Chapter 3

Constructing and Writing Proofs in Mathematics

3.1 Direct Proofs

Beginning Activity 1 (**Definition of Divides, Divisor, Multiple**)
In Section 1.2, we studied the concepts of even integers and odd integers. The definition of an even integer was a formalization of our concept of an even integer as being one that is "divisible by 2," or a "multiple of 2." We could also say that if "2 divides an integer," then that integer is an even integer. We will now extend this idea to integers other than 2. Following is a formal definition of what it means to say that a nonzero integer m divides an integer n.

Definition. A nonzero integer m **divides** an integer n provided that there is an integer q such that $n = m \cdot q$. We also say that m is a **divisor** of n, m is a **factor** of n, and n is a **multiple** of m. The integer 0 is not a divisor of any integer. If a and b are integers and $a \neq 0$, we frequently use the notation $a \mid b$ as a shorthand for "a divides b."

A Note about Notation: Be careful with the notation $a \mid b$. This does not represent the rational number $\frac{a}{b}$. The notation $a \mid b$ represents a relationship between the integers a and b and is simply a shorthand for "a divides b."

A Note about Definitions: Technically, a definition in mathematics should almost always be written using "if and only if." It is not clear why, but the convention in

mathematics is to replace the phrase "if and only if" with "if" or an equivalent. Perhaps this is a bit of laziness or the "if and only if" phrase can be a bit cumbersome. In this text, we will often use the phrase "provided that" instead.

The definition for "divides" can be written in symbolic form using appropriate quantifiers as follows: A nonzero integer m **divides** an integer n provided that $(\exists q \in \mathbb{Z})\ (n = m \cdot q)$.

1. Use the definition of divides to explain why 4 divides 32 and to explain why 8 divides -96.
2. Give several examples of two integers where the first integer does not divide the second integer.
3. According to the definition of "divides," does the integer 10 divide the integer 0? That is, is 10 a divisor of 0? Explain.
4. Use the definition of "divides" to complete the following sentence in symbolic form: "The nonzero integer m does not divide the integer n means that ...."
5. Use the definition of "divides" to complete the following sentence without using the symbols for quantifiers: "The nonzero integer m does not divide the integer n ...."
6. Give three different examples of three integers where the first integer divides the second integer and the second integer divides the third integer.

As we have seen in Section 1.2, a definition is frequently used when constructing and writing mathematical proofs. Consider the following conjecture:

Conjecture: *Let a, b, and c be integers with $a \neq 0$ and $b \neq 0$. If a divides b and b divides c, then a divides c.*

7. Explain why the examples you generated in part (6) provide evidence that this conjecture is true.

In Section 1.2, we also learned how to use a **know-show table** to help organize our thoughts when trying to construct a proof of a statement. If necessary, review the appropriate material in Section 1.2.

8. State precisely what we would assume if we were trying to write a proof of the preceding conjecture.

9. Use the definition of "divides" to make some conclusions based on your assumptions in part (8).

10. State precisely what we would be trying to prove if we were trying to write a proof of the conjecture.

11. Use the definition of divides to write an answer to the question, "How can we prove what we stated in part (10)?"

Beginning Activity 2 (Calendars and Clocks)
This activity is intended to help with understanding the concept of congruence, which will be studied at the end of this section.

1. Suppose that it is currently Tuesday.

(**a**) What day will it be 3 days from now?

(**b**) What day will it be 10 days from now?

(**c**) What day will it be 17 days from now? What day will it be 24 days from now?

(**d**) Find several other natural numbers x such that it will be Friday x days from now.

(**e**) Create a list (in increasing order) of the numbers $3, 10, 17, 24$, and the numbers you generated in Part (1d). Pick any two numbers from this list and subtract one from the other. Repeat this several times.

(**f**) What do the numbers you obtained in Part (1e) have in common?

2. Suppose that we are using a twelve-hour clock with no distinction between A.M. and P.M. Also, suppose that the current time is 5:00.

(**a**) What time will it be 4 hours from now?

(**b**) What time will it be 16 hours from now? What time will it be 28 hours from now?

(**c**) Find several other natural numbers x such that it will be 9:00 x hours from now.

(**d**) Create a list (in increasing order) of the numbers $4, 16, 28$, and the numbers you generated in Part (2c). Pick any two numbers from this list and subtract one from the other. Repeat this several times.

(**e**) What do the numbers you obtained in Part (2d) have in common?

3. This is a continuation of Part (1). Suppose that it is currently Tuesday.

(**a**) What day was it 4 days ago?

(**b**) What day was it 11 days ago? What day was it 18 days ago?

(**c**) Find several other natural numbers x such that it was Friday x days ago.

(**d**) Create a list (in increasing order) consisting of the numbers $-18, -11, -4$, the opposites of the numbers you generated in Part (3c) and the positive numbers in the list from Part (1e). Pick any two numbers from this list and subtract one from the other. Repeat this several times.

(**e**) What do the numbers you obtained in Part (3d) have in common?

Some Mathematical Terminology

In Section 1.2, we introduced the idea of a direct proof. Since then, we have used some common terminology in mathematics without much explanation. Before we proceed further, we will discuss some frequently used mathematical terms.

A **proof** in mathematics is a convincing argument that some mathematical statement is true. A proof should contain enough mathematical detail to be convincing to the person(s) to whom the proof is addressed. In essence, a proof is an argument that communicates a mathematical truth to another person (who has the appropriate mathematical background). A proof must use correct, logical reasoning and be based on previously established results. These previous results can be axioms, definitions, or previously proven theorems. These terms are discussed below.

Surprising to some is the fact that in mathematics, there are always **undefined terms**. This is because if we tried to define everything, we would end up going in circles. Simply put, we must start somewhere. For example, in Euclidean geometry, the terms "point," "line," and "contains" are undefined terms. In this text, we are using our number systems such as the natural numbers and integers as undefined terms. We often assume that these undefined objects satisfy certain properties. These assumed relationships are accepted as true without proof and are called axioms (or postulates). An **axiom** is a mathematical statement that is accepted without proof. Euclidean geometry starts with undefined terms and a set of postulates and axioms. For example, the following statement is an axiom of Euclidean geometry:

Given any two distinct points, there is exactly one line that contains these two points.

The closure properties of the number systems discussed in Section 1.1 and the properties of the number systems in Table 1.2 on page 18 are being used as axioms in this text.

A **definition** is simply an agreement as to the meaning of a particular term. For example, in this text, we have defined the terms "even integer" and "odd integer." Definitions are not made at random, but rather, a definition is usually made because a certain property is observed to occur frequently. As a result, it becomes convenient to give this property its own special name. Definitions that have been made can be used in developing mathematical proofs. In fact, most proofs require the use of some definitions.

In dealing with mathematical statements, we frequently use the terms "conjecture," "theorem," "proposition," "lemma," and "corollary." A **conjecture** is a statement that we believe is plausible. That is, we think it is true, but we have not yet developed a proof that it is true. A **theorem** is a mathematical statement for which we have a proof. A term that is often considered to be synonymous with "theorem" is **proposition**.

Often the proof of a theorem can be quite long. In this case, it is often easier to communicate the proof in smaller "pieces." These supporting pieces are often called lemmas. A **lemma** is a true mathematical statement that was proven mainly to help in the proof of some theorem. Once a given theorem has been proven, it is often the case that other propositions follow immediately from the fact that the theorem is true. These are called corollaries of the theorem. The term **corollary** is used to refer to a theorem that is easily proven once some other theorem has been proven.

Constructing Mathematical Proofs

To create a proof of a theorem, we must use correct logical reasoning and mathematical statements that we already accept as true. These statements include axioms, definitions, theorems, lemmas, and corollaries.

In Section 1.2, we introduced the use of a **know-show table** to help us organize our work when we are attempting to prove a statement. We also introduced some guidelines for writing mathematical proofs once we have created the proof. These guidelines should be reviewed before proceeding.

Please remember that when we start the process of writing a proof, we are essentially "reporting the news." That is, we have already discovered the proof, and now we need to report it. This reporting often does not describe the process of discovering the news (the investigative portion of the process).

Quite often, the first step is to develop a conjecture. This is often done after working within certain objects for some time. This is what we did in Beginning Activity 1 when we used examples to provide evidence that the following conjecture is true:

Conjecture: *Let a, b, and c be integers with $a \neq 0$ and $b \neq 0$. If a divides b and b divides c, then a divides c.*

Before we try to prove a conjecture, we should make sure we have explored some examples. This simply means to construct some specific examples where the integers a, b, and c satisfy the hypothesis of the conjecture in order to see if they also satisfy the conclusion. We did this for this conjecture in Beginning Activity 1.

We will now start a know-show table for this conjecture.

Step	**Know**	**Reason**
P	$a, b, c \in \mathbb{Z}$, $a \neq 0$, $b \neq 0$, $a \mid b$ and $b \mid c$	Hypothesis
$P1$		
$\vdots$	$\vdots$	$\vdots$
$Q1$		
Q	$a \mid c$	
Step	**Show**	**Reason**

The backward question we ask is, "How can we prove that a divides c?" One answer is to use the definition and show that there exists an integer q such that $c = a \cdot q$. This could be step $Q1$ in the know-show table.

We now have to prove that a certain integer q exists, so we ask the question, "How do we prove that this integer exists?" When we are at such a stage in the backward process of a proof, we usually turn to what is known in order to prove that the object exists or to find or construct the object we are trying to prove exists. We often say that we try to "construct" the object or at least prove it exists from the known information. So at this point, we go to the forward part of the proof to try to prove that there exists an integer q such that $c = a \cdot q$.

The forward question we ask is, "What can we conclude from the facts that $a \mid b$ and $b \mid c$?" Again, using the definition, we know that there exist integers s

and t such that $b = a \cdot s$ and $c = b \cdot t$. This could be step $P1$ in the know-show table.

The key now is to determine how to get from $P1$ to $Q1$. That is, can we use the conclusions that the integers s and t exist in order to prove that the integer q (from the backward process) exists. Using the equation $b = a \cdot s$, we can substitute $a \cdot s$ for b in the second equation, $c = b \cdot t$. This gives

$$\begin{aligned} c &= b \cdot t \\ &= (a \cdot s) \cdot t \\ &= a(s \cdot t). \end{aligned}$$

The last step used the associative property of multiplication. (See Table 1.2 on page 18.) This shows that c is equal to a times some integer. (This is because $s \cdot t$ is an integer by the closure property for integers.) So although we did not use the letter q, we have arrived at step $Q1$. The completed know-show table follows.

Step	**Know**	**Reason**
P	$a, b, c \in \mathbb{Z}, a \neq 0, b \neq 0, a \mid b$ and $b \mid c$	Hypothesis
$P1$	$(\exists s \in \mathbb{Z})\ (b = a \cdot s)$ $(\exists t \in \mathbb{Z})\ (c = b \cdot t)$	Definition of "divides"
$P2$	$c = (a \cdot s) \cdot t$	Substitution for b
$P3$	$c = a \cdot (s \cdot t)$	Associative property of multiplication
$Q1$	$(\exists q \in \mathbb{Z})\ (c = a \cdot q)$	Step $P3$ and the closure properties of the integers
Q	$a \mid c$	Definition of "divides"

Notice the similarities between what we did for this proof and many of the proofs about even and odd integers we constructed in Section 1.2. When we try to prove that a certain object exists, we often use what is called the **construction method for a proof**. The appearance of an existential quantifier in the show (or backward) portion of the proof is usually the indicator to go to what is known in order to prove the object exists.

We can now report the news by writing a formal proof.

Theorem 3.1. *Let a, b, and c be integers with $a \neq 0$ and $b \neq 0$. If a divides b and b divides c, then a divides c.*

Proof. We assume that a, b, and c are integers with $a \neq 0$ and $b \neq 0$. We further assume that a divides b and that b divides c. We will prove that a divides c.

Since a divides b and b divides c, there exist integers s and t such that

$$b = a \cdot s, \text{ and} \tag{1}$$
$$c = b \cdot t. \tag{2}$$

We can now substitute the expression for b from equation (1) into equation (2). This gives

$$c = (a \cdot s) \cdot t.$$

Using the associate property for multiplication, we can rearrange the right side of the last equation to obtain

$$c = a \cdot (s \cdot t).$$

Because both s and t are integers, and since the integers are closed under multiplication, we know that $s \cdot t \in \mathbb{Z}$. Therefore, the previous equation proves that a divides c. Consequently, we have proven that whenever a, b, and c are integers with $a \neq 0$ and $b \neq 0$ such that a divides b and b divides c, then a divides c. ■

Writing Guidelines for Equation Numbers

We wrote the proof for Theorem 3.1 according to the guidelines introduced in Section 1.2, but a new element that appeared in this proof was the use of equation numbers. Following are some guidelines that can be used for **equation numbers**.

If it is necessary to refer to an equation later in a proof, that equation should be centered and displayed. It should then be given a number. The number for the equation should be written in parentheses on the same line as the equation at the right-hand margin as in shown in the following example.

Since x is an odd integer, there exists an integer n such that

$$x = 2n + 1. \tag{1}$$

Later in the proof, there may be a line such as

Then, using the result in equation (1), we obtain ....

Notice that we did not number every equation in Theorem 3.1. We should only number those equations we will be referring to later in the proof, and we should only number equations when it is necessary. For example, instead of numbering an equation, it is often better to use a phrase such as, "the previous equation proves that ..." or "we can rearrange the terms on the right side of the previous equation." Also, note that the word "equation" is not capitalized when we are referring to an equation by number. Although it may be appropriate to use a capital "E," the usual convention in mathematics is not to capitalize.

Progress Check 3.2 (**A Property of Divisors**)

1. Give at least four different examples of integers a, b, and c with $a \neq 0$ such that a divides b and a divides c.
2. For each example in Part (1), calculate the sum $b + c$. Does the integer a divide the sum $b + c$?
3. Construct a know-show table for the following proposition: For all integers a, b, and c with $a \neq 0$, if a divides b and a divides c, then a divides $(b + c)$.

Using Counterexamples

In Section 1.2 and so far in this section, our focus has been on proving statements that involve universal quantifiers. However, another important skill for mathematicians is to be able to recognize when a statement is false and then to be able to prove that it is false. For example, suppose we want to know if the following proposition is true or false.

For each integer n, if 5 divides $\left(n^2 - 1\right)$, then 5 divides $(n - 1)$.

Suppose we start trying to prove this proposition. In the backward process, we would say that in order to prove that 5 divides $(n - 1)$, we can show that there exists an integer k such that

$$Q_1 : n - 1 = 5k \quad \text{or} \quad n = 5k + 1.$$

For the forward process, we could say that since 5 divides $\left(n^2 - 1\right)$, we know that there exists an integer m such that

$$P_1 : n^2 - 1 = 5m \quad \text{or} \quad n^2 = 5m + 1.$$

The problem is that there is no straightforward way to use P_1 to prove Q_1. At this point, it would be a good idea to try some examples for n and try to find situations in which the hypothesis of the proposition is true. (In fact, this should have been done before we started trying to prove the proposition.) The following table summarizes the results of some of these explorations with values for n.

n	$n^2 - 1$	Does 5 divide $(n^2 - 1)$	$n - 1$	Does 5 divide $(n - 1)$
1	0	yes	0	yes
2	3	no	1	no
3	8	no	2	no
4	15	yes	3	no

We can stop exploring examples now since the last row in the table provides an example where the hypothesis is true and the conclusion is false. Recall from Section 2.4 (see page 69) that a **counterexample** for a statement of the form $(\forall x \in U)\,(P(x))$ is an element a in the universal set for which $P(a)$ is false. So we have actually proved that the negation of the proposition is true.

When using a counterexample to prove a statement is false, we do not use the term "proof" since we reserve a proof for proving a proposition is true. We could summarize our work as follows:

> **Conjecture**. For each integer n, if 5 divides $(n^2 - 1)$, then 5 divides $(n - 1)$.
>
> The integer $n = 4$ is a counterexample that proves this conjecture is false. Notice that when $n = 4$, $n^2 - 1 = 15$ and 5 divides 15. Hence, the hypothesis of the conjecture is true in this case. In addition, $n - 1 = 3$ and 5 does not divide 3 and so the conclusion of the conjecture is false in this case. Since this is an example where the hypothesis is true and the conclusion is false, the conjecture is false.

As a general rule of thumb, anytime we are trying to decide if a proposition is true or false, it is a good idea to try some examples first. The examples that are chosen should be ones in which the hypothesis of the proposition is true. If one of these examples makes the conclusion false, then we have found a counterexample and we know the proposition is false. If all of the examples produce a true conclusion, then we have evidence that the proposition is true and can try to write a proof.

Progress Check 3.3 (**Using a Counterexample**)
Use a counterexample to prove the following statement is false.

> For all integers a and b, if 5 divides a or 5 divides b, then 5 divides $(5a + b)$.

CC BY NC SA

Congruence

What mathematicians call congruence is a concept used to describe cycles in the world of the integers. For example, the day of the week is a cyclic phenomenon in that the day of the week repeats every seven days. The time of the day is a cyclic phenomenon because it repeats every 12 hours if we use a 12-hour clock or every 24 hours if we use a 24-hour clock. We explored these two cyclic phenomena in Beginning Activity 2.

Similar to what we saw in Beginning Activity 2, if it is currently Monday, then it will be Wednesday 2 days from now, 9 days from now, 16 days from now, 23 days from now, and so on. In addition, it was Wednesday 5 days ago, 12 days ago, 19 days ago, and so on. Using negative numbers for time in the past, we generate the following list of numbers:

$$\ldots, \ -19, -12, -5, 2, 9, 16, 23, \ldots.$$

Notice that if we subtract any number in the list above from any other number in that list, we will obtain a multiple of 7. For example,

$$\begin{aligned} 16 - 2 &= 14 = 7 \cdot 2 \\ (-5) - (9) &= -14 = 7 \cdot (-2) \\ 16 - (-12) &= 28 = 7 \cdot 4. \end{aligned}$$

Using the concept of congruence, we would say that all the numbers in this list are congruent modulo 7, but we first have to define when two numbers are congruent modulo some natural number n.

Definition. Let $n \in \mathbb{N}$. If a and b are integers, then we say that ***a* is congruent to *b* modulo *n*** provided that n divides $a - b$. A standard notation for this is $a \equiv b \pmod{n}$. This is read as "a is congruent to b modulo n" or "a is congruent to b mod n."

Notice that we can use the definition of divides to say that n divides $(a - b)$ if and only if there exists an integer k such that $a - b = nk$. So we can write

$$\begin{aligned} a \equiv b \pmod{n} \text{ means } (\exists k \in \mathbb{Z})\,(a - b = nk)\,, \text{or} \\ a \equiv b \pmod{n} \text{ means } (\exists k \in \mathbb{Z})\,(a = b + nk)\,. \end{aligned}$$

This means that in order to find integers that are congruent to b modulo n, we only need to add multiples of n to b. For example, to find integers that are congruent to 2 modulo 5, we add multiples of 5 to 2. This gives the following list:

$$\ldots, -13, -8, -3, 2, 7, 12, 17, \ldots.$$

We can also write this using set notation and say that

$$\{a \in \mathbb{Z} | \, a \equiv 2 \pmod 5\} = \{\ldots, -13, -8, -3, 2, 7, 12, 17, \ldots\}.$$

Progress Check 3.4 (Congruence Modulo 8)

1. Determine at least eight different integers that are congruent to 5 modulo 8.
2. Use set builder notation and the roster method to specify the set of all integers that are congruent to 5 modulo 8.
3. Choose two integers that are congruent to 5 modulo 8 and add them. Then repeat this for at least five other pairs of integers that are congruent to 5 modulo 8.
4. Explain why all of the sums that were obtained in Part (3) are congruent to 2 modulo 8.

