Leftrightarrow Q$ and $(\sim P \vee Q) \wedge (\sim Q \vee P)$.

13. Give, if possible, an example of a true conditional sentence for which

★ **(a)** the converse is true. **(b)** the converse is false.
★ **(c)** the contrapositive is false. **(d)** the contrapositive is true.

14. Give, if possible, an example of a false conditional sentence for which

(a) the converse is true. **(b)** the converse is false.
(c) the contrapositive is false. **(d)** the contrapositive is true.

15. Give the converse and contrapositive of each sentence of Exercises 10(a), (b), (c), and (d). Tell whether each converse and contrapositive is true or false.

16. Determine whether each of the following is a tautology, a contradiction, or neither.

★ **(a)** $[(P \Rightarrow Q) \Rightarrow P] \Rightarrow P$.
(b) $P \Leftrightarrow P \wedge (P \vee Q)$.
(c) $P \Rightarrow Q \Leftrightarrow P \wedge \sim Q$.
★ **(d)** $P \Rightarrow [P \Rightarrow (P \Rightarrow Q)]$.
(e) $P \wedge (Q \vee \sim Q) \Leftrightarrow P$.
(f) $[Q \wedge (P \Rightarrow Q)] \Rightarrow P$.
(g) $(P \Leftrightarrow Q) \Leftrightarrow \sim(\sim P \vee Q) \vee (\sim P \wedge Q)$.
(h) $[P \Rightarrow (Q \vee R)] \Rightarrow [(Q \Rightarrow R) \vee (R \Rightarrow P)]$.
(i) $P \wedge (P \Leftrightarrow Q) \wedge \sim Q$.
(j) $(P \vee Q) \Rightarrow Q \Rightarrow P$.
(k) $[P \Rightarrow (Q \wedge R)] \Rightarrow [R \Rightarrow (P \Rightarrow Q)]$.
(l) $[P \Rightarrow (Q \wedge R)] \Rightarrow R \Rightarrow (P \Rightarrow Q)$.

17. The **inverse,** or **opposite,** of the conditional sentence $P \Rightarrow Q$ is $\sim P \Rightarrow \sim Q$.

(a) Show that $P \Rightarrow Q$ and its inverse are not equivalent forms.
(b) For what values of the propositions P and Q are $P \Rightarrow Q$ and its inverse both true?
(c) Which is equivalent to the converse of a conditional sentence, the contrapositive of its inverse, or the inverse of its contrapositive?

1.3 Quantifiers

Unless there has been a prior agreement about the value of x, the statement "$x \geq 3$" is neither true nor false. A sentence that contains variables is called an **open sentence** or **predicate**, and becomes a proposition only when its variables are assigned specific values. For example, "$x \geq 3$" is true when x is given the value 7 and false when $x = 2$.

When P is an open sentence with a variable x, the sentence is symbolized by $P(x)$. Likewise, if P has variables $x_1, x_2, x_3, \ldots, x_n$, the sentence may be denoted by $P(x_1, x_2, x_3, \ldots, x_n)$. For example, for the sentence "$x + y = 3z$" we write $P(x, y, z)$, and we see that $P(4, 5, 3)$ is true because $4 + 5 = 3(3)$, while $P(1, 2, 4)$ is false.

The collection of objects that may be substituted to make an open sentence a true proposition is called the **truth set** of the sentence. Before a truth set can be determined, we must be given or must decide what objects are available for consideration; that is, we must have specified a **universe of discourse.** In many cases the universe will be understood from the context. For a sentence such as "x likes chocolate," the universe is presumably the set of all people. We will often use the number systems $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ as our universes. (See the *Preface to the Student*.)

Example. The truth set of the open sentence "$x^2 < 5$" depends upon the collection of objects we choose for the universe of discourse. With the universe specified as the set $\mathbb{N}$, the truth set is $\{1, 2\}$. For the universe $\mathbb{Z}$, the truth set is $\{-2, -1, 0, 1, 2\}$. When the universe is $\mathbb{R}$, the truth set is the open interval $(-\sqrt{5}, \sqrt{5})$.

> **DEFINITION** With a universe specified, two open sentences $P(x)$ and $Q(x)$ are **equivalent** iff they have the same truth set.

Examples. The sentences "$3x + 2 = 20$" and "$x = 6$" are equivalent open sentences in any of the number systems we have named. On the other hand, "$x^2 = 4$" and "$x = 2$" are *not* equivalent when the universe is $\mathbb{R}$. They *are* equivalent when the universe is $\mathbb{N}$.

The notions of truth set, universe, and equivalent open sentences should not be new concepts for you. Solving an equation such as $(x^2 + 1)(x - 3) = 0$ is a matter of determining what objects x make the open sentence "$(x^2 + 1)(x - 3) = 0$" true. For the universe $\mathbb{R}$, the only solution is $x = 3$ and thus the truth set is $\{3\}$. But if we choose the universe to be $\mathbb{C}$, the equation may be replaced by the equivalent open sentence $(x + i)(x - i)(x - 3) = 0$, which has truth set (solutions) $\{3, i, -i\}$.

A sentence such as

"There is a prime number between 5060 and 5090"

is treated differently from the propositions we considered earlier. To determine whether this sentence is true in the universe $\mathbb{N}$, we might try to individually examine every natural number, checking whether it is a prime and between 5060 and 5090, until we eventually find any *one* of the primes 5077, 5081, or 5087 and conclude that the sentence is true. (A quicker way is to search through a complete list of the first thousand primes.) The key idea here is that although the open sentence "x is a prime number between 5060 and 5090" is not a proposition, the sentence

"There is a number x such that x is a prime number between 5060 and 5090"

does have a truth value. This sentence is formed from the original open sentence by applying a quantifier.

> **DEFINITION** For an open sentence $P(x)$, the sentence $(\exists x)P(x)$ is read "There exists x such that $P(x)$" or "For some x, $P(x)$." The sentence $(\exists x)P(x)$ is true iff the truth set of $P(x)$ is nonempty. The symbol $\exists$ is called the **existential quantifier**.

An open sentence $P(x)$ does not have a truth value, but the quantified sentence $(\exists x)P(x)$ does. One way to show that $(\exists x)P(x)$ is true for a particular universe is to identify an object a in the universe such that the proposition $P(a)$ is true. To show $(\exists x)P(x)$ is false, we must show that the truth set of $P(x)$ is empty.

Examples. Let's examine the truth values of these statements for the universe $\mathbb{R}$:

(a) $(\exists x)(x \geq 3)$
(b) $(\exists x)(x^2 = 0)$
(c) $(\exists x)(x^2 = -1)$

Statement (a) is true because the truth set of $x \geq 3$ contains 3, 7.02, and many other real numbers. Thus the truth set contains at least one real number. Statement (b) is true because the truth set of $x^2 = 0$ is precisely $\{0\}$ and thus is nonempty. Since the open sentence $x^2 = -1$ is never true for real numbers, the truth set of $x^2 = -1$ is empty. Statement (c) is false.

In the universe $\mathbb{N}$, only statement (a) is true. The three statements are all true in the universe $\{0, 5, i\}$ and all three statements are false in the universe $\{1, 2\}$.

Sometimes we can say $(\exists x) P(x)$ is true even when we do not know a specific object in the universe in the truth set of $P(x)$, only that there (at least) is one.

Example. Show that $(\exists x)(x^7 - 12x^3 + 16x - 3 = 0)$ is true in the universe of real numbers.

For the polynomial $f(x) = x^7 - 12x^3 + 16x - 3$, $f(0) = -3$ and $f(1) = 2$. From calculus, we know that f is continuous on $[0, 1]$. The Intermediate Value Theorem tells us there is a zero for f between 0 and 1. Even if we don't know the exact value of the zero, we know it exists. Therefore, the truth set of $x^7 - 12x^3 + 16x - 3 = 0$ is nonempty. Hence $(\exists x)(x^7 - 12x^3 + 16x - 3 = 0)$ is true.

The sentence "The square of every number is greater than 3" uses a different quantifier for the open sentence "$x^2 > 3$." To decide the truth value of the given sentence in the universe $\mathbb{N}$ it is not enough to observe that $3^2 > 3$, $4^2 > 3$, and so on. In fact, the sentence is false in $\mathbb{N}$ because 1 is in the universe but not in the truth set. The sentence is true, however, in the universe $[1.74, \infty)$ because with this universe the truth set for $x^2 > 3$ is the same as the universe.

DEFINITION For an open sentence $P(x)$, the sentence $(\forall x) P(x)$ is read "For all x, $P(x)$" and is true iff the truth set of $P(x)$ is the *entire* universe. The symbol $\forall$ is called the **universal quantifier**.

Examples. For the universe of all real numbers,

$(\forall x)(x + 2 > x)$ is true.
$(\forall x)(x > 0 \vee x = 0 \vee x < 0)$ is true. That is, every real number is positive, zero or negative.
$(\forall x)(x \geq 3)$ is false because there are (many) real numbers x for which $x \geq 3$ is false.
$(\forall x)(|x| > 0)$ is false, because 0 is not in the truth set.

There are many ways to express a quantified sentence in English. Look for key words such as "for all," "for every," "for each," or similar words that require universal quantifiers. Look for phrases such as "some," "at least one," "there exist(s)," "there is (are)," and others that indicate existential quantifiers.

You should also be alert for hidden quantifiers because natural languages allow for imprecise quantified statements where the words "for all" and "there exists" are not present. Someone who says "Polynomial functions are continuous" means that "All polynomial functions are continuous," but someone who says "Rational functions have vertical asymptotes" must mean "Some rational functions have vertical asymptotes."

We agree that "All apples have spots" is quantified with $\forall$, but what form does it have? If we limit the universe to just apples, a correct symbolization would be $(\forall x)(x \text{ has spots})$. But if the universe is all fruits, we need to be more careful. Let $A(x)$ be "x is an apple" and $S(x)$ be "x has spots." Should we write the sentence as $(\forall x)[A(x) \wedge S(x)]$ or $(\forall x)[A(x) \Rightarrow S(x)]$?

The first quantified form, $(\forall x)[A(x) \wedge S(x)]$, says "For all objects x in the universe, x is an apple and x has spots." Since we don't really intend to say that all fruits are spotted apples, this is not the meaning we want. Our other choice, $(\forall x)[A(x) \Rightarrow S(x)]$, is the correct one because it says "For all objects x in the universe, if x is an apple then x has spots." In other words, "If a fruit is an apple, then it has spots."

Now consider "Some apples have spots." Should this be $(\exists x)[A(x) \wedge S(x)]$ or $(\exists x)[A(x) \Rightarrow S(x)]$? The first form says "There is an object x such that it is an apple and it has spots," which is correct. On the other hand, $(\exists x)[A(x) \Rightarrow S(x)]$ reads "There is an object x such that, if it is an apple, then it has spots," which does *not* ensure the existence of apples with spots. The sentence $(\exists x)[A(x) \Rightarrow S(x)]$ is true in every universe for which there is an object x such that either x is not an apple or x has spots, which is not the meaning we want.

In general, a sentence of the form "All $P(x)$ are $Q(x)$" should be symbolized $(\forall x)[P(x) \Rightarrow Q(x)]$. And, *in general,* a sentence of the form "Some $P(x)$ are $Q(x)$" should be symbolized $(\exists x)[P(x) \wedge Q(x)]$.

Examples. The sentence "For every odd prime x less than 10, $x^2 + 4$ is prime" means that if x is prime, and odd, and less than 10, then $x^2 + 4$ is prime. It is written symbolically as

$$(\forall x)(x \text{ is prime } \wedge\ x \text{ is odd} \wedge x < 10 \Rightarrow x^2 + 4 \text{ is prime}).$$

The sentence "Some functions defined at 0 are not continuous at 0" can be written symbolically as $(\exists f)(f \text{ is defined at } 0 \wedge f \text{ is not continuous at } 0)$.

Example. The sentence "Some real numbers have a multiplicative inverse" could be symbolized

$$(\exists x)(x \text{ is a real number} \wedge x \text{ has a real multiplicative inverse}).$$

However, "x has an inverse" means there is some number that is an inverse for x (hidden quantifier), so a more complete symbolic translation is

$$(\exists x)[x \text{ is a real number} \wedge (\exists y)(y \text{ is a real number} \wedge xy = 1)].$$

Example. One correct translation of "Some integers are even and some integers are odd" is

$$(\exists x)(x \text{ is even}) \wedge (\exists x)(x \text{ is odd})$$

because the first quantifier $(\exists x)$ extends only as far as the word "even." After that, any variable (even x again) may be used to express "some are odd." It would be equally correct and sometimes preferable to write

$$(\exists x)(x \text{ is even}) \wedge (\exists y)(y \text{ is odd}),$$

but it would be wrong to write

$$(\exists x)(x \text{ is even} \wedge x \text{ is odd}),$$

because there is no integer that is both even and odd.

Several of our essential definitions given in the *Preface to the Student* are in fact quantified statements. For example, the definition of a rational number may be symbolized:

$$r \text{ is a rational number iff } (\exists p)(\exists q)\left(p \in \mathbb{Z} \wedge q \in \mathbb{Z} \ \wedge q \neq 0 \wedge r = \frac{p}{q}\right)$$

Statements of the form "Every element of the set A has the property P" and "Some element of the set A has property P" occur so frequently that abbreviated symbolic forms are desirable. "Every element of the set A has the property P" could be restated as "If $x \in A$, then . . ." and symbolized by

$$(\forall x \in A)\, P(x).$$

"Some element of the set A has property P" is abbreviated by

$$(\exists x \in A)\, P(x).$$

Examples. The definition of a rational number given above may be written as

$$r \text{ is a rational number iff } (\exists p \in \mathbb{Z})(\exists q \in \mathbb{Z})\left(q \neq 0 \wedge r = \frac{p}{q}\right).$$

The statement "For every rational number there is a larger integer" may be symbolized by

$$(\forall x)[x \in \mathbb{Q} \Rightarrow (\exists z)(z \in \mathbb{Z} \text{ and } z > x)]$$

or

$$(\forall x \in \mathbb{Q})(\exists z \in \mathbb{Z})(z > x).$$

DEFINITION Two quantified sentences are **equivalent in a given universe** iff they have the same truth value in that universe. Two quantified sentences are **equivalent** iff they are equivalent in every universe.

