Chapter 7

Equivalence Relations

7.1 Relations

Preview Activity 1 (**The United States of America**)
Recall from Section 5.4 that the **Cartesian product** of two sets A and B, written $A \times B$, is the set of all ordered pairs (a, b), where $a \in A$ and $b \in B$. That is, $A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}$.

Let A be the set of all states in the United States and let

$$R = \{(x, y) \in A \times A \mid x \text{ and } y \text{ have a land border in common}\}.$$

For example, since California and Oregon have a land border, we can say that (California, Oregon) $\in R$ and (Oregon, California) $\in R$. Also, since California and Michigan do not share a land border, (California, Michigan) $\notin R$ and (Michigan, California) $\notin R$.

1. Use the roster method to specify the elements in each of the following sets:

   (**a**) $B = \{y \in A \,|(\text{Michigan}, y) \in R\}$

   (**b**) $C = \{x \in A \,|(x, \text{Michigan}) \in R\}$

   (**c**) $D = \{y \in A \,|(\text{Wisconsin}, y) \in R\}$

2. Find two different examples of two ordered pairs, (x, y) and (y, z) such that $(x, y) \in R$, $(y, z) \in R$, but $(x, z) \notin R$, or explain why no such example exists. Based on this, is the following conditional statement true or false?

   For all $x, y, z \in A$, if $(x, y) \in R$ and $(y, z) \in R$, then $(x, z) \in R$.

3. Is the following conditional statement true or false? Explain.

$$\text{For all } x, y \in A, \text{ if } (x, y) \in R, \text{ then } (y, x) \in R.$$

Preview Activity 2 (The Solution Set of an Equation with Two Variables)
In Section 2.3, we introduced the concept of the **truth set of an open sentence with one variable**. This was defined to be the set of all elements in the universal set that can be substituted for the variable to make the open sentence a true proposition. Assume that x and y represent real numbers. Then the equation

$$4x^2 + y^2 = 16$$

is an open sentence with two variables. An element of the truth set of this open sentence (also called a solution of the equation) is an ordered pair (a, b) of real numbers so that when a is substituted for x and b is substituted for y, the predicate becomes a true statement (a true equation in this case). We can use set builder notation to describe the truth set S of this equation with two variables as follows:

$$S = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid 4x^2 + y^2 = 16\}.$$

When a set is a truth set of an open sentence that is an equation, we also call the set the **solution set** of the equation.

1. List four different elements of the set S.

2. The graph of the equation $4x^2 + y^2 = 16$ in the xy-coordinate plane is an ellipse. Draw the graph and explain why this graph is a representation of the truth set (solution set) of the equation $4x^2 + y^2 = 16$.

3. Describe each of the following sets as an interval of real numbers:

(**a**) $A = \{x \in \mathbb{R} \mid \text{ there exists a } y \in \mathbb{R} \text{ such that } 4x^2 + y^2 = 16\}$.

(**b**) $B = \{y \in \mathbb{R} \mid \text{ there exists an } x \in \mathbb{R} \text{ such that } 4x^2 + y^2 = 16\}$.

Introduction to Relations

In Section 6.1, we introduced the formal definition of a function from one set to another set. The notion of a function can be thought of as one way of relating the elements of one set with those of another set (or the same set). A function is a

special type of **relation** in the sense that each element of the first set, the domain, is "related" to exactly one element of the second set, the codomain.

This idea of relating the elements of one set to those of another set using ordered pairs is not restricted to functions. For example, we may say that one integer, a, is related to another integer, b, provided that a is congruent to b modulo 3. Notice that this relation of congruence modulo 3 provides a way of relating one integer to another integer. However, in this case, an integer a is related to more than one other integer. For example, since

$$5 \equiv 5 \pmod 3, \quad 5 \equiv 2 \pmod 3, \quad \text{and} \quad 5 \equiv -1 \pmod 3,$$

we can say that 5 is related to 5, 5 is related to 2, and 5 is related to -1. Notice that, as with functions, each relation of the form $a \equiv b \pmod 3$ involves two integers a and b and hence involves an ordered pair (a, b), which is an element of $\mathbb{Z} \times \mathbb{Z}$.

Definition. Let A and B be sets. A **relation R from the set A to the set B** is a subset of $A \times B$. That is, R is a collection of ordered pairs where the first coordinate of each ordered pair is an element of A, and the second coordinate of each ordered pair is an element of B.

A relation from the set A to the set A is called a **relation on the set A**. So a relation on the set A is a subset of $A \times A$.

In Section 6.1, we defined the domain and range of a function. We make similar definitions for a relation.

Definition. If R is a relation from the set A to the set B, then the subset of A consisting of all the first coordinates of the ordered pairs in R is called the **domain** of R. The subset of B consisting of all the second coordinates of the ordered pairs in R is called the **range** of R.

We use the notation $\text{dom}(R)$ for the domain of R and $\text{range}(R)$ for the range of R. So using set builder notation,

$$\text{dom}(R) = \{u \in A \mid (u, y) \in R \text{ for at least one } y \in B\}$$
$$\text{range}(R) = \{v \in B \mid (x, v) \in R \text{ for at least one } x \in A\}.$$

Example 7.1 (**Domain and Range**)
A relation was studied in each of the preview activities for this section. For Preview

Activity 2, the set $S = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid 4x^2 + y^2 = 16\}$ is a subset of $\mathbb{R} \times \mathbb{R}$ and, hence, S is a relation on $\mathbb{R}$. In Problem (3) of Preview Activity 2, we actually determined the domain and range of this relation.

$$\text{dom}(S) = A = \{x \in \mathbb{R} \mid \text{ there exists a } y \in \mathbb{R} \text{ such that } 4x^2 + y^2 = 16\}$$
$$\text{range}(S) = B = \{y \in \mathbb{R} \mid \text{ there exists an } x \in \mathbb{R} \text{ such that } 4x^2 + y^2 = 16\}$$

So from the results in Preview Activity 2, we can say that the domain of the relation S is the closed interval $[-2, 2]$ and the range of S is the closed interval $[-4, 4]$.

Progress Check 7.2 (Examples of Relations)

1. Let $T = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x^2 + y^2 = 64\}$.

(**a**) Explain why T is a relation on $\mathbb{R}$.

(**b**) Find all values of x such that $(x, 4) \in T$. Find all values of x such that $(x, 9) \in T$.

(**c**) What is the domain of the relation T? What is the range of T?

(**d**) Since T is a relation on $\mathbb{R}$, its elements can be graphed in the coordinate plane. Describe the graph of the relation T.

2. From Preview Activity 1, A is the set of all states in the United States, and

$$R = \{(x, y) \in A \times A \mid x \text{ and } y \text{ have a land border in common}\}.$$

(**a**) Explain why R is a relation on A.

(**b**) What is the domain of the relation R? What is the range of the relation R?

(**c**) Are the following statements true or false? Justify your conclusions.

i. For all $x, y \in A$, if $(x, y) \in R$, then $(y, x) \in R$.

ii. For all $x, y, z \in A$, if $(x, y) \in R$ and $(y, z) \in R$, then $(x, z) \in R$.

Some Standard Mathematical Relations

There are many different relations in mathematics. For example, two real numbers can be considered to be related if one number is less than the other number. We call this the "less than" relation on $\mathbb{R}$. If $x, y \in \mathbb{R}$ and x is less than y, we often write $x < y$. As a set of ordered pairs, this relation is $R_<$, where

$$R_< = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x < y\}.$$

With many mathematical relations, we do not write the relation as a set of ordered pairs even though, technically, it is a set of ordered pairs. Table 7.1 describes some standard mathematical relations.

Name	**Open Sentence**	**Relation as a Set of Ordered Pairs**
The "less than" relation on $\mathbb{R}$	$x < y$	$\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x < y\}$
The "equality" relation on $\mathbb{R}$	$x = y$	$\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x = y\}$
The "divides" relation on $\mathbb{Z}$	$m \mid n$	$\{(m, n) \in \mathbb{Z} \times \mathbb{Z} \mid m \text{ divides } n\}$
The "subset" relation on $\mathcal{P}(U)$	$S \subseteq T$	$\{(S, T) \in \mathcal{P}(U) \times \mathcal{P}(U) \mid S \subseteq T\}$
The "element of" relation from U to $\mathcal{P}(U)$	$x \in S$	$\{(x, S) \in U \times \mathcal{P}(U) \mid x \in S\}$
The "congruence modulo n" relation on $\mathbb{Z}$	$a \equiv b \pmod{n}$	$\{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a \equiv b \pmod{n}\}$

Table 7.1: Standard Mathematical Relations

Notation for Relations

The mathematical relations in Table 7.1 all used a relation symbol between the two elements that form the ordered pair in $A \times B$. For this reason, we often do the same thing for a general relation from the set A to the set B. So if R is a relation from A to B, and $x \in A$ and $y \in B$, we use the notation

$$\begin{array}{lll} x\,R\,y & \text{to mean} & (x, y) \in R; \text{ and} \\ x\,\not R\,y & \text{to mean} & (x, y) \notin R. \end{array}$$

In some cases, we will even use a generic relation symbol for defining a new relation or speaking about relations in a general context. Perhaps the most commonly used symbol is "$\sim$", read "tilde" or "squiggle" or "is related to." When we do this, we will write

$$x \sim y \quad \text{means the same thing as} \quad (x, y) \in R; \text{ and}$$
$$x \nsim y \quad \text{means the same thing as} \quad (x, y) \notin R.$$

Progress Check 7.3 (The Divides Relation)
Whenever we have spoken about one integer dividing another integer, we have worked with the "divides" relation on $\mathbb{Z}$. In particular, we can write

$$D = \{(m, n) \in \mathbb{Z} \times \mathbb{Z} \mid m \text{ divides } n\}.$$

In this case, we have a specific notation for "divides," and we write

$$m \mid n \quad \text{if and only if} \quad (m, n) \in D.$$

1. What is the domain of the "divides" relation? What is the range of the "divides" relation?

2. Are the following statements true or false? Explain.

   (**a**) For every nonzero integer a, $a \mid a$.

   (**b**) For all nonzero integers a and b, if $a \mid b$, then $b \mid a$.

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

Functions as Relations

If we have a function $f: A \to B$, we can generate a set of ordered pairs f that is a subset of $A \times B$ as follows:

$$f = \{(a, f(a)) \mid a \in A\} \quad \text{or} \quad f = \{(a, b) \in A \times B \mid b = f(a)\}.$$

This means that f is a relation from A to B. Since, $\text{dom}(f) = A$, we know that

(1) For every $a \in A$, there exists a $b \in B$ such that $(a, b) \in f$.

When $(a, b) \in f$, we write $b = f(a)$. In addition, to be a function, each input can produce only one output. In terms of ordered pairs, this means that there will never be two ordered pairs (a, b) and (a, c) in the function f, where $a \in A$, $b, c \in B$, and $b \neq c$. We can formulate this as a conditional statement as follows:

(2) For every $a \in A$ and every $b, c \in B$, if $(a, b) \in f$ and $(a, c) \in f$, then $b = c$.

This means that a function f from A to B is a relation from A to B that satisfies conditions (1) and (2). (See Theorem 6.22 in Section 6.5.) Not every relation, however, will be a function. For example, consider the relation T in Progress Check 7.2.

$$T = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x^2 + y^2 = 64\}$$

This relation fails condition (2) above since a counterexample comes from the facts that $(0, 8) \in T$ and $(0, -8) \in T$ and $8 \neq -8$.

Progress Check 7.4 (A Set of Ordered Pairs)
Let $F = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = x^2\}$. The set F can then be considered to be relation on $\mathbb{R}$ since it is a subset of $\mathbb{R} \times \mathbb{R}$.