We will study the concept of congruence modulo n in much more detail later in the text. For now, we will work with the definition of congruence modulo n in the context of proofs. For example, all of the examples used in Progress Check 3.4 should provide evidence that the following proposition is true.

Proposition 3.5. *For all integers a and b, if $a \equiv 5 \pmod 8$ and $b \equiv 5 \pmod 8$, then $(a + b) \equiv 2 \pmod 8$.*

Progress Check 3.6 (Proving Proposition 3.5)
We will use "backward questions" and "forward questions" to help construct a proof for Proposition 3.5. So, we might ask, "How do we prove that $(a + b) \equiv 2 \pmod 8$?" One way to answer this is to use the definition of congruence and state that $(a + b) \equiv 2 \pmod 8$ provided that 8 divides $(a + b - 2)$.

1. Use the definition of divides to determine a way to prove that 8 divides $(a + b - 2)$.

We now turn to what we know and ask, "What can we conclude from the assumptions that $a \equiv 5 \pmod 8$ and $b \equiv 5 \pmod 8$?" We can again use the definition of congruence and conclude that 8 divides $(a-5)$ and 8 divides $(b-5)$.

2. Use the definition of divides to make conclusions based on the facts that 8 divides $(a-5)$ and 8 divides $(b-5)$.
3. Solve an equation from part (2) for a and for b.
4. Use the results from part (3) to prove that 8 divides $(a+b-2)$.
5. Write a proof for Proposition 3.5.

Additional Writing Guidelines

We will now be writing many proofs, and it is important to make sure we write according to accepted guidelines so that our proofs may be understood by others. Some writing guidelines were introduced in Chapter 1. The first four writing guidelines given below can be considered general guidelines, and the last three can be considered as technical guidelines specific to writing in mathematics.

1. **Know your audience.** Every writer should have a clear idea of the intended audience for a piece of writing. In that way, the writer can give the right amount of information at the proper level of sophistication to communicate effectively. This is especially true for mathematical writing. For example, if a mathematician is writing a solution to a textbook problem for a solutions manual for instructors, the writing would be brief with many details omitted. However, if the writing was for a students' solution manual, more details would be included.
2. **Use complete sentences and proper paragraph structure.** Good grammar is an important part of any writing. Therefore, conform to the accepted rules of grammar. Pay careful attention to the structure of sentences. Write proofs using **complete sentences** but avoid run-on sentences. Also, do not forget punctuation, and always use a spell checker when using a word processor.
3. **Keep it simple**. It is often difficult to understand a mathematical argument no matter how well it is written. Do not let your writing help make it more difficult for the reader. Use simple, declarative sentences and short paragraphs, each with a simple point.

4. **Write a first draft of your proof and then revise it.** Remember that a proof is written so that readers are able to read and understand the reasoning in the proof. Be clear and concise. Include details but do not ramble. Do not be satisfied with the first draft of a proof. Read it over and refine it. Just like any worthwhile activity, learning to write mathematics well takes practice and hard work. This can be frustrating. Everyone can be sure that there will be some proofs that are difficult to construct, but remember that proofs are a very important part of mathematics. So work hard and have fun.

5. **Do not use $*$ for multiplication or $\hat{}$ for exponents.** Leave this type of notation for writing computer code. The use of this notation makes it difficult for humans to read. In addition, avoid using / for division when using a complex fraction.

   For example, it is very difficult to read $\big(x^3 - 3x^2 + 1/2\big)/(2x/3 - 7)$; the fraction

   $$\frac{x^3 - 3x^2 + \dfrac{1}{2}}{\dfrac{2x}{3} - 7}$$

   is much easier to read.

6. **Do not use a mathematical symbol at the beginning of a sentence.** For example, we should not write, "Let n be an integer. n is an odd integer provided that ...." Many people find this hard to read and often have to re-read it to understand it. It would be better to write, "An integer n is an odd integer provided that ...."

7. **Use English and minimize the use of cumbersome notation**. Do not use the special symbols for quantifiers $\forall$ (for all), $\exists$ (there exists), $\ni$ (such that), or $\therefore$ (therefore) in formal mathematical writing. It is often easier to write, and usually easier to read, if the English words are used instead of the symbols. For example, why make the reader interpret

   $$(\forall x \in \mathbb{R})\,(\exists y \in \mathbb{R})\,(x + y = 0)$$

   when it is possible to write

   For each real number x, there exists a real number y such that $x + y = 0$,

   or, more succinctly (if appropriate),

   Every real number has an additive inverse.

CC BY NC SA

Exercises for Section 3.1

⋆ **1.** Prove each of the following statements:

(**a**) For all integers a, b, and c with $a \neq 0$, if $a \mid b$ and $a \mid c$, then $a \mid (b - c)$.

(**b**) For each $n \in \mathbb{Z}$, if n is an odd integer, then n^3 is an odd integer.

(**c**) For each integer a, if 4 divides $(a - 1)$, then 4 divides $\left(a^2 - 1\right)$.

2. For each of the following, use a counterexample to prove the statement is false.

⋆ **(a)** For each odd natural number n, if $n > 3$, then 3 divides $\left(n^2 - 1\right)$.

(b) For each natural number n, $(3 \cdot 2^n + 2 \cdot 3^n + 1)$ is a prime number.

(c) For all real numbers x and y, $\sqrt{x^2 + y^2} > 2xy$.

⋆ **(d)** For each integer a, if 4 divides $\left(a^2 - 1\right)$, then 4 divides $(a - 1)$.

3. Determine if each of the following statements is true or false. If a statement is true, then write a formal proof of that statement, and if it is false, then provide a counterexample that shows it is false.

(**a**) For all integers a, b, and c with $a \neq 0$, if $a \mid b$, then $a \mid (bc)$.

⋆ **(b)** For all integers a and b with $a \neq 0$, if $6 \mid (ab)$, then $6 \mid a$ or $6 \mid b$.

(c) For all integers a, b, and c with $a \neq 0$, if a divides $(b - 1)$ and a divides $(c - 1)$, then a divides $(bc - 1)$.

⋆ **(d)** For each integer n, if 7 divides $\left(n^2 - 4\right)$, then 7 divides $(n - 2)$.

⋆ **(e)** For every integer n, $4n^2 + 7n + 6$ is an odd integer.

⋆ **(f)** For every odd integer n, $4n^2 + 7n + 6$ is an odd integer.

⋆ **(g)** For all integers a, b, and d with $d \neq 0$, if d divides both $a - b$ and $a + b$, then d divides a.

(h) For all integers a, b, and c with $a \neq 0$, if $a \mid (bc)$, then $a \mid b$ or $a \mid c$.

⋆ **4.** (**a**) If x and y are integers and $xy = 1$, explain why $x = 1$ or $x = -1$.

(**b**) Is the following proposition true or false?

For all nonzero integers a and b, if $a \mid b$ and $b \mid a$, then $a = \pm b$.

⋆ **5.** Prove the following proposition:

Let a be an integer. If there exists an integer n such that $a \mid (4n + 3)$ and $a \mid (2n + 1)$, then $a = 1$ or $a = -1$.

Hint: Use the fact that the only divisors of 1 are 1 and -1.

6. Determine if each of the following statements is true or false. If a statement is true, then write a formal proof of that statement, and if it is false, then provide a counterexample that shows it is false.

(**a**) For each integer a, if there exists an integer n such that a divides $(8n + 7)$ and a divides $(4n + 1)$, then a divides 5.

(**b**) For each integer a, if there exists an integer n such that a divides $(9n + 5)$ and a divides $(6n + 1)$, then a divides 7.

(**c**) For each integer n, if n is odd, then 8 divides $\left(n^4 + 4n^2 + 11\right)$.

(**d**) For each integer n, if n is odd, then 8 divides $\left(n^4 + n^2 + 2n\right)$.

7. Let a be an integer and let $n \in \mathbb{N}$.

(**a**) Prove that if $a \equiv 0 \pmod{n}$, then $n \mid a$.

(**b**) Prove that if $n \mid a$, then $a \equiv 0 \pmod{n}$.

⋆ **8.** Let a and b be integers. Prove that if $a \equiv 2 \pmod 3$ and $b \equiv 2 \pmod 3$, then

(**a**) $a + b \equiv 1 \pmod 3$; (**b**) $a \cdot b \equiv 1 \pmod 3$.

9. Let a and b be integers. Prove that if $a \equiv 7 \pmod 8$ and $b \equiv 3 \pmod 8$, then:

(**a**) $a + b \equiv 2 \pmod 8$; (**b**) $a \cdot b \equiv 5 \pmod 8$.

10. Determine if each of the following propositions is true or false. Justify each conclusion.

(**a**) For all integers a and b, if $ab \equiv 0 \pmod 6$, then $a \equiv 0 \pmod 6$ or $b \equiv 0 \pmod 6$.

(**b**) For each integer a, if $a \equiv 2 \pmod 8$, then $a^2 \equiv 4 \pmod 8$.

(**c**) For each integer a, if $a^2 \equiv 4 \pmod 8$, then $a \equiv 2 \pmod 8$.

cc BY NC SA

11. Let n be a natural number. Prove each of the following:

⋆ **(a)** For every integer a, $a \equiv a \pmod{n}$.
This is called the **reflexive property** of congruence modulo n.

⋆ **(b)** For all integers a and b, if $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.
This is called the **symmetric property** of congruence modulo n.

(c) For all integers a, b, and c, if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.
This is called the **transitive property** of congruence modulo n.

⋆ **12.** Let n be a natural number and let a, b, c, and d be integers. Prove each of the following.

(a) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $(a + c) \equiv (b + d) \pmod{n}$.

(b) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$.

13. **(a)** Let a, b, and c be real numbers with $a \neq 0$. Explain how to use a part of the quadratic formula (called the discriminant) to determine if the quadratic equation $ax^2 + bx + c = 0$ has two real number solutions, one real number solution, or no real number solutions. (See Exercise (11) in Section 1.2 for a statement of the quadratic formula.)

(b) Prove that if a, b, and c are real numbers for which $a > 0$ and $c < 0$, then one solution of the quadratic equation $ax^2 + bx + c = 0$ is a positive real number.

(c) Prove that if a, b, and c are real numbers, if $a \neq 0$, $b > 0$ and $\frac{b}{2} < \sqrt{ac}$, then the quadratic equation $ax^2 + bx + c = 0$ has no real number solution.

14. Let h and k be real numbers and let r be a positive number. The equation for a circle whose center is at the point (h, k) and whose radius is r is

$$(x - h)^2 + (y - k)^2 = r^2.$$

We also know that if a and b are real numbers, then

- The point (a, b) is inside the circle if $(a - h)^2 + (b - k)^2 < r^2$.
- The point (a, b) is on the circle if $(a - h)^2 + (b - k)^2 = r^2$.

- The point (a, b) is outside the circle if $(a-h)^2 + (b-k)^2 > r^2$.

Prove that all points on or inside the circle whose equation is $(x-1)^2 + (y-2)^2 = 4$ are inside the circle whose equation is $x^2 + y^2 = 26$.

15. Let r be a positive real number. The equation for a circle of radius r whose center is the origin is $x^2 + y^2 = r^2$.

(**a**) Use implicit differentiation to determine $\dfrac{dy}{dx}$.

(**b**) Let (a, b) be a point on the circle with $a \neq 0$ and $b \neq 0$. Determine the slope of the line tangent to the circle at the point (a, b).

(**c**) Prove that the radius of the circle to the point (a, b) is perpendicular to the line tangent to the circle at the point (a, b). **Hint**: Two lines (neither of which is horizontal) are perpendicular if and only if the products of their slopes is equal to -1.

16. Determine if each of the following statements is true or false. Provide a counterexample for statements that are false and provide a complete proof for those that are true.

(**a**) For all real numbers x and y, $\sqrt{xy} \leq \dfrac{x+y}{2}$.

(**b**) For all real numbers x and y, $xy \leq \left(\dfrac{x+y}{2}\right)^2$.

(**c**) For all nonnegative real numbers x and y, $\sqrt{xy} \leq \dfrac{x+y}{2}$.

17. Use one of the true inequalities in Exercise (16) to prove the following proposition.

For each real number a, the value of x that gives the maximum value of $y = x(a-x)$ is $x = \dfrac{a}{2}$.

18. (**a**) State the Pythagorean Theorem for right triangles.

The diagrams in Figure 3.1 will be used for the problems in this exercise.

(**b**) In the diagram on the left, x is the length of a side of the equilateral triangle and h is the length of an altitude of the equilateral triangle. The labeling in the diagram shows the fact that the altitude intersects the base of the equilateral triangle at the midpoint of the base. Use the

CC BY NC SA

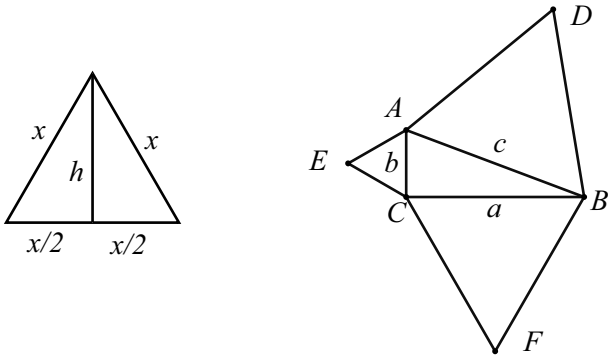

Figure 3.1: Diagrams for Exercise (18)

Pythagorean Theorem to prove that the area of this equilateral triangle is $\frac{\sqrt{3}}{4}x^2$.

(**c**) In the diagram on the right, $\triangle ABC$ is a right triangle. In addition, there has been an equilateral triangle constructed on each side of this right triangle. Prove that the area of the equilateral triangle on the hypotenuse is equal to the sum of the areas of the equilateral triangles constructed on the other two sides of the right triangle.

19. Evaluation of proofs

This type of exercise will appear frequently in the book. In each case, there is a proposed proof of a proposition. However, the proposition may be true or may be false.

- If a proposition is false, the proposed proof is, of course, incorrect. In this situation, you are to find the error in the proof and then provide a counterexample showing that the proposition is false.
- If a proposition is true, the proposed proof may still be incorrect. In this case, you are to determine why the proof is incorrect and then write a correct proof using the writing guidelines that have been presented in this book.
- If a proposition is true and the proof is correct, you are to decide if the proof is well written or not. If it is well written, then you simply must indicate that this is an excellent proof and needs no revision. On the other hand, if the proof is not well written, then you must then revise the proof by writing it according to the guidelines presented in this text.

cc BY NC SA

(**a**) **Proposition**. If m is an even integer, then $(5m + 4)$ is an even integer.

Proof. We see that $5m + 4 = 10n + 4 = 2(5n + 2)$. Therefore, $(5m + 4)$ is an even integer. ■

(**b**) **Proposition**. For all real numbers x and y, if $x \neq y$, $x > 0$, and $y > 0$, then $\frac{x}{y} + \frac{y}{x} > 2$.

Proof. Since x and y are positive real numbers, xy is positive and we can multiply both sides of the inequality by xy to obtain

$$\left(\frac{x}{y} + \frac{y}{x}\right) \cdot xy > 2 \cdot xy$$
$$x^2 + y^2 > 2xy.$$

By combining all terms on the left side of the inequality, we see that $x^2 - 2xy + y^2 > 0$ and then by factoring the left side, we obtain $(x - y)^2 > 0$. Since $x \neq y$, $(x - y) \neq 0$ and so $(x - y)^2 > 0$. This proves that if $x \neq y$, $x > 0$, and $y > 0$, then $\frac{x}{y} + \frac{y}{x} > 2$. ■

(**c**) **Proposition**. For all integers a, b, and c, if $a \mid (bc)$, then $a \mid b$ or $a \mid c$.

Proof. We assume that a, b, and c are integers and that a divides bc. So, there exists an integer k such that $bc = ka$. We now factor k as $k = mn$, where m and n are integers. We then see that

$$bc = mna.$$

This means that $b = ma$ or $c = na$ and hence, $a \mid b$ or $a \mid c$. ■

(**d**) **Proposition**. For all positive integers a, b, and c, $\left(a^b\right)^c = a^{(b^c)}$.

This proposition is false as is shown by the following counterexample: If we let $a = 2$, $b = 3$, and $c = 2$, then

$$\left(a^b\right)^c = a^{(b^c)}$$
$$\left(2^3\right)^2 = 2^{(3^2)}$$
$$8^2 = 2^9$$
$$64 \neq 512$$

CC BY NC SA

Explorations and Activities

20. Congruence Modulo 6.

(**a**) Find several integers that are congruent to 5 modulo 6 and then square each of these integers.

(**b**) For each integer m from Part (20a), determine an integer k so that $0 \leq k < 6$ and $m^2 \equiv k \pmod 6$. What do you observe?

(**c**) Based on the work in Part (20b), complete the following conjecture:

For each integer m, if $m \equiv 5 \pmod 6$, then ....

(**d**) Complete a know-show table for the conjecture in Part (20c) or write a proof of the conjecture.

21. Pythagorean Triples. Three natural numbers a, b, and c with $a < b < c$ are called a Pythagorean triple provided that $a^2 + b^2 = c^2$. See Exercise (13) on page 30 in Section 1.2. Three natural numbers are called **consecutive natural numbers** if they can be written in the form m, $m + 1$, and $m + 2$, where m is a natural number.

(**a**) Determine all Pythagorean triples consisting of three consecutive natural numbers. (State a theorem and prove it.)

(**b**) Determine all Pythagorean triples that can be written in the form m, $m + 7$, and $m + 8$, where m is a natural number. State a theorem and prove it.

3.2 More Methods of Proof

Beginning Activity 1 (Using the Contrapositive)
The following statement was proven in Exercise (3c) on page 28 in Section 1.2.

If n is an odd integer, then n^2 is an odd integer.

Now consider the following proposition:

For each integer n, if n^2 is an odd integer, then n is an odd integer.

1. After examining several examples, decide whether you think this proposition is true or false.

2. Try completing the following know-show table for a direct proof of this proposition. The question is, "Can we perform algebraic manipulations to get from the 'know' portion of the table to the 'show' portion of the table?" Be careful with this! Remember that we are working with integers and we want to make sure that we can end up with an integer q as stated in Step $Q1$.

Step	**Know**	**Reason**
P	n^2 is an odd integer.	Hypothesis
$P1$	$(\exists k \in \mathbb{Z})\ (n^2 = 2k + 1)$	Definition of "odd integer"
$\vdots$	$\vdots$	$\vdots$
$Q1$	$(\exists q \in \mathbb{Z})\ (n = 2q + 1)$	
Q	n is an odd integer.	Definition of "odd integer"
Step	**Show**	**Reason**

Recall that the contrapositive of the conditional statement $P \rightarrow Q$ is the conditional statement $\neg Q \rightarrow \neg P$, which is logically equivalent to the original conditional statement. (It might be a good idea to review Beginning Activity 2 from Section 2.2 on page 44.) Consider the following proposition once again:

> For each integer n, if n^2 is an odd integer, then n is an odd integer.

3. Write the contrapositive of this conditional statement. Please note that "not odd" means "even." (We have not proved this, but it can be proved using the Division Algorithm in Section 3.5.)

4. Complete a know-show table for the contrapositive statement from Part (3).

5. By completing the proof in Part (4), have you proven the given proposition? That is, have you proven that if n^2 is an odd integer, then n is an odd integer? Explain.