Example. $(\forall x)(x > 3)$ and $(\forall x)(x \geq 4)$ are equivalent in the universe of integers (because both are false), the universe of natural numbers greater than 10 (because both are true), and in many other universes. However, if we chose a number between 3 and 4, say 3.7, and let U be the universe of real numbers larger than 3.7, then $(\forall x)(x > 3)$ is true and $(\forall x)(x \geq 4)$ is false in U. The sentences are not equivalent in this universe, so they are not equivalent sentences.

As was noted with propositional forms, it is necessary to make a distinction between a quantified sentence and its logical form. With the universe all integers, the sentence "All integers are odd" is an instance of the logical form $(\forall x)P(x)$, where $P(x)$ is "x is odd." The form itself, $(\forall x)P(x)$, is neither true nor false, but becomes false when "x is odd" is substituted for $P(x)$ and the universe is all integers.

The pair of quantified forms $(\exists x)([P(x) \wedge Q(x)]$ and $(\exists x)([Q(x) \wedge P(x)]$ are equivalent because for any choices of P and Q, $P \wedge Q$ and $Q \wedge P$ are equivalent propositional forms. Another pair of equivalent sentences is $(\forall x)[P(x) \Rightarrow Q(x)]$ and $(\forall x)[\sim Q(x) \Rightarrow \sim P(x)]$.

The next two equivalences are essential for reasoning about quantifiers.

Theorem 1.3.1 If $A(x)$ is an open sentence with variable x, then

(a) $\sim(\forall x)A(x)$ is equivalent to $(\exists x) \sim A(x)$.
(b) $\sim(\exists x)A(x)$ is equivalent to $(\forall x) \sim A(x)$.

Proof.

(a) Let U be any universe.
The sentence $\sim(\forall x)A(x)$ is true in U
iff $(\forall x)A(x)$ is false in U
iff the truth set of $A(x)$ is not the universe
iff the truth set of $\sim A(x)$ is nonempty
iff $(\exists x) \sim A(x)$ is true in U.

(b) The proof of this part is Exercise 7. ■

Theorem 1.3.1 is helpful for finding useful denials (that is, simplified forms of negations) of quantified sentences. For example, in the universe of natural numbers, the sentence "All primes are odd" is symbolized $(\forall x)(x \text{ is prime} \Rightarrow x \text{ is odd})$. The negation is $\sim(\forall x)(x \text{ is prime} \Rightarrow x \text{ is odd})$. By applying Theorem 1.3.1(a), this becomes $(\exists x)[\sim(x \text{ is prime} \Rightarrow x \text{ is odd})]$. By Theorem 1.2.2(c) this is equivalent to $(\exists x)[x \text{ is prime} \wedge \sim(x \text{ is odd})]$. We read this last statement as "There exists a number that is prime and is not odd" or "Some prime number is even."

Example. A simplified denial of $(\forall x)(\exists y)(\exists z)(\forall u)(\exists v)(x + y + z > 2u + v)$ begins with its negation

$$\sim(\forall x)(\exists y)(\exists z)(\forall u)(\exists v)(x + y + z > 2u + v).$$

After 5 applications of Theorem 1.3.1, beginning with the outermost quantifier $(\forall x)$, we arrive at the simplified form

$$(\exists x)(\forall y)(\forall z)(\exists u)(\forall v)(x + y + z \leq 2u + v).$$

Example. For the universe of all real numbers, find a denial of "Every positive real number has a multiplicative inverse."

The sentence is symbolized $(\forall x)[x > 0 \Rightarrow (\exists y)(xy = 1)]$. The negation and successively rewritten equivalents are:

$$\sim(\forall x)[x > 0 \Rightarrow (\exists y)(xy = 1)]$$
$$(\exists x) \sim[x > 0 \Rightarrow (\exists y)(xy = 1)]$$
$$(\exists x)[x > 0 \wedge \sim(\exists y)(xy = 1)]$$
$$(\exists x)[x > 0 \wedge (\forall y) \sim(xy = 1)]$$
$$(\exists x)[x > 0 \wedge (\forall y)(xy \neq 1)]$$

This last sentence may be translated as "There is a positive real number that has no multiplicative inverse."

Example. For the universe of living things, find a denial of "Some children do not like clowns."

The sentence is $(\exists x)$ [x is a child $\wedge$ $(\forall y)$(y is a clown $\Rightarrow$ x does not like y)]. Its negation and several equivalents are:

$\sim(\exists x)$ [x is a child $\wedge$ $(\forall y)$(y is a clown $\Rightarrow$ x does not like y)]

$(\forall x) \sim$[x is a child $\wedge$ $(\forall y)$(y is a clown $\Rightarrow$ x does not like y)]

$(\forall x)$[x is a child $\Rightarrow$ $\sim(\forall y)$(y is a clown $\Rightarrow$ x does not like y)]

$(\forall x)$[x is a child $\Rightarrow$ $(\exists y) \sim$(y is a clown $\Rightarrow$ x does not like y)]

$(\forall x)$[x is a child $\Rightarrow$ $(\exists y)$(y is a clown $\wedge$ $\sim x$ does not like y)]

$(\forall x)$[x is a child $\Rightarrow$ $(\exists y)$(y is a clown $\wedge$ x likes y)]

The denial we seek is "Every child has some clown that he/she likes."

We sometimes hear statements like the complaint one fan had after a great Little League baseball game. "The game was fine," he said, "but everybody didn't get to play." We easily understand that the fan did not mean this literally, because otherwise there would have been no game. The meaning we understand is "Not everyone got to play" or "Some team members did not play." Such misuse of quantifiers, while tolerated in casual conversations, is always to be avoided in mathematics.

The $\exists!$ quantifier, defined next, is a special case of the existential quantifier.

DEFINITION For an open sentence $P(x)$, the proposition $(\exists! x)P(x)$ is read "**there exists a unique x such that $P(x)$**" and is true iff the truth set of $P(x)$ has *exactly one element*. The symbol $\exists!$ is called the **unique existential quantifier.**

Recall that for $(\exists x)P(x)$ to be true it is unimportant how many elements are in the truth set of $P(x)$, as long as there is at least one. For $(\exists! x)P(x)$ to be true, the number of elements in the truth set of $P(x)$ is crucial—there must be exactly one.

In the universe of natural numbers, $(\exists! x)$ (x is even and x is prime) is true because the truth set of "x is even and x is prime" contains only the number 2. The sentence $(\exists! x)(x^2 = 4)$ is true in the universe of natural numbers, but false in the universe of all integers.

Theorem 1.3.2 If $A(x)$ is an open sentence with variable x, then

(a) $(\exists! x)A(x) \Rightarrow (\exists x)A(x)$.
(b) $(\exists! x)A(x)$ is equivalent to $(\exists x)A(x) \wedge (\forall y)(\forall z)(A(y) \wedge A(z) \Rightarrow y = z)$.

Part (a) of Theorem 1.3.2 says that $\exists!$ is indeed a special case of the quantifier $\exists$. Part (b) says that "There exists a unique x such that $A(x)$" is equivalent to "There is an x such that $A(x)$ and if both $A(y)$ and $A(z)$, then $y = z$." The proofs are left to Exercise 11.

Exercises 1.3

1. Translate the following English sentences into symbolic sentences with quantifiers. The universe for each is given in parentheses.
   ★ **(a)** Not all precious stones are beautiful. (All stones)
   ☆ **(b)** All precious stones are not beautiful. (All stones)
   (c) Some isosceles triangle is a right triangle. (All triangles)
   (d) No right triangle is isosceles. (All triangles)
   (e) All people are honest or no one is honest. (All people)
   (f) Some people are honest and some people are not honest. (All people)
   (g) Every nonzero real number is positive or negative. (Real numbers)
   ★ **(h)** Every integer is greater than -4 or less than 6. (Real numbers)
   (i) Every integer is greater than some integer. (Integers)
   ★ **(j)** No integer is greater than every other integer. (Integers)
   (k) Between any integer and any larger integer, there is a real number. (Real numbers)
   ★ **(l)** There is a smallest positive integer. (Real numbers)
   ★ **(m)** No one loves everybody. (All people)
   (n) Everybody loves someone. (All people)
   (o) For every positive real number x, there is a unique real number y such that $2^y = x$. (Real numbers)

☆ 2. For each of the propositions in Exercise 1, write a useful denial, and give a translation into ordinary English.

3. Translate these definitions from the *Preface to the Student* into quantified sentences.
   (a) The integer x is **even**.
   (b) The integer x is **odd**.

(c) The integer a **divides** the integer b.
(d) The natural number n is **prime**.
(e) The natural number n is **composite**.

4. Translate these definitions in this text into quantified sentences. You need not know the specifics of the terms and symbols to complete this exercise.
(a) The relation R is **symmetric**. (See page 147.)
(b) The relation R is **transitive**. (See page 147.)
(c) The function f is **one-to-one**. (See page 208.)
(d) The operation $*$ is **commutative**. (See page 277.)

☆ **5.** The sentence "People dislike taxes" might be interpreted to mean "All people dislike all taxes," "All people dislike some taxes," "Some people dislike all taxes," or "Some people dislike some taxes." Give a symbolic translation for each of these interpretations.

6. Let $T = \{17\}$, $U = \{6\}$, $V = \{24\}$, and $W = \{2, 3, 7, 26\}$. In which of these four different universes is the statement true?
★ **a)** $(\exists x)(x \text{ is odd} \Rightarrow x > 8)$.
b) $(\exists x)(x \text{ is odd } \wedge x > 8)$.
c) $(\forall x)(x \text{ is odd } \Rightarrow x > 8)$.
d) $(\forall x)(x \text{ is odd} \wedge x > 8)$.

7. **(a)** Complete this proof of Theorem 1.3.1(b):
Proof: Let U be any universe.
The sentence $\sim(\exists x)\, A(x)$ is true in U
iff . . .
iff $(\forall x) \sim A(x)$ is true in U.

☆ **(b)** Give a proof of part (b) of Theorem 1.3.1 that uses part (a).

8. Which of the following are true? The universe for each statement is given in parentheses.
(a) $(\forall x)(x + x \geq x)$. $(\mathbb{R})$
★ **(b)** $(\forall x)(x + x \geq x)$. $(\mathbb{N})$
(c) $(\exists x)(2x + 3 = 6x + 7)$. $(\mathbb{N})$
(d) $(\exists x)(3^x = x^2)$. $(\mathbb{R})$
★ **(e)** $(\exists x)(3^x = x)$. $(\mathbb{R})$
(f) $(\exists x)(3(2 - x) = 5 + 8(1 - x))$. $(\mathbb{R})$
(g) $(\forall x)(x^2 + 6x + 5 \geq 0)$. $(\mathbb{R})$
★ **(h)** $(\forall x)(x^2 + 4x + 5 \geq 0)$. $(\mathbb{R})$
(i) $(\exists x)(x^2 - x + 41 \text{ is prime})$. $(\mathbb{N})$
(j) $(\forall x)(x^2 - x + 41 \text{ is prime})$. $(\mathbb{N})$
(k) $(\forall x)(x^3 + 17x^2 + 6x + 100 \geq 0)$. $(\mathbb{R})$
(l) $(\forall x)(\forall y)[x < y \Rightarrow (\exists w)(x < w < y)]$. $(\mathbb{Q})$

9. Give an English translation for each. The universe is given in parentheses.
(a) $(\forall x)(x \geq 1)$. $(\mathbb{N})$
★ **(b)** $(\exists! x)(x \geq 0 \wedge x \leq 0)$. $(\mathbb{R})$
(c) $(\forall x)(x \text{ is prime} \wedge x \neq 2 \Rightarrow x \text{ is odd})$. $(\mathbb{N})$
★ **(d)** $(\exists! x)(\log_e x = 1)$. $(\mathbb{R})$

(e) $\sim(\exists x)(x^2 < 0)$. ($\mathbb{R}$)
(f) $(\exists! x)(x^2 = 0)$. ($\mathbb{R}$)
(g) $(\forall x)(x \text{ is odd} \Rightarrow x^2 \text{ is odd})$. ($\mathbb{N}$)

10. Which of the following are true in the universe of all real numbers?
★ **(a)** $(\forall x)(\exists y)(x + y = 0)$.
(b) $(\exists x)(\forall y)(x + y = 0)$.
(c) $(\exists x)(\exists y)(x^2 + y^2 = -1)$.
★ **(d)** $(\forall x)[x > 0 \Rightarrow (\exists y)(y < 0 \wedge xy > 0)]$.
(e) $(\forall y)(\exists x)(\forall z)(xy = xz)$.
★ **(f)** $(\exists x)(\forall y)(x \le y)$.
(g) $(\forall y)(\exists x)(x \le y)$.
(h) $(\exists! y)(y < 0 \wedge y + 3 > 0)$.
★ **(i)** $(\exists! x)(\forall y)(x = y^2)$.
(j) $(\forall y)(\exists! x)(x = y^2)$.
(k) $(\exists! x)(\exists! y)(\forall w)(w^2 > x - y)$.

11. Let $A(x)$ be an open sentence with variable x.
☆ **(a)** Prove Theorem 1.3.2 (a).
☆ **(b)** Show that the converse of Theorem 1.3.2 (a) is false.
(c) Prove Theorem 1.3.2 (b).
(d) Prove that $(\exists! x)A(x)$ is equivalent to $(\exists x)[A(x) \wedge (\forall y)(A(y) \Rightarrow x = y)]$.
★ **(e)** Find a useful denial for $(\exists! x)A(x)$.

12. **(a)** Write the symbolic form for the definition of "f is continuous at a."
(b) Write the symbolic form of the statement of the Mean Value Theorem.
(c) Write the symbolic form for the definition of "$\lim_{x \to a} f(x) = L$."
(d) Write a useful denial of each sentence in parts (a), (b), and (c).

13. Which of the following are denials of $(\exists! x)P(x)$?
(a) $(\forall x)P(x) \vee (\forall x)\sim P(x)$.
(b) $(\forall x) \sim P(x) \vee (\exists y)(\exists z)(y \ne z \wedge P(y) \wedge P(z))$.
(c) $(\forall x)[P(x) \Rightarrow (\exists y)(P(y) \wedge x \ne y)]$.
★ **(d)** $\sim(\forall x)(\forall y)[(P(x) \wedge P(y)) \Rightarrow x = y]$.