1. List five different ordered pairs that are in the set F.
2. Use the roster method to specify the elements of each of the following the sets:

   (**a**) $A = \{x \in \mathbb{R} \mid (x, 4) \in F\}$ (**c**) $C = \{y \in \mathbb{R} \mid (5, y) \in F\}$

   (**b**) $B = \{x \in \mathbb{R} \mid (x, 10) \in F\}$ (**d**) $D = \{y \in \mathbb{R} \mid (-3, y) \in F\}$

3. Since each real number x produces only one value of y for which $y = x^2$, the set F can be used to define a function from the set $\mathbb{R}$ to $\mathbb{R}$. Draw a graph of this function.

Visual Representations of Relations

In Progress Check 7.4, we were able to draw a graph of a relation as a way to visualize the relation. In this case, the relation was a function from $\mathbb{R}$ to $\mathbb{R}$. In addition, in Progress Check 7.2, we were also able to use a graph to represent a relation. In this case, the graph of the relation $T = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x^2 + y^2 = 64\}$ is a circle of radius 8 whose center is at the origin.

When R is a relation from a subset of the real numbers $\mathbb{R}$ to a subset of $\mathbb{R}$, we can often use a graph to provide a visual representation of the relation. This is especially true if the relation is defined by an equation or even an inequality. For example, if

$$R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y \geq x^2\},$$

then we can use the following graph as a way to visualize the points in the plane that are also in this relation.

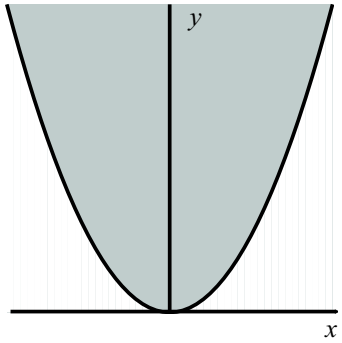


Figure 7.1: Graph of $y \geq x^2$

The points (x, y) in the relation R are the points on the graph of $y = x^2$ or are in the shaded region. This because for these points, $y \geq x^2$. One of the shortcomings of this type of graph is that the graph of the equation and the shaded region are actually unbounded and so we can never show the entire graph of this relation. However, it does allow us to see that the points in this relation are either on the parabola defined by the equation $y = x^2$ or are "inside" the parabola.

When the domain or range of a relation is infinite, we cannot provide a visualization of the entire relation. However, if A is a (small) finite set, a relation R on A can be specified by simply listing all the ordered pairs in R. For example, if $A = \{1, 2, 3, 4\}$, then

$$R = \{(1, 1), (4, 4), (1, 3), (3, 2), (1, 2), (2, 1)\}$$

is a relation on A. A convenient way to represent such a relation is to draw a point in the plane for each of the elements of A and then for each $(x, y) \in R$ (or $x\, R\, y$), we draw an arrow starting at the point x and pointing to the point y. If $(x, x) \in R$ (or $x\, R\, x$), we draw a loop at the point x. The resulting diagram is called a **directed graph** or a **digraph**. The diagram in Figure 7.2 is a digraph for the relation R.

In a directed graph, the points are called the **vertices**. So each element of A corresponds to a **vertex**. The arrows, including the loops, are called the **directed edges** of the directed graph. We will make use of these directed graphs in the next section when we study equivalence relations.

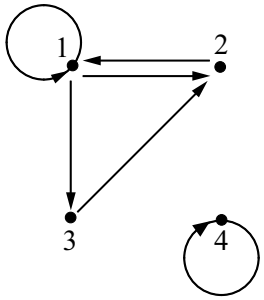


Figure 7.2: Directed Graph for a Relation

Progress Check 7.5 (**The Directed Graph of a Relation**)
Let $A = \{1, 2, 3, 4, 5, 6\}$. Draw a directed graph for the following two relations on the set A. For each relation, it may be helpful to arrange the vertices of A as shown in Figure 7.3.

$R = \{(x, y) \in A \times A \mid x \text{ divides } y\}$, $\quad T = \{(x, y) \in A \times A \mid x + y \text{ is even}\}$.

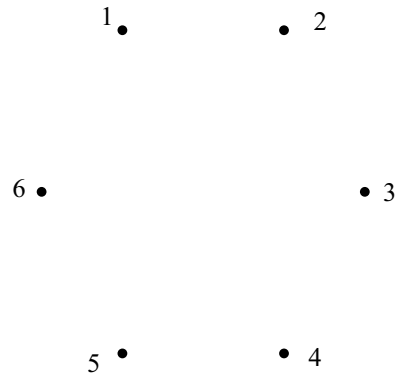


Figure 7.3: Vertices for A

Exercises 7.1

⋆ **1.** Let $A = \{a, b, c\}$, $B = \{p, q, r\}$, and let R be the set of ordered pairs defined by $R = \{(a, p), (b, q), (c, p), (a, q)\}$.

(**a**) Use the roster method to list all the elements of $A \times B$. Explain why $A \times B$ can be considered to be a relation from A to B.

(**b**) Explain why R is a relation from A to B.

(**c**) What is the domain of R? What is the range of R?

⋆ **2.** Let $A = \{a, b, c\}$ and let $R = \{(a, a), (a, c), (b, b), (b, c), (c, a), (c, b)\}$ (so R is a relation on A). Are the following statements true or false? Explain.

(**a**) For each $x \in A$, $x \, R \, x$.

(**b**) For every $x, y \in A$, if $x \, R \, y$, then $y \, R \, x$.

(**c**) For every $x, y, z \in A$, if $x \, R \, y$ and $y \, R \, z$, then $x \, R \, z$.

(**d**) R is a function from A to A.

3. Let A be the set of all female citizens of the United States. Let D be the relation on A defined by

$$D = \{(x, y) \in A \times A \mid x \text{ is a daughter of } y\}.$$

That is, $x \, D \, y$ means that x is a daughter of y.

⋆ **(a)** Describe those elements of A that are in the domain of D.

⋆ **(b)** Describe those elements of A that are in the range of D.

(c) Is the relation D a function from A to A? Explain.

⋆ **4.** Let U be a nonempty set, and let R be the "subset relation" on $\mathcal{P}(U)$. That is,

$$R = \{(S, T) \in \mathcal{P}(U) \times \mathcal{P}(U) \mid S \subseteq T\}.$$

(**a**) Write the open sentence $(S, T) \in R$ using standard subset notation.

(**b**) What is the domain of this subset relation, R?

(**c**) What is the range of this subset relation, R?

(**d**) Is R a function from $\mathcal{P}(U)$ to $\mathcal{P}(U)$? Explain.

5. Let U be a nonempty set, and let R be the "element of" relation from U to $\mathcal{P}(U)$. That is,

$$R = \{(x, S) \in U \times \mathcal{P}(U) \mid x \in S\}.$$

(**a**) What is the domain of this "element of" relation, R?

(**b**) What is the range of this "element of" relation, R?

(**c**) Is R a function from U to $\mathcal{P}(U)$? Explain.

⋆ **6.** Let $S = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x^2 + y^2 = 100\}$.

(**a**) Determine the set of all values of x such that $(x, 6) \in S$, and determine the set of all values of x such that $(x, 9) \in S$.

(**b**) Determine the domain and range of the relation S and write each set using set builder notation.

(**c**) Is the relation S a function from $\mathbb{R}$ to $\mathbb{R}$? Explain.

(**d**) Since S is a relation on $\mathbb{R}$, its elements can be graphed in the coordinate plane. Describe the graph of the relation S. Is the graph consistent with your answers in Exercises (6a) through (6c)? Explain.

7. Repeat Exercise (6) using the relation on $\mathbb{R}$ defined by

$$S = \left\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = \sqrt{100 - x^2}\right\}.$$

What is the connection between this relation and the relation in Exercise (6)?

8. Determine the domain and range of each of the following relations on $\mathbb{R}$ and sketch the graph of each relation.

(**a**) $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x^2 + y^2 = 10\}$

(**b**) $S = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y^2 = x + 10\}$

(**c**) $T = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid |x| + |y| = 10\}$

(**d**) $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x^2 = y^2\}$

9. Let R be the relation on $\mathbb{Z}$ where for all $a, b \in \mathbb{Z}$, $a\,R\,b$ if and only if $|a - b| \leq 2$.

⋆ (**a**) Use set builder notation to describe the relation R as a set of ordered pairs.

⋆ (**b**) Determine the domain and range of the relation R.

(**c**) Use the roster method to specify the set of all integers x such that $x\,R\,5$ and the set of all integers x such that $5\,R\,x$.

(**d**) If possible, find integers x and y such that $x\,R\,8$, $8\,R\,y$, but $x \not R\, y$.

(e) If $b \in \mathbb{Z}$, use the roster method to specify the set of all $x \in \mathbb{Z}$ such that $x \, R \, b$.

10. Let $R_< = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x < y\}$. This means that $R_<$ is the "less than" relation on $\mathbb{R}$.

(**a**) What is the domain of the relation $R_<$?

(**b**) What is the range of the relation $R_<$?

(**c**) Is the relation $R_<$ a function from $\mathbb{R}$ to $\mathbb{R}$? Explain.

Note: Remember that a relation is a set. Consequently, we can talk about one relation being a subset of another relation. Another thing to remember is that the elements of a relation are ordered pairs.

Explorations and Activities

11. The Inverse of a Relation. In Section 6.5, we introduced the **inverse of a function**. If A and B are nonempty sets and if $f : A \to B$ is a function, then the inverse of f, denoted by f^{-1}, is defined as

$$\begin{aligned} f^{-1} &= \{(b, a) \in B \times A \mid f(a) = b\} \\ &= \{(b, a) \in B \times A \mid (a, b) \in f\}. \end{aligned}$$

Now that we know about relations, we see that f^{-1} is always a relation from B to A. The concept of the inverse of a function is actually a special case of the more general concept of the inverse of a relation, which we now define.

Definition. Let R be a relation from the set A to the set B. The **inverse of R**, written R^{-1} and read "R inverse," is the relation from B to A defined by

$$\begin{aligned} R^{-1} &= \{(y, x) \in B \times A \mid (x, y) \in R\}, \text{ or} \\ R^{-1} &= \{(y, x) \in B \times A \mid x \, R \, y\}. \end{aligned}$$

That is, R^{-1} is the subset of $B \times A$ consisting of all ordered pairs (y, x) such that $x \, R \, y$.

For example, let D be the "divides" relation on $\mathbb{Z}$. See Progress Check 7.3. So

$$D = \{(m, n) \in \mathbb{Z} \times \mathbb{Z} \mid m \text{ divides } n\}.$$

This means that we can write $m \mid n$ if and only if $(m, n) \in D$. So, in this case,

$$\begin{aligned} D^{-1} &= \{(n, m) \in \mathbb{Z} \times \mathbb{Z} \mid (m, n) \in D\} \\ &= \{(n, m) \in \mathbb{Z} \times \mathbb{Z} \mid m \text{ divides } n\}. \end{aligned}$$

Now, if we would like to focus on the first coordinate instead of the second coordinate in D^{-1}, we know that "m divides n" means the same thing as "n is a multiple of m." Hence,

$$D^{-1} = \{(n, m) \in \mathbb{Z} \times \mathbb{Z} \mid n \text{ is a multiple of } m\}.$$

We can say that the inverse of the "divides" relation on $\mathbb{Z}$ is the "is a multiple of" relation on $\mathbb{Z}$.

Theorem 7.6, which follows, contains some elementary facts about inverse relations.