Beginning Activity 2 (A Biconditional Statement)

1. In Exercise (4a) from Section 2.2, we constructed a truth table to prove that the biconditional statement, $P \leftrightarrow Q$, is logically equivalent to $(P \rightarrow Q) \wedge (Q \rightarrow P)$. Complete this exercise if you have not already done so.

2. Suppose that we want to prove a biconditional statement of the form $P \leftrightarrow Q$. Explain a method for completing this proof based on the logical equivalency in part (1).

3. Let n be an integer. Assume that we have completed the proofs of the following two statements:

- If n is an odd integer, then n^2 is an odd integer.
- If n^2 is an odd integer, then n is an odd integer.

(See Exercise (3c) from Section 1.2 and Beginning Activity 1.) Have we completed the proof of the following proposition?

For each integer n, n is an odd integer if and only if n^2 is an odd integer.

Explain.

Review of Direct Proofs

In Sections 1.2 and 3.1, we studied direct proofs of mathematical statements. Most of the statements we prove in mathematics are conditional statements that can be written in the form $P \rightarrow Q$. A direct proof of a statement of the form $P \rightarrow Q$ is based on the definition that a conditional statement can only be false when the hypothesis, P, is true and the conclusion, Q, is false. Thus, if the conclusion is true whenever the hypothesis is true, then the conditional statement must be true. So, in a direct proof,

- We start by assuming that P is true.
- From this assumption, we logically deduce that Q is true.

We have used the so-called forward and backward method to discover how to logically deduce Q from the assumption that P is true.

Proof Using the Contrapositive

As we saw in Beginning Activity 1, it is sometimes difficult to construct a direct proof of a conditional statement. This is one reason we studied logical equivalencies in Section 2.2. Knowing that two expressions are logically equivalent tells us that if we prove one, then we have also proven the other. In fact, once we know the truth value of a statement, then we know the truth value of any other statement that is logically equivalent to it.

One of the most useful logical equivalencies in this regard is that a conditional statement $P \rightarrow Q$ is logically equivalent to its contrapositive, $\neg Q \rightarrow \neg P$. This

means that if we prove the contrapositive of the conditional statement, then we have proven the conditional statement. The following are some important points to remember.

- A conditional statement is logically equivalent to its contrapositive.
- Use a direct proof to prove that $\neg Q \rightarrow \neg P$ is true.
- Caution: One difficulty with this type of proof is in the formation of correct negations. (We need to be very careful doing this.)
- We might consider using a proof by contrapositive when the statements P and Q are stated as negations.

Writing Guidelines

One of the basic rules of writing mathematical proofs is to keep the reader informed. So when we prove a result using the contrapositive, we indicate this within the first few lines of the proof. For example,

- We will prove this theorem by proving its contrapositive.
- We will prove the contrapositive of this statement.

In addition, make sure the reader knows the status of every assertion that you make. That is, make sure you state whether an assertion is an assumption of the theorem, a previously proven result, a well-known result, or something from the reader's mathematical background. Following is a completed proof of a statement from Beginning Activity 1.

Theorem 3.7. *For each integer n, if n^2 is an even integer, then n is an even integer.*

Proof. We will prove this result by proving the contrapositive of the statement, which is

> For each integer n, if n is an odd integer, then n^2 is an odd integer.

However, in Theorem 1.8 on page 22, we have already proven that if x and y are odd integers, then $x \cdot y$ is an odd integer. So using $x = y = n$, we can conclude that if n is an odd integer, then $n \cdot n$, or n^2, is an odd integer. We have thus proved the contrapositive of the theorem, and consequently, we have proved that if n^2 is an even integer, then n is an even integer. ■

CC BY NC SA

Using Other Logical Equivalencies

As was noted in Section 2.2, there are several different logical equivalencies. Fortunately, there are only a small number that we often use when trying to write proofs, and many of these are listed in Theorem 2.8 at the end of Section 2.2. We will illustrate the use of one of these logical equivalencies with the following proposition:

For all real numbers a and b, if $a \neq 0$ and $b \neq 0$, then $ab \neq 0$.

First, notice that the hypothesis and the conclusion of the conditional statement are stated in the form of negations. This suggests that we consider the contrapositive. Care must be taken when we negate the hypothesis since it is a conjunction. We use one of De Morgan's Laws as follows:

$$\neg (a \neq 0 \ \wedge \ b \neq 0) \equiv (a = 0) \vee (b = 0) .$$

Progress Check 3.8 (Using Another Logical Equivalency)

1. In English, write the contrapositive of, "For all real numbers a and b, if $a \neq 0$ and $b \neq 0$, then $ab \neq 0$."

The contrapositive is a conditional statement in the form $X \rightarrow (Y \vee Z)$. The difficulty is that there is not much we can do with the hypothesis $(ab = 0)$ since we know nothing else about the real numbers a and b. However, if we knew that a was not equal to zero, then we could multiply both sides of the equation $ab = 0$ by $\frac{1}{a}$. This suggests that we consider using the following logical equivalency based on a result in Theorem 2.8 on page 48:

$$X \rightarrow (Y \vee Z) \equiv (X \wedge \neg Y) \rightarrow Z.$$

2. In English, use this logical equivalency to write a statement that is logically equivalent to the contrapositive from Part (1).

The logical equivalency in Part (2) makes sense because if we are trying to prove $Y \vee Z$, we only need to prove that at least one of Y or Z is true. So the idea is to prove that if Y is false, then Z must be true.

3. Use the ideas presented in the progress check to complete the proof of the following proposition.

Proposition 3.9. *For all real numbers a and b, if $a \neq 0$ and $b \neq 0$, then $ab \neq 0$.*

Proof. We will prove the contrapositive of this proposition, which is

For all real numbers a and b, if $ab = 0$, then $a = 0$ or $b = 0$.

This contrapositive, however, is logically equivalent to the following:

For all real numbers a and b, if $ab = 0$ and $a \neq 0$, then $b = 0$.

To prove this, we let a and b be real numbers and assume that $ab = 0$ and $a \neq 0$. We can then multiply both sides of the equation $ab = 0$ by $\frac{1}{a}$. This gives

Now complete the proof.
⋮

Therefore, $b = 0$. This completes the proof of a statement that is logically equivalent to the contrapositive, and hence, we have proven the proposition. ■

Proofs of Biconditional Statements

In Beginning Activity 2, we used the following logical equivalency:

$$(P \leftrightarrow Q) \equiv (P \rightarrow Q) \wedge (Q \rightarrow P)\,.$$

This logical equivalency suggests one method for proving a biconditional statement written in the form "P if and only if Q." This method is to construct separate proofs of the two conditional statements $P \rightarrow Q$ and $Q \rightarrow P$. For example, since we have now proven each of the following:

- For each integer n, if n is an even integer, then n^2 is an even integer. (Exercise (3c) on page 28 in Section 1.2)
- For each integer n, if n^2 is an even integer, then n is an even integer. (Theorem 3.7)

we can state the following theorem.

CC BY NC SA

Theorem 3.10. *For each integer n, n is an even integer if and only if n^2 is an even integer.*

Writing Guidelines

When proving a biconditional statement using the logical equivalency $(P \leftrightarrow Q) \equiv (P \rightarrow Q) \wedge (Q \rightarrow P)$, we actually need to prove two conditional statements. The proof of each conditional statement can be considered as one of two parts of the proof of the biconditional statement. Make sure that the start and end of each of these parts is indicated clearly. This is illustrated in the proof of the following proposition.

Proposition 3.11. *Let $x \in \mathbb{R}$. The real number x equals 2 if and only if $x^3 - 2x^2 + x = 2$.*

Proof. We will prove this biconditional statement by proving the following two conditional statements:

- For each real number x, if x equals 2 , then $x^3 - 2x^2 + x = 2$.
- For each real number x, if $x^3 - 2x^2 + x = 2$, then x equals 2.

For the first part, we assume $x = 2$ and prove that $x^3 - 2x^2 + x = 2$. We can do this by substituting $x = 2$ into the expression $x^3 - 2x^2 + x$. This gives

$$\begin{aligned} x^3 - 2x^2 + x &= 2^3 - 2\left(2^2\right) + 2 \\ &= 8 - 8 + 2 \\ &= 2. \end{aligned}$$

This completes the first part of the proof.

For the second part, we assume that $x^3 - 2x^2 + x = 2$ and from this assumption, we will prove that $x = 2$. We will do this by solving this equation for x. To do so, we first rewrite the equation $x^3 - 2x^2 + x = 2$ by subtracting 2 from both sides:

$$x^3 - 2x^2 + x - 2 = 0.$$

We can now factor the left side of this equation by factoring an x^2 from the first two terms and then factoring $(x - 2)$ from the resulting two terms. This is shown

below.

$$x^3 - 2x^2 + x - 2 = 0$$
$$x^2(x-2) + (x-2) = 0$$
$$(x-2)\left(x^2+1\right) = 0$$

Now, in the real numbers, if a product of two factors is equal to zero, then one of the factors must be zero. So this last equation implies that

$$x - 2 = 0 \text{ or } x^2 + 1 = 0.$$

The equation $x^2 + 1 = 0$ has no real number solution. So since x is a real number, the only possibility is that $x - 2 = 0$. From this we can conclude that x must be equal to 2.

Since we have now proven both conditional statements, we have proven that $x = 2$ if and only if $x^3 - 2x^2 + x = 2$. ■

Constructive Proofs

We all know how to solve an equation such as $3x + 8 = 23$, where x is a real number. To do so, we first add -8 to both sides of the equation and then divide both sides of the resulting equation by 3. Doing so, we obtain the following result:

$$\text{If } x \text{ is a real number and } 3x + 8 = 23, \text{ then } x = 5.$$

Notice that the process of solving the equation actually does not prove that $x = 5$ is a solution of the equation $3x + 8 = 23$. This process really shows that if there is a solution, then that solution must be $x = 5$. To show that this is a solution, we use the process of substituting 5 for x in the left side of the equation as follows: If $x = 5$, then

$$3x + 8 = 3(5) + 8 = 15 + 8 = 23.$$

This proves that $x = 5$ is a solution of the equation $3x + 8 = 23$. Hence, we have proven that $x = 5$ is the only real number solution of $3x + 8 = 23$.

We can use this same process to show that any linear equation has a real number solution. An equation of the form

$$ax + b = c,$$

cc BY NC SA

where a, b, and c are real numbers with $a \neq 0$, is called a **linear equation in one variable**.

Proposition 3.12. *If a, b, and c are real numbers with $a \neq 0$, then the linear equation $ax + b = c$ has exactly one real number solution, which is $x = \dfrac{c-b}{a}$.*

Proof. Assume that a, b, and c are real numbers with $a \neq 0$. We can solve the linear equation $ax + b = c$ by adding $-b$ to both sides of the equation and then dividing both sides of the resulting equation by a (since $a \neq 0$), to obtain

$$x = \frac{c-b}{a}.$$

This shows that if there is a solution, then it must be $x = \dfrac{c-b}{a}$. We also see that if $x = \dfrac{c-b}{a}$, then

$$\begin{aligned} ax + b &= a\left(\frac{c-b}{a}\right) + b \\ &= (c-b) + b \\ &= c. \end{aligned}$$

Therefore, the linear equation $ax + b = c$ has exactly one real number solution and the solution is $x = \dfrac{c-b}{a}$. ■

The proof given for Proposition 3.12 is called a **constructive proof.** This is a technique that is often used to prove a so-called **existence theorem.** The objective of an existence theorem is to prove that a certain mathematical object exists. That is, the goal is usually to prove a statement of the form

There exists an x such that $P(x)$.

For a constructive proof of such a proposition, we actually name, describe, or explain how to construct some object in the universe that makes $P(x)$ true. This is what we did in Proposition 3.12 since in the proof, we actually proved that $\dfrac{c-b}{a}$ is a solution of the equation $ax + b = c$. In fact, we proved that this is the only solution of this equation.

Nonconstructive Proofs

Another type of proof that is often used to prove an existence theorem is the so-called **nonconstructive proof.** For this type of proof, we make an argument that an object in the universal set that makes $P(x)$ true must exist but we never construct or name the object that makes $P(x)$ true. The advantage of a constructive proof over a nonconstructive proof is that the constructive proof will yield a procedure or algorithm for obtaining the desired object.

The proof of the **Intermediate Value Theorem** from calculus is an example of a nonconstructive proof. The Intermediate Value Theorem can be stated as follows:

> If f is a continuous function on the closed interval $[a, b]$ and if q is any real number strictly between $f(a)$ and $f(b)$, then there exists a number c in the interval (a, b) such that $f(c) = q$.

The Intermediate Value Theorem can be used to prove that a solution to some equations must exist. This is shown in the next example.

Example 3.13 (**Using the Intermediate Value Theorem**)
Let x represent a real number. We will use the Intermediate Value Theorem to prove that the equation $x^3 - x + 1 = 0$ has a real number solution.

To investigate solutions of the equation $x^3 - x + 1 = 0$, we will use the function

$$f(x) = x^3 - x + 1.$$

Notice that $f(-2) = -5$ and that $f(0) = 1$. Since $f(-2) < 0$ and $f(0) > 0$, the Intermediate Value Theorem tells us that there is a real number c between -2 and 0 such that $f(c) = 0$. This means that there exists a real number c between -2 and 0 such that

$$c^3 - c + 1 = 0,$$

and hence c is a real number solution of the equation $x^3 - x + 1 = 0$. This proves that the equation $x^3 - x + 1 = 0$ has at least one real number solution.

Notice that this proof does not tell us how to find the exact value of c. It does, however, suggest a method for approximating the value of c. This can be done by finding smaller and smaller intervals $[a,\ b]$ such that $f(a)$ and $f(b)$ have opposite signs.

cc BY NC SA

Exercises for Section 3.2

⋆ **1.** Let n be an integer. Prove each of the following:

(**a**) If n is even, then n^3 is even.

(**b**) If n^3 is even, then n is even.

(**c**) The integer n is even if and only if n^3 is an even integer.

(**d**) The integer n is odd if and only if n^3 is an odd integer.

2. In Section 3.1, we defined congruence modulo n where n is a natural number. If a and b are integers, we will use the notation $a \not\equiv b \pmod{n}$ to mean that a is not congruent to b modulo n.

⋆ **(a)** Write the contrapositive of the following conditional statement:

For all integers a and b, if $a \not\equiv 0 \pmod{6}$ and $b \not\equiv 0 \pmod{6}$, then $ab \not\equiv 0 \pmod{6}$.

(b) Is this statement true or false? Explain.

⋆ **3.** (**a**) Write the contrapositive of the following statement:

For all positive real numbers a and b, if $\sqrt{ab} \neq \dfrac{a+b}{2}$, then $a \neq b$.

(**b**) Is this statement true or false? Prove the statement if it is true or provide a counterexample if it is false.

⋆ **4.** Are the following statements true or false? Justify your conclusions.

(**a**) For each $a \in \mathbb{Z}$, if $a \equiv 2 \pmod{5}$, then $a^2 \equiv 4 \pmod{5}$.

(**b**) For each $a \in \mathbb{Z}$, if $a^2 \equiv 4 \pmod{5}$, then $a \equiv 2 \pmod{5}$.

(**c**) For each $a \in \mathbb{Z}$, $a \equiv 2 \pmod{5}$ if and only if $a^2 \equiv 4 \pmod{5}$.

5. Is the following proposition true or false?

For all integers a and b, if ab is even, then a is even or b is even.

Justify your conclusion by writing a proof if the proposition is true or by providing a counterexample if it is false.

⋆ **6.** Consider the following proposition: For each integer a, $a \equiv 3 \pmod{7}$ if and only if $\left(a^2 + 5a\right) \equiv 3 \pmod{7}$.

(**a**) Write the proposition as the conjunction of two conditional statements.

(**b**) Determine if the two conditional statements in Part (a) are true or false. If a conditional statement is true, write a proof, and if it is false, provide a counterexample.

(**c**) Is the given proposition true or false? Explain.

7. Consider the following proposition: For each integer a, $a \equiv 2 \pmod 8$ if and only if $\left(a^2 + 4a\right) \equiv 4 \pmod 8$.

(**a**) Write the proposition as the conjunction of two conditional statements.

(**b**) Determine if the two conditional statements in Part (a) are true or false. If a conditional statement is true, write a proof, and if it is false, provide a counterexample.

(**c**) Is the given proposition true or false? Explain.

8. For a right triangle, suppose that the hypotenuse has length c feet and the lengths of the sides are a feet and b feet.

(**a**) What is a formula for the area of this right triangle? What is an isosceles triangle?

(**b**) State the Pythagorean Theorem for right triangles.

⋆ **(c)** Prove that the right triangle described above is an isosceles triangle if and only if the area of the right triangle is $\frac{1}{4}c^2$.

⋆ **9.** A real number x is defined to be a **rational number** provided

$$\text{there exist integers } m \text{ and } n \text{ with } n \neq 0 \text{ such that } x = \frac{m}{n}.$$

A real number that is not a rational number is called an **irrational number.**

It is known that if x is a positive rational number, then there exist positive integers m and n with $n \neq 0$ such that $x = \frac{m}{n}$.

Is the following proposition true or false? Explain.

For each positive real number x, if x is irrational, then $\sqrt{x}$ is irrational.

⋆ **10.** Is the following proposition true or false? Justify your conclusion.

For each integer n, n is even if and only if 4 divides n^2.

11. Prove that for each integer a, if $a^2 - 1$ is even, then 4 divides $a^2 - 1$.

12. Prove that for all integers a and m, if a and m are the lengths of the sides of a right triangle and $m + 1$ is the length of the hypotenuse, then a is an odd integer.

13. Prove the following proposition:

If $p, q \in \mathbb{Q}$ with $p < q$, then there exists an $x \in \mathbb{Q}$ with $p < x < q$.

14. Are the following propositions true or false? Justify your conclusion.

(**a**) There exist integers x and y such that $4x + 6y = 2$.

(**b**) There exist integers x and y such that $6x + 15y = 2$.

(**c**) There exist integers x and y such that $6x + 15y = 9$.

⋆ **15.** Prove that there exists a real number x such that $x^3 - 4x^2 = 7$.

16. Let y_1, y_2, y_3, y_4 be real numbers. The **mean**, $\overline{y}$, of these four numbers is defined to be the sum of the four numbers divided by 4. That is,

$$\overline{y} = \frac{y_1 + y_2 + y_3 + y_4}{4}.$$

Prove that there exists a y_i with $1 \leq i \leq 4$ such that $y_i \geq \overline{y}$.

Hint: One way is to let $y_{\max}$ be the largest of y_1, y_2, y_3, y_4.

17. Let a and b be natural numbers such that $a^2 = b^3$. Prove each of the propositions in Parts (a) through (d). (The results of Exercise (1) and Theorem 3.10 may be helpful.)

(**a**) If a is even, then 4 divides a.

⋆ (**b**) If 4 divides a, then 4 divides b.

(**c**) If 4 divides b, then 8 divides a.

(**d**) If a is even, then 8 divides a.

(**e**) Give an example of natural numbers a and b such that a is even and $a^2 = b^3$, but b is not divisible by 8.

⋆ **18.** Prove the following proposition:

Let a and b be integers with $a \neq 0$. If a does not divide b, then the equation $ax^3 + bx + (b + a) = 0$ does not have a solution that is a natural number.

Hint: It may be necessary to factor a sum of cubes. Recall that

$$u^3 + v^3 = (u + v)\left(u^2 - uv + v^2\right).$$

19. Evaluation of Proofs
See the instructions for Exercise (19) on page 100 from Section 3.1.

(**a**) **Proposition**. If m is an odd integer, then $(m + 6)$ is an odd integer.