★ **14.** *Riddle:* What is the English translation of the symbolic statement $\forall\exists\exists\forall$?

1.4 Basic Proof Methods I

In mathematics, a **theorem** is a statement that describes a pattern or relationship among quantities or structures and a **proof** is a justification of the truth of a theorem. Before beginning to examine valid proof techniques it is recommended that you review the comments about proofs and the definitions in the *Preface to the Student*.

We cannot define all terms nor prove all statements from previous ones. We begin with an initial set of statements, called **axioms** (or **postulates**), that are *assumed to be true*. We then derive theorems that are true in any situation where the axioms are true. The Pythagorean* Theorem, for example, is a theorem whose proof is ultimately based on the five axioms of Euclidean† geometry. In a situation where the Euclidean axioms are not all true (which can happen), the Pythagorean Theorem may not be true.

There must also be an initial set of **undefined terms**—concepts fundamental to the context of study. In geometry, the concept of a point is an undefined term. In this text the real numbers are not formally defined. Instead, they are described in the *Preface to the Student* as the decimal numbers along the number line. While a precise definition of a real number could be given‡, doing so would take us far from our intended goals.

From the axioms and undefined terms, new concepts (new **definitions**) can be introduced. And finally, new theorems can be proved. The structure of a proof for a particular theorem depends greatly on the logical form of the theorem. Proofs may require some ingenuity or insightfulness to put together the right statements to build the justification. Nevertheless, much can be gained in the beginning by studying the fundamental components found in proofs and examples that exhibit them. The four rules that follow provide guidance about what statements are allowed in a proof, and when.

Some steps in a proof may be statements of axioms of the basic theory upon which the discussion rests. Other steps may be previously proved results. Still other steps may be assumptions you wish to introduce. In any proof you may

At any time state an assumption, an axiom, or a previously proved result.

The statement of an assumption generally takes the form "Assume P" to alert the reader that the statement is not derived from a previous step or steps. We must be careful about making assumptions, because we can only be certain that what we proved will be true *when all the assumptions are true*. The most common assumptions are hypotheses given as components in the statement of the theorem to be proved. We will discuss assumptions in more detail later in this section.

The statement of an axiom is usually easily identified as such by the reader because it is a statement about a very fundamental fact assumed about the theory. Sometimes the axiom is so well known that its statement is omitted from proofs, but there are cases (such as the Axiom of Choice in Chapter 5) for which it is prudent to mention the axiom in every proof employing it.

Proof steps that use previously proven results help build a rich theory from the basic assumptions. In calculus, for example, before one proves that the derivative of $\sin x$ is $\cos x$, there is a proof of the separate result that $\lim_{\Delta x \to 0} \frac{\sin \Delta x}{\Delta x} = 1$. It is easier to prove this result first, then cite the result in the proof of the fact that the derivative of $\sin x$ is $\cos x$.

* Pythagoras, latter half of the 6th century, B.C.E., was a Greek mathematician and philosopher who founded a secretive religious society based on mathematical and metaphysical thought. Although Pythagoras is regularly given credit for the theorem named for him, the result was known to Babylonian and Indian mathematicians centuries earlier.

† Euclid of Alexandria, circa 300 B.C.E., made his immortal contribution to mathematics with his famous text on geometry and number theory. His *Elements* sets forth a small number of axioms from which additional definitions and many familiar geometric results were developed in a rigorous way. Other geometries, based on different sets of axioms, did not begin to appear until the 1800s.

‡ See the references cited in Section 7.5.

An important skill for proof writing is the ability to rewrite a complex statement in an equivalent form that is more useful or helps to clarify its meaning. You may:

At any time state a sentence equivalent to any statement earlier in the proof.

This **replacement rule** is often used in combination with the equivalences of Theorems 1.1.1 and 1.2.2 to rewrite a statement involving logical connectives. For example, suppose we have been able to establish the step

"It is not the case that x is even and prime."

Because the form of this statement is $\sim(P \wedge Q)$, where P is "x is even" and Q is "x is prime," we may deduce that

"x is not even or x is not prime,"

which has form $\sim P \vee \sim Q$. We have applied the replacement rule, using one of De Morgan's Laws. A working knowledge of the equivalences of Theorems 1.1.1 and 1.2.2 is essential.

The replacement rule allows you to use definitions in two ways. First, if you are told or have shown that x is odd, then you can correctly state that for some natural number k, $x = 2k + 1$. You now have an equation to use. Second, if you need to prove that x is odd, then the definition gives you something equivalent to work toward: It suffices to show that x can be expressed as $x = 2k + 1$, for some natural number k. You'll find it useful in writing proofs to keep in mind these two ways we use definitions.

Example. If a proof contains the line "The product of real numbers a and b is zero," we could assert that "Either $a = 0$ or $b = 0$." In this example, the equivalence of the two statements comes from our knowledge of the real numbers that $(ab = 0) \Leftrightarrow (a = 0 \text{ or } b = 0)$.

Tautologies are important both because a statement that has the form of a tautology may be used as a step in a proof, and because tautologies are used to create rules for making deductions in a proof. The **tautology rule** says that you may:

At any time state a sentence whose symbolic translation is a tautology.

For example, if a proof involves a real number x, you may at any time assert "Either $x > 0$ or $x \leq 0$," since this is an instance of the tautology $P \vee \sim P$.

The rules above allow us to reword a statement or say something that's always true or is assumed to be true. The next rule is the one that allows us to make a connection so that we can get from statement P to a *different* statement Q.

The most fundamental rule of reasoning is **modus ponens**, which is based on the tautology $[P \wedge (P \Rightarrow Q)] \Rightarrow Q$. As we have seen in Section 1.2, what this means is that when P and $P \Rightarrow Q$ are both true, we may deduce that Q must also be true. The **modus ponens rule** says you may:

At any time after P and $P \Rightarrow Q$ appear in a proof, state that Q is true.

Example. From calculus we know that if a function f is differentiable on an interval (a, b), then f is continuous on the interval (a, b). A proof writer who had already written:

f is differentiable on the interval (a, b)

could use modus ponens to write as a subsequent step:

Therefore f is continuous on the interval (a, b).

This deduction uses the statements D, $D \Rightarrow C$, and C, where D is the statement "f is differentiable on interval (a, b)" and C is "f is continuous on the interval (a, b)."

Notice that in this example it would make the proof shorter and easier to read if we didn't write out the sentence $D \Rightarrow C$ in the proof. This is because the connection between differentiability and continuity is a well-known theorem, which the proof writer may assume that the reader knows.

When we use modus ponens to deduce statement Q from P and $P \Rightarrow Q$, the statement P could be an instance of a tautology, a simple or compound proposition whose components are either hypotheses, axioms, earlier statements deduced in the proof, or statements of previously proved theorems. Likewise, $P \Rightarrow Q$ may have been deduced earlier in the proof or may be a previous theorem, axiom, or tautology.

Example. You are at a crime scene and have established the following facts:

(1) If the crime did not take place in the billiard room, then Colonel Mustard is guilty.

(2) The lead pipe is not the weapon.

(3) Either Colonel Mustard is not guilty or the weapon used was a lead pipe.

From these facts and modus ponens, you may construct a proof that shows the crime took place in the billiard room:

Proof.

Statement (1)	$\sim B \Rightarrow M$
Statement (2)	$\sim L$
Statement (3)	$\sim M \vee L$
Statements (1) and (2) and (3)	$(\sim B \Rightarrow M) \wedge \sim L \wedge (\sim M \vee L)$
Statements (1), (2), and (3) imply the crime took place in the billiard room.	$[(\sim B \Rightarrow M) \wedge \sim L \wedge (\sim M \vee L)] \Rightarrow B$ is a tautology (see Exercise 2).
Therefore, the crime took place in the billiard room.	B

■

The last three statements above are an application of the modus ponens rule: We deduced Q from the statements P and $P \Rightarrow Q$, where Q is B and P is $(\sim B \Rightarrow M) \wedge \sim L \wedge (\sim M \vee L)$.

The previous example shows the power of pure reasoning: It is the *forms* of the propositions and not their meanings that allowed us to make the deductions.

Because our proofs are always about mathematical phenomena, we also need to understand the subject matter of the proof—the concepts involved and how they are related. Therefore, when you develop a strategy to construct a proof, keep in mind both the logical form of the theorem's statement and the mathematical concepts involved.

You won't find truth tables displayed or referred to in proofs that you encounter in mathematics: It is expected that readers are familiar with the rules of logic and correct forms of proof. As a general rule, when you write a step in a proof, ask yourself if deducing that step is valid in the sense that it uses one of the four rules above. If the step follows as a result of the use of a tautology, it is not necessary to cite the tautology in your proof. In fact, with practice you should eventually come to write proofs without purposefully thinking about tautologies. What *is* necessary is that every step be justifiable.

The first—and most important—proof method is the **direct proof** of statement of the form $P \Rightarrow Q$, which proceeds in a step by step fashion from the antecedent P to the consequent Q. Since $P \Rightarrow Q$ is false only when P is true and Q is false, it suffices to show that this situation cannot happen. The direct way to proceed is to assume that P is true and show (deduce) that Q is also true. A direct proof of $P \Rightarrow Q$ will have the following form:

DIRECT PROOF OF $P \Rightarrow Q$

Proof.

Assume P.

$\vdots$

Therefore, Q.

Thus, $P \Rightarrow Q$. ■

Some of the examples that follow actually involve quantified sentences. Since we won't consider proofs with quantifiers until Section 1.6, you should imagine for now that a variable represents some fixed object. Out first example proves the familiar fact that "If x is odd, then $x + 1$ is even." You should think of x as being some particular integer.

Example. Let x be an integer. Prove that if x is odd, then $x + 1$ is even.

Proof. ⟨*The theorem has the form $P \Rightarrow Q$, where P is "x is odd" and Q is "$x + 1$ is even."*⟩ Let x be an integer. ⟨*We may assume this hypothesis since it is given in the statement of the theorem.*⟩ Suppose x is odd. ⟨*We assume that the antecedent P is true. The goal is to derive the consequent Q as our last step.*⟩ From the definition of odd, $x = 2k + 1$ for some integer k. ⟨*This deduction is the replacement* *of P by an equivalent statement—the definition of "odd." We now have an equation to use.*⟩ Then $x + 1 = (2k + 1) + 1$ for some integer k. ⟨*This is another replacement using an algebraic property of* $\mathbb{N}$.⟩ Since $(2k + 1) + 1 = 2k + 2 = 2(k + 1)$, $x + 1$ is the product of 2 and an integer. ⟨*Another equivalent using algebra*.⟩ Thus $x + 1$ is even. ⟨*We have deduced* Q.⟩

Therefore, if x is an odd integer, then $x + 1$ is even. ⟨*We conclude that* $P \Rightarrow Q$.⟩ ■

In this example, we did not worry about what would happen if x were not odd. Remember that it is appropriate to assume P is true when giving a direct proof of $P \Rightarrow Q$. (If P is false, it does not matter what the truth of Q is; the statement we are trying to prove, $P \Rightarrow Q$, will be true.) The process of assuming that the antecedent is true and proceeding step by step to show the consequent is true is what makes this type of proof direct.

This example also includes parenthetical comments offset by ⟨ . . . ⟩ and in italics to explain how and why a proof is proceeding as it is. Such comments are not a requisite part of the proof, but are inserted to help clarify the workings of the proof. The proof above would stand alone as correct with all the comments deleted, or it could be written in shorter form, as follows.

Proof. Let x be an integer. Suppose x is odd. Then $x = 2k + 1$ for some integer k. Then $x + 1 = (2k + 1) + 1 = 2k + 2 = 2(k + 1)$. Since $k + 1$ is an integer and $x + 1 = 2(k + 1)$, $x + 1$ is even.

Therefore, if x is an odd integer, then $x + 1$ is even. ■

Great latitude is allowed for differences in taste and style among proof writers. Generally, in advanced mathematics, only the minimum amount of explanation is included in a proof. The reader is expected to know the definitions and previous results and be able to fill in computations and deductions as necessary. In this text, we shall include parenthetical comments for more complete explanations.

Example. Suppose a, b, and c are integers. Prove that if a divides b and b divides c, then a divides c.

Proof. Let a, b, and c be integers. ⟨*We start by assuming that the hypothesis is true*.⟩ Suppose a divides b and b divides c. ⟨*The antecedent is the compound sentence "a divides b and b divides c*."⟩ Then $b = ak$ for some integer k and $c = bm$ for some integer m. ⟨*We replaced the assumptions by equivalents using the definition of "divides." Notice that we did not assume that k and m are the same integer.*⟩ ⟨*To show that a divides c, we must write c as a multiple of a.*⟩ Therefore, $c = bm = (ak)m = a(km)$. Then c is a multiple of a. ⟨*We use the fact that if k and m are integers, then km is an integer*.⟩

Therefore, if a divides b and b divides c, then a divides c. ■

Both of the above examples and many more to follow use the following strategy for developing a direct proof of a conditional sentence:

1. Determine precisely the hypotheses (if any) and the antecedent and consequent.
2. Replace (if necessary) the antecedent with a more usable equivalent.
3. Replace (if necessary) the consequent by something equivalent and more readily shown.
4. Beginning with the assumption of the antecedent, develop a chain of statements that leads to the consequent. Each statement in the chain must be deducible from its predecessors or other known results.

As you write a proof, be sure it is not just a string of symbols. Every step of your proof should express a complete sentence. Be sure to include important connective words.

Example. Suppose a, b, and c are integers. Prove that if a divides b and a divides c, then a divides $b - c$.

Proof. Suppose a, b, and c are integers and a divides b and a divides c. ⟨*Now use the definition of divides.*⟩ Then $b = an$ for some integer n and $c = am$ for some integer m. Thus, $b - c = an - am = a(n - m)$. Since $n - m$ is an integer ⟨*using the fact that the difference of two integers is an integer*⟩, a divides $b - c$. ■

Our next example of a direct proof, which comes from an exercise in precalculus mathematics, involves a point (x, y) in the Cartesian plane (Figure 1.4.1). It uses algebraic properties available to students in such a class.

Example. Prove that if $x < -4$ and $y > 2$, then the distance from (x, y) to $(1, -2)$ is at least 6.