Theorem 7.6. *Let R be a relation from the set A to the set B. Then*

- *The domain of R^{-1} is the range of R. That is, $dom\left(R^{-1}\right) = range(R)$.*
- *The range of R^{-1} is the domain of R. That is, $range\left(R^{-1}\right) = dom(R)$.*
- *The inverse of R^{-1} is R. That is, $\left(R^{-1}\right)^{-1} = R$.*

To prove the first part of Theorem 7.6, observe that the goal is to prove that two sets are equal,

$$\text{dom}\left(R^{-1}\right) = \text{range}(R).$$

One way to do this is to prove that each is a subset of the other. To prove that $\text{dom}\left(R^{-1}\right) \subseteq \text{range}(R)$, we can start by choosing an arbitrary element of $\text{dom}\left(R^{-1}\right)$. So let $y \in \text{dom}\left(R^{-1}\right)$. The goal now is to prove that $y \in \text{range}(R)$. What does it mean to say that $y \in \text{dom}\left(R^{-1}\right)$? It means that there exists an $x \in A$ such that

$$(y, x) \in R^{-1}.$$

Now what does it mean to say that $(y, x) \in R^{-1}$? It means that $(x, y) \in R$. What does this tell us about y?

Complete the proof of the first part of Theorem 7.6. Then, complete the proofs of the other two parts of Theorem 7.6.

7.2 Equivalence Relations

Preview Activity 1 (Properties of Relations)
In previous mathematics courses, we have worked with the equality relation. For example, let R be the relation on $\mathbb{Z}$ defined as follows: For all $a, b \in \mathbb{Z}$, $a\,R\,b$ if and only if $a = b$. We know this equality relation on $\mathbb{Z}$ has the following properties:

- For each $a \in \mathbb{Z}$, $a = a$ and so $a\,R\,a$.
- For all $a, b \in \mathbb{Z}$, if $a = b$, then $b = a$. That is, if $a\,R\,b$, then $b\,R\,a$.
- For all $a, b, c \in \mathbb{Z}$, if $a = b$ and $b = c$, then $a = c$. That is, if $a\,R\,b$ and $b\,R\,c$, then $a\,R\,c$.

In mathematics, when something satisfies certain properties, we often ask if other things satisfy the same properties. Before investigating this, we will give names to these properties.

Definition. Let A be a nonempty set and let R be a relation on A.

- The relation R is **reflexive on A** provided that for each $x \in A$, $x\,R\,x$ or, equivalently, $(x, x) \in R$.
- The relation R is **symmetric** provided that for every $x, y \in A$, if $x\,R\,y$, then $y\,R\,x$ or, equivalently, for every $x, y \in A$, if $(x, y) \in R$, then $(y, x) \in R$.
- The relation R is **transitive** provided that for every $x, y, z \in A$, if $x\,R\,y$ and $y\,R\,z$, then $x\,R\,z$ or, equivalently, for every $x, y, z \in A$, if $(x, y) \in R$ and $(y, z) \in R$, then $(x, z) \in R$.

Before exploring examples, for each of these properties, it is a good idea to understand what it means to say that a relation does not satisfy the property. So let A be a nonempty set and let R be a relation on A.

1. Carefully explain what it means to say that the relation R is not reflexive on the set A.
2. Carefully explain what it means to say that the relation R is not symmetric.
3. Carefully explain what it means to say that the relation R is not transitive.

To illustrate these properties, we let $A = \{1, 2, 3, 4\}$ and define the relations R and T on A as follows:

$$R = \{(1, 1), (2, 2), (3, 3), (4, 4), (1, 3), (3, 2)\}$$
$$T = \{(1, 1), (1, 4), (2, 4), (4, 1), (4, 2)\}$$

4. Draw a directed graph for the relation R. Then explain why the relation R is reflexive on A, is not symmetric, and is not transitive.

5. Draw a directed graph for the relation T. Is the relation T reflexive on A? Is the relation T symmetric? Is the relation T transitive? Explain.

Preview Activity 2 (Review of Congruence Modulo *n*)

1. Let $a, b \in \mathbb{Z}$ and let $n \in \mathbb{N}$. On page 92 of Section 3.1, we defined what it means to say that a is congruent to b modulo n. Write this definition and state two different conditions that are equivalent to the definition.

2. Explain why congruence modulo n is a relation on $\mathbb{Z}$.

3. Carefully review Theorem 3.30 and the proofs given on page 148 of Section 3.5. In terms of the properties of relations introduced in Preview Activity 1, what does this theorem say about the relation of congruence modulo n on the integers?

4. Write a complete statement of Theorem 3.31 on page 150 and Corollary 3.32.

5. Write a proof of the symmetric property for congruence modulo n. That is, prove the following:

   Let $a, b \in \mathbb{Z}$ and let $n \in \mathbb{N}$. If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.

Directed Graphs and Properties of Relations

In Section 7.1, we used directed graphs, or digraphs, to represent relations on finite sets. Three properties of relations were introduced in Preview Activity 1 and will be repeated in the following descriptions of how these properties can be visualized on a directed graph.

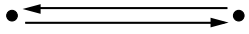
Let A be a nonempty set and let R be a relation on A.

- The relation R is **reflexive on A** provided that for each $x \in A$, $x \, R \, x$ or, equivalently, $(x, x) \in R$.

  This means that if a reflexive relation is represented on a digraph, there would have to be a loop at each vertex, as is shown in the following figure.

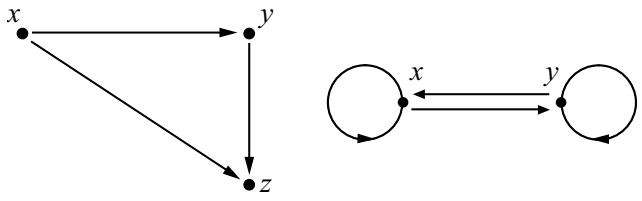
- The relation R is **symmetric** provided that for every $x, y \in A$, if $x \, R \, y$, then $y \, R \, x$ or, equivalently, for every $x, y \in A$, if $(x, y) \in R$, then $(y, x) \in R$.

  This means that if a symmetric relation is represented on a digraph, then anytime there is a directed edge from one vertex to a second vertex, there would be a directed edge from the second vertex to the first vertex, as is shown in the following figure.



- The relation R is **transitive** provided that for every $x, y, z \in A$, if $x \, R \, y$ and $y \, R \, z$, then $x \, R \, z$ or, equivalently, for every $x, y, z \in A$, if $(x, y) \in R$ and $(y, z) \in R$, then $(x, z) \in R$. So if a transitive relation is represented by a digraph, then anytime there is a directed edge from a vertex x to a vertex y and a directed edge from y to a vertex z, there would be a directed edge from x to z.

  In addition, if a transitive relation is represented by a digraph, then anytime there is a directed edge from a vertex x to a vertex y and a directed edge from y to the vertex x, there would be loops at x and y. These two situations are illustrated as follows:



Progress Check 7.7 (Properties of Relations)
Let $A = \{a, b, c, d\}$ and let R be the following relation on A:

$$R = \{(a, a), (b, b), (a, c), (c, a), (b, d), (d, b)\}.$$

Draw a directed graph for the relation R and then determine if the relation R is reflexive on A, if the relation R is symmetric, and if the relation R is transitive.

Definition of an Equivalence Relation

In mathematics, as in real life, it is often convenient to think of two different things as being essentially the same. For example, when you go to a store to buy a cold soft drink, the cans of soft drinks in the cooler are often sorted by brand and type of soft drink. The Coca Colas are grouped together, the Pepsi Colas are grouped together, the Dr. Peppers are grouped together, and so on. When we choose a particular can of one type of soft drink, we are assuming that all the cans are essentially the same. Even though the specific cans of one type of soft drink are physically different, it makes no difference which can we choose. In doing this, we are saying that the cans of one type of soft drink are equivalent, and we are using the mathematical notion of an equivalence relation.

An equivalence relation on a set is a relation with a certain combination of properties that allow us to sort the elements of the set into certain classes. In this section, we will focus on the properties that define an equivalence relation, and in the next section, we will see how these properties allow us to sort or partition the elements of the set into certain classes.

Definition. Let A be a nonempty set. A relation $\sim$ on the set A is an **equivalence relation** provided that $\sim$ is reflexive, symmetric, and transitive. For $a, b \in A$, if $\sim$ is an equivalence relation on A and $a \sim b$, we say that ***a* is equivalent to *b***.

Most of the examples we have studied so far have involved a relation on a small finite set. For these examples, it was convenient to use a directed graph to represent the relation. It is now time to look at some other type of examples, which may prove to be more interesting. In these examples, keep in mind that there is a subtle difference between the reflexive property and the other two properties. The reflexive property states that some ordered pairs actually belong to the relation R, or some elements of A are related. The reflexive property has a universal quantifier and, hence, we must prove that for all $x \in A$, $x\,R\,x$. Symmetry and transitivity, on

the other hand, are defined by conditional sentences. We often use a direct proof for these properties, and so we start by assuming the hypothesis and then showing that the conclusion must follow from the hypothesis.

Example 7.8 (**A Relation that Is Not an Equivalence Relation**)
Let M be the relation on $\mathbb{Z}$ defined as follows:

For $a, b \in \mathbb{Z}$, $a \, M \, b$ if and only if a is a multiple of b.

So $a \, M \, b$ if and only if there exists a $k \in \mathbb{Z}$ such that $a = bk$.

- The relation M is reflexive on $\mathbb{Z}$ since for each $x \in \mathbb{Z}$, $x = x \cdot 1$ and, hence, $x \, M \, x$.
- Notice that $4 \, M \, 2$, but $2 \not M \, 4$. So there exist integers x and y such that $x \, M \, y$ but $y \not M \, x$. Hence, the relation M is not symmetric.
- Now assume that $x \, M \, y$ and $y \, M \, z$. Then there exist integers p and q such that
$$x = yp \text{ and } y = zq.$$
Using the second equation to make a substitution in the first equation, we see that $x = z \, (pq)$. Since $pq \in \mathbb{Z}$, we have shown that x is a multiple of z and hence $x \, M \, z$. Therefore, M is a transitive relation.

The relation M is reflexive on $\mathbb{Z}$ and is transitive, but since M is not symmetric, it is not an equivalence relation on $\mathbb{Z}$.

Progress Check 7.9 (**A Relation that Is an Equivalence Relation**)
Define the relation $\sim$ on $\mathbb{Q}$ as follows: For all $a, b \in \mathbb{Q}$, $a \sim b$ if and only if $a - b \in \mathbb{Z}$. For example:

- $\frac{3}{4} \sim \frac{7}{4}$ since $\frac{3}{4} - \frac{7}{4} = -1$ and $-1 \in \mathbb{Z}$.
- $\frac{3}{4} \not\sim \frac{1}{2}$ since $\frac{3}{4} - \frac{1}{2} = \frac{1}{4}$ and $\frac{1}{4} \notin \mathbb{Z}$.

To prove that $\sim$ is reflexive on $\mathbb{Q}$, we note that for all $a \in \mathbb{Q}$, $a - a = 0$. Since $0 \in \mathbb{Z}$, we conclude that $a \sim a$. Now prove that the relation $\sim$ is symmetric and transitive, and hence, that $\sim$ is an equivalence relation on $\mathbb{Q}$.

Congruence Modulo *n*

One of the important equivalence relations we will study in detail is that of congruence modulo n. We reviewed this relation in Preview Activity 2.

Theorem 3.30 on page 148 tells us that congruence modulo n is an equivalence relation on $\mathbb{Z}$. Recall that by the Division Algorithm, if $a \in \mathbb{Z}$, then there exist unique integers q and r such that

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

Theorem 3.31 and Corollary 3.32 then tell us that $a \equiv r \pmod{n}$. That is, a is congruent modulo n to its remainder r when it is divided by n. When we use the term "remainder" in this context, we always mean the remainder r with $0 \leq r < n$ that is guaranteed by the Division Algorithm. We can use this idea to prove the following theorem.