Proof. For $m + 6$ to be an odd integer, there must exist an integer n such that

$$m + 6 = 2n + 1.$$

By subtracting 6 from both sides of this equation, we obtain

$$\begin{aligned} m &= 2n - 6 + 1 \\ &= 2(n - 3) + 1. \end{aligned}$$

By the closure properties of the integers, $(n - 3)$ is an integer, and hence, the last equation implies that m is an odd integer. This proves that if m is an odd integer, then $m + 6$ is an odd integer. ■

(**b**) **Proposition**. For all integers m and n, if mn is an even integer, then m is even or n is even.

Proof. For either m or n to be even, there exists an integer k such that $m = 2k$ or $n = 2k$. So if we multiply m and n, the product will contain a factor of 2 and, hence, mn will be even. ■

Explorations and Activities

20. Using a Logical Equivalency. Consider the following proposition:

Proposition. For all integers a and b, if 3 does not divide a and 3 does not divide b, then 3 does not divide the product $a \cdot b$.

(**a**) Notice that the hypothesis of the proposition is stated as a conjunction of two negations ("3 does not divide a and 3 does not divide b"). Also, the conclusion is stated as the negation of a sentence ("3 does not divide the product $a \cdot b$."). This often indicates that we should consider using a proof of the contrapositive. If we use the symbolic form $(\neg Q \wedge \neg R) \rightarrow \neg P$ as a model for this proposition, what is P, what is Q, and what is R?

(**b**) Write a symbolic form for the contrapositive of $(\neg Q \wedge \neg R) \rightarrow \neg P$.

(**c**) Write the contrapositive of the proposition as a conditional statement in English.

We do not yet have all the tools needed to prove the proposition or its contrapositive. However, later in the text, we will learn that the following proposition is true.

Proposition X. Let a be an integer. If 3 does not divide a, then there exist integers x and y such that $3x + ay = 1$.

(**d**) i. Find integers x and y guaranteed by Proposition X when $a = 5$.
ii. Find integers x and y guaranteed by Proposition X when $a = 2$.
iii. Find integers x and y guaranteed by Proposition X when $a = -2$.

(**e**) Assume that Proposition X is true and use it to help construct a proof of the contrapositive of the given proposition. In doing so, you will most likely have to use the logical equivalency $P \rightarrow (Q \vee R) \equiv (P \wedge \neg Q) \rightarrow R$.

3.3 Proof by Contradiction

Beginning Activity 1 (**Proof by Contradiction**)

On page 40 in Section 2.1, we defined a **tautology** to be a compound statement S that is true for all possible combinations of truth values of the component statements that are part of S. We also defined **contradiction** to be a compound statement that is false for all possible combinations of truth values of the component statements that are part of S.

That is, a tautology is necessarily true in all circumstances, and a contradiction is necessarily false in all circumstances.

1. Use truth tables to explain why $(P \vee \neg P)$ is a tautology and $(P \wedge \neg P)$ is a contradiction.

Another method of proof that is frequently used in mathematics is a **proof by contradiction.** This method is based on the fact that a statement X can only be true or false (and not both). The idea is to prove that the statement X is true by showing that it cannot be false. This is done by assuming that X is false and proving that this leads to a contradiction. (The contradiction often has the form $(R \wedge \neg R)$, where R is some statement.) When this happens, we can conclude that the assumption that the statement X is false is incorrect and hence X cannot be false. Since it cannot be false, then X must be true.

A logical basis for the contradiction method of proof is the tautology

$$[\neg X \to C] \to X,$$

where X is a statement and C is a contradiction. The following truth table establishes this tautology.

X	C	$\neg X$	$\neg X \to C$	$(\neg X \to C) \to X$
T	F	F	T	T
F	F	T	F	T

This tautology shows that if $\neg X$ leads to a contradiction, then X must be true. The previous truth table also shows that the statement $\neg X \to C$ is logically equivalent to X. This means that if we have proved that $\neg X$ leads to a contradiction, then we have proved statement X. So if we want to prove a statement X using a proof by contradiction, we assume that $\neg X$ is true and show that this leads to a contradiction.

When we try to prove the conditional statement, "If P then Q" using a proof by contradiction, we must assume that $P \to Q$ is false and show that this leads to a contradiction.

2. Use a truth table to show that $\neg (P \to Q)$ is logically equivalent to $P \wedge \neg Q$.

The preceding logical equivalency shows that when we assume that $P \to Q$ is false, we are assuming that P is true and Q is false. If we can prove that this leads to a contradiction, then we have shown that $\neg (P \to Q)$ is false and hence that $P \to Q$ is true.

3. Give a counterexample to show that the following statement is false.

$$\text{For each real number } x, \frac{1}{x(1-x)} \geq 4.$$

4. When a statement is false, it is sometimes possible to add an assumption that will yield a true statement. This is usually done by using a conditional statement. So instead of working with the statement in (3), we will work with a related statement that is obtained by adding an assumption (or assumptions) to the hypothesis.

$$\text{For each real number } x, \text{ if } 0 < x < 1, \text{ then } \frac{1}{x(1-x)} \geq 4.$$

To begin a proof by contradiction for this statement, we need to assume the negation of the statement. To do this, we need to negate the entire statement, including the quantifier. Recall that the negation of a statement with a universal quantifier is a statement that contains an existential quantifier. (See Theorem 2.16 on page 67.) With this in mind, carefully write down all assumptions made at the beginning of a proof by contradiction for this statement.

Beginning Activity 2 (**Constructing a Proof by Contradiction**)
Consider the following proposition:

Proposition. For all real numbers x and y, if $x \neq y$, $x > 0$, and $y > 0$, then $\frac{x}{y} + \frac{y}{x} > 2$.

To start a proof by contradiction, we assume that this statement is false; that is, we assume the negation is true. Because this is a statement with a universal quantifier, we assume that there exist real numbers x and y such that $x \neq y$, $x > 0$, $y > 0$ and that $\frac{x}{y} + \frac{y}{x} \leq 2$. (Notice that the negation of the conditional sentence is a conjunction.)

For this proof by contradiction, we will only work with the know column of a know-show table. This is because we do not have a specific goal. The goal is to obtain some contradiction, but we do not know ahead of time what that contradiction will be. Using our assumptions, we can perform algebraic operations on the inequality

$$\frac{x}{y} + \frac{y}{x} \leq 2 \tag{2}$$

until we obtain a contradiction.

1. Try the following algebraic operations on the inequality in (2). First, multiply both sides of the inequality by xy, which is a positive real number since $x > 0$ and $y > 0$. Then, subtract $2xy$ from both sides of this inequality and finally, factor the left side of the resulting inequality.

2. Explain why the last inequality you obtained leads to a contradiction.

By obtaining a contradiction, we have proved that the proposition cannot be false, and hence, must be true.

Writing Guidelines: Keep the Reader Informed

A very important piece of information about a proof is the method of proof to be used. So when we are going to prove a result using the contrapositive or a proof by contradiction, we indicate this at the start of the proof.

- We will prove this result by proving the contrapositive of the statement.
- We will prove this statement using a proof by contradiction.
- We will use a proof by contradiction.

We have discussed the logic behind a proof by contradiction in the beginning activities for this section. The basic idea for a proof by contradiction of a proposition is to assume the proposition is false and show that this leads to a contradiction. We can then conclude that the proposition cannot be false, and hence, must be true. When we assume a proposition is false, we are, in effect, assuming that its negation is true. This is one reason why it is so important to be able to write negations of propositions quickly and correctly. We will illustrate the process with the proposition discussed in Beginning Activity 1.

Proposition 3.14. *For each real number x, if $0 < x < 1$, then* $\dfrac{1}{x(1-x)} \geq 4$.

Proof. We will use a proof by contradiction. So we assume that the proposition is false, or that there exists a real number x such that $0 < x < 1$ and

$$\frac{1}{x(1-x)} < 4. \tag{1}$$

We note that since $0 < x < 1$, we can conclude that $x > 0$ and that $(1-x) > 0$. Hence, $x(1-x) > 0$ and if we multiply both sides of inequality (1) by $x(1-x)$, we obtain

$$1 < 4x(1-x).$$

We can now use algebra to rewrite the last inequality as follows:

$$\begin{aligned} 1 &< 4x - 4x^2 \\ 4x^2 - 4x + 1 &< 0 \\ (2x-1)^2 &< 0 \end{aligned}$$

However, $(2x-1)$ is a real number and the last inequality says that a real number squared is less than zero. This is a contradiction since the square of any real number

cc BY NC SA

must be greater than or equal to zero. Hence, the proposition cannot be false, and we have proved that for each real number x, if $0 < x < 1$, then $\dfrac{1}{x(1-x)} \geq 4$. ■

Progress Check 3.15 (**Starting a Proof by Contradiction**)
One of the most important parts of a proof by contradiction is the very first part, which is to state the assumptions that will be used in the proof by contradiction. This usually involves writing a clear negation of the proposition to be proven. Review De Morgan's Laws and the negation of a conditional statement in Section 2.2. (See Theorem 2.8 on page 48.) Also, review Theorem 2.16 (on page 67) and then write a negation of each of the following statements. (Remember that a real number is "not irrational" means that the real number is rational.)

1. For each real number x, if x is irrational, then $\sqrt[3]{x}$ is irrational.
2. For each real number x, $\left(x + \sqrt{2}\right)$ is irrational or $\left(-x + \sqrt{2}\right)$ is irrational.
3. For all integers a and b, if 5 divides ab, then 5 divides a or 5 divides b.
4. For all real numbers a and b, if $a > 0$ and $b > 0$, then $\dfrac{2}{a} + \dfrac{2}{b} \neq \dfrac{4}{a+b}$.

Important Note

A proof by contradiction is often used to prove a conditional statement $P \to Q$ when a direct proof has not been found and it is relatively easy to form the negation of the proposition. The advantage of a proof by contradiction is that we have an additional assumption with which to work (since we assume not only P but also $\neg Q$). The disadvantage is that there is no well-defined goal to work toward. The goal is simply to obtain some contradiction. There usually is no way of telling beforehand what that contradiction will be, so we have to stay alert for a possible absurdity. Thus, when we set up a know-show table for a proof by contradiction, we really only work with the know portion of the table.

Progress Check 3.16 (**Exploration and a Proof by Contradiction**)
Consider the following proposition:

For each integer n, if $n \equiv 2 \pmod 4$, then $n \not\equiv 3 \pmod 6$.

CC BY NC SA

1. Determine at least five different integers that are congruent to 2 modulo 4, and determine at least five different integers that are congruent to 3 modulo 6. Are there any integers that are in both of these lists?

2. For this proposition, why does it seem reasonable to try a proof by contradiction?

3. For this proposition, state clearly the assumptions that need to be made at the beginning of a proof by contradiction, and then use a proof by contradiction to prove this proposition.

Proving that Something Does Not Exist

In mathematics, we sometimes need to prove that something does not exist or that something is not possible. Instead of trying to construct a direct proof, it is sometimes easier to use a proof by contradiction so that we can assume that the something exists. For example, suppose we want to prove the following proposition:

Proposition 3.17. *For all integers x and y, if x and y are odd integers, then there does not exist an integer z such that $x^2 + y^2 = z^2$.*

Notice that the conclusion involves trying to prove that an integer with a certain property does not exist. If we use a proof by contradiction, we can assume that such an integer z exists. This gives us more with which to work.

Progress Check 3.18 Complete the following proof of Proposition 3.17:

Proof. We will use a proof by contradiction. So we assume that there exist integers x and y such that x and y are odd and there exists an integer z such that $x^2 + y^2 = z^2$. Since x and y are odd, there exist integers m and n such that $x = 2m + 1$ and $y = 2n + 1$.

1. Use the assumptions that x and y are odd to prove that $x^2 + y^2$ is even and hence, z^2 is even. (See Theorem 3.7 on page 105.)

We can now conclude that z is even. (See Theorem 3.7 on page 105.) So there exists an integer k such that $z = 2k$. If we substitute for x, y, and z in the equation $x^2 + y^2 = z^2$, we obtain

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

2. Use the previous equation to obtain a contradiction. **Hint**: One way is to use algebra to obtain an equation where the left side is an odd integer and the right side is an even integer. ■

Rational and Irrational Numbers

One of the most important ways to classify real numbers is as a rational number or an irrational number. Following is the definition of rational (and irrational) numbers given in Exercise (9) from Section 3.2.

Definition. A real number x is defined to be a **rational number** provided that there exist integers m and n with $n \neq 0$ such that $x = \frac{m}{n}$. A real number that is not a rational number is called an **irrational number.**

This may seem like a strange distinction because most people are quite familiar with the rational numbers (fractions) but the irrational numbers seem a bit unusual. However, there are many irrational numbers such as $\sqrt{2}$, $\sqrt{3}$, $\sqrt[3]{2}$, π, and the number e. We are discussing these matters now because we will soon prove that $\sqrt{2}$ is irrational in Theorem 3.20.

We use the symbol $\mathbb{Q}$ to stand for the set of rational numbers. There is no standard symbol for the set of irrational numbers. Perhaps one reason for this is because of the closure properties of the rational numbers. We introduced closure properties in Section 1.1, and the rational numbers $\mathbb{Q}$ are closed under addition, subtraction, multiplication, and division by nonzero rational numbers. This means that if $x, y \in \mathbb{Q}$, then

- $x + y$, $x - y$, and xy are in $\mathbb{Q}$; and
- If $y \neq 0$, then $\frac{x}{y}$ is in $\mathbb{Q}$.

The basic reasons for these facts are that if we add, subtract, multiply, or divide two fractions, the result is a fraction. One reason we do not have a symbol for the irrational numbers is that the irrational numbers are not closed under these operations. For example, we will prove that $\sqrt{2}$ is irrational in Theorem 3.20. We then see that

$$\sqrt{2}\sqrt{2} = 2 \quad \text{and} \quad \frac{\sqrt{2}}{\sqrt{2}} = 1,$$

which shows that the product of irrational numbers can be rational and the quotient of irrational numbers can be rational.

It is also important to realize that every integer is a rational number since any integer can be written as a fraction. For example, we can write $3 = \frac{3}{1}$. In general, if $n \in \mathbb{Z}$, then $n = \frac{n}{1}$, and hence, $n \in \mathbb{Q}$.

Because the rational numbers are closed under the standard operations and the definition of an irrational number simply says that the number is not rational, we often use a proof by contradiction to prove that a number is irrational. This is illustrated in the next proposition.

Proposition 3.19. *For all real numbers x and y, if x is rational and $x \neq 0$ and y is irrational, then $x \cdot y$ is irrational.*

Proof. We will use a proof by contradiction. So we assume that there exist real numbers x and y such that x is rational, $x \neq 0$, y is irrational, and $x \cdot y$ is rational. Since $x \neq 0$, we can divide by x, and since the rational numbers are closed under division by nonzero rational numbers, we know that $\frac{1}{x} \in \mathbb{Q}$. We now know that $x \cdot y$ and $\frac{1}{x}$ are rational numbers and since the rational numbers are closed under multiplication, we conclude that

$$\frac{1}{x} \cdot (xy) \in \mathbb{Q}.$$

However, $\frac{1}{x} \cdot (xy) = y$ and hence, y must be a rational number. Since a real number cannot be both rational and irrational, this is a contradiction to the assumption that y is irrational. We have therefore proved that for all real numbers x and y, if x is rational and $x \neq 0$ and y is irrational, then $x \cdot y$ is irrational. ■

The Square Root of 2 Is an Irrational Number

The proof that the square root of 2 is an irrational number is one of the classic proofs in mathematics, and every mathematics student should know this proof. This is why we will be doing some preliminary work with rational numbers and integers before completing the proof. The theorem we will be proving can be stated as follows:

Theorem 3.20. *If r is a real number such that $r^2 = 2$, then r is an irrational number.*

This is stated in the form of a conditional statement, but it basically means that $\sqrt{2}$ is irrational (and that $-\sqrt{2}$ is irrational). That is, $\sqrt{2}$ cannot be written as a quotient of integers with the denominator not equal to zero.

In order to complete this proof, we need to be able to work with some basic facts that follow about rational numbers and even integers.

1. Each integer m is a rational number since m can be written as $m = \dfrac{m}{1}$.

2. Notice that $\dfrac{2}{3} = \dfrac{4}{6}$, since

$$\frac{4}{6} = \frac{2 \cdot 2}{3 \cdot 2} = \frac{2}{2} \cdot \frac{2}{3} = \frac{2}{3}$$

We can also show that $\dfrac{15}{12} = \dfrac{5}{4}$, $\dfrac{10}{-8} = \dfrac{-5}{4}$, and $\dfrac{-30}{-16} = \dfrac{15}{8}$

Item (2) was included to illustrate the fact that a rational number can be written as a fraction in "lowest terms" with a positive denominator. This means that any rational number can be written as a quotient $\dfrac{m}{n}$, where m and n are integers, $n > 0$, and m and n have no common factor greater than 1.

3. If n is an integer and n^2 is even, what can be conclude about n. Refer to Theorem 3.7 on page 105.

In a proof by contradiction of a conditional statement $P \rightarrow Q$, we assume the negation of this statement or $P \wedge \neg Q$. So in a proof by contradiction of Theorem 3.20, we will assume that r is a real number, $r^2 = 2$, and r is not irrational (that is, r is rational).

Theorem 3.20. *If r is a real number such that $r^2 = 2$, then r is an irrational number.*

Proof. We will use a proof by contradiction. So we assume that the statement of the theorem is false. That is, we assume that

r is a real number, $r^2 = 2$, and r is a rational number.

Since r is a rational number, there exist integers m and n with $n > 0$ such that

$$r = \frac{m}{n}$$

and m and n have no common factor greater than 1. We will obtain a contradiction by showing that m and n must both be even. Squaring both sides of the last equation and using the fact that $r^2 = 2$, we obtain

$$\begin{aligned} 2 &= \frac{m^2}{n^2} \\ m^2 &= 2n^2. \end{aligned} \tag{1}$$

Equation (1) implies that m^2 is even, and hence, by Theorem 3.7, m must be an even integer. This means that there exists an integer p such that $m = 2p$. We can now substitute this into equation (1), which gives

$$\begin{aligned} (2p)^2 &= 2n^2 \\ 4p^2 &= 2n^2. \end{aligned} \tag{2}$$

We can divide both sides of equation (2) by 2 to obtain $n^2 = 2p^2$. Consequently, n^2 is even and we can once again use Theorem 3.7 to conclude that n is an even integer.

We have now established that both m and n are even. This means that 2 is a common factor of m and n, which contradicts the assumption that m and n have no common factor greater than 1. Consequently, the statement of the theorem cannot be false, and we have proved that if r is a real number such that $r^2 = 2$, then r is an irrational number. ■

Exercises for Section 3.3

1. This exercise is intended to provide another rationale as to why a proof by contradiction works.

Suppose that we are trying to prove that a statement P is true. Instead of proving this statement, assume that we prove that the conditional statement "If $\neg P$, then C" is true, where C is some contradiction. Recall that a contradiction is a statement that is always false.

⋆ **(a)** In symbols, write a statement that is a disjunction and that is logically equivalent to $\neg P \to C$.

(b) Since we have proven that $\neg P \to C$ is true, then the disjunction in Exercise (1a) must also be true. Use this to explain why the statement P must be true.

(c) Now explain why P must be true if we prove that the negation of P implies a contradiction.

2. Are the following statements true or false? Justify each conclusion.

⋆ **(a)** For all integers a and b, if a is even and b is odd, then 4 does not divide $(a^2 + b^2)$.

⋆ **(b)** For all integers a and b, if a is even and b is odd, then 6 does not divide $(a^2 + b^2)$.

(c) For all integers a and b, if a is even and b is odd, then 4 does not divide $(a^2 + 2b^2)$.