Proof. Assume that $x < -4$ and $y > 2$. Then $x - 1 < -5$, so $(x - 1)^2 > 25$. Also $y + 2 > 4$, so $(y + 2)^2 > 16$. Therefore,

$$\sqrt{(x-1)^2 + (y+2)^2} > \sqrt{25 + 16} > \sqrt{36},$$

so the distance from (x, y) to $(1, -2)$ is at least 6. ■

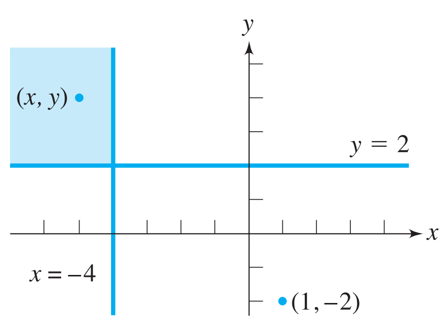

Figure 1.4.1

To get a sense of how a proof of $P \Rightarrow Q$ should proceed, it is sometimes useful to "work backward" from what is to be proved: To show that a consequent is true, decide what statement could be used to prove it, another statement that could be used to prove that one, and so forth. Continue until you reach a hypothesis, the antecedent, or a fact known to be true. After doing such preliminary work, construct a proof "forward" so that your conclusion is the consequent.

Example. Let a and b be positive real numbers. Prove that if $a < b$, then $b^2 - a^2 > 0$.

Proof. ⟨*Working backward, rewrite* $b^2 - a^2 > 0$ *as* $(b-a)(b+a) > 0$. *This inequality will be true when both* $b - a > 0$ *and* $b + a > 0$. *The first inequality* $b - a > 0$ *will be true because we will assume the antecedent* $a < b$. *The second inequality* $b + a > 0$ *is true because of our hypothesis that a and b are positive. We now proceed with the direct proof.*⟩ Assume a and b are positive real numbers and that $a < b$. Since both a and b are positive, $b + a > 0$. Since $a < b$, $b - a > 0$. Because the product of two positive real numbers is positive, $(b-a)(b+a) > 0$. Therefore $b^2 - a^2 > 0$. ■

It is often helpful to work both ways—backward from what is to be proved and forward from the hypothesis—until you reach a common statement from each direction.

Example. Prove that if $x^2 \le 1$, then $x^2 - 7x > -10$.

Working backward from $x^2 - 7x > -10$, we note that this can be deduced from $x^2 - 7x + 10 > 0$. This can be deduced from $(x-5)(x-2) > 0$, which could be concluded if we knew that $x - 5$ and $x - 2$ were both positive or both negative.

Working forward from $x^2 \le 1$, we have $-1 \le x \le 1$, so $x \le 1$. Therefore, $x < 5$ and $x < 2$, from which we can conclude that $x - 5 < 0$ and $x - 2 < 0$, which is exactly what we need.

Proof. Assume that $x^2 \le 1$. Then $-1 \le x \le 1$. Therefore $x \le 1$. Thus $x < 5$ and $x < 2$, and so we have $x - 5 < 0$ and $x - 2 < 0$. Therefore, $(x-5)(x-2) > 0$. Thus $x^2 - 7x + 10 > 0$. Hence $x^2 - 7x > -10$. ■

We now consider direct proofs of statements of the form $P \Rightarrow Q$ when either P or Q is itself a compound proposition. We have in fact already constructed proofs of statements of the form $(P \wedge Q) \Rightarrow R$. When we give a direct proof of a statement of this form, we have the advantage of assuming both P and Q at the beginning of the proof, as we did in the proof (above) that if a divides b and a divides c, then a divides $b - c$.

A proof of a statement symbolized by $P \Rightarrow (Q \wedge R)$ would probably have two parts. In one part we prove $P \Rightarrow Q$ and in the other part we prove $P \Rightarrow R$. We would use this method to prove the statement "If two parallel lines are cut by a transversal, then corresponding angles are equal and corresponding lines are equal."

To prove a conditional sentence whose consequent is a disjunction, that is, a sentence of the form $P \Rightarrow (Q \vee R)$, one often proves either the equivalent $P \wedge \sim Q \Rightarrow R$ or the equivalent $P \wedge \sim R \Rightarrow Q$. For instance, to prove "If the polynomial *f* has degree 4, then *f* has a real zero or *f* can be written as the product of two irreducible quadratics," we would prove "If *f* has degree 4 and no real zeros, then *f* can be written as the product of two irreducible quadratics."

A statement of the form $(P \vee Q) \Rightarrow R$ has the meaning: "If either P is true or Q is true, then R is true," or "In case either P or Q is true, R must be true." A natural way to prove such a statement is by cases, so the proof outline would have the form:

Case 1. Assume P. . . . Therefore R.
Case 2. Assume Q. . . . Therefore R.

This method is valid because of the tautology

$$[(P \vee Q) \Rightarrow R] \Leftrightarrow [(P \Rightarrow R) \wedge (Q \Rightarrow R)].$$

The statement "If a quadrilateral has opposite sides equal or opposite angles equal, then it is a parallelogram" is proved by showing both "A quadrilateral with opposite sides equal is a parallelogram" and "A quadrilateral with opposite angles equal is a parallelogram."

The two similar statement forms $(P \Rightarrow Q) \Rightarrow R$ and $P \Rightarrow (Q \Rightarrow R)$ have remarkably dissimilar direct proof outlines. For $(P \Rightarrow Q) \Rightarrow R$, we assume $P \Rightarrow Q$ and deduce R. We cannot assume P; we must assume $P \Rightarrow Q$. On the other hand, in a direct proof of $P \Rightarrow (Q \Rightarrow R)$, we do assume P and show $Q \Rightarrow R$. Furthermore, after the assumption of P, a direct proof of $Q \Rightarrow R$ begins by assuming Q is true as well. This is not surprising since $P \Rightarrow (Q \Rightarrow R)$ is equivalent to $(P \wedge Q) \Rightarrow R$.

The main lesson to be learned from this discussion is that the method of proof you choose will depend on the form of the statement to be proved. The outlines we have given are the most natural, but not the only ways, to construct correct proofs. Of course constructing a proof also requires knowledge of the subject matter.

Example. Suppose n is an odd integer. Then $n = 4j + 1$ for some integer j, or $n = 4i - 1$ for some integer i.

Proof. Suppose n is odd. Then $n = 2m + 1$ for some integer m. ⟨*A little experimentation shows that when m is even, for example when n is* $2(-2) + 1$, $2(0) + 1, 2(2) + 1, 2(4) + 1$, *etc., n has the form* $4j + 1$; *otherwise n has the form* $4i - 1$. *We now show that* $(P \vee Q) \Rightarrow (R_1 \vee R_2)$, *where P is "m is even," Q is "m is odd,"* R_1 *is* "$n = 4j + 1$ *for some integer j," and* R_2 *is* "$n = 4i - 1$ *for some integer i." The method we choose is to show that* $P \Rightarrow R_1$ *and* $Q \Rightarrow R_2$.⟩

Case 1. If m is even, then $m = 2j$ for some integer j, and so $n = 2(2j) + 1 = 4j + 1$.
Case 2. If m is odd, then $m = 2k + 1$ for some integer k. In this case, $n = 2(2k + 1) + 1 = 4k + 3 = 4(k + 1) - 1$. Choosing i to be the integer $k + 1$, we have $n = 4i - 1$. ■

The form of proof known as **proof by exhaustion** consists of an examination of every possible case. The statement to be proved may have any form P. For example, to prove that every number x in the closed interval $[0, 5]$ has a certain property, we might consider the cases $x = 0$, $0 < x < 5$, and $x = 5$. The exhaustive method was our method in the example above, and in the proof of Theorem 1.1.1, where we examined all four combinations of truth values for two propositions. Naturally, the idea of proof by exhaustion is appealing only when the number of cases is small, or when large numbers of cases can be systematically handled. Care must be taken to ensure that all possible cases have been considered.

Example. Let x be a real number. Prove that $-|x| \le x \le |x|$.

Proof. ⟨*Since the absolute value of* x *is defined by cases* ($|x| = x$ *if* $x \ge 0$; $|x| = -x$ *if* $x < 0$) *this proof will proceed by cases*.⟩

Case 1. Suppose $x \ge 0$. Then $|x| = x$. Since $x \ge 0$, we have $-x \le x$. Hence, $-x \le x \le x$, which is $-|x| \le x \le |x|$ in this case.

Case 2. Suppose $x < 0$. Then $|x| = -x$. Since $x < 0$, $x \le -x$. Hence, we have $x \le x \le -x$, or $-(-x) \le x \le -x$, which is $-|x| \le x \le |x|$.

Thus, in all cases we have $-|x| \le x \le |x|$. ■

There have been instances of truly exhausting proofs involving great numbers of cases. In 1976, Kenneth Appel and Wolfgang Haken of the University of Illinois announced a proof of the Four-Color Theorem. The original version of their proof of the famous Four-Color Conjecture contains 1,879 cases and took $3\frac{1}{2}$ years to develop.*

Finally, there are proofs by exhaustion with cases so similar in reasoning that we may simply present a single case and alert the reader with the phrase "without loss of generality" that this case represents the essence of arguments for the other cases. Here is an example.

Example. Prove that for the integers m and n, one of which is even and the other odd, $m^2 + n^2$ has the form $4k + 1$ for some integer k.

Proof. Let m and n be integers. Without loss of generality, we may assume that m is even and n is odd. ⟨*The case where m is odd and n is even is similar*.⟩ Then there exist integers s and t such that $m = 2s$ and $n = 2t + 1$. Therefore, $m^2 + n^2 = (2s)^2 + (2t + 1)^2 = 4s^2 + 4t^2 + 4t + 1 = 4(s^2 + t^2 + t) + 1$. Since $s^2 + t^2 + t$ is an integer, $m^2 + n^2$ has the form $4k + 1$ for some integer k. ■

* The Four-Color Theorem involves coloring regions or countries on a map in such a way that no two adjacent countries have the same color. It states that four colors are sufficient, no matter how intertwined the countries may be. The fact that the proof depended so heavily on the computer for checking cases raised questions about the nature of proof. Verifying the 1,879 cases required more than 10 billion calculations. Many people wondered whether there might have been at least one error in a process so lengthy that it could not be carried out by one human being in a lifetime. Haken and Appel's proof has since been improved, and the Four-Color Theorem is accepted; but the debate about the role of computers in proof continues.

Exercises 1.4

1. Analyze the logical form of each of the following statements and construct just the outline of a proof. Since the statements may contain terms with which you are not familiar, you should not (and perhaps could not) provide any details of the proof.

★ **(a)** Outline a direct proof that if $(G, *)$ is a cyclic group, then $(G, *)$ is abelian.

(b) Outline a direct proof that if **B** is a nonsingular matrix, then the determinant of **B** is not zero.

(c) Suppose A, B, and C are sets. Outline a direct proof that if A is a subset of B and B is a subset of C, then A is a subset of C.

(d) Outline a direct proof that if the maximum value of the differentiable function f on the closed interval $[a, b]$ occurs at x_0, then either $x_0 = a$ or $x_0 = b$ or $f'(x_0) = 0$.

(e) Outline a direct proof that if **A** is a diagonal matrix, then **A** is invertible whenever all its diagonal entries are nonzero.

2. A theorem of linear algebra states that if **A** and **B** are invertible matrices, then the product **AB** is invertible. As in Exercise 1, outline

(a) a direct proof of the theorem.

(b) a direct proof of the converse of the theorem.

3. Verify that $[(\sim B \Rightarrow M) \wedge \sim L \wedge (\sim M \vee L)] \Rightarrow B$ is a tautology. See the example on page 30.

4. These facts have been established at a crime scene.

(i) If Professor Plum is not guilty, then the crime took place in the kitchen.

(ii) If the crime took place at midnight, Professor Plum is guilty.

(iii) Miss Scarlet is innocent if and only if the weapon was not the candlestick.

(iv) Either the weapon was the candlestick or the crime took place in the library.

(v) Either Miss Scarlet or Professor Plum is guilty.

Use the above and the additional fact(s) below to solve the case. Explain your answer.

★ **(a)** The crime lab determines that the crime took place in the library.

(b) The crime lab determines that the crime did not take place in the library.

(c) The crime lab determines that the crime was committed at noon with the revolver.

(d) The crime took place at midnight in the conservatory. (Give a complete answer.)

5. Let x and y be integers. Prove that

(a) if x and y are even, then $x + y$ is even.

(b) if x is even, then xy is even.

(c) if x and y are even, then xy is divisible by 4.

(d) if x and y are even, then $3x - 5y$ is even.

(e) if x and y are odd, then $x + y$ is even.

(f) if x and y are odd, then $3x - 5y$ is even.
(g) if x and y are odd, then xy is odd.
★ **(h)** if x is even and y is odd, then $x + y$ is odd.
(i) if x is even and y is odd, then xy is even.

6. Let a and b be real numbers. Prove that
(a) $|ab| = |a||b|$.
(b) $|a - b| = |b - a|$.
(c) $\left|\frac{a}{b}\right| = \frac{|a|}{|b|}$, for $b \neq 0$.
☆ **(d)** $|a + b| \le |a| + |b|$.
(e) if $|a| \le b$, then $-b \le a \le b$.
(f) if $-b \le a \le b$, then $|a| \le b$.

7. Suppose a, b, c, and d are integers. Prove that
(a) $2a - 1$ is odd.
★ **(b)** if a is even, then $a + 1$ is odd.
(c) if a is odd, then $a + 2$ is odd.
☆ **(d)** $a(a + 1)$ is even.
(e) 1 divides a.
(f) a divides a.
★ **(g)** if a and b are positive and a divides b, then $a \le b$.
(h) if a divides b, then a divides bc.
★ **(i)** if a and b are positive and $ab = 1$, then $a = b = 1$.
(j) if a and b are positive, a divides b and b divides a, then $a = b$.
(k) if a divides b and c divides d, then ac divides bd.
(l) if ab divides c, then a divides c.
(m) if ac divides bc, then a divides b.

8. Give two proofs that if n is a natural number, then $n^2 + n + 3$ is odd.
(a) Use two cases.
(b) Use Exercises 7(d) and 5(h).