Theorem 7.10. *Let $n \in \mathbb{N}$ and let $a, b \in \mathbb{Z}$. Then $a \equiv b \pmod{n}$ if and only if a and b have the same remainder when divided by n.*

Proof. Let $n \in \mathbb{N}$ and let $a, b \in \mathbb{Z}$. We will first prove that if a and b have the same remainder when divided by n, then $a \equiv b \pmod{n}$. So assume that a and b have the same remainder when divided by n, and let r be this common remainder. Then, by Theorem 3.31,

$$a \equiv r \pmod{n} \text{ and } b \equiv r \pmod{n}.$$

Since congruence modulo n is an equivalence relation, it is a symmetric relation. Hence, since $b \equiv r \pmod{n}$, we can conclude that $r \equiv b \pmod{n}$. Combining this with the fact that $a \equiv r \pmod{n}$, we now have

$$a \equiv r \pmod{n} \text{ and } r \equiv b \pmod{n}.$$

We can now use the transitive property to conclude that $a \equiv b \pmod{n}$. This proves that if a and b have the same remainder when divided by n, then $a \equiv b \pmod{n}$.

We will now prove that if $a \equiv b \pmod{n}$, then a and b have the same remainder when divided by n. Assume that $a \equiv b \pmod{n}$, and let r be the least nonnegative remainder when b is divided by n. Then $0 \leq r < n$ and, by Theorem 3.31,

$$b \equiv r \pmod{n}.$$

Now, using the facts that $a \equiv b \pmod{n}$ and $b \equiv r \pmod{n}$, we can use the transitive property to conclude that

$$a \equiv r \pmod{n}.$$

This means that there exists an integer q such that $a - r = nq$ or that

$$a = nq + r.$$

Since we already know that $0 \leq r < n$, the last equation tells us that r is the least nonnegative remainder when a is divided by n. Hence we have proven that if $a \equiv b \pmod{n}$, then a and b have the same remainder when divided by n. ■

Examples of Other Equivalence Relations

1. The relation $\sim$ on $\mathbb{Q}$ from Progress Check 7.9 is an equivalence relation.

2. Let A be a nonempty set. The **equality relation on A** is an equivalence relation. This relation is also called the **identity relation on A** and is denoted by I_A, where
$$I_A = \{(x, x) \mid x \in A\}.$$

3. Define the relation $\sim$ on $\mathbb{R}$ as follows:

   For $a, b \in \mathbb{R}$, $a \sim b$ if and only if there exists an integer k such that $a - b = 2k\pi$.

   We will prove that the relation $\sim$ is an equivalence relation on $\mathbb{R}$. The relation $\sim$ is reflexive on $\mathbb{R}$ since for each $a \in \mathbb{R}$, $a - a = 0 = 2 \cdot 0 \cdot \pi$.

   Now, let $a, b \in \mathbb{R}$ and assume that $a \sim b$. We will prove that $b \sim a$. Since $a \sim b$, there exists an integer k such that

   $$a - b = 2k\pi.$$

   By multiplying both sides of this equation by -1, we obtain

   $$\begin{aligned}(-1)(a - b) &= (-1)(2k\pi) \\ b - a &= 2(-k)\pi.\end{aligned}$$

   Since $-k \in \mathbb{Z}$, the last equation proves that $b \sim a$. Hence, we have proven that if $a \sim b$, then $b \sim a$ and, therefore, the relation $\sim$ is symmetric.

To prove transitivity, let $a, b, c \in \mathbb{R}$ and assume that $a \sim b$ and $b \sim c$. We will prove that $a \sim c$. Now, there exist integers k and n such that

$$a - b = 2k\pi \text{ and } b - c = 2n\pi.$$

By adding the corresponding sides of these two equations, we see that

$$\begin{aligned}(a - b) + (b - c) &= 2k\pi + 2n\pi \\ a - c &= 2(k + n)\pi.\end{aligned}$$

By the closure properties of the integers, $k + n \in \mathbb{Z}$. So this proves that $a \sim c$ and, hence the relation $\sim$ is transitive.

We have now proven that $\sim$ is an equivalence relation on $\mathbb{R}$. This equivalence relation is important in trigonometry. If $a \sim b$, then there exists an integer k such that $a - b = 2k\pi$ and, hence, $a = b + k(2\pi)$. Since the sine and cosine functions are periodic with a period of 2π, we see that

$$\begin{aligned}\sin a &= \sin(b + k(2\pi)) = \sin b, \text{ and} \\ \cos a &= \cos(b + k(2\pi)) = \cos b.\end{aligned}$$

Therefore, when $a \sim b$, each of the trigonometric functions have the same value at a and b.

4. For an example from Euclidean geometry, we define a relation P on the set $\mathcal{L}$ of all lines in the plane as follows:

For $l_1, l_2 \in \mathcal{L}$, $l_1 \, P \, l_2$ if and only if l_1 is parallel to l_2 or $l_1 = l_2$.

We added the second condition to the definition of P to ensure that P is reflexive on $\mathcal{L}$. Theorems from Euclidean geometry tell us that if l_1 is parallel to l_2, then l_2 is parallel to l_1, and if l_1 is parallel to l_2 and l_2 is parallel to l_3, then l_1 is parallel to l_3. (Drawing pictures will help visualize these properties.) This tells us that the relation P is reflexive, symmetric, and transitive and, hence, an equivalence relation on $\mathcal{L}$.

Progress Check 7.11 (Another Equivalence Relation)
Let U be a finite, nonempty set and let $\mathcal{P}(U)$ be the power set of U. Recall that $\mathcal{P}(U)$ consists of all subsets of U. (See page 222.) Define the relation $\approx$ on $\mathcal{P}(U)$ as follows:

$$\text{For } A, B \in \mathcal{P}(U), A \approx B \text{ if and only if } \text{card}(A) = \text{card}(B).$$

For the definition of the cardinality of a finite set, see page 223. This relation states that two subsets of U are equivalent provided that they have the same number of elements. Prove that $\approx$ is an equivalence relation on the power set $\mathcal{P}(U)$.

Exercises 7.2

⋆ **1.** Let $A = \{a, b\}$ and let $R = \{(a, b)\}$. Is R an equivalence relation on A? If not, is R reflexive, symmetric, or transitive? Justify all conclusions.

2. Let $A = \{a, b, c\}$. For each of the following, draw a directed graph that represents a relation with the specified properties.

(**a**) A relation on A that is symmetric but not transitive

(**b**) A relation on A that is transitive but not symmetric

(**c**) A relation on A that is symmetric and transitive but not reflexive on A

(**d**) A relation on A that is not reflexive on A, is not symmetric, and is not transitive

(**e**) A relation on A, other than the identity relation, that is an equivalence relation on A

⋆ **3.** Let $A = \{1, 2, 3, 4, 5\}$. The identity relation on A is

$$I_A = \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5)\}.$$

Determine an equivalence relation on A that is different from I_A or explain why this is not possible.

⋆ **4.** Let $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid |x| + |y| = 4\}$. Then R is a relation on $\mathbb{R}$. Is R an equivalence relation on $\mathbb{R}$? If not, is R reflexive, symmetric, or transitive? Justify all conclusions.

5. A relation R is defined on $\mathbb{Z}$ as follows: For all $a, b \in \mathbb{Z}$, $a\,R\,b$ if and only if $|a - b| \leq 3$. Is R an equivalence relation on $\mathbb{R}$? If not, is R reflexive, symmetric, or transitive? Justify all conclusions.

⋆ **6.** Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^2 - 4$ for each $x \in \mathbb{R}$. Define a relation $\sim$ on $\mathbb{R}$ as follows:

$$\text{For } a, b \in \mathbb{R}, a \sim b \text{ if and only if } f(a) = f(b).$$

(**a**) Is the relation $\sim$ an equivalence relation on $\mathbb{R}$? Justify your conclusion.

(**b**) Determine all real numbers in the set $C = \{x \in \mathbb{R} \mid x \sim 5\}$.

7. Repeat Exercise (6) using the function $f: \mathbb{R} \to \mathbb{R}$ that is defined by $f(x) = x^2 - 3x - 7$ for each $x \in \mathbb{R}$.

8. (**a**) Repeat Exercise (6a) using the function $f: \mathbb{R} \to \mathbb{R}$ that is defined by $f(x) = \sin x$ for each $x \in \mathbb{R}$.

(**b**) Determine all real numbers in the set $C = \{x \in \mathbb{R} \mid x \sim \pi\}$.

9. Define the relation $\sim$ on $\mathbb{Q}$ as follows: For $a, b \in \mathbb{Q}$, $a \sim b$ if and only if $a - b \in \mathbb{Z}$. In Progress Check 7.9, we showed that the relation $\sim$ is an equivalence relation on $\mathbb{Q}$.

(**a**) List four different elements of the set $C = \left\{x \in \mathbb{Q} \mid x \sim \frac{5}{7}\right\}$.

(**b**) Use set builder notation (without using the symbol $\sim$) to specify the set C.

(**c**) Use the roster method to specify the set C.

10. Let $\sim$ and $\approx$ be relations on $\mathbb{Z}$ defined as follows:

- For $a, b \in \mathbb{Z}$, $a \sim b$ if and only if 2 divides $a + b$.
- For $a, b \in \mathbb{Z}$, $a \approx b$ if and only if 3 divides $a + b$.

(**a**) Is $\sim$ an equivalence relation on $\mathbb{Z}$? If not, is this relation reflexive, symmetric, or transitive?

(**b**) Is $\approx$ an equivalence relation on $\mathbb{Z}$? If not, is this relation reflexive, symmetric, or transitive?

11. Let U be a finite, nonempty set and let $\mathcal{P}(U)$ be the power set of U. That is, $\mathcal{P}(U)$ is the set of all subsets of U. Define the relation $\sim$ on $\mathcal{P}(U)$ as follows: For $A, B \in \mathcal{P}(U)$, $A \sim B$ if and only if $A \cap B = \emptyset$. That is, the ordered pair (A, B) is in the relation $\sim$ if and only if A and B are disjoint.

Is the relation $\sim$ an equivalence relation on $\mathcal{P}(U)$? If not, is it reflexive, symmetric, or transitive? Justify all conclusions.

12. Let U be a nonempty set and let $\mathcal{P}(U)$ be the power set of U. That is, $\mathcal{P}(U)$ is the set of all subsets of U.

For A and B in $\mathcal{P}(U)$, define $A \sim B$ to mean that there exists a bijection $f : A \to B$. Prove that $\sim$ is an equivalence relation on $\mathcal{P}(U)$.

Hint: Use results from Sections 6.4 and 6.5.

13. Let $\sim$ and $\approx$ be relations on $\mathbb{Z}$ defined as follows:

- For $a, b \in \mathbb{Z}$, $a \sim b$ if and only if $2a + 3b \equiv 0 \pmod 5$.
- For $a, b \in \mathbb{Z}$, $a \approx b$ if and only if $a + 3b \equiv 0 \pmod 5$.

(**a**) Is $\sim$ an equivalence relation on $\mathbb{Z}$? If not, is this relation reflexive, symmetric, or transitive?

(**b**) Is $\approx$ an equivalence relation on $\mathbb{Z}$? If not, is this relation reflexive, symmetric, or transitive?

14. Let $\sim$ and $\approx$ be relations on $\mathbb{R}$ defined as follows:

- For $x, y \in \mathbb{R}$, $x \sim y$ if and only if $xy \geq 0$.
- For $x, y \in \mathbb{R}$, $x \approx y$ if and only if $xy \leq 0$.

(**a**) Is $\sim$ an equivalence relation on $\mathbb{R}$? If not, is this relation reflexive, symmetric, or transitive?