⋆ **(d)** For all integers a and b, if a is odd and b is odd, then 4 divides $(a^2 + 3b^2)$.

⋆ **3.** Consider the following statement:

For each positive real number r, if $r^2 = 18$, then r is irrational.

(a) If you were setting up a proof by contradiction for this statement, what would you assume? Carefully write down all conditions that you would assume.

(b) Complete a proof by contradiction for this statement.

4. Prove that the cube root of 2 is an irrational number. That is, prove that if r is a real number such that $r^3 = 2$, then r is an irrational number.

⋆ **5.** Prove the following propositions:

(a) For all real numbers x and y, if x is rational and y is irrational, then $x + y$ is irrational.

(b) For all nonzero real numbers x and y, if x is rational and y is irrational, then xy is irrational.

6. Are the following statements true or false? Justify each conclusion.

⋆ **(a)** For each positive real number x, if x is irrational, then x^2 is irrational.

⋆ **(b)** For each positive real number x, if x is irrational, then $\sqrt{x}$ is irrational.

(c) For every pair of real numbers x and y, if $x + y$ is irrational, then x is irrational and y is irrational.

(d) For every pair of real numbers x and y, if $x + y$ is irrational, then x is irrational or y is irrational.

7. (**a**) Give an example that shows that the sum of two irrational numbers can be a rational number.

(**b**) Now explain why the following proof that $\left(\sqrt{2} + \sqrt{5}\right)$ is an irrational number is not a valid proof: Since $\sqrt{2}$ and $\sqrt{5}$ are both irrational numbers, their sum is an irrational number. Therefore, $\left(\sqrt{2} + \sqrt{5}\right)$ is an irrational number.

Note: You may even assume that we have proven that $\sqrt{5}$ is an irrational number. (We have not proven this.)

(**c**) Is the real number $\sqrt{2}+\sqrt{5}$ a rational number or an irrational number? Justify your conclusion.

8. (**a**) Prove that for each real number x, $\left(x + \sqrt{2}\right)$ is irrational or $\left(-x + \sqrt{2}\right)$ is irrational.

(**b**) Generalize the proposition in Part (a) for any irrational number (instead of just $\sqrt{2}$) and then prove the new proposition.

9. Is the following statement true or false?

For all positive real numbers x and y, $\sqrt{x + y} \leq \sqrt{x} + \sqrt{y}$.

10. Is the following proposition true or false? Justify your conclusion.

For each real number x, $x\,(1 - x) \leq \dfrac{1}{4}$.

⋆ **11.** (**a**) Is the base 2 logarithm of 32, $\log_2(32)$, a rational number or an irrational number? Justify your conclusion.

(**b**) Is the base 2 logarithm of 3, $\log_2(3)$, a rational number or an irrational number? Justify your conclusion.

⋆ **12.** In Exercise (15) in Section 3.2, we proved that there exists a real number solution to the equation $x^3 - 4x^2 = 7$. Prove that there is no integer x such that $x^3 - 4x^2 = 7$.

cc BY NC SA

13. Prove each of the following propositions:

⋆ **(a)** For each real number θ, if $0 < \theta < \dfrac{\pi}{2}$, then $[\sin(\theta) + \cos(\theta)] > 1$.

(b) For all real numbers a and b, if $a \neq 0$ and $b \neq 0$, then $\sqrt{a^2 + b^2} \neq a + b$.

(c) If n is an integer greater than 2, then for all integers m, n does not divide m or $n + m \neq nm$.

(d) For all real numbers a and b, if $a > 0$ and $b > 0$, then

$$\frac{2}{a} + \frac{2}{b} \neq \frac{4}{a+b}.$$

⋆ **14.** Prove that there do not exist three consecutive natural numbers such that the cube of the largest is equal to the sum of the cubes of the other two.

15. Three natural numbers a, b, and c with $a < b < c$ are called a **Pythagorean triple** provided that $a^2 + b^2 = c^2$. For example, the numbers 3, 4, and 5 form a Pythagorean triple, and the numbers 5, 12, and 13 form a Pythagorean triple.

(**a**) Verify that if $a = 20$, $b = 21$, and $c = 29$, then $a^2 + b^2 = c^2$, and hence, 20, 21, and 29 form a Pythagorean triple.

(**b**) Determine two other Pythagorean triples. That is, find integers a, b, and c such that $a^2 + b^2 = c^2$.

(**c**) Is the following proposition true or false? Justify your conclusion.
For all integers a, b, and c, if $a^2 + b^2 = c^2$, then a is even or b is even.

16. Consider the following proposition: There are no integers a and b such that $b^2 = 4a + 2$.

(**a**) Rewrite this statement in an equivalent form using a universal quantifier by completing the following:

For all integers a and b, ...

(**b**) Prove the statement in Part (a).

17. Is the following statement true or false? Justify your conclusion.

For each integer n that is greater than 1, if a is the smallest positive factor of n that is greater than 1, then a is prime.

See Exercise (13) in Section 2.4 (page 78) for the definition of a prime number and the definition of a composite number.

18. A **magic square** is a square array of natural numbers whose rows, columns, and diagonals all sum to the same number. For example, the following is a 3 by 3 magic square since the sum of the 3 numbers in each row is equal to 15, the sum of the 3 numbers in each column is equal to 15, and the sum of the 3 numbers in each diagonal is equal to 15.

8	3	4
1	5	9
6	7	2

Prove that the following 4 by 4 square cannot be completed to form a magic square.

	1		2
3	4	5	
6	7		8
9		10	

19. Using only the digits 1 through 9 one time each, is it possible to construct a 3 by 3 magic square with the digit 3 in the center square? That is, is it possible to construct a magic square of the form

a	b	c
d	3	e
f	g	h

where a, b, c, d, e, f, g, h are all distinct digits, none of which is equal to 3? Either construct such a magic square or prove that it is not possible.

20. Evaluation of proofs
See the instructions for Exercise (19) on page 100 from Section 3.1.

(**a**) **Proposition**. For each real number x, if x is irrational and m is an integer, then mx is irrational.

Proof. We assume that x is a real number and is irrational. This means that for all integers a and b with $b \neq 0$, $x \neq \frac{a}{b}$. Hence, we may conclude that $mx \neq \frac{ma}{b}$ and, therefore, mx is irrational. ■

CC BY NC SA

(**b**) **Proposition**. For all real numbers x and y, if x is irrational and y is rational, then $x + y$ is irrational.

Proof. We will use a proof by contradiction. So we assume that the proposition is false, which means that there exist real numbers x and y where $x \notin \mathbb{Q}$, $y \in \mathbb{Q}$, and $x + y \in \mathbb{Q}$. Since the rational numbers are closed under subtraction and $x + y$ and y are rational, we see that

$$(x + y) - y \in \mathbb{Q}.$$

However, $(x + y) - y = x$, and hence we can conclude that $x \in \mathbb{Q}$. This is a contradiction to the assumption that $x \notin \mathbb{Q}$. Therefore, the proposition is not false, and we have proven that for all real numbers x and y, if x is irrational and y is rational, then $x + y$ is irrational. ■

(**c**) **Proposition**. For each real number x, $x(1 - x) \leq \frac{1}{4}$.

Proof. A proof by contradiction will be used. So we assume the proposition is false. This means that there exists a real number x such that $x(1 - x) > \frac{1}{4}$. If we multiply both sides of this inequality by 4, we obtain $4x(1 - x) > 1$. However, if we let $x = 3$, we then see that

$$\begin{aligned} 4x(1 - x) &> 1 \\ 4 \cdot 3(1 - 3) &> 1 \\ -12 &> 1 \end{aligned}$$

The last inequality is clearly a contradiction and so we have proved the proposition. ■

Explorations and Activities

21. A Proof by Contradiction. Consider the following proposition:

Proposition. Let a, b, and c be integers. If 3 divides a, 3 divides b, and $c \equiv 1 \pmod 3$, then the equation

$$ax + by = c$$

has no solution in which both x and y are integers.

Complete the following proof of this proposition:

CC BY NC SA

Proof. A proof by contradiction will be used. So we assume that the statement is false. That is, we assume that there exist integers a, b, and c such that 3 divides both a and b, that $c \equiv 1 \pmod 3$, and that the equation

$$ax + by = c$$

has a solution in which both x and y are integers. So there exist integers m and n such that

$$am + bn = c.$$

Hint: Now use the facts that 3 divides a, 3 divides b, and $c \equiv 1 \pmod 3$.

22. Exploring a Quadratic Equation. Consider the following proposition:

Proposition. For all integers m and n, if n is odd, then the equation

$$x^2 + 2mx + 2n = 0$$

has no integer solution for x.

(**a**) What are the solutions of the equation when $m = 1$ and $n = -1$? That is, what are the solutions of the equation $x^2 + 2x - 2 = 0$?

(**b**) What are the solutions of the equation when $m = 2$ and $n = 3$? That is, what are the solutions of the equation $x^2 + 4x + 6 = 0$?

(**c**) Solve the resulting quadratic equation for at least two more examples using values of m and n that satisfy the hypothesis of the proposition.

(**d**) For this proposition, why does it seem reasonable to try a proof by contradiction?

(**e**) For this proposition, state clearly the assumptions that need to be made at the beginning of a proof by contradiction.

(**f**) Use a proof by contradiction to prove this proposition.

3.4 Using Cases in Proofs

Beginning Activity 1 (Using a Logical Equivalency)

1. Complete a truth table to show that $(P \vee Q) \to R$ is logically equivalent to $(P \to R) \wedge (Q \to R)$.

2. Suppose that you are trying to prove a statement that is written in the form $(P \vee Q) \rightarrow R$. Explain why you can complete this proof by writing separate and independent proofs of $P \rightarrow R$ and $Q \rightarrow R$.

3. Now consider the following proposition:

   Proposition. For all integers x and y, if xy is odd, then x is odd and y is odd.

   Write the contrapositive of this proposition.

4. Now prove that if x is an even integer, then xy is an even integer. Also, prove that if y is an even integer, then xy is an even integer.

5. Use the results proved in part (4) and the explanation in part (2) to explain why we have proved the contrapositive of the proposition in part (3).

Beginning Activity 2 (Using Cases in a Proof)
The work in Beginning Activity 1 was meant to introduce the idea of using cases in a proof. The method of using cases is often used when the hypothesis of the proposition is a disjunction. This is justified by the logical equivalency

$$[(P \vee Q) \rightarrow R] \equiv [(P \rightarrow R) \wedge (Q \rightarrow R)] .$$

See Theorem 2.8 on page 48 and Exercise (6) on page 50.

In some other situations when we are trying to prove a proposition or a theorem about an element x in some set U, we often run into the problem that there does not seem to be enough information about x to proceed. For example, consider the following proposition:

Proposition 1. If n is an integer, then $\left(n^2 + n\right)$ is an even integer.

If we were trying to write a direct proof of this proposition, the only thing we could assume is that n is an integer. This is not much help. In a situation such as this, we will sometimes use cases to provide additional assumptions for the forward process of the proof. Cases are usually based on some common properties that the element x may or may not possess. The cases must be chosen so that they exhaust all possibilities for the object x in the hypothesis of the original proposition. For Proposition 1, we know that an integer must be even or it must be odd. We can thus use the following two cases for the integer n:

- The integer n is an even integer;

- The integer n is an odd integer.

1. Complete the proof for the following proposition:

Proposition 2: If n is an even integer, then $n^2 + n$ is an even integer.

Proof. Let n be an even integer. Then there exists an integer m such that $n = 2m$. Substituting this into the expression $n^2 + n$ yields ....

2. Construct a proof for the following proposition:

Proposition 3: If n is an odd integer, then $n^2 + n$ is an even integer.

3. Explain why the proofs of Proposition 2 and Proposition 3 can be used to construct a proof of Proposition 1.

Some Common Situations to Use Cases

When using cases in a proof, the main rule is that the cases must be chosen so that they exhaust all possibilities for an object x in the hypothesis of the original proposition. Following are some common uses of cases in proofs.

When the hypothesis is, "n is an integer."	Case 1: n is an even integer. Case 2: n is an odd integer.		
When the hypothesis is, "m and n are integers."	Case 1: m and n are even. Case 2: m is even and n is odd. Case 3: m is odd and n is even. Case 4: m and n are both odd.		
When the hypothesis is, "x is a real number."	Case 1: x is rational. Case 2: x is irrational.		
When the hypothesis is, "x is a real number."	Case 1: $x = 0$. Case 2: $x \neq 0$.	OR	Case 1: $x > 0$. Case 2: $x = 0$. Case 3: $x < 0$.

CC BY NC SA

When the hypothesis is, "a and b are real numbers."	Case 1: $a = b$. Case 2: $a \neq b$.	OR	Case 1: $a > b$. Case 2: $a = b$. Case 3: $a < b$.

Writing Guidelines for a Proof Using Cases

When writing a proof that uses cases, we use all the other writing guidelines. In addition, we make sure that it is clear where each case begins. This can be done by using a new paragraph with a label such as "Case 1," or it can be done by starting a paragraph with a phrase such as, "In the case where ...."

Progress Check 3.21 (**Using Cases: *n* Is Even or *n* Is Odd**)
Complete the proof of the following proposition:

Proposition. *For each integer n, $n^2 - 5n + 7$ is an odd integer.*

Proof. Let n be an integer. We will prove that $n^2 - 5n + 7$ is an odd integer by examining the case where n is even and the case where n is odd.

Case 1. The integer n is even. In this case, there exists an integer m such that $n = 2m$. Therefore, ...

As another example of using cases, consider a situation where we know that a and b are real numbers and $ab = 0$. If we want to make a conclusion about b, the temptation might be to divide both sides of the equation by a. However, we can only do this if $a \neq 0$. So, we consider two cases: one when $a = 0$ and the other when $a \neq 0$.

Proposition 3.22. *For all real numbers a and b, if $ab = 0$, then $a = 0$ or $b = 0$.*

Proof. We let a and b be real numbers and assume that $ab = 0$. We will prove that $a = 0$ or $b = 0$ by considering two cases: (1) $a = 0$, and (2) $a \neq 0$.

In the case where $a = 0$, the conclusion of the proposition is true and so there is nothing to prove.

In the case where $a \neq 0$, we can multiply both sides of the equation $ab = 0$

by $\frac{1}{a}$ and obtain

$$\frac{1}{a} \cdot ab = \frac{1}{a} \cdot 0$$
$$b = 0.$$

So in both cases, $a = 0$ or $b = 0$, and this proves that for all real numbers a and b, if $ab = 0$, then $a = 0$ or $b = 0$. ■

Absolute Value

Most students by now have studied the concept of the absolute value of a real number. We use the notation $|x|$ to stand for the absolute value of the real number x. One way to think of the absolute value of x is as the "distance" between x and 0 on the number line. For example,

$$|5| = 5 \quad \text{and} \quad |-7| = 7.$$

Although this notion of absolute value is convenient for determining the absolute value of a specific number, if we want to prove properties about absolute value, we need a more careful and precise definition.

Definition. For $x \in \mathbb{R}$, we define $|x|$, called the **absolute value of x**, by

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

Let's first see if this definition is consistent with our intuitive notion of absolute value by looking at two specific examples.

- Since $5 > 0$, we see that $|5| = 5$, which should be no surprise.
- Since $-7 < 0$, we see that $|-7| = -(-7) = 7$.

Notice that the definition of the absolute value of x is given in two parts, one for when $x \geq 0$ and the other for when $x < 0$. This means that when attempting to prove something about absolute value, we often uses cases. This will be illustrated in Theorem 3.23.

Theorem 3.23. *Let a be a positive real number. For each real number x,*

1. *$|x| = a$ if and only if $x = a$ or $x = -a$.*
2. *$|-x| = |x|$.*

Proof. The proof of Part (2) is part of Exercise (10). We will prove Part (1).

We let a be a positive real number and let $x \in \mathbb{R}$. We will first prove that if $|x| = a$, then $x = a$ or $x = -a$. So we assume that $|x| = a$. In the case where $x \geq 0$, we see that $|x| = x$, and since $|x| = a$, we can conclude that $x = a$.

In the case where $x < 0$, we see that $|x| = -x$. Since $|x| = a$, we can conclude that $-x = a$ and hence that $x = -a$. These two cases prove that if $|x| = a$, then $x = a$ or $x = -a$.

We will now prove that if $x = a$ or $x = -a$, then $|x| = a$. We start by assuming that $x = a$ or $x = -a$. Since the hypothesis of this conditional statement is a disjunction, we use two cases. When $x = a$, we see that

$$|x| = |a| = a \quad \text{since } a > 0.$$

When $x = -a$, we conclude that

$$|x| = |-a| = -(-a) \quad \text{since } -a < 0,$$

and hence, $|x| = a$. This proves that if $x = a$ or $x = -a$, then $|x| = a$. Because we have proven both conditional statements, we have proven that $|x| = a$ if and only if $x = a$ or $x = -a$. ■

Progress Check 3.24 (Equations Involving Absolute Values)

1. What is $|4.3|$ and what is $|-\pi|$?
2. Use the properties of absolute value in Proposition 3.23 to help solve the following equations for t, where t is a real number.

   (a) $|t| = 12$.

   (b) $|t + 3| = 5$.

   (c) $|t - 4| = \frac{1}{5}$.

   (d) $|3t - 4| = 8$.

Although solving equations involving absolute values may not seem to have anything to do with writing proofs, the point of Progress Check 3.24 is to emphasize the importance of using cases when dealing with absolute value. The following theorem provides some important properties of absolute value.

Theorem 3.25. *Let a be a positive real number. For all real numbers x and y,*

1. $|x| < a$ *if and only if* $-a < x < a$.
2. $|xy| = |x|\,|y|$.
3. $|x + y| \leq |x| + |y|$. *This is known as the* ***Triangle Inequality***.

Proof. We will prove Part (1). The proof of Part (2) is included in Exercise (10), and the proof of Part (3) is Exercise (14). For Part (1), we will prove the biconditional proposition by proving the two associated conditional propositions.

So we let a be a positive real number and let $x \in \mathbb{R}$ and first assume that $|x| < a$. We will use two cases: either $x \geq 0$ or $x < 0$.

- In the case where $x \geq 0$, we know that $|x| = x$ and so the inequality $|x| < a$ implies that $x < a$. However, we also know that $-a < 0$ and that $x > 0$. Therefore, we conclude that $-a < x$ and, hence, $-a < x < a$.
- When $x < 0$, we see that $|x| = -x$. Therefore, the inequality $|x| < a$ implies that $-x < a$, which in turn implies that $-a < x$. In this case, we also know that $x < a$ since x is negative and a is positive. Hence, $-a < x < a$.

So in both cases, we have proven that $-a < x < a$ and this proves that if $|x| < a$, then $-a < x < a$. We now assume that $-a < x < a$.

- If $x \geq 0$, then $|x| = x$ and hence, $|x| < a$.
- If $x < 0$, then $|x| = -x$ and so $x = -|x|$. Thus, $-a < -|x|$. By multiplying both sides of the last inequality by -1, we conclude that $|x| < a$.

These two cases prove that if $-a < x < a$, then $|x| < a$. Hence, we have proven that $|x| < a$ if and only if $-a < x < a$. ■

Exercises for Section 3.4

⋆ **1.** In Beginning Activity 2, we proved that if n is an integer, then $n^2 + n$ is an even integer. We define two integers to be **consecutive integers** if one of the integers is one more than the other integer. This means that we can represent consecutive integers as m and $m + 1$, where m is some integer.

Explain why the result proven in Beginning Activity 2 can be used to prove that the product of any two consecutive integers is divisible by 2.