9. Let a, b, and c be integers and x, y, and z be real numbers. Use the technique of working backward from the desired conclusion to prove that
(a) if x and y are nonnegative, then $\frac{x+y}{2} \ge \sqrt{xy}$.
Where in the proof do we use the fact that x and y are nonnegative?
(b) if a divides b and a divides $b + c$, then a divides $3c$.
(c) if $ab > 0$ and $bc < 0$, then $ax^2 + bx + c = 0$ has two real solutions.
(d) if $x^3 + 2x^2 < 0$, then $2x + 5 < 11$.
(e) if an isosceles triangle has sides of length x, y, and z, where $x = y$ and $z = \sqrt{2xy}$, then it is a right triangle.

10. Recall that except for degenerate cases, the graph of $Ax^2 + Bxy + Cy^2 + Dx + Ey + F = 0$ is

an ellipse iff $B^2 - 4AC < 0$,
a parabola iff $B^2 - 4AC = 0$,
a hyperbola iff $B^2 - 4AC > 0$.

★ **(a)** Prove that the graph of the equation is an ellipse whenever $A > C > B > 0$.

(b) Prove that the graph of the equation is a hyperbola if $AC < 0$ or $B < C < 4A < 0$.

(c) Prove that if the graph is a parabola, then $BC = 0$ or $A = B^2/(4C)$.

Proofs to Grade

11. Exercises throughout the text with this title ask you to examine "Proofs to Grade." These are allegedly true claims and supposed "proofs" of the claims. You should decide the merit of the claim and the validity of the proof and then assign a grade of

A (correct), if the claim and proof are correct, even if the proof is not the simplest or the proof you would have given.

C (partially correct), if the claim is correct *and* the proof is largely correct. The proof may contain one or two incorrect statements or justifications, but the errors are easily correctable.

F (failure), if the claim is incorrect, or the main idea of the proof is incorrect, or there are too many errors.

You must justify assignments of grades other than A and if the proof is incorrect, explain what is incorrect and why.

★ **(a)** Suppose a is an integer.

Claim. If a is odd then $a^2 + 1$ is even.

"Proof." Let a. Then, by squaring an odd we get an odd. An odd plus odd is even. So $a^2 + 1$ is even. ■

(b) Suppose a, b, and c are integers.

Claim. If a divides b and a divides c, then a divides $b + c$.

"Proof." Suppose a divides b and a divides c. Then for some integer q, $b = aq$, and for some integer q, $c = aq$. Then $b + c = aq + aq = 2aq = a(2q)$, so a divides $b + c$. ■

★ **(c)** Suppose x is a positive real number.

Claim. The sum of x and its reciprocal is greater than or equal to 2. That is,

$$x + \frac{1}{x} \geq 2.$$

"Proof." Multiplying by x, we get $x^2 + 1 \geq 2x$. By algebra, $x^2 - 2x + 1 \geq 0$. Thus, $(x - 1)^2 \geq 0$. Any real number squared is greater than or equal to zero, so $x + \frac{1}{x} \geq 2$ is true. ■

★ **(d)** Suppose m is an integer.

Claim. If m^2 is odd, then m is odd.

"Proof." Assume m is odd. Then $m = 2k + 1$ for some integer k. Therefore, $m^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, which is odd. Therefore, if m^2 is odd, then m is odd. ■

(e) Suppose a is an integer.

Claim. $a^3 + a^2$ is even.

"Proof." $a^3 + a^2 = a^2(a + 1)$, which is always an odd number times an even number. Therefore, $a^3 + a^2$ is even. ■

1.5 Basic Proof Methods II

In the last section, we saw that the method of direct proof for $P \Rightarrow Q$ proceeds as a chain of statements from the antecedent to the consequent. This is the most basic form of proof and is the foundation for several other proof techniques. The techniques in this section are based on tautologies that replace the statement to be proved by an equivalent statement or statements. We call these **indirect proofs.**

A **proof by contraposition** or **contrapositive proof** for a conditional sentence $P \Rightarrow Q$ makes use of the tautology $(P \Rightarrow Q) \Leftrightarrow (\sim Q \Rightarrow \sim P)$. Since $P \Rightarrow Q$ and $\sim Q \Rightarrow \sim P$ are equivalent statements, we first give a proof of $\sim Q \Rightarrow \sim P$ and then conclude by replacement that $P \Rightarrow Q$.

PROOF BY CONTRAPOSITION OF $P \Rightarrow Q$

Proof.
Assume $\sim Q$.
⋮
Therefore, $\sim P$.
Thus, $\sim Q \Rightarrow \sim P$
Therefore, $P \Rightarrow Q$. ■

This method can work well when the connection between denials of P and Q are easier to understand than the connection between P and Q themselves, or when the statement of either P and Q is itself a negation.

In the following examples of proof by contraposition we use familiar properties of inequalities and the property that every integer is either even or odd, but not both. As in the last section, we assume that variables represent fixed quantities.

Example. Let m be an integer. Prove that if m^2 is even, then m is even.

Proof. ⟨*The antecedent is P, "m^2 is even" and the consequent is Q, "m is even."*⟩ Suppose that the integer m is not even. ⟨*Suppose* $\sim Q$.⟩ Then m is odd so $m = 2k + 1$ for some integer k. Then

$$m^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

Since m^2 is twice an integer, plus 1, m^2 is odd. ⟨*Since k is an integer,* $2k^2 + 2k$ *is an integer.*⟩ Therefore, m^2 is not even. ⟨*We have concluded* $\sim P$.⟩

Thus, if m is not even, then m^2 is not even. By contraposition, if m^2 is even, then m is even. ■

Example. Let x and y be real numbers such that $x < 2y$. Prove that if $7xy \le 3x^2 + 2y^2$, then $3x \le y$.

Proof. Suppose x and y are real numbers and $x < 2y$. ⟨*Let P be* $7xy \le 3x^2 + 2y^2$ *and* Q *be* $3x \le y$.⟩ Suppose $3x > y$. ⟨*We assume* $\sim Q$.⟩ Then $2y - x > 0$ and $3x - y > 0$. Therefore, $(2y - x)(3x - y) = 7xy - 3x^2 - 2y^2 > 0$. Hence, $7xy > 3x^2 + 2y^2$.

We have shown that if $3x > y$, then $7xy > 3x^2 + 2y^2$. Therefore, by contraposition, if $7xy \le 3x^2 + 2y^2$, then $3x \le y$. ∎

Another indirect proof technique is **proof by contradiction.** The logic behind such a proof is that if a statement cannot be false, then it must be true. Thus, to prove by contradiction that a statement P is true, we temporarily assume that P is false and then see what would happen. If what happens is an impossibility—that is, a contradiction—then we know that P must be true. Here is an example of a proof by contradiction.

Example. Prove that the graphs of $y = x^2 + x + 2$ and $y = x - 2$ do not intersect.

Proof. Suppose the graphs of $y = x^2 + x + 2$ and $y = x - 2$ do intersect at some point (a, b). ⟨*Suppose* $\sim P$.⟩ Since (a, b) is a point on both graphs, $b = a^2 + a + 2$ and $b = a - 2$. Therefore, $a - 2 = a^2 + a + 2$, so $a^2 = -4$. Thus, $a^2 < 0$. But a is a real number, so $a^2 \ge 0$. This is impossible. ⟨*The statement* $a^2 < 0 \wedge a^2 \ge 0$ *is a contradiction*.⟩ Therefore, the graphs do not intersect. ∎

A proof by contradiction is based on the tautology $P \Leftrightarrow [(\sim P) \Rightarrow (Q \wedge \sim Q)]$. That is, to prove a proposition P, we prove $(\sim P) \Rightarrow (Q \wedge \sim Q)$ for some proposition Q. In the example above, Q is the statement $a^2 < 0$. A proof by contradiction has the following form:

PROOF OF *P* BY CONTRADICTION

Proof.

Suppose $\sim P$.

⋮

Therefore, Q.

⋮

Therefore, $\sim Q$.

Hence, $Q \wedge \sim Q$ a contradiction.

Thus, P. ∎

Two aspects about proofs by contradiction are especially noteworthy. First, this method of proof can be applied to any proposition P, whereas direct proofs and proofs by contraposition can be used only for conditional sentences. Second, the proposition Q does not appear on the left side of the tautology. The strategy of proving P by proving $\sim P \Rightarrow (Q \wedge \sim Q)$, then, has an advantage and a disadvantage. We don't know what proposition to use for Q, but any proposition that will do the job is a good one. This means a proof by contradiction may require a spark of insight to determine a useful Q.

The next proof by contradiction is a classical result whose proof can be traced back to Hippasus, a disciple of Pythagoras, circa 500 B.C.E. One of several legends has it that Hippasus proved that $\sqrt{2}$ is not a rational number while traveling by ship with his Pythagorean colleagues. The Pythagoreans, steadfast believers that all numbers are rational*, supposedly threw him into the sea to drown.

The proof relies on the definition of a rational number: r is rational iff $r = \frac{a}{b}$ for some integers a and b, with $b \neq 0$. We may assume that that a and b have no common factors, because otherwise we would simply reduce $\frac{a}{b}$ by cancelling any common factors.

Example. $\sqrt{2}$ is an irrational number.

Proof. Assume that $\sqrt{2}$ is a rational number. ⟨*We assume* $\sim P$.⟩ Then $\sqrt{2} = \dfrac{a}{b}$ for some integers a and b, where $b \neq 0$ and a and b have no common factors. ⟨*The statement Q is "a and b have no common factors."*⟩ From $\sqrt{2} = \dfrac{a}{b}$ we have $2 = \dfrac{a^2}{b^2}$, which implies that $2b^2 = a^2$. Therefore a^2 is even and so a is even. (Recall the example we proved on page 40.) It follows that there exists an integer k such that $a = 2k$ and therefore

$$\begin{aligned} 2b^2 &= a^2 \\ &= (2k)^2 \\ &= 4k^2. \end{aligned}$$

Thus $b^2 = 2k^2$, which shows b^2 is even. Therefore b is even. Since both a and b are even, a and b do have a common factor of 2. ⟨*We have deduced the statement* $\sim Q$.⟩ This is a contradiction. We conclude that $\sqrt{2}$ is irrational. ■

Recall that a natural number greater than 1 is prime iff its only positive divisors are 1 and itself. The next proof by contradiction, attributed to Euclid, shows that there are infinitely many primes. By this we mean that it is impossible to list all of the prime numbers from the first to the kth (last) one, where k is a natural number. It uses the fundamental result that every natural number greater than 1 has a prime divisor.

Example. The set of primes is infinite.

Proof. Suppose the set of primes is finite. ⟨*Suppose* $\sim P$. *This means that the set of primes has k elements for some natural number k. Then the set of all primes can be listed, from the first one to the kth (last) one.*⟩ Let $p_1, p_2, p_3, \ldots, p_k$ be all those primes. Let n be one more than the product of all of them: $n = (p_1 p_2 p_3 \ldots p_k) + 1$. ⟨*We made up a number n which will not have any of the* p_i *as prime factors.*⟩ Then n is a natural number, so n has a prime divisor q. Since q is prime, $q > 1$. ⟨*The Q statement is*

* You may wonder why $\sqrt{2}$ is important or why it should be the first number to be proved irrational. The ancient Greeks geometers constructed numbers (lengths of line segments) using only a compass and a straightedge. It's easy to construct a square with sides of length 1, for which the length of a diagonal is $\sqrt{2}$. The fundamental Pythagorean belief that all numbers that arise in nature are either integers or ratios of integers is disproved by the irrationality of $\sqrt{2}$.

"$q > 1$.") Since q is a prime and $p_1, p_2, p_3, \ldots, p_k$ are *all* the primes, q is one of the p_i in the list. Thus, q divides the product $p_1 p_2 p_3 \ldots p_k$. Since q divides n, q divides the difference $n - (p_1 p_2 p_3 \ldots p_k)$. But this difference is 1, so $q = 1$. ⟨*This is* $\sim Q$.⟩ From the contradiction, $q > 1$ and $q = 1$, we conclude that the assumption that the set of primes is finite is false. Therefore, the set of primes is infinite. ■

Example. Prove the square shown in Figure 1.5.1(a) cannot be completed to form a "magic square" whose rows, columns, and diagonals all sum to the same number.

1	2	3	
	4	5	6
7		8	
	9		10

(a)

1	2	3	a
b	4	5	6
7	c	8	d
e	9	f	10

(b)

Figure 1.5.1

Proof. Suppose the square can be completed with entries a, b, c, d, e, f, as shown in Figure 1.5.1(b). Since the sums of the second row and second column are the same, $b + 15 = c + 15$. Thus, $b = c$. Comparing the sums of the first column and the lower-left to upper-right diagonal, $1 + b + 7 + e = e + c + 5 + a$. Thus, $a = 3$ and the first row sums to 9. Thus, the "magic sum" is 9. ⟨*This is our Q statement.*⟩ But the main diagonal sum $(1 + 4 + 8 + 10 = 23)$ is not 9. ⟨*This is our* $\sim Q$ *statement.*⟩ This is a contradiction. We conclude that the square cannot be completed. ■

Proofs of biconditional sentences $P \Leftrightarrow Q$ often make use of the tautology $(P \Leftrightarrow Q) \Leftrightarrow (P \Rightarrow Q) \wedge (Q \Rightarrow P)$. Proofs of $P \Leftrightarrow Q$ generally have the following two-part form:

TWO-PART PROOF OF $P \Leftrightarrow Q$
Proof.
(i) Show $P \Rightarrow Q$.
(ii) Show $Q \Rightarrow P$.
Therefore, $P \Leftrightarrow Q$. ■

The separate proofs of parts (i) and (ii) may use different methods. Often the proof of one part is easier than the other. This is true, for example, of the proof that

"The natural number p is prime iff there is no positive integer greater than 1 and less than or equal to $\sqrt{x}$ that divides x."

It immediately follows from the definition of prime that "x is prime" implies "there is no positive integer greater than 1 and less than or equal to $\sqrt{x}$ that divides x." The converse requires more thought and is an exercise in the next section.

The **parity** of an integer is the attribute of being either odd or even. The integer 31 has odd parity while 42 has even parity. The integers 12 and 15 have opposite parity. The next example is a proof of a biconditional statement about parity with a two part proof. Both parts of the proof have two cases. The proof we give is not the shortest possible, but it does illustrate the two part approach to proving a biconditional statement.

Example. Let m and n be integers. Then m and n have the same parity iff $m^2 + n^2$ is even.