(**b**) Is $\approx$ an equivalence relation on $\mathbb{R}$? If not, is this relation reflexive, symmetric, or transitive?

15. Define the relation $\approx$ on $\mathbb{R} \times \mathbb{R}$ as follows: For $(a, b), (c, d) \in \mathbb{R} \times \mathbb{R}$, $(a, b) \approx (c, d)$ if and only if $a^2 + b^2 = c^2 + d^2$.

(**a**) Prove that $\approx$ is an equivalence relation on $\mathbb{R} \times \mathbb{R}$.

(**b**) List four different elements of the set

$$C = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid (x, y) \approx (4, 3)\}.$$

⋆ **(c)** Give a geometric description of the set C.

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

(**a**) **Proposition**. Let R be a relation on a set A. If R is symmetric and transitive, then R is reflexive.

Proof. Let $x, y \in A$. If $x \, R \, y$, then $y \, R \, x$ since R is symmetric. Now, $x \, R \, y$ and $y \, R \, x$, and since R is transitive, we can conclude that $x \, R \, x$. Therefore, R is reflexive. ■

(**b**) **Proposition**. Let $\sim$ be a relation on $\mathbb{Z}$ where for all $a, b \in \mathbb{Z}$, $a \sim b$ if and only if $(a + 2b) \equiv 0 \pmod 3$. The relation $\sim$ is an equivalence relation on $\mathbb{Z}$.

Proof. Assume $a \sim a$. Then $(a + 2a) \equiv 0 \pmod 3$ since $(3a) \equiv 0 \pmod 3$. Therefore, $\sim$ is reflexive on $\mathbb{Z}$. In addition, if $a \sim b$, then $(a + 2b) \equiv 0 \pmod 3$, and if we multiply both sides of this congruence by 2, we get

$$\begin{aligned} 2\,(a + 2b) &\equiv 2 \cdot 0 \pmod 3 \\ (2a + 4b) &\equiv 0 \pmod 3 \\ (2a + b) &\equiv 0 \pmod 3 \\ (b + 2a) &\equiv 0 \pmod 3\,. \end{aligned}$$

This means that $b \sim a$ and hence, $\sim$ is symmetric.

We now assume that $(a + 2b) \equiv 0 \pmod 3$ and $(b + 2c) \equiv 0 \pmod 3$. By adding the corresponding sides of these two congruences, we obtain

$$\begin{aligned} (a + 2b) + (b + 2c) &\equiv 0 + 0 \pmod 3 \\ (a + 3b + 2c) &\equiv 0 \pmod 3 \\ (a + 2c) &\equiv 0 \pmod 3\,. \end{aligned}$$

Hence, the relation $\sim$ is transitive and we have proved that $\sim$ is an equivalence relation on $\mathbb{Z}$. ■

Explorations and Activities

17. Other Types of Relations. In this section, we focused on the properties of a relation that are part of the definition of an equivalence relation. However, there are other properties of relations that are of importance. We will study two of these properties in this activity.

A relation R on a set A is a **circular relation** provided that for all x, y, and z in A, if $x\,R\,y$ and $y\,R\,z$, then $z\,R\,x$.

(**a**) Carefully explain what it means to say that a relation R on a set A is not circular.

(**b**) Let $A = \{1, 2, 3\}$. Draw a directed graph of a relation on A that is circular and draw a directed graph of a relation on A that is not circular.

(**c**) Let $A = \{1, 2, 3\}$. Draw a directed graph of a relation on A that is circular and not transitive and draw a directed graph of a relation on A that is transitive and not circular.

(**d**) Prove the following proposition:

A relation R on a set A is an equivalence relation if and only if it is reflexive and circular.

A relation R on a set A is an **antisymmetric relation** provided that for all $x, y \in A$, if $x\,R\,y$ and $y\,R\,x$, then $x = y$.

(**e**) Carefully explain what it means to say that a relation on a set A is not antisymmetric.

(**f**) Let $A = \{1, 2, 3\}$. Draw a directed graph of a relation on A that is antisymmetric and draw a directed graph of a relation on A that is not antisymmetric.

(**g**) Are the following propositions true or false? Justify all conclusions.

- If a relation R on a set A is both symmetric and antisymmetric, then R is transitive.
- If a relation R on a set A is both symmetric and antisymmetric, then R is reflexive.

7.3 Equivalence Classes

Preview Activity 1 (Sets Associated with a Relation)
As was indicated in Section 7.2, an equivalence relation on a set A is a relation with a certain combination of properties (reflexive, symmetric, and transitive) that allow us to sort the elements of the set into certain classes. This is done by means of certain subsets of A that are associated with the elements of the set A. This will be illustrated with the following example. Let $A = \{a, b, c, d, e\}$, and let R be the relation on the set A defined as follows:

$a\,R\,a$	$b\,R\,b$	$c\,R\,c$	$d\,R\,d$	$e\,R\,e$
$a\,R\,b$	$b\,R\,a$	$b\,R\,e$	$e\,R\,b$	
$a\,R\,e$	$e\,R\,a$	$c\,R\,d$	$d\,R\,c$	

For each $y \in A$, define the subset $R[y]$ of A as follows:

$$R[y] = \{x \in A \mid x\,R\,y\}\,.$$

That is, $R[y]$ consists of those elements in A such that $x\,R\,y$. For example, using $y = a$, we see that $a\,R\,a$, $b\,R\,a$, and $e\,R\,a$, and so $R[a] = \{a, b, e\}$.

1. Determine $R[b]$, $R[c]$, $R[d]$, and $R[e]$.

2. Draw a directed graph for the relation R and explain why R is an equivalence relation on A.

3. Which of the sets $R[a]$, $R[b]$, $R[c]$, $R[d]$, and $R[e]$ are equal?

4. Which of the sets $R[a]$, $R[b]$, $R[c]$, $R[d]$, and $R[e]$ are disjoint?

As we will see in this section, the relationships between these sets are typical for an equivalence relation. The following example will show how different this can be for a relation that is not an equivalence relation.

Let $A = \{a, b, c, d, e\}$, and let S be the relation on the set A defined as follows:

$b\,S\,b$	$c\,S\,c$	$d\,S\,d$	$e\,S\,e$
$a\,S\,b$	$a\,S\,d$	$b\,S\,c$	
$c\,S\,d$	$d\,S\,c$		

5. Draw a digraph that represents the relation S on A. Explain why S is not an equivalence relation on A.

For each $y \in A$, define the subset $S[y]$ of A as follows:

$$S[y] = \{x \in A \mid x\,S\,y\} = \{x \in A \mid (x, y) \in S\}.$$

For example, using $y = b$, we see that $S[b] = \{a, b\}$ since $(a, b) \in S$ and $(b, b) \in S$. In addition, we see that $S[a] = \emptyset$ since there is no $x \in A$ such that $(x, a) \in S$.

6. Determine $S[c]$, $S[d]$, and $S[e]$.

7. Which of the sets $S[a]$, $S[b]$, $S[c]$, $S[d]$, and $S[e]$ are equal?

8. Which of the sets $S[b]$, $S[c]$, $S[d]$, and $S[e]$ are disjoint?

Preview Activity 2 (Congruence Modulo 3)
An important equivalence relation that we have studied is congruence modulo n on the integers. We can also define subsets of the integers based on congruence modulo n. We will illustrate this with congruence modulo 3. For example, we can define $C[0]$ to be the set of all integers a that are congruent to 0 modulo 3. That is,

$$C[0] = \{a \in \mathbb{Z} \mid a \equiv 0 \pmod 3\}.$$

Since an integer a is congruent to 0 modulo 3 if and only if 3 divides a, we can use the roster method to specify this set as follows:

$$C[0] = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}.$$

1. Use the roster method to specify each of the following sets:

(**a**) The set $C[1]$ of all integers a that are congruent to 1 modulo 3. That is, $C[1] = \{a \in \mathbb{Z} \mid a \equiv 1 \pmod 3\}$.

(**b**) The set $C[2]$ of all integers a that are congruent to 2 modulo 3. That is, $C[2] = \{a \in \mathbb{Z} \mid a \equiv 2 \pmod 3\}$.

(**c**) The set $C[3]$ of all integers a that are congruent to 3 modulo 3. That is, $C[3] = \{a \in \mathbb{Z} \mid a \equiv 3 \pmod 3\}$.

2. Now consider the three sets, $C[0]$, $C[1]$, and $C[2]$.

(**a**) Determine the intersection of any two of these sets. That is, determine $C[0] \cap C[1]$, $C[0] \cap C[2]$, and $C[1] \cap C[2]$.

(**b**) Let $n = 734$. What is the remainder when n is divided by 3? Which of the three sets, if any, contains $n = 734$?

(**c**) Repeat Part (2b) for $n = 79$ and for $n = -79$.

(**d**) Do you think that $C[0] \cup C[1] \cup C[2] = \mathbb{Z}$? Explain.

(**e**) Is the set $C[3]$ equal to one of the sets $C[0]$, $C[1]$, or $C[2]$?

(**f**) We can also define $C[4] = \{a \in \mathbb{Z} \mid a \equiv 4 \pmod 3\}$. Is this set equal to any of the previous sets we have studied in this part? Explain.

The Definition of an Equivalence Class

We have indicated that an equivalence relation on a set is a relation with a certain combination of properties (reflexive, symmetric, and transitive) that allow us to sort the elements of the set into certain classes. We saw this happen in the preview activities. We can now illustrate specifically what this means. For example, in Preview Activity 2, we used the equivalence relation of congruence modulo 3 on $\mathbb{Z}$ to construct the following three sets:

$$C[0] = \{a \in \mathbb{Z} \mid a \equiv 0 \pmod 3\},$$
$$C[1] = \{a \in \mathbb{Z} \mid a \equiv 1 \pmod 3\}, \text{ and}$$
$$C[2] = \{a \in \mathbb{Z} \mid a \equiv 2 \pmod 3\}.$$

The main results that we want to use now are Theorem 3.31 and Corollary 3.32 on page 150. This corollary tells us that for any $a \in \mathbb{Z}$, a is congruent to precisely one of the integers 0, 1, or 2. Consequently, the integer a must be congruent to 0, 1, or 2, and it cannot be congruent to two of these numbers. Thus

1. For each $a \in \mathbb{Z}$, $a \in C[0]$, $a \in C[1]$, or $a \in C[2]$; and
2. $C[0] \cap C[1] = \emptyset$, $C[0] \cap C[2] = \emptyset$, and $C[1] \cap C[2] = \emptyset$.

This means that the relation of congruence modulo 3 sorts the integers into three distinct sets, or classes, and that each pair of these sets have no elements in common. So if we use a rectangle to represent $\mathbb{Z}$, we can divide that rectangle into three smaller rectangles, corresponding to $C[0]$, $C[1]$, and $C[2]$, and we might picture this situation as follows:

The Integers

$C[0]$ consisting of all integers with a remainder of 0 when divided by 3	$C[1]$ consisting of all integers with a remainder of 1 when divided by 3	$C[2]$ consisting of all integers with a remainder of 2 when divided by 3

Each integer is in exactly one of the three sets $C[0]$, $C[1]$, or $C[2]$, and two integers are congruent modulo 3 if and only if they are in the same set. We will see that, in a similar manner, if n is any natural number, then the relation of congruence modulo n can be used to sort the integers into n classes. We will also see that in general, if we have an equivalence relation R on a set A, we can sort the elements of the set A into classes in a similar manner.

Definition. Let $\sim$ be an equivalence relation on a nonempty set A. For each $a \in A$, the **equivalence class of *a*** determined by $\sim$ is the subset of A, denoted by $[a]$, consisting of all the elements of A that are equivalent to a. That is,

$$[a] = \{x \in A \mid x \sim a\}.$$

We read $[a]$ as "the equivalence class of a" or as "bracket a."