⋆ **2.** Prove that if u is an odd integer, then the equation $x^2 + x - u = 0$ has no solution that is an integer.

⋆ **3.** Prove that if n is an odd integer, then $n = 4k + 1$ for some integer k or $n = 4k + 3$ for some integer k.

⋆ **4.** Prove the following proposition:

For each integer a, if $a^2 = a$, then $a = 0$ or $a = 1$.

5. (**a**) Prove the following proposition:

For all integers a, b, and d with $d \neq 0$, if d divides a or d divides b, then d divides the product ab.

Hint: Notice that the hypothesis is a disjunction. So use two cases.

(**b**) Write the contrapositive of the proposition in Exercise (5a).

⋆ **(c)** Write the converse of the proposition in Exercise (5a). Is the converse true or false? Justify your conclusion.

6. Are the following propositions true or false? Justify all your conclusions. If a biconditional statement is found to be false, you should clearly determine if one of the conditional statements within it is true. In that case, you should state an appropriate theorem for this conditional statement and prove it.

⋆ **(a)** For all integers m and n, m and n are consecutive integers if and only if 4 divides $\left(m^2 + n^2 - 1\right)$.

(b) For all integers m and n, 4 divides $\left(m^2 - n^2\right)$ if and only if m and n are both even or m and n are both odd.

7. Is the following proposition true or false? Justify your conclusion with a counterexample or a proof.

For each integer n, if n is odd, then $8 \mid \left(n^2 - 1\right)$.

⋆ **8.** Prove that there are no natural numbers a and n with $n \geq 2$ and $a^2 + 1 = 2^n$.

9. Are the following propositions true or false? Justify each conclusion with a counterexample or a proof.

(**a**) For all integers a and b with $a \neq 0$, the equation $ax + b = 0$ has a rational number solution.

(**b**) For all integers a, b, and c, if a, b, and c are odd, then the equation $ax^2 + bx + c = 0$ has no solution that is a rational number.

Hint: Do not use the quadratic formula. Use a proof by contradiction and recall that any rational number can be written in the form $\frac{p}{q}$, where p and q are integers, $q > 0$, and p and q have no common factor greater than 1.

(**c**) For all integers a, b, c, and d, if a, b, c, and d are odd, then the equation $ax^3 + bx^2 + cx + d = 0$ has no solution that is a rational number.

10. ⋆ (**a**) Prove Part (2) of Proposition 3.23.

For each $x \in \mathbb{R}$, $|-x| = |x|$.

(**b**) Prove Part (2) of Theorem 3.25.

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

11. Let a be a positive real number. In Part (1) of Theorem 3.25, we proved that for each real number x, $|x| < a$ if and only if $-a < x < a$. It is important to realize that the sentence $-a < x < a$ is actually the conjunction of two inequalities. That is, $-a < x < a$ means that $-a < x$ and $x < a$.

⋆ (**a**) Complete the following statement: For each real number x, $|x| \geq a$ if and only if ....

(**b**) Prove that for each real number x, $|x| \leq a$ if and only if $-a \leq x \leq a$.

(**c**) Complete the following statement: For each real number x, $|x| > a$ if and only if ....

12. Prove each of the following:

(**a**) For each nonzero real number x , $\left|x^{-1}\right| = \dfrac{1}{|x|}$.

(**b**) For all real numbers x and y, $|x - y| \geq |x| - |y|$.

Hint: An idea that is often used by mathematicians is to add 0 to an expression "intelligently". In this case, we know that $(-y) + y = 0$. Start by adding this "version" of 0 inside the absolute value sign of $|x|$.

(**c**) For all real numbers x and y, $||x| - |y|| \leq |x - y|$.

13. Evaluation of proofs

See the instructions for Exercise (19) on page 100 from Section 3.1.

(**a**) **Proposition**. For all nonzero integers a and b, if $a + 2b \neq 3$ and $9a + 2b \neq 1$, then the equation $ax^3 + 2bx = 3$ does not have a solution that is a natural number.

Proof. We will prove the contrapositive, which is

For all nonzero integers a and b, if the equation $ax^3+2bx = 3$ has a solution that is a natural number, then $a+2b = 3$ or $9a+2b = 1$.

So we let a and b be nonzero integers and assume that the natural number n is a solution of the equation $ax^3 + 2bx = 3$. So we have

$$an^3 + 2bn = 3 \qquad \text{or}$$
$$n\left(an^2 + 2b\right) = 3.$$

So we can conclude that $n = 3$ and $an^2 + 2b = 1$. Since we now have the value of n, we can substitute it in the equation $an^3 + 2bn = 3$ and obtain $27a + 6b = 3$. Dividing both sides of this equation by 3 shows that $9a + 2b = 1$. So there is no need for us to go any further, and this concludes the proof of the contrapositive of the proposition. ■

(**b**) **Proposition**. For all nonzero integers a and b, if $a + 2b \neq 3$ and $9a + 2b \neq 1$, then the equation $ax^3 + 2bx = 3$ does not have a solution that is a natural number.

Proof. We will use a proof by contradiction. Let us assume that there exist nonzero integers a and b such that $a + 2b = 3$ and $9a + 2b = 1$ and $an^3 + 2bn = 3$, where n is a natural number. First, we will solve one equation for $2b$; doing this, we obtain

$$\begin{aligned} a + 2b &= 3 \\ 2b &= 3 - a. \end{aligned} \tag{1}$$

We can now substitute for $2b$ in $an^3 + 2bn = 3$. This gives

$$\begin{aligned} an^3 + (3 - a)n &= 3 \\ an^3 + 3n - an &= 3 \\ n\left(an^2 + 3 - a\right) &= 3. \end{aligned} \tag{2}$$

By the closure properties of the integers, $\left(an^2 + 3 - a\right)$ is an integer and, hence, equation (2) implies that n divides 3. So $n = 1$ or $n = 3$. When we substitute $n = 1$ into the equation $an^3 + 2bn = 3$, we obtain $a + 2b = 3$. This is a contradiction since we are told in the proposition that $a + 2b \neq 3$. This proves that the negation of the proposition is false and, hence, the proposition is true. ■

Explorations and Activities

14. Proof of the Triangle Inequality.

(**a**) Verify that the triangle inequality is true for several different real numbers x and y. Be sure to have some examples where the real numbers are negative.

(**b**) Explain why the following proposition is true: For each real number r, $-|r| \leq r \leq |r|$.

(**c**) Now let x and y be real numbers. Apply the result in Part (14b) to both x and y. Then add the corresponding parts of the two inequalities to obtain another inequality. Use this to prove that $|x + y| \leq |x| + |y|$.

3.5 The Division Algorithm and Congruence

Beginning Activity 1 (Quotients and Remainders)

1. Let $a = 27$ and $b = 4$. We will now determine several pairs of integers q and r so that $27 = 4q + r$. For example, if $q = 2$ and $r = 19$, we obtain $4 \cdot 2 + 19 = 27$. The following table is set up for various values of q. For each q, determine the value of r so that $4q + r = 27$.

q	1	2	3	4	5	6	7	8	9	10
r		19						-5		
$4q + r$	27	27	27	27	27	27	27	27	27	27

2. What is the smallest positive value for r that you obtained in your examples from Part (1)?

Division is not considered an operation on the set of integers since the quotient of two integers need not be an integer. However, we have all divided one integer by another and obtained a quotient and a remainder. For example, if we divide 113 by 5, we obtain a quotient of 22 and a remainder of 3. We can write this as $\frac{113}{5} = 22 + \frac{3}{5}$. If we multiply both sides of this equation by 5 and then use the

distributive property to "clear the parentheses," we obtain

$$5 \cdot \frac{113}{5} = 5\left(22 + \frac{3}{5}\right)$$
$$113 = 5 \cdot 22 + 3$$

This is the equation that we use when working in the integers since it involves only multiplication and addition of integers.

3. What are the quotient and the remainder when we divide 27 by 4? How is this related to your answer for Part (2)?

4. Repeat part (1) using $a = -17$ and $b = 5$. So the object is to find integers q and r so that $-17 = 5q + r$. Do this by completing the following table.

q	-7	-6	-5	-4	-3	-2	-1
r	18					-7	
$5q + r$	-17	-17	-17	-17	-17	-17	-17

5. The convention we will follow is that the remainder will be the smallest positive integer r for which $-17 = 5q + r$ and the quotient will be the corresponding value of q. Using this convention, what is the quotient and what is the remainder when -17 is divided by 5?

Beginning Activity 2 (Some Work with Congruence Modulo *n*)

1. Let n be a natural number and let a and b be integers.

(**a**) Write the definition of "a is congruent to b modulo n," which is written $a \equiv b \pmod{n}$.

(**b**) Use the definition of "divides" to complete the following:

When we write $a \equiv b \pmod{n}$, we may conclude that there exists an integer k such that ....

We will now explore what happens when we multiply several pairs of integers where the first one is congruent to 3 modulo 6 and the second is congruent to 5 modulo 6. We can use set builder notation and the roster method to specify the set A of all integers that are congruent to 3 modulo 6 as follows:

$$A = \{a \in \mathbb{Z} \mid a \equiv 3 \pmod{6}\} = \{\ldots, -15, -9, -3, 3, 9, 15, 21, \ldots\}.$$

2. Use the roster method to specify the set B of all integers that are congruent to 5 modulo 6.

$$B = \{b \in \mathbb{Z} \mid b \equiv 5 \pmod 6\} = \cdots \qquad .$$

Notice that $15 \in A$ and $11 \in B$ and that $15 + 11 = 26$. Also notice that $26 \equiv 2 \pmod 6$ and that 2 is the smallest positive integer that is congruent to 26 (mod 6).

3. Now choose at least four other pairs of integers a and b where $a \in A$ and $b \in B$. For each pair, calculate $(a + b)$ and then determine the smallest positive integer r for which $(a + b) \equiv r \pmod 6$. **Note**: The integer r will satisfy the inequalities $0 \leq r < 6$.

4. Prove that for all integers a and b, if $a \equiv 3 \pmod 6$ and $b \equiv 5 \pmod 6$, then $(a + b) \equiv 2 \pmod 6$.

The Division Algorithm

Beginning Activity 1 was an introduction to a mathematical result known as the Division Algorithm. One of the purposes of this beginning activity was to illustrate that we have already worked with this result, perhaps without knowing its name. For example, when we divide 337 by 6, we often write

$$\frac{337}{6} = 56 + \frac{1}{6}.$$

When we multiply both sides of this equation by 6, we get

$$337 = 6 \cdot 56 + 1.$$

When we are working within the system of integers, the second equation is preferred over the first since the second one uses only integers and the operations of addition and multiplication, and the integers are closed under addition and multiplication. Following is a complete statement of the Division Algorithm.

The Division Algorithm
For all integers a and b with $b > 0$, there exist unique integers q and r such that

$$a = bq + r \text{ and } 0 \leq r < b.$$

Some Comments about the Division Algorithm

1. The Division Algorithm can be proven, but we have not yet studied the methods that are usually used to do so. In this text, we will treat the Division Algorithm as an axiom of the integers. The work in Beginning Activity 1 provides some rationale that this is a reasonable axiom.

2. The statement of the Division Algorithm contains the new phrase, "there exist unique integers q and r such that ...." This means that there is only one pair of integers q and r that satisfy both the conditions $a = bq + r$ and $0 \leq r < b$. As we saw in Beginning Activity 1, there are several different ways to write the integer a in the form $a = bq + r$. However, there is only one way to do this and satisfy the additional condition that $0 \leq r < b$.

3. In light of the previous comment, when we speak of **the quotient** and **the remainder** when we "divide an integer a by the positive integer b," we will always mean the quotient (q) and the remainder (r) guaranteed by the Division Algorithm. So the remainder r is the least nonnegative integer such that there exists an integer (quotient) q with $a = bq + r$.

4. If $a < 0$, then we must be careful when writing the result of the Division Algorithm. For example, in parts (4) and (5) of Beginning Activity 1, with $a = -17$ and $b = 5$, we obtained $-17 = 5 \cdot (-4) + 3$, and so the quotient is -4 and the remainder is 3. Notice that this is different than the result from a calculator, which would be $\frac{-17}{5} = -3.4$. But this means

$$\frac{-17}{5} = -\left(3 + \frac{4}{10}\right) = -3 - \frac{2}{5}.$$

   If we multiply both sides of this equation by 5, we obtain

$$-17 = 5\,(-3) + (-2)\,.$$

   This is not the result guaranteed by the Division Algorithm since the value of -2 does not satisfy the result of being greater than or equal to 0 and less than 5.

5. One way to look at the Division Algorithm is that the integer a is either going to be a multiple of b, or it will lie between two multiples of b. Suppose that a is not a multiple of b and that it lies between the multiples $b \cdot q$ and $b\,(q + 1)$, where q is some integer. This is shown on the number line in Figure 3.2.

CC BY NC SA

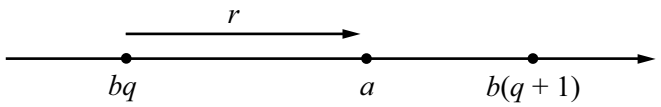

Figure 3.2: Remainder for the Division Algorithm

If r represents the distance from $b \cdot q$ to a, then

$$r = a - b \cdot q, \text{ or}$$
$$a = b \cdot q + r.$$

From the diagram, also notice that r is less than the distance between $b \cdot q$ and $b\,(q + 1)$. Algebraically, this distance is

$$\begin{aligned} b\,(q + 1) - b \cdot q &= b \cdot q + b - b \cdot q \\ &= b. \end{aligned}$$

Thus, in the case where a is not a multiple of b, we get $0 < r < b$.

6. We have been implicitly using the fact that an integer cannot be both even and odd. There are several ways to understand this fact, but one way is through the Division Algorithm. When we classify an integer as even or odd, we are doing so on the basis of the remainder (according to the Division Algorithm) when the integer is "divided" by 2. If $a \in \mathbb{Z}$, then by the Division Algorithm there exist unique integers q and r such that

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

This means that the remainder, r, can only be zero or one (and not both). When $r = 0$, the integer is even, and when $r = 1$, the integer is odd.

Progress Check 3.26 (Using the Division Algorithm)

1. What are the possible remainders (according to the Division Algorithm) when an integer is

(**a**) Divided by 4? (**b**) Divided by 9?

2. For each of the following, find the quotient and remainder (guaranteed by the Division Algorithm) and then summarize the results by writing an equation of the form $a = bq + r$, where $0 \leq r < b$.

CC BY NC SA

(**a**) When 17 is divided by 3.
(**b**) When -17 is divided by 3.
(**c**) When 73 is divided by 7.
(**d**) When -73 is divided by 7.
(**e**) When 436 is divided by 27.
(**f**) When 539 is divided by 110.

Using Cases Determined by the Division Algorithm

The Division Algorithm can sometimes be used to construct cases that can be used to prove a statement that is true for all integers. We have done this when we divided the integers into the even integers and the odd integers since even integers have a remainder of 0 when divided by 2 and odd integers have a remainder of 1 when divided by 2.

Sometimes it is more useful to divide the integer a by an integer other than 2. For example, if a is divided by 3, there are three possible remainders: 0, 1, and 2. If a is divided by 4, there are four possible remainders: 0, 1, 2, and 3. The remainders form the basis for the cases.

If the hypothesis of a proposition is that "n is an integer," then we can use the Division Algorithm to claim that there are unique integers q and r such that

$$n = 3q + r \text{ and } 0 \leq r < 3.$$

We can then divide the proof into the following three cases: (1) $r = 0$; (2) $r = 1$; and (3) $r = 2$. This is done in Proposition 3.27.

Proposition 3.27. *If n is an integer, then 3 divides $n^3 - n$.*

Proof. Let n be an integer. We will show that 3 divides $n^3 - n$ by examining the three cases for the remainder when n is divided by 3. By the Division Algorithm, there exist unique integers q and r such that

$$n = 3q + r, \text{ and } 0 \leq r < 3.$$

This means that we can consider the following three cases: (1) $r = 0$; (2) $r = 1$; and (3) $r = 2$.

In the case where $r = 0$, we have $n = 3q$. By substituting this into the expression $n^3 - n$, we get

$$\begin{aligned} n^3 - n &= (3q)^3 - (3q) \\ &= 27q^3 - 3q \\ &= 3\left(9q^3 - q\right). \end{aligned}$$

Since $\left(9q^3 - q\right)$ is an integer, the last equation proves that $3 \mid \left(n^3 - n\right)$.

In the second case, $r = 1$ and $n = 3q + 1$. When we substitute this into $\left(n^3 - n\right)$, we obtain

$$\begin{aligned} n^3 - n &= (3q+1)^3 - (3q+1) \\ &= \left(27q^3 + 27q^2 + 9q + 1\right) - (3q+1) \\ &= 27q^3 + 27q^2 + 6q \\ &= 3\left(9q^3 + 9q^2 + 2q\right). \end{aligned}$$

Since $\left(9q^3 + 9q^2 + 2q\right)$ is an integer, the last equation proves that $3 \mid \left(n^3 - n\right)$.

The last case is when $r = 2$. The details for this case are part of Exercise (1). Once this case is completed, we will have proved that 3 divides $n^3 - n$ in all three cases. Hence, we may conclude that if n is an integer, then 3 divides $n^3 - n$. ■

Properties of Congruence

Most of the work we have done so far has involved using definitions to help prove results. We will continue to prove some results but we will now prove some theorems about congruence (Theorem 3.28 and Theorem 3.30) that we will then use to help prove other results.

Let $n \in \mathbb{N}$. Recall that if a and b are integers, then we say that a is congruent to b modulo n provided that n divides $a - b$, and we write $a \equiv b \pmod{n}$. (See Section 3.1.) We are now going to prove some properties of congruence that are direct consequences of the definition. One of these properties was suggested by the work in Beginning Activity 2 and is Part (1) of the next theorem.

Theorem 3.28 (Properties of Congruence Modulo *n*). *Let n be a natural number and let a, b, c, and d be integers. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then*

1. $(a + c) \equiv (b + d) \pmod{n}$.
2. $ac \equiv bd \pmod{n}$.
3. *For each $m \in \mathbb{N}$, $a^m \equiv b^m \pmod{n}$.*

Proof. We will prove Parts (2) and (3). The proof of Part (1) is Progress Check 3.29. Let n be a natural number and let a, b, c, and d be integers. Assume that $a \equiv b \pmod{n}$ and that $c \equiv d \pmod{n}$. This means that n divides $a - b$ and that

n divides $c - d$. Hence, there exist integers k and q such that $a - b = nk$ and $c - d = nq$. We can then write $a = b + nk$ and $c = d + nq$ and obtain

$$\begin{aligned} ac &= (b + nk)(d + nq) \\ &= bd + bnq + dnk + n^2kq \\ &= bd + n(bq + dk + nkq). \end{aligned}$$

By subtracting bd from both sides of the last equation, we see that

$$ac - bd = n(bq + dk + nkq).$$

Since $bq + dk + nkq$ is an integer, this proves that $n \mid (ac - bd)$, and hence we can conclude that $ac \equiv bd \pmod{n}$. This completes the proof of Part (2).

Part (2) basically means that if we have two congruences, we can multiply the corresponding sides of these congruences to obtain another congruence. We have assumed that $a \equiv b \pmod{n}$ and so we write this twice as follows:

$$\begin{aligned} &a \equiv b \pmod{n}, \quad \text{and} \\ &a \equiv b \pmod{n}. \end{aligned}$$

If we now use the result in Part (2) and multiply the corresponding sides of these two congruences, we obtain $a^2 \equiv b^2 \pmod{n}$. We can then use this congruence and the congruence $a \equiv b \pmod{n}$ and the result in Part (2) to conclude that

$$a^2 \cdot a \equiv b^2 \cdot b \pmod{n},$$

or that $a^3 \equiv b^3 \pmod{n}$. We can say that we can continue with this process to prove Part (3), but this is not considered to be a formal proof of this result. To construct a formal proof for this, we could use a proof by mathematical induction. This will be studied in Chapter 4. See Exercise (13) in Section 4.1. ■

Progress Check 3.29 (Proving Part (1) of Theorem 3.28)
Prove part (1) of Theorem 3.28.