Proof.

(i) Suppose m and n have the same parity. We have two cases.

(a) If both m and n are even then $m = 2k$ and $n = 2j$ for some integers k and j. Then $m^2 + n^2 = (2k)^2 + (2j)^2 = 2(2k^2 + 2j^2)$, which is even.

(b) If both m and n are odd then $m = 2k + 1$ and $n = 2j + 1$ for some integers k and j. Then $m^2 + n^2 = (2k + 1)^2 + (2j + 1)^2 = 2(2k^2 + 2k + 2j^2 + 2j + 1)$, which is even.

In both cases $m^2 + n^2$ is even.

(ii) Suppose $m^2 + n^2$ is even. ⟨*To show that n has the same parity as m, we use some previous examples and exercises about even and odd integers*.⟩ Again we have two cases.

(a) If m is even, then m^2 is even. Therefore, since $m^2 + n^2$ is even and m^2 is even, $n^2 = (m^2 + n^2) - m^2$ is even. From n^2 is even, we conclude that n is even.

(b) If m is odd, then m^2 is odd. Therefore, since $m^2 + n^2$ is even and m^2 is odd, $n^2 = (m^2 + n^2) - m^2$ is odd. From n^2 is odd, we conclude that n is odd.

Hence, if m is even, then n is even, and if m is odd, then n is odd. Therefore, m and n have the same parity. ■

In some cases it is possible to prove a biconditional sentence $P \Leftrightarrow Q$ that uses the "iff" connective throughout. This amounts to starting with P and then replacing it with a sequence of equivalent statements, the last one being Q. With n intermediate statements $R_1, R_2, \ldots, R_n$, a biconditional proof of $P \Leftrightarrow Q$ has the form:

BICONDITIONAL PROOF OF $P \Leftrightarrow Q$

Proof.

P iff R_1
iff R_2
...
iff R_n
iff Q. ■

Example. The triangle in Figure 1.5.2 has sides of length a, b, and c. Use the Law of Cosines to prove that the triangle is a right triangle with hypotenuse c if and only if $a^2 + b^2 = c^2$.

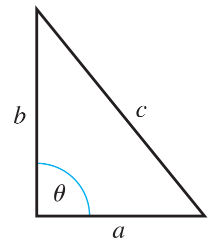

Figure 1.5.2

Proof. By the Law of Cosines, $a^2 + b^2 = c^2 - 2ab\cos\theta$, where θ is the angle between the sides of length a and b. Therefore,

$$\begin{aligned} a^2 + b^2 = c^2 \quad &\text{iff} \quad 2ab\cos\theta = 0 \\ &\text{iff} \quad \cos\theta = 0 \\ &\text{iff} \quad \theta = 90°. \end{aligned}$$

Thus, $a^2 + b^2 = c^2$ iff the triangle is a right triangle with hypotenuse c. ■

As the following example shows, many theorems are amenable to more than one proof technique. Two of the proofs below will use the fact that if a prime (2 in our case) divides the product of two integers, then it must divide at least one of the integers. This property, known as Euclid's Lemma, will be proved in Section 1.7.

Example. For given integers x and y, give a direct proof, a proof by contraposition, and a proof by contradiction of the following statement: If x and y are odd integers, then xy is odd.

Direct Proof. Assume x is odd and y is odd. Then integers m and n exist so that $x = 2m + 1$ and $y = 2n + 1$. Thus,

$$\begin{aligned} xy &= (2m + 1)(2n + 1) \\ &= 4mn + 2m + 2n + 1 \\ &= 2(2mn + m + n) + 1. \end{aligned}$$

Thus xy is an odd integer. ■

Proof by Contraposition. ⟨*The contrapositive of* x *is odd* $\wedge$ y *is odd* $\Rightarrow$ xy *is odd is the statement* xy *is even* $\Rightarrow \sim$(x *is odd* $\wedge$ y *is odd*), *or equivalently,*

$$xy \text{ is even} \Rightarrow (x \text{ is even} \vee y \text{ is even}).\rangle$$

Assume xy is even. Thus, 2 is a factor of xy. But since 2 is a prime number and 2 divides the product xy, then either 2 divides x or 2 divides y by Euclid's Lemma. We have shown that if xy is even, then either x or y is even. Thus, if x and y are odd, then xy is odd. ■

Proof by Contradiction. Suppose that the statement "If x and y are odd integers, then xy is odd" is false. Then x is odd and y is odd, and xy is not odd. Since xy is not odd, xy is even. Therefore 2 divides xy. Then by Euclid's Lemma, 2 divides x or 2 divides y. Thus either x is even or y is even. But x is odd and y is odd. This is a contradiction. We conclude that if x and y are odd integers, then xy is odd. ■

By now you may have the impression that, given a set of axioms and definitions of a mathematical system, any properly stated proposition in that system can be proved true or proved false. This is not the case. There are important examples in mathematics of **consistent axiom systems** (so that there exist structures satisfying all the axioms) for which there are statements such that neither the statement nor its negation can be proved. It is not a matter of these statements being difficult to prove or that no one has yet been clever enough to devise a proof; it has been proved that there can be no proof of either the statement or its negation within the system. Such statements are called **undecidable** in the system because their truth is independent of the truth of the axioms.

The classic case of an undecidable statement involves the fifth of five postulates that Euclid set forth as his basis for plane geometry: "Given a line and a point not on that line, exactly one line can be drawn through the point parallel to the line." For centuries, some thought Euclid's axioms were not independent, believing that the fifth postulate could be proved from the other four. It was not until the 19th century that it became clear that the fifth postulate was undecidable. There are now theories of Euclidean geometry for which the fifth postulate is assumed true and non-Euclidean geometries for which it is assumed false. Both are perfectly reasonable subjects for mathematical study and application.

Exercises 1.5

1. Analyze the logical form of each of the following statements and construct just the outline of a proof by the given method. Since the statements may contain terms with which you are not familiar, you should not (and perhaps could not) provide any details of the proof.

★ **(a)** Outline a proof by contraposition that if $(G, *)$ is a cyclic group, then $(G, *)$ is abelian.

(b) Outline a proof by contraposition that if **B** is a nonsingular matrix, then the determinant of **B** is not zero.

★ **(c)** Outline a proof by contradiction that the set of natural numbers is not finite.

(d) Outline a proof by contradiction that the multiplicative inverse of a nonzero real number x is unique.

★ **(e)** Outline a two-part proof that the inverse of the function f from A to B is a function from B to A if and only if f is one-to-one and onto B.

(f) Outline a two-part proof that a subset A of the real numbers is compact if and only if A is closed and bounded.

2. A theorem of linear algebra states that if **A** and **B** are invertible matrices, then the product **AB** is invertible. As in Exercise 1,

(a) outline a proof of the theorem by contraposition.
(b) outline a proof of the converse of the theorem by contraposition.
(c) outline a proof of the theorem by contradiction.
(d) outline a proof of the converse of the theorem by contradiction.
(e) outline a two-part proof that **A** and **B** are invertible matrices if and only if the product **AB** is invertible.

3. Let x, y, and z be integers. Write a proof by contraposition to show that

★ **(a)** if x is even, then $x + 1$ is odd.
(b) if x is odd, then $x + 2$ is odd.
(c) if x^2 is not divisible by 4, then x is odd.
(d) if xy is even, then either x or y is even.
☆ **(e)** if $x + y$ is even, then x and y have the same parity.
(f) if xy is odd, then both x and y are odd.
(g) if 8 does not divide $x^2 - 1$, then x is even.
(h) if x does not divide yz, then x does not divide z.

4. Write a proof by contraposition to show that for any real number x,

(a) if $x^2 + 2x < 0$, then $x < 0$.
★ **(b)** if $x^2 - 5x + 6 < 0$, then $2 < x < 3$.
(c) if $x^3 + x > 0$, then $x > 0$.

5. A circle has center $(2, 4)$.

(a) Prove that $(-1, 5)$ and $(5, 1)$ are not both on the circle.
(b) Prove that if the radius is less than 5, then the circle does not intersect the line $y = x - 6$.
(c) Prove that if $(0, 3)$ is not inside the circle, then $(3, 1)$ is not inside the circle.

6. Suppose a and b are positive integers. Write a proof by contradiction to show that

(a) if a divides b, then $a \le b$.
★ **(b)** if ab is odd, then both a and b are odd.
(c) if a is odd, then $a + 1$ is even.
(d) if $a - b$ is odd, then $a + b$ is odd.
(e) if $a < b$ and $ab < 3$, then $a = 1$.

7. Suppose a, b, c, and d are positive integers. Write a proof of each biconditional statement.

(a) ac divides bc if and only if a divides b.
(b) $a + 1$ divides b and b divides $b + 3$ if and only if $a = 2$ and $b = 3$.
(c) a is odd if and only if $a + 1$ is even.
(d) $a + c = b$ and $2b - a = d$ if and only if $a = b - c$ and $b + c = d$.

8. Let m and n be integers. Then prove that m and n have different parity iff $m^2 - n^2$ is odd.

9. Prove by contradiction that if n is a natural number, then

$$\frac{n}{n+1} > \frac{n}{n+2}.$$

10. Prove that $\sqrt{5}$ is not a rational number.

11. Three real numbers, x, y, and z, are chosen between 0 and 1 with $0 < x < y < z < 1$. Prove that at least two of the numbers x, y, and z are within $\frac{1}{2}$ unit from one another.

Proofs to Grade

12. Assign a grade of A (correct), C (partially correct), or F (failure) to each. Justify assignments of grades other than A.

(a) Suppose m is an integer.
Claim. If m^2 is odd, then m is odd.
"Proof." Assume that m^2 is not odd. Then m^2 is even and $m^2 = 2k$ for some integer k. Thus $2k$ is a perfect square; that is, $\sqrt{2k}$ is an integer. If $\sqrt{2k}$ is odd, then $\sqrt{2k} = 2n + 1$ for some integer n, which means $m^2 = 2k = (2n+1)^2 = 4n^2 + 4n + 1 = 2(2n^2 + 2n) + 1$. Thus m^2 is odd, contrary to our assumption. Therefore $\sqrt{2k} = m$ must be even. Thus if m^2 is not odd, then m is not odd. Hence if m^2 is odd, then m is odd. ■

★ **(b)** Suppose t is a real number.
Claim. If t is irrational, then $5t$ is irrational.
"Proof." Suppose $5t$ is rational. Then $5t = p/q$, where p and q are integers and $q \neq 0$. Therefore, $t = p/(5q)$, where p and $5q$ are integers and $5q \neq 0$, so t is rational. Therefore, if t is irrational, then $5t$ is irrational. ■

(c) Suppose x and y are integers.
Claim. If x and y are even then $x + y$ is even.
"Proof." Suppose x and y are even but $x + y$ is odd. Then, for some integer k, $x + y = 2k + 1$. Therefore, $x + y + (-2)k = 1$. The left side of the equation is even because it is the sum of even numbers. However, the right side, 1, is odd. Since an even cannot equal an odd, we have a contradiction. Therefore, $x + y$ is even. ■

(d) Suppose a, b, and c are integers.
Claim. If a divides both b and c, then a divides $b + c$.
"Proof." Assume that a does not divide $b + c$. Then there is no integer k such that $ak = b + c$. However, a divides b, so $am = b$ for some integer m; and a divides c, so $an = c$ for some integer n. Thus $am + an = a(m+n) = b + c$. Therefore $k = m + n$ is an integer satisfying $ak = b + c$. Thus the assumption that a does not divide $b + c$ is false, and a does divide $b + c$. ■

1.6 Proofs Involving Quantifiers

Recall that in our first example of a direct proof in Section 1.4 we proved the statement "If x is odd then $x + 1$ is even." That statement has the meaning "For every integer x, if x is odd then $x + 1$ is even." We dealt with the quantifier in that example by asking you to think of the variable x as some fixed integer. This section discusses specifically the proof methods for statements with quantifiers.

To prove a proposition of the form $(\forall x)P(x)$, we must show that $P(x)$ is true for every object x in the universe. A direct proof is begun by letting x represent an arbitrary object in the universe, and then showing that $P(x)$ is true for that object. In the proof we may use only properties of x that are shared by every element of the universe. Then, since x is arbitrary, we can conclude that $(\forall x)P(x)$ is true.

Thus a **direct proof** of $(\forall x)P(x)$ has the following form:

DIRECT PROOF OF $(\forall x)P(x)$

Proof.

Let x be an arbitrary object in the universe. (The universe should be named or its objects described.)

⋮

Hence $P(x)$ is true.

Since x is arbitrary, $(\forall x)P(x)$ is true. ■

A review of the proof examples in Sections 1.4 and 1.5 shows that whenever the statement was universally quantified, the proof given had the form of a complete proof, because each begins with an assumption such as "Let x be an integer" or "Let x and y be real numbers."

Example. Prove that for every natural number n, $4n^2 - 6.8n + 2.88 > 0$.

Proof. ⟨*The statement has the form* $(\forall x)P(x)$, *where the universe is* $\mathbb{N}$ *and* $P(x)$ *is* "$4n^2 - 6.8n + 2.88 > 0$."⟩ Let n be a natural number. Then $n \geq 1$, so $n - .8$ and $n - .9$ are both positive. Therefore $4(n - .8)(n - .9) = 4n^2 - 6.8n + 2.88$ is positive. We conclude that $4n^2 - 6.8n + 2.88 > 0$ for all natural numbers n. ■

Since the open sentence $P(x)$ in $(\forall x)P(x)$ will often be a combination of other open sentences joined by the logical connectives, the selection of an appropriate proof technique will depend on the logical form of $P(x)$. In the next example $P(x)$ has the form of a conditional sentence.

Example. If x is an even integer, then x^2 is an even integer.

Proof. ⟨*The statement has the form* $(\forall x)(A(x) \Rightarrow B(x))$, *where the universe is* $\mathbb{Z}$, $A(x)$ *is "x is even," and* $B(x)$ *is "x^2 is even."*⟩ Let $x \in \mathbb{Z}$. ⟨*We give a direct proof of* $A(x) \Rightarrow B(x)$, *which we begin by assuming* $A(x)$.⟩ Assume x is even. Then $x = 2k$ for some integer k. Thus $x^2 = (2k)^2 = 2(2k^2)$. Since $2k^2$ is an integer, x^2 is even. Since x is arbitrary, we have that for all $x \in \mathbb{Z}$, if x is even, then x^2 is even. ■

It is essential in a direct proof of $(\forall x)P(x)$ that the first step assume nothing about x other than it is an object in the universe. In the example above there are *two* assumptions about the variable x — for two very different reasons. The assumption "Let $x \in \mathbb{Z}$" appears first because we are assuming x is an object in the universe.