Notes

1. We use the notation $[a]$ when only one equivalence relation is being used. If there is more than one equivalence relation, then we need to distinguish between the equivalence classes for each relation. We often use something like $[a]_{\sim}$, or if R is the name of the relation, we can use $R[a]$ or $[a]_R$ for the equivalence class of a determined by R. In any case, always remember that when we are working with any equivalence relation on a set A if $a \in A$, then *the equivalence class* $[a]$ *is a subset of* A.

2. We know that each integer has an equivalence class for the equivalence relation of congruence modulo 3. But as we have seen, there are really only three *distinct* equivalence classes. Using the notation from the definition, they are:

$$[0] = \{a \in \mathbb{Z} \mid a \equiv 0 \pmod 3\}, \quad [1] = \{a \in \mathbb{Z} \mid a \equiv 1 \pmod 3\}, \text{ and}$$
$$[2] = \{a \in \mathbb{Z} \mid a \equiv 2 \pmod 3\}.$$

Progress Check 7.12 (**Equivalence Classes from Preview Activity 1**)
Without using the terminology at that time, we actually determined the equivalence classes of the equivalence relation R in Preview Activity 1. What are the distinct equivalence classes for this equivalence relation?

Congruence Modulo *n* and Congruence Classes

In Preview Activity 2, we used the notation $C[k]$ for the set of all integers that are congruent to k modulo 3. We could have used a similar notation for equivalence classes, and this would have been perfectly acceptable. However, the notation $[a]$ is probably the most common notation for the equivalence class of a. We will now use this same notation when dealing with congruence modulo n when only one congruence relation is under consideration.

Definition. Let $n \in \mathbb{N}$. Congruence modulo n is an equivalence relation on $\mathbb{Z}$. So for $a \in \mathbb{Z}$,

$$[a] = \{x \in \mathbb{Z} \mid x \equiv a \pmod{n}\}.$$

In this case, $[a]$ is called the **congruence class of *a* modulo *n***.

We have seen that congruence modulo 3 divides the integers into three distinct congruence classes. Each congruence class consists of those integers with the same remainder when divided by 3. In a similar manner, if we use congruence modulo 2, we simply divide the integers into two classes. One class will consist of all the integers that have a remainder of 0 when divided by 2, and the other class will consist of all the integers that have a remainder of 1 when divided by 2. That is, congruence modulo 2 simply divides the integers into the even and odd integers.

Progress Check 7.13 (**Congruence Modulo 4**)
Determine all of the distinct congruence classes for the equivalence relation of congruence modulo 4 on the integers. Specify each congruence class using the roster method.

Properties of Equivalence Classes

As we have seen, in Preview Activity 1, the relation R was an equivalence relation. For that activity, we used $R[y]$ to denote the equivalence class of $y \in A$, and we observed that these equivalence classes were either equal or disjoint.

However, in Preview Activity 1, the relation S was not an equivalence relation, and hence we do not use the term "equivalence class" for this relation. We should note, however, that the sets $S[y]$ were not equal and were not disjoint. This exhibits one of the main distinctions between equivalence relations and relations that are not equivalence relations.

In Theorem 7.14, we will prove that if $\sim$ is an equivalence relation on the set A, then we can "sort" the elements of A into distinct equivalence classes. The properties of equivalence classes that we will prove are as follows: (1) Every element of A is in its own equivalence class; (2) two elements are equivalent if and only if their equivalence classes are equal; and (3) two equivalence classes are either identical or they are disjoint.

Theorem 7.14. *Let A be a nonempty set and let $\sim$ be an equivalence relation on the set A. Then,*

1. *For each $a \in A$, $a \in [a]$.*

2. *For each $a, b \in A$, $a \sim b$ if and only if $[a] = [b]$.*

3. *For each $a, b \in A$, $[a] = [b]$ or $[a] \cap [b] = \emptyset$.*

Proof. Let A be a nonempty set and assume that $\sim$ is an equivalence relation on A. To prove the first part of the theorem, let $a \in A$. Since $\sim$ is an equivalence relation on A, it is reflexive on A. Thus, $a \sim a$, and we can conclude that $a \in [a]$.

The second part of this theorem is a biconditional statement. We will prove it by proving two conditional statements. We will first prove that if $a \sim b$, then $[a] = [b]$. So let $a, b \in A$ and assume that $a \sim b$. We will now prove that the two sets $[a]$ and $[b]$ are equal. We will do this by proving that each is a subset of the other.

First, assume that $x \in [a]$. Then, by definition, $x \sim a$. Since we have assumed that $a \sim b$, we can use the transitive property of $\sim$ to conclude that $x \sim b$, and this means that $x \in [b]$. This proves that $[a] \subseteq [b]$.

We now assume that $y \in [b]$. This means that $y \sim b$, and hence by the symmetric property, that $b \sim y$. Again, we are assuming that $a \sim b$. So we have

$$a \sim b \text{ and } b \sim y.$$

We use the transitive property to conclude that $a \sim y$ and then, using the symmetric property, we conclude that $y \sim a$. This proves that $y \in [a]$ and, hence, that $[b] \subseteq [a]$. This means that we can conclude that if $a \sim b$, then $[a] = [b]$.

We must now prove that if $[a] = [b]$, then $a \sim b$. Let $a, b \in A$ and assume that $[a] = [b]$. Using the first part of the theorem, we know that $a \in [a]$ and since the two sets are equal, this tells us that $a \in [b]$. Hence by the definition of $[b]$, we conclude that $a \sim b$. This completes the proof of the second part of the theorem.

For the third part of the theorem, let $a, b \in A$. Since this part of the theorem is a disjunction, we will consider two cases: Either

$$[a] \cap [b] = \emptyset \quad \text{or} \quad [a] \cap [b] \neq \emptyset.$$

In the case where $[a] \cap [b] = \emptyset$, the first part of the disjunction is true, and hence there is nothing to prove. So we assume that $[a] \cap [b] \neq \emptyset$ and will show that $[a] = [b]$. Since $[a] \cap [b] \neq \emptyset$, there is an element x in A such that

$$x \in [a] \cap [b].$$

This means that $x \in [a]$ and $x \in [b]$. Consequently, $x \sim a$ and $x \sim b$, and so we can use the second part of the theorem to conclude that $[x] = [a]$ and $[x] = [b]$. Hence, $[a] = [b]$, and we have proven that $[a] = [b]$ or $[a] \cap [b] = \emptyset$. ■

Theorem 7.14 gives the primary properties of equivalence classes. Consequences of these properties will be explored in the exercises. The following table restates the properties in Theorem 7.14 and gives a verbal description of each one.

Formal Statement from Theorem 7.14	**Verbal Description**
For each $a \in A$, $a \in [a]$.	Every element of A is in its own equivalence class.
For each $a, b \in A$, $a \sim b$ if and only if $[a] = [b]$.	Two elements of A are equivalent if and only if their equivalence classes are equal.
For each $a, b \in A$, $[a] = [b]$ or $[a] \cap [b] = \emptyset$.	Any two equivalence classes are either equal or they are disjoint. This means that if two equivalence classes are not disjoint then they must be equal.

Progress Check 7.15 (Equivalence Classes)
Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^2 - 4$ for each $x \in \mathbb{R}$. Define a relation $\sim$ on $\mathbb{R}$ as follows:

$$\text{For } a, b \in \mathbb{R}, a \sim b \text{ if and only if } f(a) = f(b).$$

In Exercise (6) of Section 7.2, we proved that $\sim$ is an equivalence relation on $\mathbb{R}$. Consequently, each real number has an equivalence class. For this equivalence relation,

1. Determine the equivalence classes of 5, -5, 10, -10, π, and $-\pi$.
2. Determine the equivalence class of 0.
3. If $a \in \mathbb{R}$, use the roster method to specify the elements of the equivalence class $[a]$.

The results of Theorem 7.14 are consistent with all the equivalence relations studied in the preview activities and in the progress checks. Since this theorem applies to all equivalence relations, it applies to the relation of congruence modulo n on the integers. Because of the importance of this equivalence relation, these results for congruence modulo n are given in the following corollary.

Corollary 7.16. *Let $n \in \mathbb{N}$. For each $a \in \mathbb{Z}$, let $[a]$ represent the congruence class of a modulo n.*

1. *For each $a \in \mathbb{Z}$, $a \in [a]$.*
2. *For each $a, b \in \mathbb{Z}$, $a \equiv b \pmod{n}$ if and only if $[a] = [b]$.*
3. *For each $a, b \in \mathbb{Z}$, $[a] = [b]$ or $[a] \cap [b] = \emptyset$.*

For the equivalence relation of congruence modulo n, Theorem 3.31 and Corollary 3.32 tell us that each integer is congruent to its remainder when divided by n, and that each integer is congruent modulo n to precisely one of one of the integers $0, 1, 2, \ldots, n-1$. This means that each integer is in precisely one of the congruence classes $[0]$, $[1]$, $[2]$, $\ldots$, $[n-1]$. Hence, Corollary 7.16 gives us the following result.

Corollary 7.17. *Let $n \in \mathbb{N}$. For each $a \in \mathbb{Z}$, let $[a]$ represent the congruence class of a modulo n.*

1. $\mathbb{Z} = [0] \cup [1] \cup [2] \cup \cdots \cup [n-1]$
2. *For $j, k \in \{0, 1, 2, \ldots, n-1\}$, if $j \neq k$, then $[j] \cap [k] = \emptyset$.*

Partitions and Equivalence Relations

A partition of a set A is a collection of subsets of A that "breaks up" the set A into disjoint subsets. Technically, each pair of distinct subsets in the collection must be disjoint. We then say that the collection of subsets is **pairwise disjoint**. We introduce the following formal definition.

Definition. Let A be a nonempty set, and let $\mathcal{C}$ be a collection of subsets of A. The collection of subsets $\mathcal{C}$ is a **partition of A** provided that

1. For each $V \in \mathcal{C}$, $V \neq \emptyset$.
2. For each $x \in A$, there exists a $V \in \mathcal{C}$ such that $x \in V$.
3. For every $V, W \in \mathcal{C}$, $V = W$ or $V \cap W = \emptyset$.

There is a close relation between partitions and equivalence classes since the equivalence classes of an equivalence relation form a partition of the underlying set, as will be proven in Theorem 7.18. The proof of this theorem relies on the results in Theorem 7.14.

Theorem 7.18. *Let $\sim$ be an equivalence relation on the nonempty set A. Then the collection $\mathcal{C}$ of all equivalence classes determined by $\sim$ is a partition of the set A.*

Proof. Let $\sim$ be an equivalence relation on the nonempty set A, and let $\mathcal{C}$ be the collection of all equivalence classes determined by $\sim$. That is,

$$\mathcal{C} = \{[a] \mid a \in A\}.$$

We will use Theorem 7.14 to prove that $\mathcal{C}$ is a partition of A.

Part (1) of Theorem 7.14 states that for each $a \in A$, $a \in [a]$. In terms of the equivalence classes, this means that each equivalence class is nonempty since each element of A is in its own equivalence class. Consequently, $\mathcal{C}$, the collection of all equivalence classes determined by $\sim$, satisfies the first two conditions of the definition of a partition.

We must now show that the collection $\mathcal{C}$ of all equivalence classes determined by $\sim$ satisfies the third condition for being a partition. That is, we need to show that any two equivalence classes are either equal or are disjoint. However, this is exactly the result in Part (3) of Theorem 7.14.

Hence, we have proven that the collection $\mathcal{C}$ of all equivalence classes determined by $\sim$ is a partition of the set A. ■

Note: Theorem 7.18 has shown us that if $\sim$ is an equivalence relation on a nonempty set A, then the collection of the equivalence classes determined by $\sim$ form a partition of the set A.