Exercise (11) in Section 3.1 gave three important properties of congruence modulo n. Because of their importance, these properties are stated and proved in Theorem 3.30. Please remember that textbook proofs are usually written in final form of "reporting the news." Before reading these proofs, it might be instructive to first try to construct a know-show table for each proof.

Theorem 3.30 (Properties of Congruence Modulo n). *Let $n \in \mathbb{N}$, and let a, b, and c be integers.*

1. *For every integer a, $a \equiv a \pmod{n}$.*

   *This is called the **reflexive property** of congruence modulo n.*

2. *If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.*

   *This is called the **symmetric property** of congruence modulo n.*

3. *If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.*

   *This is called the **transitive property** of congruence modulo n.*

Proof. We will prove the reflexive property and the transitive property. The proof of the symmetric property is Exercise (3).

Let $n \in \mathbb{N}$, and let $a \in \mathbb{Z}$. We will show that $a \equiv a \pmod{n}$. Notice that

$$a - a = 0 = n \cdot 0.$$

This proves that n divides $(a - a)$ and hence, by the definition of congruence modulo n, we have proven that $a \equiv a \pmod{n}$.

To prove the transitive property, we let $n \in \mathbb{N}$, and let a, b, and c be integers. We assume that $a \equiv b \pmod{n}$ and that $b \equiv c \pmod{n}$. We will use the definition of congruence modulo n to prove that $a \equiv c \pmod{n}$. Since $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, we know that $n \mid (a - b)$ and $n \mid (b - c)$. Hence, there exist integers k and q such that

$$\begin{aligned} a - b &= nk \\ b - c &= nq. \end{aligned}$$

By adding the corresponding sides of these two equations, we obtain

$$(a - b) + (b - c) = nk + nq.$$

If we simplify the left side of the last equation and factor the right side, we get

$$a - c = n(k + q).$$

By the closure property of the integers, $(k + q) \in \mathbb{Z}$, and so this equation proves that $n \mid (a - c)$ and hence that $a \equiv c \pmod{n}$. This completes the proof of the transitive property of congruence modulo n. ■

CC BY NC SA

Using Cases Based on Congruence Modulo *n*

Notice that the set of all integers that are congruent to 2 modulo 7 is

$$\{n \in \mathbb{Z} \mid n \equiv 2 \pmod 7\} = \{\ldots, -19, -12, -5, 2, 9, 16, 23, \ldots\}.$$

If we divide any integer in this set by 7 and write the result according to the Division Algorithm, we will get a remainder of 2. For example,

$$\begin{aligned} 2 &= 7 \cdot 0 + 2 & \qquad -5 &= 7(-1) + 2 \\ 9 &= 7 \cdot 1 + 2 & -12 &= 7(-2) + 2 \\ 16 &= 7 \cdot 2 + 2 & -19 &= 7(-3) + 2 \\ 23 &= 7 \cdot 3 + 2. \end{aligned}$$

Is this a coincidence or is this always true? Let's look at the general case. For this, let n be a natural number and let $a \in \mathbb{Z}$. By the Division Algorithm, there exist unique integers q and r such that

$$a = nq + r \text{ and } 0 \leq r < n.$$

By subtracting r from both sides of the equation $a = nq + r$, we obtain

$$a - r = nq.$$

But this implies that $n \mid (a - r)$ and hence that $a \equiv r \pmod n$. We have proven the following result.

Theorem 3.31. *Let $n \in \mathbb{N}$ and let $a \in \mathbb{Z}$. If $a = nq + r$ and $0 \leq r < n$ for some integers q and r, then $a \equiv r \pmod n$.*

This theorem says that an integer is congruent (mod n) to its remainder when it is divided by n. Since this remainder is unique and since the only possible remainders for division by n are $0, 1, 2, \ldots, n-1$, we can state the following result.

Corollary 3.32. *If $n \in \mathbb{N}$, then each integer is congruent, modulo n, to precisely one of the integers $0, 1, 2, \ldots, n-1$. That is, for each integer a, there exists a unique integer r such that*

$$a \equiv r \pmod n \quad \text{and} \quad 0 \leq r < n.$$

Corollary 3.32 can be used to set up cases for an integer in a proof. If $n \in \mathbb{N}$ and $a \in \mathbb{Z}$, then we can consider n cases for a. The integer a could be congruent to

$0, 1, 2, \ldots,$ or $n-1$ modulo n. For example, if we assume that 5 does not divide an integer a, then we know a is not congruent to 0 modulo 5, and hence, that a must be congruent to 1, 2, 3, or 4 modulo 5. We can use these as 4 cases within a proof. For example, suppose we wish to determine the values of a^2 modulo 5 for integers that are not congruent to 0 modulo 5. We begin by squaring some integers that are not congruent to 0 modulo 5. We see that

$$\begin{array}{lll} 1^2 = 1 & \text{and} & 1 \equiv 1 \pmod 5 . \\ 3^2 = 9 & \text{and} & 9 \equiv 4 \pmod 5 . \\ 6^2 = 36 & \text{and} & 36 \equiv 1 \pmod 5 . \\ 8^2 = 64 & \text{and} & 64 \equiv 4 \pmod 5 . \\ 9^2 = 81 & \text{and} & 81 \equiv 1 \pmod 5 . \end{array}$$

These explorations indicate that the following proposition is true and we will now outline a method to prove it.

Proposition 3.33. *For each integer a, if $a \not\equiv 0 \pmod 5$, then $a^2 \equiv 1 \pmod 5$ or $a^2 \equiv 4 \pmod 5$.*

Proof. We will prove this proposition using cases for a based on congruence modulo 5. In doing so, we will use the results in Theorem 3.28 and Theorem 3.30. Because the hypothesis is $a \not\equiv 0 \pmod 5$, we can use four cases, which are: (1) $a \equiv 1 \pmod 5$, (2) $a \equiv 2 \pmod 5$, (3) $a \equiv 3 \pmod 5$, and (4) $a \equiv 4 \pmod 5$. Following are proofs for the first and fourth cases.

Case 1. ($a \equiv 1 \pmod 5$). In this case, we use Theorem 3.28 to conclude that

$$a^2 \equiv 1^2 \pmod 5 \quad \text{or} \quad a^2 \equiv 1 \pmod 5 .$$

This proves that if $a \equiv 1 \pmod 5$, then $a^2 \equiv 1 \pmod 5$.

Case 4. ($a \equiv 4 \pmod 5$). In this case, we use Theorem 3.28 to conclude that

$$a^2 \equiv 4^2 \pmod 5 \quad \text{or} \quad a^2 \equiv 16 \pmod 5 .$$

We also know that $16 \equiv 1 \pmod 5$. So we have $a^2 \equiv 16 \pmod 5$ and $16 \equiv 1 \pmod 5$, and we can now use the transitive property of congruence (Theorem 3.30) to conclude that $a^2 \equiv 1 \pmod 5$. This proves that if $a \equiv 4 \pmod 5$, then $a^2 \equiv 1 \pmod 5$.

Progress Check 3.34 (Using Properties of Congruence)
Complete a proof of Proposition 3.33 by completing proofs for the other two cases. **Note**: It is possible to prove Proposition 3.33 using only the definition of congruence instead of using the properties that we have proved about congruence. However, such a proof would involve a good deal of algebra. One of the advantages of using the properties is that it avoids the use of complicated algebra in which it is easy to make mistakes.

In the proof of Proposition 3.33, we used four cases. Sometimes it may seem a bit overwhelming when confronted with a proof that requires several cases. For example, if we want to prove something about some integers modulo 6, we may have to use six cases. However, there are sometimes additional assumptions (or conclusions) that can help reduce the number of cases that must be considered. This will be illustrated in the next progress check.

Progress Check 3.35 (Using Cases Modulo 6)
Suppose we want to determine the possible values for a^2 modulo 6 for odd integers that are not multiples of 3. Before beginning to use congruence arithmetic (as in the proof of Proposition 3.33) in each of the possible six cases, we can show that some of the cases are not possible under these assumptions. (In some sense, we use a short proof by contradiction for these cases.) So assume that a is an odd integer. Then:

- If $a \equiv 0 \pmod 6$, then there exists an integer k such that $a = 6k$. But then $a = 2(3k)$ and hence, a is even. Since we assumed that a is odd, this case is not possible.
- If $a \equiv 2 \pmod 6$, then there exists an integer k such that $a = 6k + 2$. But then $a = 2(3k + 1)$ and hence, a is even. Since we assumed that a is odd, this case is not possible.

1. Prove that if a is an odd integer, then a cannot be congruent to 4 modulo 6.
2. Prove that if a is an integer and 3 does not divide a, then a cannot be congruent to 3 modulo 6.
3. So if a is an odd integer that is not a multiple of 3, then a must be congruent to 1 or 5 modulo 6. Use these two cases to prove the following proposition:

Proposition 3.36. *For each integer a, if a is an odd integer that is not multiple of 3, then $a^2 \equiv 1 \pmod 6$.*

Exercises for Section 3.5

1. Complete the details for the proof of Case 3 of Proposition 3.27.

⋆ **2.** (**a**) Use cases based on congruence modulo 3 and properties of congruence to prove that for each integer n, $n^3 \equiv n \pmod 3$.

(**b**) Explain why the result in Part (a) proves that for each integer n, 3 divides $(n^3 - n)$. Compare this to the proof of the same result in Proposition 3.27.

⋆ **3.** Prove the symmetric property of congruence stated in Theorem 3.30.

⋆ **4.** Consider the following proposition: For each integer a, if 3 divides a^2, then 3 divides a.

(**a**) Write the contrapositive of this proposition.

(**b**) Prove the proposition by proving its contrapositive. **Hint**: Consider using cases based on the Division Algorithm using the remainder for "division by 3." There will be two cases.

⋆ **5.** (**a**) Let $n \in \mathbb{N}$ and let $a \in \mathbb{Z}$. Explain why n divides a if and only if $a \equiv 0 \pmod n$.

(**b**) Let $a \in \mathbb{Z}$. Explain why if $a \not\equiv 0 \pmod 3$, then $a \equiv 1 \pmod 3$ or $a \equiv 2 \pmod 3$.

(**c**) Is the following proposition true or false? Justify your conclusion.

For each $a \in \mathbb{Z}$, if $a \not\equiv 0 \pmod 3$, then $a^2 \equiv 1 \pmod 3$.

⋆ **6.** Prove the following proposition by proving its contrapositive. (**Hint**: Use case analysis. There are several cases.)

For all integers a and b, if $ab \equiv 0 \pmod 3$, then $a \equiv 0 \pmod 3$ or $b \equiv 0 \pmod 3$.

⋆ **7.** (**a**) Explain why the following proposition is equivalent to the proposition in Exercise (6).

For all integers a and b, if $3 \mid ab$, then $3 \mid a$ or $3 \mid b$.

(**b**) Prove that for each integer a, if 3 divides a^2, then 3 divides a.

8. ⋆ (**a**) Prove that the real number $\sqrt{3}$ is an irrational number. That is, prove that

If r is a positive real number such that $r^2 = 3$, then r is irrational.

(b) Prove that the real number $\sqrt{12}$ is an irrational number.

⋆ **9.** Prove that for each natural number n, $\sqrt{3n+2}$ is not a natural number.

10. Extending the idea in Exercise (1) of Section 3.4, we can represent three consecutive integers as m, $m+1$, and $m+2$, where m is an integer.

(a) Explain why we can also represent three consecutive integers as $k-1$, k, and $k+1$, where k is an integer.

⋆ **(b)** Explain why Proposition 3.27 proves that the product of any three consecutive integers is divisible by 3.

⋆ **(c)** Prove that the product of three consecutive integers is divisible by 6.

11. **(a)** Use the result in Proposition 3.33 to help prove that the integer $m = 5,344,580,232,468,953,153$ is not a perfect square. Recall that an integer n is a perfect square provided that there exists an integer k such that $n = k^2$. **Hint**: Use a proof by contradiction.

(b) Is the integer $n = 782,456,231,189,002,288,438$ a perfect square? Justify your conclusion.

12. **(a)** Use the result in Proposition 3.33 to help prove that for each integer a, if 5 divides a^2, then 5 divides a.

(b) Prove that the real number $\sqrt{5}$ is an irrational number.

13. **(a)** Prove that for each integer a, if $a \not\equiv 0 \pmod 7$, then $a^2 \not\equiv 0 \pmod 7$.

(b) Prove that for each integer a, if 7 divides a^2, then 7 divides a.

(c) Prove that the real number $\sqrt{7}$ is an irrational number.

14. **(a)** If an integer has a remainder of 6 when it is divided by 7, is it possible to determine the remainder of the square of that integer when it is divided by 7? If so, determine the remainder and prove that your answer is correct.

(b) If an integer has a remainder of 11 when it is divided by 12, is it possible to determine the remainder of the square of that integer when it is divided by 12? If so, determine the remainder and prove that your answer is correct.

(c) Let n be a natural number greater than 2. If an integer has a remainder of $n-1$ when it is divided by n, is it possible to determine the remainder of the square of that integer when it is divided by n? If so, determine the remainder and prove that your answer is correct.

cc BY NC SA

15. Let n be a natural number greater than 4 and let a be an integer that has a remainder of $n-2$ when it is divided by n. Make whatever conclusions you can about the remainder of a^2 when it is divided by n. Justify all conclusions.

16. Is the following proposition true or false? Justify your conclusion with a proof or a counterexample.

For each natural number n, if 3 does not divide $\left(n^2+2\right)$, then n is not a prime number or $n=3$.

17. (**a**) Is the following proposition true or false? Justify your conclusion with a counterexample or a proof.

For each integer n, if n is odd, then $n^2 \equiv 1 \pmod 8$.

(**b**) Compare this proposition to the proposition in Exercise (7) from Section 3.4. Are these two propositions equivalent? Explain.

(**c**) Is the following proposition true or false? Justify your conclusion with a counterexample or a proof.

For each integer n, if n is odd and n is not a multiple of 3, then $n^2 \equiv 1 \pmod{24}$.

18. Prove the following proposition:

For all integers a and b, if 3 divides $\left(a^2+b^2\right)$, then 3 divides a and 3 divides b.

19. Is the following proposition true or false? Justify your conclusion with a counterexample or a proof.

For each integer a, 3 divides a^3+23a.

20. Are the following statements true or false? Either prove the statement is true or provide a counterexample to show it is false.

(**a**) For all integers a and b, if $a \cdot b \equiv 0 \pmod 6$, then $a \equiv 0 \pmod 6$ or $b \equiv 0 \pmod 6$.

(**b**) For all integers a and b, if $a \cdot b \equiv 0 \pmod 8$, then $a \equiv 0 \pmod 8$ or $b \equiv 0 \pmod 8$.

(**c**) For all integers a and b, if $a \cdot b \equiv 1 \pmod 6$, then $a \equiv 1 \pmod 6$ or $b \equiv 1 \pmod 6$.

(**d**) For all integers a and b, if $ab \equiv 7 \pmod{12}$, then either $a \equiv 1 \pmod{12}$ or $a \equiv 7 \pmod{12}$.

21. (**a**) Determine several pairs of integers a and b such that $a \equiv b \pmod 5$. For each such pair, calculate $4a + b$, $3a + 2b$, and $7a + 3b$. Are each of the resulting integers congruent to 0 modulo 5?

(**b**) Prove or disprove the following proposition:

Let m and n be integers such that $(m + n) \equiv 0 \pmod 5$ and let $a, b \in \mathbb{Z}$. If $a \equiv b \pmod 5$, then $(ma + nb) \equiv 0 \pmod 5$.

22. Evaluation of proofs

See the instructions for Exercise (19) on page 100 from Section 3.1.

(**a**) **Proposition**. For all integers a and b, if $(a + 2b) \equiv 0 \pmod 3$, then $(2a + b) \equiv 0 \pmod 3$.

Proof. We assume $a, b \in \mathbb{Z}$ and $(a + 2b) \equiv 0 \pmod 3$. This means that 3 divides $a + 2b$ and, hence, there exists an integer m such that $a + 2b = 3m$. Hence, $a = 3m - 2b$. For $(2a + b) \equiv 0 \pmod 3$, there exists an integer x such that $2a + b = 3x$. Hence,

$$\begin{aligned} 2(3m - 2b) + b &= 3x \\ 6m - 3b &= 3x \\ 3(2m - b) &= 3x \\ 2m - b &= x. \end{aligned}$$

Since $(2m - b)$ is an integer, this proves that 3 divides $(2a + b)$ and hence, $(2a + b) \equiv 0 \pmod 3$. ■

(**b**) **Proposition**. For each integer m, 5 divides $\left(m^5 - m\right)$.

Proof. Let $m \in \mathbb{Z}$. We will prove that 5 divides $\left(m^5 - m\right)$ by proving that $\left(m^5 - m\right) \equiv 0 \pmod 5$. We will use cases.

For the first case, if $m \equiv 0 \pmod 5$, then $m^5 \equiv 0 \pmod 5$ and, hence, $\left(m^5 - m\right) \equiv 0 \pmod 5$.

For the second case, if $m \equiv 1 \pmod 5$, then $m^5 \equiv 1 \pmod 5$ and, hence, $\left(m^5 - m\right) \equiv (1 - 1) \pmod 5$, which means that $\left(m^5 - m\right) \equiv 0 \pmod 5$.

For the third case, if $m \equiv 2 \pmod 5$, then $m^5 \equiv 32 \pmod 5$ and, hence, $\left(m^5 - m\right) \equiv (32 - 2) \pmod 5$, which means that $\left(m^5 - m\right) \equiv 0 \pmod 5$. ■

CC BY NC SA

Explorations and Activities

23. Using a Contradiction to Prove a Case Is Not Possible. Explore the statements in Parts (a) and (b) by considering several examples where the hypothesis is true.

(**a**) If an integer a is divisible by both 4 and 6, then it divisible by 24.

(**b**) If an integer a is divisible by both 2 and 3, then it divisible by 6.

(**c**) What can you conclude from the examples in Part (a)?

(**d**) What can you conclude from the examples in Part (b)?

The proof of the following proposition based on Part (b) uses cases. In this proof, however, we use cases and a proof by contradiction to prove that a certain integer cannot be odd. Hence, it must be even. Complete the proof of the proposition.

Proposition. Let $a \in \mathbb{Z}$. If 2 divides a and 3 divides a, then 6 divides a.

Proof: Let $a \in \mathbb{Z}$ and assume that 2 divides a and 3 divides a. We will prove that 6 divides a. Since 3 divides a, there exists an integer n such that

$$a = 3n.$$

The integer n is either even or it is odd. We will show that it must be even by obtaining a contradiction if it assumed to be odd. So, assume that n is odd. (Now complete the proof.)

24. The Last Two Digits of a Large Integer.
Notice that $7,381,272 \equiv 72 \pmod{100}$ since $7,381,272 - 72 = 7,381,200$, which is divisible by 100. In general, if we start with an integer whose decimal representation has more than two digits and subtract the integer formed by the last two digits, the result will be an integer whose last two digits are 00. This result will be divisible by 100. Hence, any integer with more than 2 digits is congruent modulo 100 to the integer formed by its last two digits.