We make the statement "Assume x is even" because we are initiating a direct proof of a conditional sentence, which starts by assuming the antecedent.

It is a mistake to give an example (or several examples) of the statement "If x is even, then x^2 is even" and then claim that the statement has been proved for all natural numbers n. Examples may sometimes help decide whether a statement is true. Examples can also help guide our thinking about how to proceed with a proof. However, we cannot prove that a universally quantified statement is true by showing that it's true for selected values of the variable.

The next example involves two quantifiers.

Example. For all rational numbers x and y, $\frac{x+y}{2}$ is a rational number.

Proof. ⟨*The statement has the form* $(\forall x)(\forall y)P(x, y)$, *where the universe is* $\mathbb{Q}$ *and* $P(x, y)$ is "$\frac{x+y}{2}$ *is rational*."⟩ Let x and y be rational numbers. Then

$$\frac{x+y}{2} = \frac{1}{2}\left(\frac{p}{q} + \frac{s}{t}\right) = \frac{1}{2}\left(\frac{pt+qs}{qt}\right) = \frac{pt+qs}{2qt}.$$

Both $pt + qs$ and $2qt$ are integers and $2qt \neq 0$. ⟨*The sums and products of integers are integers. The product of three nonzero numbers is not zero.*⟩ Therefore, $\frac{x+y}{2}$ is a rational number. ■

The method of proof by contradiction is often used to prove statements of the form $(\forall x)P(x)$. Since $\sim(\forall x)P(x)$ is equivalent to $(\exists x)\sim P(x)$, the form of the proof is as follows:

PROOF OF $(\forall x)P(x)$ BY CONTRADICTION
Proof.
Suppose $\sim(\forall x)P(x)$.
Then $(\exists x)\sim P(x)$.
Let t be an object such that $\sim P(t)$.
⋮
Therefore $Q \wedge \sim Q$.
Thus $(\exists x)\sim P(x)$ is false, so $(\forall x)P(x)$ is true. ■

The following example of a proof by contradiction comes from an exercise in a trigonometry class. It uses algebraic and trigonometric properties available to students in the class.

Example. Prove that for all $x \in \left(0, \frac{\pi}{2}\right)$, $\sin x + \cos x > 1$.

Proof. ⟨*The statement has the form* $(\forall x)P(x)$, *where the universe is the open interval* $\left(0, \frac{\pi}{2}\right)$ *and* $P(x)$ *is* "$\sin x + \cos x > 1$."⟩ Suppose that the statement is false. Then there exists a real number t, with $0 < t < \frac{\pi}{2}$, such that $\sin t + \cos t \leq 1$. ⟨*We have deduced* $(\exists t) \sim P(t)$.⟩ Since the functions $\sin x$ and $\cos x$ are positive for every $x \in \left(0, \frac{\pi}{2}\right)$ $\sin t > 0$ and $\cos t > 0$. Therefore,

$$\begin{aligned} 0 &< \sin t + \cos t \leq 1 \\ 0 &< (\sin t + \cos t)^2 \leq 1^2 = 1 \\ 0 &< \sin^2 t + 2 \sin t \cos t + \cos^2 t \leq 1 \\ 0 &< 1 + 2 \sin t \cos t \leq 1 \\ -1 &< 2 \sin t \cos t \leq 0. \end{aligned}$$

⟨*We use the identity* $\sin^2 t + \cos^2 t = 1$.⟩ But $2 \sin t \cos t \leq 0$ is impossible since both $\sin t$ and $\cos t$ are positive. Therefore, if $0 < x < \frac{\pi}{2}$, then $\sin x + \cos x > 1$. ■

Notice the different roles that the symbols "x" and "t" play in the above example. The variable x is used to express the statement of the theorem and also appears as the independent variable in the sine and cosine functions. The symbol t represents some fixed value in $\left(0, \frac{\pi}{2}\right)$ with the property that $\sin t + \cos t \leq 1$.

There are several ways to prove existence theorems—that is, propositions of the form $(\exists x) P(x)$. In a **constructive proof** we actually name an object a in the universe such that $P(a)$ is true, which directly verifies that the truth set of $P(x)$ is nonempty. Some constructive proofs are quite easy to devise. For example, to prove that "There is an even prime natural number," we simply observe that 2 is prime and 2 is even.

Other constructive proofs have eluded mathematicians for centuries. The question of whether any nth power is a sum of fewer than n nth powers was raised by Leonard Euler* in the mid 1700s. A computer search in 1968 discovered a fifth power that was the sum of four fifth powers. Here is an example for fourth powers.

Example. Prove that there exists a natural number whose fourth power is the sum of three other fourth powers.

Proof. 20,615,673 is one such number because

$$20615673^4 = 2682440^4 + 15365639^4 + 18796760^4.$$ ■

Another strategy to prove $(\exists x) P(x)$ is to show that there must be some object for which $P(x)$ is true, without ever actually producing a particular object. Both Rolle's Theorem and the Mean Value Theorem from calculus are good examples of this. Here is another.

* Leonard Euler (1707–1783) was a brilliant Swiss mathematician who spent much of his career at the Imperial Russian Academy of Sciences in St. Petersburg and the Berlin Academy. He made profound contributions to calculus, number theory, and graph theory as well as physics and astronomy. He was the first to introduce the idea of function and the familiar $f(x)$ notation.

Example. Prove that the polynomial

$$r(x) = x^{71} - 2x^{39} + 5x - 0.3$$

has a real zero.

Proof. ⟨*The universe is* $\mathbb{R}$. *The statement has the form* $(\exists t)(r(t) = 0)$.⟩ By the Fundamental Theorem of Algebra[†], $r(x)$ has 71 zeros that are either real or complex. Since the polynomial has real coefficients, its nonreal zeros come in pairs ⟨*by the Complex Root Theorem*⟩. Hence the number of nonreal zeros is even, and that leaves an odd number of real zeros. Therefore, $r(x)$ has at least one real zero. ∎

Existence theorems may also be proved by **contradiction.** The proof technique has the following form:

> **PROOF OF $(\exists x)P(x)$ BY CONTRADICTION**
> **Proof.**
> Suppose $\sim(\exists x)P(x)$.
> Then $(\forall x) \sim P(x)$
> ⋮
> Therefore, $\sim Q \wedge Q$, a contradiction.
> Thus $\sim(\exists x)P(x)$ is false.
> Therefore $(\exists x)P(x)$ is true. ∎

The core of a proof of $(\exists x)P(x)$ by contradiction involves making deductions from the statement $(\forall x) \sim P(x)$.

Example. Starting at 9 a.m. on Monday a hiker walked from a base camp up a mountain trail and reached the summit at exactly 3 p.m. The hiker camped for the night and then hiked back down the same trail, again starting at 9 a.m. On this second walk the hiker stopped to look at a scenic overlook, but walked faster on other parts of the trail and returned to the starting point in exactly six hours. Prove that there is some point on the trail that the hiker passed at the identical time on the two days.

Proof. Clearly, the point on the trail is not at the base camp or summit. ⟨*The universe is the open interval* $(0, 6)$, *representing the time between* $t = 0$ (9 *a.m.*) and $t = 6$ (3 *p.m.*) *along the trail. The statement has the form* $\exists t \in (0, 6)$ (*the point on the trail at time t on Monday is the same as the point on the trail at time t on Tuesday*).⟩ Suppose there is no such point along the trail. Then for every time $t \in (0, 6)$, the point where the hiker is at time t on Monday is different from the point where the hiker is at time t on Tuesday. Have two other people simultaneously walk the trail, starting at 9 a.m. One goes up the trail at exactly the pace set by the hiker on

[†] The Fundamental Theorem of Algebra says that every polynomial in one variable with complex coefficients and degree $n > 0$ has exactly n zeros, counting multiplicities.

Monday and the other walks down the trail at exactly the pace set by the hiker on Tuesday. Since these two people are at different points at every time between 9 a.m. and noon, they will never meet. But they must meet at some point on the trail. This is a contradiction. Therefore there is some point on the trail that the hiker passed at the same time on the two days. ■

Sometimes a statement to be proved has the form $(\exists x)P(x) \Rightarrow Q$. As a first step, we assume $(\exists x)P(x)$. However, the fact that *some* object x in the universe has the property $P(x)$ does not give us much to work with. A useful next step is to name some particular object that has the property and use the property of the object to derive Q.

Example. The graph of $x^2 + y^2 = r^2$, with $r > 0$, is a circle with center $(0, 0)$ and radius r. Prove that if one of the x-intercepts of the circle has rational coordinates, then all four intercepts have rational coordinates.

Proof. Suppose an x-intercept $(a, 0)$ of the circle has rational coordinates. Then a is a rational number and $a^2 + 0^2 = r^2$, so $a^2 = r^2$ and $a = \pm r$. Then the other x-intercept is $(-a, 0)$. To find the y-intercepts, we solve $0^2 + y^2 = r^2$ and find $y = \pm r = \pm a$. Therefore, the four intercepts are $(a, 0)$, $(-a, 0)$, $(0, a)$, and $(0, -a)$, all of which have rational coordinates. ■

Many statements have more than one quantifier. We must deal with each in succession, starting from the left.

Example. Between any two rational numbers x and y, where $x < y$, there is always another rational number z.

Proof. ⟨*The statement may be symbolized* $(\forall x \in \mathbb{Q})(\forall y \in \mathbb{Q})[x < y \Rightarrow (\exists z \in \mathbb{Q})(x < z < y)]$. *We begin with the two universal quantifers.*⟩ Suppose x and y are rational numbers. Assume that $x < y$. ⟨*Now we must prove the existence of a rational number* z *with the given property.*⟩ We choose $z = \dfrac{x+y}{2}$. By a previous example, z is a rational number. Furthermore,

$$x = \frac{x+x}{2} < \frac{x+y}{2} < \frac{y+y}{2} = y.$$

Therefore $x < z < y$. ■

Example. Prove that for every natural number n, there is a natural number M such that for all natural numbers $m > M$,

$$\frac{1}{m} < \frac{1}{3n}.$$

Proof. ⟨*The statement may be symbolized by*

$$(\forall n \in \mathbb{N})(\exists M \in \mathbb{N})(\forall m \in \mathbb{N})\left(m > M \Rightarrow \frac{1}{m} < \frac{1}{3n}\right).$$

We begin with the universal quantifier on the left.⟩ Let n be a natural number. ⟨*We must prove the existence of a natural number M with the given property.*⟩ Choose M to be $3n$. Let m be a natural number, and suppose $m > M$. Then $m > 3n$, and $3mn > 0$, so dividing by $3mn$ we have $\frac{1}{m} < \frac{1}{3n}$. ⟨*The choice of 3n for M is the result of some scratchwork, working backward from the intended conclusion* $\frac{1}{m} < \frac{1}{3n}$.⟩ ■

Example. There is a real number with the property that for any two larger numbers there is another real number that is larger than the sum of the two numbers and less than their product.

Proof. ⟨*The universe is* $\mathbb{R}$. *A symbolic form of the statement is*

$$(\exists z)(\forall x)(\forall y)[(x > z \wedge y > z) \Rightarrow (\exists w)(x + y < w < xy)].$$

We must choose z so that the statement

$$(x > z \wedge y > z) \Rightarrow (\exists w)(x + y < w < xy)$$

will be true for all x and y.⟩ We chose $z = 2$. ⟨*To understand this choice for z, first notice that* $x + y$ *is not always less than* xy. *For example, let* $x = 1.6$ *and* $y = 1.4$.⟩ Let x and y be real numbers such that $x > z$ and $y > z$. Without loss of generality, we may assume that $y \geq x$. ⟨*Otherwise, we could rename x and y.*⟩ Then

$$x + y \leq 2y < xy.$$

Now choose w to be the midpoint between $x + y$ and xy, so $w = \frac{(x + y) + xy}{2}$. We have $x + y < w < xy$. ■

A proof of a statement about unique existence always involves multiple quantifiers. The standard technique for proving a proposition of the form $(\exists!x)P(x)$ is based on proving the equivalent statement: $(\exists x)P(x) \wedge (\forall y)(\forall z)[P(y) \wedge P(z) \Rightarrow y = z]$. Since the main connective is a conjunction, the method will have two parts:

PROOF OF $(\exists!x)P(x)$

Proof.

(i) Prove that $(\exists x)P(x)$ is true. Use any method.

(ii) Prove that $(\forall y)(\forall z)[P(y) \wedge P(z) \Rightarrow y = z]$.

Assume that y and z are objects in the universe such that $P(y)$ and $P(z)$ are true.

⋮

Therefore, $y = z$.

From (i) and (ii) conclude that $(\exists!x)P(x)$ is true. ■

Example. Every nonzero real number has a unique multiplicative inverse.

Proof. ⟨*The statement has the form* $(\forall x \in \mathbb{R})(x \neq 0 \Rightarrow (\exists! y \in \mathbb{R})(xy = 1)$.⟩ Let $x \neq 0$. ⟨*We show there is a unique real number* y *such that* $xy = 1$ *in two steps: First show that such a number* y *exists, and then show that* x *cannot have two different inverses*.⟩

(i) ⟨*This part is a constructive proof*.⟩ Let $y = \frac{1}{x}$. Since $x \neq 0$, y is a real number. Then $xy = x\left(\frac{1}{x}\right) = 1$. Therefore, x has a multiplicative inverse.

(ii) Now suppose that y and z are multiplicative inverses for x. ⟨*We do not assume that this* y *is the same as the* y *in part* (i).⟩ Then $xy = 1$ and $xz = 1$, so

$$\begin{aligned} xy &= xz \\ xy - xz &= 0 \\ x(y - z) &= 0. \end{aligned}$$

Since $x \neq 0$, $y - z = 0$. Therefore $y = z$. ■

Great care must be taken in proofs that contain expressions involving more than one quantifier. Here are some manipulations of quantifiers that permit valid deductions.