This process can be reversed. This means that given a partition $\mathcal{C}$ of a nonempty set A, we can define an equivalence relation on A whose equivalence classes are precisely the subsets of A that form the partition. This will be explored in Exercise (12).

Exercises 7.3

⋆ **1.** Let $A = \{a, b, c, d, e\}$ and let $\sim$ be the relation on A that is represented by the directed graph in Figure 7.4.

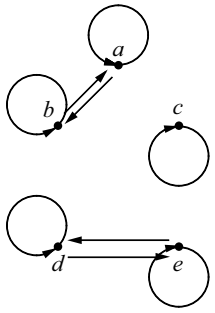


Figure 7.4: Directed Graph for the Relation in Exercise (1)

Prove that $\sim$ is an equivalence relation on the set A, and determine all of the equivalence classes determined by this equivalence relation.

⋆ **2.** Let $A = \{a, b, c, d, e, f\}$, and assume that $\sim$ is an equivalence relation on A. Also assume that it is known that

$$\begin{array}{lll} a \sim b & a \not\sim c & e \sim f \\ a \sim d & a \not\sim f & e \not\sim c. \end{array}$$

Draw a complete directed graph for the equivalence relation $\sim$ on the set A, and then determine all of the equivalence classes for this equivalence relation.

⋆ **3.** Let $A = \{0, 1, 2, 3, \ldots, 999, 1000\}$. Define the relation R on A as follows:

For $x, y \in A$, $x \, R \, y$ if and only if x and y have the same number of digits.

Prove that R is an equivalence relation on the set A and determine all of the distinct equivalence classes determined by R.

4. Determine all of the congruence classes for the relation of congruence modulo 5 on the set of integers.

5. Let $R_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$.

⋆ **(a)** Define the relation $\sim$ on R_9 as follows: For all $a, b \in R_9$, $a \sim b$ if and only if $a^2 \equiv b^2 \pmod 9$. Prove that $\sim$ is an equivalence relation on R_9 and determine all of the distinct equivalence classes of this equivalence relation.

(b) Define the relation $\approx$ on R_9 as follows: For all $a, b \in R_9$, $a \approx b$ if and only if $a^3 \equiv b^3 \pmod 9$. Prove that $\approx$ is an equivalence relation on R_9 and determine all of the distinct equivalence classes of this equivalence relation.

6. Define the relation $\sim$ on $\mathbb{Q}$ as follows: For $a, b \in \mathbb{Q}$, $a \sim b$ if and only if $a - b \in \mathbb{Z}$. In Progress Check 7.9 of Section 7.2, we showed that the relation $\sim$ is an equivalence relation on $\mathbb{Q}$. Also, see Exercise (9) in Section 7.2.

⋆ **(a)** Prove that $\left[\frac{5}{7}\right] = \left\{ m + \frac{5}{7} \middle| m \in \mathbb{Z} \right\}$.

(b) If $a \in \mathbb{Z}$, then what is the equivalence class of a?

(c) If $a \in \mathbb{Z}$, prove that there is a bijection from $[a]$ to $\left[\frac{5}{7}\right]$.

7. Define the relation $\sim$ on $\mathbb{R}$ as follows:

For $x, y \in \mathbb{R}$, $x \sim y$ if and only if $x - y \in \mathbb{Q}$.

(a) Prove that $\sim$ is an equivalence relation on $\mathbb{R}$.

(b) List four different real numbers that are in the equivalence class of $\sqrt{2}$.

(c) If $a \in \mathbb{Q}$, what is the equivalence class of a?

(d) Prove that $\left[\sqrt{2}\right] = \left\{ r + \sqrt{2} \mid r \in \mathbb{Q} \right\}$.

(e) If $a \in \mathbb{Q}$, prove that there is a bijection from $[a]$ to $\left[\sqrt{2}\right]$.

8. Define the relation $\sim$ on $\mathbb{Z}$ as follows: For $a, b \in \mathbb{Z}$, $a \sim b$ if and only if $2a + 3b \equiv 0 \pmod 5$. The relation $\sim$ is an equivalence relation on $\mathbb{Z}$. (See Exercise (13) in Section 7.2). Determine all the distinct equivalence classes for this equivalence relation.

9. Let $A = \mathbb{Z} \times (\mathbb{Z} - \{0\})$. That is, $A = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid b \neq 0\}$. Define the relation $\approx$ on A as follows:

For $(a, b), (c, d) \in A$, $(a, b) \approx (c, d)$ if and only if $ad = bc$.

⋆ **(a)** Prove that $\approx$ is an equivalence relation on A.

(b) Why was it necessary to include the restriction that $b \neq 0$ in the definition of the set A?

⋆ **(c)** Determine an equation that gives a relation between a and b if $(a, b) \in A$ and $(a, b) \approx (2, 3)$.

(d) Determine at least four different elements in $[(2,3)]$, the equivalence class of $(2,3)$.

(e) Use set builder notation to describe $[(2,3)]$, the equivalence class of $(2,3)$.

10. For $(a,b),(c,d) \in \mathbb{R} \times \mathbb{R}$, define $(a,b) \sim (c,d)$ if and only if $a^2 + b^2 = c^2 + d^2$. In Exercise (15) of Section 7.2, we proved that $\sim$ is an equivalence relation on $\mathbb{R} \times \mathbb{R}$.

(**a**) Determine the equivalence class of $(0,0)$.

(**b**) Use set builder notation (and do not use the symbol $\sim$) to describe the equivalence class of $(2,3)$ and then give a geometric description of this equivalence class.

(**c**) Give a geometric description of a typical equivalence class for this equivalence relation.

(**d**) Let $\mathbb{R}^* = \{x \in \mathbb{R} \mid x \geq 0\}$. Prove that there is a one-to-one correspondence (bijection) between $\mathbb{R}^*$ and the set of all equivalence classes for this equivalence relation.

11. Let A be a nonempty set and let $\sim$ be an equivalence relation on A. Prove each of the following:

(**a**) For each $a, b \in A$, $a \sim b$ if and only if $[a] \cap [b] = \emptyset$.

(**b**) For each $a, b \in A$, if $[a] \neq [b]$, then $[a] \cap [b] = \emptyset$.

(**c**) For each $a, b \in A$, if $[a] \cap [b] \neq \emptyset$ then $[a] = [b]$.

Explorations and Activities

12. A Partition Defines an Equivalence Relation. Let $A = \{a,b,c,d,e\}$ and let $\mathcal{C} = \{\{a,b,c\},\{d,e\}\}$.

(**a**) Explain why $\mathcal{C}$ is a partition of A.

Define a relation $\sim$ on A as follows: For $x, y \in A$, $x \sim y$ if and only if there exists a set U in $\mathcal{C}$ such that $x \in U$ and $y \in U$.

(**b**) Prove that $\sim$ is an equivalence relation on the set A, and then determine all the equivalence classes for $\sim$. How does the collection of all equivalence classes compare to $\mathcal{C}$?

What we did for the specific partition in Part (12b) can be done for any partition of a set. So to generalize Part (12b), we let A be a nonempty set and let $\mathcal{C}$ be a partition of A. We then define a relation $\sim$ on A as follows:

For $x, y \in A$, $x \sim y$ if and only if there exists a set U in $\mathcal{C}$ such that $x \in U$ and $y \in U$.

(**c**) Prove that $\sim$ is an equivalence relation on the set A.

(**d**) Let $a \in A$ and let $U \in \mathcal{C}$ such that $a \in U$. Prove that $[a] = U$.

13. Equivalence Relations on a Set of Matrices. The following exercises require a knowledge of elementary linear algebra. We let $\mathcal{M}_{n,n}(\mathbb{R})$ be the set of all n by n matrices with real number entries.

(**a**) Define a relation $\sim$ on $\mathcal{M}_{n,n}(\mathbb{R})$ as follows: For all $A, B \in \mathcal{M}_{n,n}(\mathbb{R})$, $A \sim B$ if and only if there exists an invertible matrix P in $\mathcal{M}_{n,n}(\mathbb{R})$ such that $B = PAP^{-1}$. Is $\sim$ an equivalence relation on $\mathcal{M}_{n,n}(\mathbb{R})$? Justify your conclusion.

(**b**) Define a relation R on $\mathcal{M}_{n,n}(\mathbb{R})$ as follows: For all $A, B \in \mathcal{M}_{n,n}(\mathbb{R})$, $A\,R\,B$ if and only if $\det(A) = \det(B)$. Is R an equivalence relation on $\mathcal{M}_{n,n}(\mathbb{R})$? Justify your conclusion.

(**c**) Let $\sim$ be an equivalence relation on $\mathbb{R}$. Define a relation $\approx$ on $\mathcal{M}_{n,n}(\mathbb{R})$ as follows: For all $A, B \in \mathcal{M}_{n,n}(\mathbb{R})$, $A \approx B$ if and only if $\det(A) \sim \det(B)$. Is $\approx$ an equivalence relation on $\mathcal{M}_{n,n}(\mathbb{R})$? Justify your conclusion.

7.4 Modular Arithmetic

Preview Activity 1 (Congruence Modulo 6)
For this activity, we will only use the relation of congruence modulo 6 on the set of integers.

1. Find five different integers a such that $a \equiv 3 \pmod 6$ and find five different integers b such that $b \equiv 4 \pmod 6$. That is, find five different integers in [3], the congruence class of 3 modulo 6 and five different integers in [4], the congruence class of 4 modulo 6.

2. Calculate $s = a + b$ using several values of a in [3] and several values of b in [4] from Part (1). For each sum s that is calculated, find r so that $0 \leq r < 6$ and $s \equiv r \pmod 6$. What do you observe?

3. Calculate $p = a \cdot b$ using several values of a in [3] and several values of b in [4] from Part (1). For each product p that is calculated, find r so that $0 \leq r < 6$ and $p \equiv r \pmod 6$. What do you observe?

4. Calculate $q = a^2$ using several values of a in [3] from Part (1). For each product q that is calculated, find r so that $0 \leq r < 6$ and $q \equiv r \pmod 6$. What do you observe?

Preview Activity 2 (The Remainder When Dividing by 9)

If a and b are integers with $b > 0$, then from the Division Algorithm, we know that there exist unique integers q and r such that

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

In this activity, we are interested in the remainder r. Notice that $r = a - bq$. So, given a and b, if we can calculate q, then we can calculate r.

We can use the "int" function on a calculator to calculate q. [The "int" function is the "greatest integer function." If x is a real number, then $\text{int}(x)$ is the greatest integer that is less than or equal to x.]

So, in the context of the Division Algorithm, $q = \text{int}\left(\frac{a}{b}\right)$. Consequently,

$$r = a - b \cdot \text{int}\left(\frac{a}{b}\right).$$

If n is a positive integer, we will let $s(n)$ denote the sum of the digits of n. For example, if $n = 731$, then

$$s(731) = 7 + 3 + 1 = 11.$$

For each of the following values of n, calculate

- The remainder when n is divided by 9, and
- The value of $s(n)$ and the remainder when $s(n)$ is divided by 9.

1. $n = 498$ **3.** $n = 4672$ **5.** $n = 51381$

2. $n = 7319$ **4.** $n = 9845$ **6.** $n = 305877$

What do you observe?

The Integers Modulo *n*

Let $n \in \mathbb{N}$. Since the relation of congruence modulo n is an equivalence relation on $\mathbb{Z}$, we can discuss its equivalence classes. Recall that in this situation, we refer to the equivalence classes as congruence classes.

Definition. Let $n \in \mathbb{N}$. The set of congruence classes for the relation of congruence modulo n on $\mathbb{Z}$ is the set of **integers modulo n**, or the set of integers mod n. We will denote this set of congruence classes by $\mathbb{Z}_n$.