(**a**) Start by squaring both sides of the congruence $3^4 \equiv 81 \pmod{100}$ to prove that $3^8 \equiv 61 \pmod{100}$ and then prove that $3^{16} \equiv 21 \pmod{100}$. What does this tell you about the last two digits in the decimal representation of 3^{16}?

(**b**) Use the two congruences in Part (24a) and laws of exponents to determine r where $3^{20} \equiv r \pmod{100}$ and $r \in \mathbb{Z}$ with $0 \leq r < 100$. What does this tell you about the last two digits in the decimal representation of 3^{20}?

(**c**) Determine the last two digits in the decimal representation of 3^{400}.

(**d**) Determine the last two digits in the decimal representation of 4^{804}.
Hint: One way is to determine the "mod 100 values" for 4^2, 4^4, 4^8, 4^{16}, 4^{32}, 4^{64}, and so on. Then use these values and laws of exponents to determine r, where $4^{804} \equiv r \pmod{100}$ and $r \in \mathbb{Z}$ with $0 \leq r < 100$.

(**e**) Determine the last two digits in the decimal representation of 3^{3356}.

(**f**) Determine the last two digits in the decimal representation of 7^{403}.

3.6 Review of Proof Methods

This section is different from others in the text. It is meant primarily as a review of the proof methods studied in Chapter 3. So the first part of the section will be a description of some of the main proof techniques introduced in Chapter 3. The most important part of this section is the set of exercises since these exercises will provide an opportunity to use the proof techniques that we have studied so far.

We will now give descriptions of three of the most common methods used to prove a conditional statement.

Direct Proof of a Conditional Statement $(P \to Q)$

- **When is it indicated**? This type of proof is often used when the hypothesis and the conclusion are both stated in a "positive" manner. That is, no negations are evident in the hypothesis and conclusion.

- **Description of the process**. Assume that P is true and use this to conclude that Q is true. That is, we use the forward-backward method and work forward from P and backward from Q.

- **Why the process makes sense**. We know that the conditional statement $P \to Q$ is automatically true when the hypothesis is false. Therefore, because our goal is to prove that $P \to Q$ is true, there is nothing to do in the case that P is false. Consequently, we may assume that P is true. Then, in order for $P \to Q$ to be true, the conclusion Q must also be true. (When P is true, but Q is false, $P \to Q$ is false.) Thus, we must use our assumption that P is true to show that Q is also true.

Proof of a Conditional Statement $(P \rightarrow Q)$ Using the Contrapositive

- **When is it indicated**? This type of proof is often used when both the hypothesis and the conclusion are stated in the form of negations. This often works well if the conclusion contains the operator "or"; that is, if the conclusion is in the form of a disjunction. In this case, the negation will be a conjunction.

- **Description of the process**. We prove the logically equivalent statement $\neg Q \rightarrow \neg P$. The forward-backward method is used to prove $\neg Q \rightarrow \neg P$. That is, we work forward from $\neg Q$ and backward from $\neg P$.

- **Why the process makes sense**. When we prove $\neg Q \rightarrow \neg P$, we are also proving $P \rightarrow Q$ because these two statements are logically equivalent. When we prove the contrapositive of $P \rightarrow Q$, we are doing a direct proof of $\neg Q \rightarrow \neg P$. So we assume $\neg Q$ because, when doing a direct proof, we assume the hypothesis, and $\neg Q$ is the hypothesis of the contrapositive. We must show $\neg P$ because it is the conclusion of the contrapositive.

Proof of $(P \rightarrow Q)$ Using a Proof by Contradiction

- **When is it indicated**? This type of proof is often used when the conclusion is stated in the form of a negation, but the hypothesis is not. This often works well if the conclusion contains the operator "or"; that is, if the conclusion is in the form of a disjunction. In this case, the negation will be a conjunction.

- **Description of the process**. Assume P and $\neg Q$ and work forward from these two assumptions until a contradiction is obtained.

- **Why the process makes sense**. The statement $P \rightarrow Q$ is either true or false. In a proof by contradiction, we show that it is true by eliminating the only other possibility (that it is false). We show that $P \rightarrow Q$ cannot be false by assuming it is false and reaching a contradiction. Since we assume that $P \rightarrow Q$ is false, and the only way for a conditional statement to be false is for its hypothesis to be true and its conclusion to be false, we assume that P is true and that Q is false (or, equivalently, that $\neg Q$ is true). When we reach a contradiction, we know that our original assumption that $P \rightarrow Q$ is false is incorrect. Hence, $P \rightarrow Q$ cannot be false, and so it must be true.

Other Methods of Proof

The methods of proof that were just described are three of the most common types of proof. However, we have seen other methods of proof and these are described below.

Proofs that Use a Logical Equivalency

As was indicated in Section 3.2, we can sometimes use a logical equivalency to help prove a statement. For example, in order to prove a statement of the form

$$P \to (Q \vee R)\,, \tag{1}$$

it is sometimes possible to use the logical equivalency

$$[P \to (Q \vee R)] \equiv [(P \wedge \neg Q) \to R]\,.$$

We would then prove the statement

$$(P \wedge \neg Q) \to R. \tag{2}$$

Most often, this would use a direct proof for statement (2) but other methods could also be used. Because of the logical equivalency, by proving statement (2), we have also proven the statement (1).

Proofs that Use Cases

When we are trying to prove a proposition or a theorem, we often run into the problem that there does not seem to be enough information to proceed. In this situation, we will sometimes use cases to provide additional assumptions for the forward process of the proof. When this is done, the original proposition is divided into a number of separate cases that are proven independently of each other. The cases must be chosen so that they exhaust all possibilities for the hypothesis of the original proposition. This method of case analysis is justified by the logical equivalency

$$(P \vee Q) \to R \equiv (P \to R) \wedge (Q \to R)\,,$$

which was established in Beginning Activity 1 in Section 3.4.

Constructive Proof

This is a technique that is often used to prove a so-called **existence theorem.** The objective of an existence theorem is to prove that a certain mathematical object exists. That is, the goal is usually to prove a statement of the form

$$\text{There exists an } x \text{ such that } P(x).$$

For a constructive proof of such a proposition, we actually name, describe, or explain how to construct some object in the universe that makes $P(x)$ true.

Nonconstructive Proof

Another type of proof that is often used to prove an existence theorem is the so-called **nonconstructive proof.** For this type of proof, we make an argument that an object in the universal set that makes $P\ (x)$ true must exist but we never construct or name the object that makes $P\ (x)$ true.

Exercises for Section 3.6

1. Let h and k be real numbers and let r be a positive number. The equation for a circle whose center is at the point (h, k) and whose radius is r is

$$(x-h)^2 + (y-k)^2 = r^2.$$

We also know that if a and b are real numbers, then

- The point (a, b) is inside the circle if $(a-h)^2 + (b-k)^2 < r^2$.
- The point (a, b) is on the circle if $(a-h)^2 + (b-k)^2 = r^2$.
- The point (a, b) is outside the circle if $(a-h)^2 + (b-k)^2 > r^2$.

Prove that all points on or inside the circle whose equation is $(x-1)^2 + (y-2)^2 = 4$ are inside the circle whose equation is $x^2 + y^2 = 26$.

2. (Exercise (15), Section 3.1) Let r be a positive real number. The equation for a circle of radius r whose center is the origin is $x^2 + y^2 = r^2$.

(**a**) Use implicit differentiation to determine $\dfrac{dy}{dx}$.

(**b**) (Exercise (17), Section 3.2) Let (a, b) be a point on the circle with $a \neq 0$ and $b \neq 0$. Determine the slope of the line tangent to the circle at the point (a, b).

(**c**) Prove that the radius of the circle to the point (a, b) is perpendicular to the line tangent to the circle at the point (a, b). **Hint**: Two lines (neither of which is horizontal) are perpendicular if and only if the products of their slopes is equal to -1.

3. Are the following statements true or false? Justify your conclusions.

(**a**) For each integer a, if 3 does not divide a, then 3 divides $2a^2 + 1$.

(**b**) For each integer a, if 3 divides $2a^2 + 1$, then 3 does not divide a.

(**c**) For each integer a, 3 does not divide a if and only if 3 divides $2a^2 + 1$.

4. Prove that for each real number x and each irrational number q, $(x + q)$ is irrational or $(x - q)$ is irrational.

5. Prove that there exist irrational numbers u and v such that u^v is a rational number.

Hint: We have proved that $\sqrt{2}$ is irrational. For the real number $q = \sqrt{2}^{\sqrt{2}}$, either q is rational or q is irrational. Use this disjunction to set up two cases.

6. (Exercise (17), Section 3.2) Let a and b be natural numbers such that $a^2 = b^3$. Prove each of the propositions in Parts (6a) through (6d). (The results of Exercise (1) and Theorem 3.10 from Section 3.2 may be helpful.)

(**a**) If a is even, then 4 divides a.

(**b**) If 4 divides a, then 4 divides b.

(**c**) If 4 divides b, then 8 divides a.

(**d**) If a is even, then 8 divides a.

(**e**) Give an example of natural numbers a and b such that a is even and $a^2 = b^3$, but b is not divisible by 8.

7. (Exercise (18), Section 3.2) Prove the following proposition:

Let a and b be integers with $a \neq 0$. If a does not divide b, then the equation $ax^3 + bx + (b + a) = 0$ does not have a solution that is a natural number.

Hint: It may be necessary to factor a sum of cubes. Recall that

$$u^3 + v^3 = (u + v)\left(u^2 - uv + v^2\right).$$

8. Recall that a **Pythagorean triple** consists of three natural numbers a, b, and c such that $a < b < c$ and $a^2 + b^2 = c^2$. Are the following propositions true or false? Justify your conclusions.

(**a**) For all $a, b, c \in \mathbb{N}$ such that $a < b < c$, if a, b, and c form a Pythagorean triple, then 3 divides a or 3 divides b.

(**b**) For all $a, b, c \in \mathbb{N}$ such that $a < b < c$, if a, b, and c form a Pythagorean triple, then 5 divides a or 5 divides b or 5 divides c.

9. (**a**) Prove that there exists a Pythagorean triple a, b, and c, where $a = 5$ and b and c are consecutive natural numbers.

(**b**) Prove that there exists a Pythagorean triple a, b, and c, where $a = 7$ and b and c are consecutive natural numbers.

(**c**) Let m be an odd natural number that is greater than 1. Prove that there exists a Pythagorean triple a, b, and c, where $a = m$ and b and c are consecutive natural numbers.

10. One of the most famous unsolved problems in mathematics is a conjecture made by Christian Goldbach in a letter to Leonhard Euler in 1742. The conjecture made in this letter is now known as **Goldbach's Conjecture**. The conjecture is as follows:

> *Every even integer greater than 2 can be expressed as the sum of two (not necessarily distinct) prime numbers.*

Currently, it is not known if this conjecture is true or false.

(**a**) Write 50, 142, and 150 as a sum of two prime numbers.

(**b**) Prove the following:

> If Goldbach's Conjecture is true, then every integer greater than 5 can be written as a sum of three prime numbers.

(**c**) Prove the following:

> If Goldbach's Conjecture is true, then every odd integer greater than 7 can be written as a sum of three odd prime numbers.

11. Two prime numbers that differ by 2 are called **twin primes**. For example, 3 and 5 are twin primes, 5 and 7 are twin primes, and 11 and 13 are twin primes. Determine at least two other pairs of twin primes. Is the following proposition true or false? Justify your conclusion.

> For all natural numbers p and q if p and q are twin primes other than 3 and 5, then $pq + 1$ is a perfect square and 36 divides $pq + 1$.

12. Are the following statements true or false? Justify your conclusions.

(**a**) For all integers a and b, $(a+b)^2 \equiv \left(a^2+b^2\right) \pmod 2$.

(**b**) For all integers a and b, $(a+b)^3 \equiv \left(a^3+b^3\right) \pmod 3$.

(**c**) For all integers a and b, $(a+b)^4 \equiv \left(a^4+b^4\right) \pmod 4$.

(**d**) For all integers a and b, $(a+b)^5 \equiv \left(a^5+b^5\right) \pmod 5$.

If any of the statements above are false, write a new statement of the following form that is true (and prove that it is true):

For all integers a and b, $(a+b)^n \equiv (a^n + \text{ something } + b^n) \pmod n$.

13. Let a, b, c, and d be real numbers with $a \neq 0$ and let $f(x) = ax^3 + bx^2 + cx + d$.

(**a**) Determine the derivative and second derivative of the cubic function f.

(**b**) Prove that the cubic function f has at most two critical points and has exactly one inflection point.

Explorations and Activities

14. **A Special Case of Fermat's Last Theorem**. We have already seen examples of **Pythagorean triples**, which are natural numbers a, b, and c where $a^2 + b^2 = c^2$. For example, 3, 4, and 5 form a Pythagorean triple as do 5, 12, and 13. One of the famous mathematicians of the 17th century was Pierre de Fermat (1601 – 1665). Fermat made an assertion that for each natural number n with $n \geq 3$, there are no positive integers a, b, and c for which $a^n + b^n = c^n$. This assertion was discovered in a margin of one of Fermat's books after his death, but Fermat provided no proof. He did, however, state that he had discovered a truly remarkable proof but the margin did not contain enough room for the proof.

This assertion became known as **Fermat's Last Theorem** but it more properly should have been called Fermat's Last Conjecture. Despite the efforts of mathematicians, this "theorem" remained unproved until Andrew Wiles, a British mathematician, first announced a proof in June of 1993. However, it was soon recognized that this proof had a serious gap, but a widely accepted version of the proof was published by Wiles in 1995. Wiles' proof uses many concepts and techniques that were unknown at the time of Fermat. We

cc BY NC SA

cannot discuss the proof here, but we will explore and prove the following proposition, which is a (very) special case of Fermat's Last Theorem.

Proposition. There do not exist prime numbers a, b, and c such that $a^3 + b^3 = c^3$.

Although Fermat's Last Theorem implies this proposition is true, we will use a proof by contradiction to prove this proposition. For a proof by contradiction, we assume that

there exist prime numbers a, b, and c such that $a^3 + b^3 = c^3$.

Since 2 is the only even prime number, we will use the following cases: (1) $a = b = 2$; (2) a and b are both odd; and (3) one of a and b is odd and the other one is 2.

(**a**) Show that the case where $a = b = 2$ leads to a contradiction and hence, this case is not possible.

(**b**) Show that the case where a and b are both odd leads to a contradiction and hence, this case is not possible.

(**c**) We now know that one of a or b must be equal to 2. So we assume that $b = 2$ and that a is an odd prime. Substitute $b = 2$ into the equation $b^3 = c^3 - a^3$ and then factor the expression $c^3 - a^3$. Use this to obtain a contradiction.

(**d**) Write a complete proof of the proposition.

15. The purpose of this exploration is to investigate the possibilities for which integers cannot be the sum of the cubes of two or three integers.

(**a**) If x is an integer, what are the possible values (between 0 and 8, inclusive) for x^3 modulo 9?

(**b**) If x and y are integers, what are the possible values for $x^3 + y^3$ (between 0 and 8, inclusive) modulo 9?

(**c**) If k is an integer and $k \equiv 3 \pmod 9$, can k be equal to the sum of the cubes of two integers? Explain.

(**d**) If k is an integer and $k \equiv 4 \pmod 9$, can k be equal to the sum of the cubes of two integers? Explain.

(**e**) State and prove a theorem of the following form: For each integer k, if (conditions on k), then k cannot be written as the sum of the cubes of two integers. Be as complete with the conditions on k as possible based on the explorations in Part (b).

(**f**) If x, y, and z are integers, what are the possible values (between 0 and 8, inclusive) for $x^3 + y^3 + z^3$ modulo 9?

(**g**) If k is an integer and $k \equiv 4 \pmod 9$, can k be equal to the sum of the cubes of three integers? Explain.

(**h**) State and prove a theorem of the following form: For each integer k, if (conditions on k), then k cannot be written as the sum of the cubes of three integers. Be as complete with the conditions on k as possible based on the explorations in Part (f).

Note: Andrew Booker, a mathematician at the University of Bristol in the United Kingdom, recently discovered that 33 can be written as the sum of the cubes of three integers. Booker used a trio of 16-digit integers, two of which were negative. Following is a link to an article about this discovery.

http://gvsu.edu/s/10c

3.7 Chapter 3 Summary

Important Definitions

- Divides, divisor, page 82
- Factor, multiple, page 82
- Proof, page 85
- Undefined term, page 85
- Axiom, page 85
- Definition, page 86
- Conjecture, page 86
- Theorem, page 86
- Proposition, page 86
- Lemma, page 86
- Corollary, page 86
- Congruence modulo n, page 92
- Tautology, page 40
- Contradiction, page 40
- Absolute value, page 135

Important Theorems and Results about Even and Odd Integers

- **Exercise (1), Section 1.2**
  If m is an even integer, then $m + 1$ is an odd integer.
  If m is an odd integer, then $m + 1$ is an even integer.

- **Exercise (2), Section 1.2**
  If x is an even integer and y is an even integer, then $x + y$ is an even integer.
  If x is an even integer and y is an odd integer, then $x + y$ is an odd integer.
  If x is an odd integer and y is an odd integer, then $x + y$ is an even integer.

- **Exercise (3), Section 1.2**. *If x is an even integer and y is an integer, then $x \cdot y$ is an even integer.*

- **Theorem 1.8**. *If x is an odd integer and y is an odd integer, then $x \cdot y$ is an odd integer.*

- **Theorem 3.7**. *The integer n is an even integer if and only if n^2 is an even integer.*
  Beginning Activity 2 in Section 3.2. *The integer n is an odd integer if and only if n^2 is an odd integer.*

Important Theorems and Results about Divisors

- **Theorem 3.1**. *For all integers a, b, and c with $a \neq 0$, if $a \mid b$ and $b \mid c$, then $a \mid c$.*

- **Exercise (3), Section 3.1**. *For all integers a, b, and c with $a \neq 0$,*
  If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.
  If $a \mid b$ and $a \mid c$, then $a \mid (b - c)$.

- **Exercise (3a), Section 3.1**. *For all integers a, b, and c with $a \neq 0$, if $a \mid b$, then $a \mid (bc)$.*

- **Exercise (4), Section 3.1**. *For all nonzero integers a and b, if $a \mid b$ and $b \mid a$, then $a = \pm b$.*

The Division Algorithm

Let a and b be integers with $b > 0$. Then there exist unique integers q and r such that

$$a = bq + r \text{ and } 0 \leq r < b.$$

CC BY NC SA

Important Theorems and Results about Congruence

- **Theorem 3.28**. *Let $a, b, c \in \mathbb{Z}$ and let $n \in \mathbb{N}$. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then*

  $$(a + c) \equiv (b + d) \pmod{n}.$$

  $$ac \equiv bd \pmod{n}.$$

  For each $m \in \mathbb{N}$, $a^m \equiv b^m \pmod{n}$.

- **Theorem 3.30**. *For all integers a, b, and c,*

  Reflexive Property. $a \equiv a \pmod{n}$.
  Symmetric Property. *If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.*
  Transitive Property. *If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.*

- **Theorem 3.31**. *Let $a \in \mathbb{Z}$ and let $n \in \mathbb{N}$. If $a = nq + r$ and $0 \leq r < n$ for some integers q and r, then $a \equiv r \pmod{n}$.*

- **Corollary 3.32**. *Each integer is congruent, modulo n, to precisely one of the integers $0, 1, 2, \ldots, n - 1$. That is, for each integer a, there exists a unique integer r such that*

  $$a \equiv r \pmod{n} \quad \text{and} \quad 0 \leq r < n.$$

CC BY NC SA