1. $(\forall x)(\forall y)P(x, y) \Leftrightarrow (\forall y)(\forall x)P(x, y)$.
2. $(\exists x)(\exists y)P(x, y) \Leftrightarrow (\exists y)(\exists x)P(x, y)$.
3. $[(\forall x)P(x) \vee (\forall x)Q(x)] \Rightarrow (\forall x)[P(x) \vee Q(x)]$.
4. $(\forall x)[P(x) \Rightarrow Q(x)] \Rightarrow [(\forall x)P(x) \Rightarrow (\forall x)Q(x)]$.
5. $(\forall x)[P(x) \wedge Q(x)] \Leftrightarrow [(\forall x)P(x) \wedge (\forall x)Q(x)]$.
6. $(\exists x)(\forall y)P(x, y) \Rightarrow (\forall y)(\exists x)P(x, y)$.

You should convince yourself that each of these is a logically valid conditional or biconditional. For example, the last on the list is always true because if $(\exists x)(\forall y)P(x, y)$ is true, then there is (at least) one x that makes $P(x, y)$ true no matter what y is. Therefore, for any y, $(\exists x)P(x, y)$ is true because this particular x exists.

It is important to be aware of the most common *incorrect deductions* making use of quantifiers. We list four here and show by example that each is not valid. Notice that statements 2, 3, and 4 in the following list are the converses, respectively, of valid deductions of statements 3, 4, and 6 above.

1. $(\exists x)P(x) \Rightarrow (\forall x)P(x)$ *is not valid*.
   The implication says that if some object has property P, then all objects have property P. If the universe is all integers and $P(x)$ is the sentence "x is odd," then $P(5)$ is true and $P(8)$ is false. Thus, $(\exists x)P(x)$ is true and $(\forall x)P(x)$ is false, so the implication fails.
2. $(\forall x)[P(x) \vee Q(x)] \Rightarrow [(\forall x)P(x) \vee (\forall x)Q(x)]$ *is not valid*.
   This implication says that if every object has one of two properties, then either every object has the first property or every object has the second property.

Suppose the universe is the integers, $P(x)$ is "x is odd" and $Q(x)$ is "x is even." Then it is true that "All integers are either odd or even" but false that "Either all integers are odd or all integers are even."

3. $[(\forall x)P(x) \Rightarrow (\forall x)Q(x)] \Rightarrow (\forall x)[P(x) \Rightarrow Q(x)]$ *is not valid*.
The implication says that if every object has property P implies every object has property Q, then every object that has property P must also have property Q. Again, let the universe be the integers and let $P(x)$ be "x is odd" and $Q(x)$ be "x is even." Because $(\forall x)P(x)$ is false, $(\forall x)P(x) \Rightarrow (\forall x)Q(x)$ is true. However, $(\forall x)[P(x) \Rightarrow Q(x)]$ is false.

4. $(\forall y)(\exists x)P(x, y) \Rightarrow (\exists x)(\forall y)P(x, y)$ *is not valid*.
This is probably the most troublesome of all the possibilities for dealing with quantifiers. The implication says that if for every y there is some x that satisfies P, then there is an x that works with every y to satisfy P. Let the universe be the set of all married people and $P(x, y)$ be the sentence "x is married to y." Then $(\forall y)(\exists x)P(x, y)$ is true, since everyone is married to someone. But $(\exists x)(\forall y)P(x, y)$ would be translated as "There is some married person who is married to every married person," which is clearly false.

There are times when we will want to prove a quantified statement is *false*. We know that $(\forall x)P(x)$ is false precisely when $\sim(\forall x)P(x)$ is true and $\sim(\forall x)P(x)$ is equivalent to $(\exists x)\sim P(x)$. Therefore, one way to prove $(\forall x)P(x)$ is false is to prove $(\exists x)\sim P(x)$ is true.

A constructive proof of $(\exists x)(\sim P(x))$ names an object a in the universe such that $P(a)$ is false. The object a is called a **counterexample** to $(\forall x)P(x)$. The number 2 is a counterexample to the statement "All primes are odd." The function $f(x) = |x|$ is a counterexample to "Every function that is continuous at 0 is differentiable at 0."

Example. Some beginning algebra students believe that $(x + y)^2 = x^2 + y^2$. In symbolic terms, they believe that $(\forall x)(\forall y)[(x + y)^2 = x^2 + y^2]$ is true in the universe of real numbers. This mistake could be corrected by providing a counterexample—for instance, $x = 3$ and $y = 4$.

Our last example in this section is a proof of a statement of the form $\sim(\exists x)P(x)$, which means it is also an example of a proof of an equivalent statement of the form $(\forall x)\sim P(x)$. We proved in Section 1.4 that every odd integer can be written in the form $4j - 1$ or $4k + 1$. We now show that there does not exist an integer that can be written in both of these forms. The proof is by contradiction.

Example. There is no odd integer that can be expressed in the form $4j - 1$ and in the form $4k + 1$ for integers j and k.

Proof. Suppose n is an odd integer, and suppose $n = 4j - 1$ and $n = 4k + 1$ for integers j and k. Then $4j - 1 = 4k + 1$, so $4j - 4k = 2$. Therefore, $2j - 2k = 1$. The left side of this equation is $2(j - k)$, which is even, but 1 is odd. This is a contradiction. ■

Exercises 1.6

1. Prove that
★ **(a)** there exist integers m and n such that $2m + 7n = 1$.
(b) there exist integers m and n such that $15m + 12n = 3$.
★ **(c)** there do not exist integers m and n such that $2m + 4n = 7$.
(d) there do not exist integers m and n such that $12m + 15n = 1$.
(e) for every integer t, if there exist integers m and n such that $15m+16n=t$, then there exist integers r and s such that $3r + 8s = t$.
☆ **(f)** if there exist integers m and n such that $12m + 15n = 1$, then m and n are both positive.
(g) for every odd integer m, if m has the form $4k + 1$ for some integer k, then $m + 2$ has the form $4j - 1$ for some integer j.
(h) for every odd integer m, $m^2 = 8k + 1$ for some integer k. (*Hint:* Use the fact that $k(k + 1)$ is an even integer for every integer k.)
(i) for all odd integers m and n, if $mn = 4k - 1$ for some integer k, then m or n is of the form $4j - 1$ for some integer j.

2. Prove that for all integers a, b, and c,
(a) if c divides a and c divides b, then for all integers x and y, c divides $ax + by$.
★ **(b)** if a divides $b - 1$ and a divides $c - 1$, then a divides $bc - 1$.
(c) if a divides b, then for all natural numbers n, a^n divides b^n.
(d) if a is odd, $c > 0$, c divides a and c divides $a + 2$, then $c = 1$.
(e) if there exist integers m and n such that $am + bn = 1$ and $c \neq \pm 1$, then c does not divide a or c does not divide b.

3. Prove that if every even natural number greater than 2 is the sum of two primes,* then every odd natural number greater than 5 is the sum of three primes.

4. Provide either a proof or a counterexample for each of these statements.
(a) For all positive integers x, $x^2 + x + 41$ is a prime.
(b) $(\forall x)(\exists y)(x + y = 0)$. (Universe of all reals)
(c) $(\forall x)(\forall y)(x > 1 \wedge y > 0 \Rightarrow y^x > x)$. (Universe of all reals)
(d) For integers a, b, c, if a divides bc, then either a divides b or a divides c.
(e) For integers a, b, c, and d, if a divides $b - c$ and a divides $c - d$, then a divides $b - d$.
(f) For all positive real numbers x, $x^2 - x \geq 0$.
(g) For all positive real numbers x, $2^x > x + 1$.
☆ **(h)** For every positive real number x, there is a positive real number y less than x with the property that for all positive real numbers z, $yz \geq z$.
☆ **(i)** For every positive real number x, there is a positive real number y with the property that if $y < x$, then for all positive real numbers z, $yz \geq z$.

5. **(a)** Prove that the natural number x is prime iff $x > 1$ and there is no positive integer greater than 1 and less than or equal to $\sqrt{x}$ that divides x.

* No one knows whether every even number greater than 2 is the sum of two prime numbers. This is the famous Goldbach Conjecture, proposed by the Prussian mathematician Christian Goldbach in 1742. You should search the Web to learn about the million dollar prize (never claimed) for proving Goldbach's Conjecture. Fortunately, you don't have to prove Goldbach's Conjecture to do this exercise.

(b) Prove that if p is a prime number and $p \neq 3$, then 3 divides $p^2 + 2$. (*Hint:* When p is divided by 3, the remainder is either 0, 1, or 2. That is, for some integer k, $p = 3k$ or $p = 3k + 1$ or $p = 3k + 2$.)

6. Prove that
   (a) for every natural number n, $\frac{1}{n} \leq 1$. (*Hint:* Use the fact that $n \geq 1$ and divide by the positive number n.)
   (b) there is a natural number M such that for all natural numbers $n > M$, $\frac{1}{n} < 0.13$.
   ★ (c) for every natural number n, there is a natural number M such that $2n < M$.
   (d) there is a natural number M such that for every natural number n, $\frac{1}{n} < M$.
   (e) there is no largest natural number.
   (f) there is no smallest positive real number.
   ★ (g) for every real number $\varepsilon > 0$, there is a natural number M such that for all natural numbers $n > M$, $\frac{1}{n} < \varepsilon$.
   ☆ (h) for every real number $\varepsilon > 0$, there is a natural number M such that if $m > n > M$, then $\frac{1}{n} - \frac{1}{m} < \varepsilon$.
   (i) there is a natural number K such that $\frac{1}{r^2} < 0.01$ whenever r is a real number larger than K.
   (j) there exist integers L and G such that $L < G$ and for every real number x, if $L < x < G$, then $40 > 10 - 2x > 12$.
   (k) there exists an odd integer M such that for all real numbers r larger than M, $\frac{1}{2r} < 0.01$.
   (l) for every natural number x there is an integer k such that $3.3x + k < 50$.
   (m) there exist integers $x < 100$ and $y < 30$ such that $x + y < 128$ and for all real numbers r and s, if $r > x$ and $s > y$, then $(r - 50)(s - 20) > 390$.
   (n) for every pair of positive real numbers x and y where $x < y$, there exists a natural number M such that if n is a natural number and $n > M$, then $\frac{1}{n} < (y - x)$.

Proofs to Grade

7. Assign a grade of A (correct), C (partially correct), or F (failure) to each. Justify assignments of grades other than A.
   ★ (a) **Claim.** Every polynomial of degree 3 with real coefficients has a real zero.
   "Proof." The polynomial $p(x) = x^3 - 8$ has degree 3, real coefficients, and a real zero ($x = 2$). Thus the statement "Every polynomial of degree 3 with real coefficients does not have a real zero" is false, and hence its denial, "Every polynomial of degree 3 with real coefficients has a real zero," is true. ■
   ★ (b) **Claim.** There is a unique polynomial whose first derivative is $2x + 3$ and which has a zero at $x = 1$.
   "Proof." The antiderivative of $2x + 3$ is $x^2 + 3x + C$. If we let $p(x) = x^2 + 3x - 4$, then $p'(x) = 2x + 3$ and $p(1) = 0$. So $p(x)$ is the desired polynomial. ■

(c) **Claim.** Every prime number greater than 2 is odd.
"Proof." The prime numbers greater than 2 are 3, 5, 7, 11, 13, 17, 19, ... None of these are even, so all of them are odd. ■

★ **(d)** **Claim.** There exists an irrational number r such that $r^{\sqrt{2}}$ is rational.
"Proof." If $\sqrt{3}^{\sqrt{2}}$ is rational, then $r = \sqrt{3}$ is the desired example. Otherwise, $\sqrt{3}^{\sqrt{2}}$ is irrational and $(\sqrt{3}^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{3})^2 = 3$, which is rational. Therefore either $\sqrt{3}$ or $\sqrt{3}^{\sqrt{2}}$ is an irrational number r such that $r^{\sqrt{2}}$ is rational. ■

(e) **Claim.** For every real number x, $|x| \geq 0$.
"Proof." We proceed by three cases: $x > 0$, $x = 0$, and $x < 0$.

Case 1. $x > 0$. Choose, for example, $x = 4$. Then $|4| = 4$. Thus $|x| \geq 0$.
Case 2. $x = 0$. Then $|0| = 0$. Thus, $|x| \geq 0$.
Case 3. $x < 0$. Choose, for example, $x = -5$. Then $|-5| = 5$. Thus $|x| \geq 0$. ■

(f) **Claim.** If x is prime, then $x + 7$ is composite.
"Proof." Let x be a prime number. If $x = 2$, then $x + 7 = 9$, which is composite. If $x \neq 2$, then x is odd, so $x + 7$ is even and greater than 2. In this case, too, $x + 7$ is composite. Therefore, if x is prime, then $x + 7$ is composite. ■

(g) **Claim.** For all irrational numbers t, $t - 8$ is irrational.
"Proof." Suppose there exists an irrational number t such that $t - 8$ is rational. Then $t - 8 = \frac{p}{q}$, where p and q are integers and $q \neq 0$. Then $t = \frac{p}{q} + 8 = \dfrac{p + 8q}{q}$, with $p + 8q$ and q integers and $q \neq 0$. This is a contradiction because t is irrational. Therefore, for all irrational numbers t, $t - 8$ is irrational. ■

(h) **Claim.** For real numbers x and y, if $xy = 0$ then $x = 0$ or $y = 0$.
"Proof."

Case 1. If $x = 0$, then $xy = 0y = 0$.
Case 2. If $y = 0$, then $xy = x0 = 0$.

In either case, $xy = 0$. ■

☆ **(i)** **Claim.** For every real number $\varepsilon > 0$, there is a natural number K such that for all real numbers $x > K$, $\dfrac{1}{4x} < \varepsilon$.
"Proof." Let $\varepsilon > 0$ be a real number. Let K be $\dfrac{1}{2\varepsilon}$. Assume x is a real number and $x > K$. Then $x > \dfrac{1}{2\varepsilon}$, so $x > \dfrac{1}{4\varepsilon}$. Therefore, $4x\varepsilon > 1$, so $\dfrac{1}{4x} < \varepsilon$. ■

(j) **Claim.** For every natural number n, $n \leq n^2$.
"Proof." Let n be a natural number. Since n is a natural number, $1 \leq n$. Since n is positive, $n \cdot 1 \leq n \cdot n$. Therefore, $n \leq n^2$ for all natural numbers n. ■