Corollary 7.17 tells us that

$$\mathbb{Z} = [0] \cup [1] \cup [2] \cup \cdots \cup [n-1].$$

In addition, we know that each integer is congruent to precisely one of the integers $0, 1, 2, \ldots, n-1$. This tells us that one way to represent $\mathbb{Z}_n$ is

$$\mathbb{Z}_n = \{[0], [1], [2], \ldots, [n-1]\}.$$

Consequently, even though each integer has a congruence class, the set $\mathbb{Z}_n$ has only n distinct congruence classes.

The set of integers $\mathbb{Z}$ is more than a set. We can add and multiply integers. That is, there are the arithmetic operations of addition and multiplication on the set $\mathbb{Z}$, and we know that $\mathbb{Z}$ is closed with respect to these two operations.

One of the basic problems dealt with in modern algebra is to determine if the arithmetic operations on one set "transfer" to a related set. In this case, the related set is $\mathbb{Z}_n$. For example, in the integers modulo 5, $\mathbb{Z}_5$, is it possible to add the congruence classes [4] and [2] as follows?

$$\begin{aligned} [4] \oplus [2] &= [4+2] \\ &= [6] \\ &= [1]. \end{aligned}$$

We have used the symbol $\oplus$ to denote addition in $\mathbb{Z}_5$ so that we do not confuse it with addition in $\mathbb{Z}$. This looks simple enough, but there is a problem. The congruence classes [4] and [2] are not numbers, *they are infinite sets*. We have to make sure that we get the same answer no matter what element of [4] we use and no matter what element of [2] we use. For example,

$$\begin{aligned} 9 \equiv 4 \pmod 5 \quad &\text{and so} \quad [9] = [4]. \text{ Also,} \\ 7 \equiv 2 \pmod 5 \quad &\text{and so} \quad [7] = [2]. \end{aligned}$$

Do we get the same result if we add [9] and [7] in the way we did when we added [4] and [2]? The following computation confirms that we do:

$$\begin{aligned}[9] \oplus [7] &= [9 + 7] \\ &= [16] \\ &= [1].\end{aligned}$$

This is one of the ideas that was explored in Preview Activity 1. The main difference is that in this activity, we used the relation of congruence, and here we are using congruence classes. All of the examples in Preview Activity 1 should have illustrated the properties of congruence modulo 6 in the following table. The left side shows the properties in terms of the congruence relation and the right side shows the properties in terms of the congruence classes.

If $a \equiv 3 \pmod 6$ and $b \equiv 4 \pmod 6$, then • $(a + b) \equiv (3 + 4) \pmod 6$; • $(a \cdot b) \equiv (3 \cdot 4) \pmod 6$.	If $[a] = [3]$ and $[b] = [4]$ in $\mathbb{Z}_6$, then • $[a + b] = [3 + 4]$; • $[a \cdot b] = [3 \cdot 4]$.

These are illustrations of general properties that we have already proved in Theorem 3.28. We repeat the statement of the theorem here because it is so important for defining the operations of addition and multiplication in $\mathbb{Z}_n$.

Theorem 3.28. *Let n be a natural number and let a, b, c, and d be integers. Then*

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

Since $x \equiv y \pmod n$ if and only if $[x] = [y]$, we can restate the result of this Theorem 3.28 in terms of congruence classes in $\mathbb{Z}_n$.

Corollary 7.19. *Let n be a natural number and let a, b, c, and d be integers. Then, in $\mathbb{Z}_n$,*

1. *If* $[a] = [b]$ *and* $[c] = [d]$, *then* $[a + c] = [b + d]$.

2. *If* $[a] = [b]$ *and* $[c] = [d]$, *then* $[a \cdot c] = [b \cdot d]$.

3. *If* $[a] = [b]$ *and* $m \in \mathbb{N}$, *then* $[a^m] = [b^m]$.

Because of Corollary 7.19, we know that the following formal definition of addition and multiplication of congruence classes in $\mathbb{Z}_n$ is independent of the choice of the elements we choose from each class. We say that these definitions of addition and multiplication are **well defined**.

Definition. Let $n \in \mathbb{N}$. **Addition and multiplication** in $\mathbb{Z}_n$ are defined as follows: For $[a], [c] \in \mathbb{Z}_n$,

$$[a] \oplus [c] = [a + c] \text{ and } [a] \odot [c] = [ac].$$

The term **modular arithmetic** is used to refer to the operations of addition and multiplication of congruence classes in the integers modulo n.

So if $n \in \mathbb{N}$, then we have an addition and multiplication defined on $\mathbb{Z}_n$, the integers modulo n.

Always remember that for each of the equations in the definitions, the operations on the left, $\oplus$ and $\odot$, are the new operations that are being defined. The operations on the right side of the equations ($+$ and $\cdot$) are the known operations of addition and multiplication in $\mathbb{Z}$.

Since $\mathbb{Z}_n$ is a finite set, it is possible to construct addition and multiplication tables for $\mathbb{Z}_n$. In constructing these tables, we follow the convention that all sums and products should be in the form $[r]$, where $0 \leq r < n$. For example, in $\mathbb{Z}_3$, we see that by the definition, $[1] \oplus [2] = [3]$, but since $3 \equiv 0 \pmod 3$, we see that $[3] = [0]$ and so we write

$$[1] \oplus [2] = [3] = [0].$$

Similarly, by definition, $[2] \odot [2] = [4]$, and in $\mathbb{Z}_3$, $[4] = [1]$. So we write

$$[2] \odot [2] = [4] = [1].$$

The complete addition and multiplication tables for $\mathbb{Z}_3$ are

$\oplus$	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

$\odot$	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

Progress Check 7.20 (Modular Arithmetic in $\mathbb{Z}_2$, $\mathbb{Z}_5$, and $\mathbb{Z}_6$)

1. Construct addition and multiplication tables for $\mathbb{Z}_2$, the integers modulo 2.

2. Verify that the following addition and multiplication tables for $\mathbb{Z}_5$ are correct.

$\oplus$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

$\odot$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

3. Construct complete addition and multiplication tables for $\mathbb{Z}_6$.

4. In the integers, the following statement is true. We sometimes call this the zero product property for the integers.

   For all $a, b \in \mathbb{Z}$, if $a \cdot b = 0$, then $a = 0$ or $b = 0$.

   Write the contrapositive of the conditional statement in this property.

5. Are the following statements true or false? Justify your conclusions.

   (**a**) For all $[a], [b] \in \mathbb{Z}_5$, if $[a] \odot [b] = [0]$, then $[a] = [0]$ or $[b] = [0]$.

   (**b**) For all $[a], [b] \in \mathbb{Z}_6$, if $[a] \odot [b] = [0]$, then $[a] = [0]$ or $[b] = [0]$.

Divisibility Tests

Congruence arithmetic can be used to prove certain divisibility tests. For example, you may have learned that a natural number is divisible by 9 if the sum of its digits is divisible by 9. As an easy example, note that the sum of the digits of 5823 is equal to $5 + 8 + 2 + 3 = 18$, and we know that 18 is divisible by 9. It can also be verified that 5823 is divisible by 9. (The quotient is 647.) We can actually generalize this property by dealing with remainders when a natural number is divided by 9.

Let $n \in \mathbb{N}$ and let $s(n)$ denote the sum of the digits of n. For example, if $n = 7319$, then $s(7319) = 7 + 3 + 1 + 9 = 20$. In Preview Activity 2, we saw that

$$7319 \equiv 2 \pmod 9 \text{ and } 20 \equiv 2 \pmod 9.$$

In fact, for every example in Preview Activity 2, we saw that n and $s(n)$ were congruent modulo 9 since they both had the same remainder when divided by 9. The concepts of congruence and congruence classes can help prove that this is always true.

We will use the case of $n = 7319$ to illustrate the general process. We must use our standard place value system. By this, we mean that we will write 7319 as follows:

$$7319 = \left(7 \times 10^3\right) + \left(3 \times 10^2\right) + \left(1 \times 10^1\right) + \left(9 \times 10^0\right). \tag{1}$$

The idea is to now use the definition of addition and multiplication in $\mathbb{Z}_9$ to convert equation (1) to an equation in $\mathbb{Z}_9$. We do this as follows:

$$\begin{aligned}
[7319] &= [\left(7 \times 10^3\right) + \left(3 \times 10^2\right) + \left(1 \times 10^1\right) + \left(9 \times 10^0\right)] \\
&= [7 \times 10^3] \oplus [3 \times 10^2] \oplus [1 \times 10^1] \oplus [9 \times 10^0] \\
&= \left([7] \odot [10^3]\right) \oplus \left([3] \odot [10^2]\right) \oplus \left([1] \odot [10^1]\right) \oplus ([9] \odot [1]). \qquad (2)
\end{aligned}$$

Since $10^3 \equiv 1 \pmod 9$, $10^2 \equiv 1 \pmod 9$ and $10 \equiv 1 \pmod 9$, we can conclude that $[10^3] = [1]$, $[10^2] = [1]$ and $[10] = [1]$. Hence, we can use these facts and equation (2) to obtain

$$\begin{aligned}
[7319] &= \left([7] \odot [10^3]\right) \oplus \left([3] \odot [10^2]\right) \oplus ([1] \odot [10]) \oplus ([9] \odot [1]) \\
&= ([7] \odot [1]) \oplus ([3] \odot [1]) \oplus ([1] \odot [1]) \oplus ([9] \odot [1]) \\
&= [7] \oplus [3] \oplus [1] \oplus [9] \\
&= [7 + 3 + 1 + 9]. \qquad (3)
\end{aligned}$$

Equation (3) tells us that 7319 has the same remainder when divided by 9 as the sum of its digits. It is easy to check that the sum of the digits is 20 and hence has a remainder of 2. This means that when 7319 is divided by 9, the remainder is 2.

To prove that any natural number has the same remainder when divided by 9 as the sum of its digits, it is helpful to introduce notation for the decimal representation of a natural number. The notation we will use is similar to the notation for the number 7319 in equation (1).

In general, if $n \in \mathbb{N}$, and $n = a_k a_{k-1} \cdots a_1 a_0$ is the decimal representation of n, then

$$n = \left(a_k \times 10^k\right) + \left(a_{k-1} \times 10^{k-1}\right) + \cdots + \left(a_1 \times 10^1\right) + \left(a_0 \times 10^0\right).$$

This can also be written using summation notation as follows:

$$n = \sum_{j=0}^{k} \left(a_j \times 10^j\right).$$

Using congruence classes for congruence modulo 9, we have

$$\begin{aligned}
[n] &= [\left(a_k \times 10^k\right) + \left(a_{k-1} \times 10^{k-1}\right) + \cdots + \left(a_1 \times 10^1\right) + \left(a_0 \times 10^0\right)] \\
&= [a_k \times 10^k] \oplus [a_{k-1} \times 10^{k-1}] \oplus \cdots \oplus [a_1 \times 10^1] \oplus [a_0 \times 10^0] \\
&= \left([a_k] \odot [10^k]\right) \oplus \left([a_{k-1}] \odot [10^{k-1}]\right) \oplus \cdots \\
&\qquad \oplus \left([a_1] \odot [10^1]\right) \oplus \left([a_0] \odot [10^0]\right). \qquad (4)
\end{aligned}$$

One last detail is needed. It is given in Proposition 7.21. The proof by mathematical induction is Exercise (6).

Proposition 7.21. *If n is a nonnegative integer, then $10^n \equiv 1 \pmod 9$, and hence for the equivalence relation of congruence modulo 9, $[10^n] = [1]$.*

If we let $s(n)$ denote the sum of the digits of n, then

$$s(n) = a_k + a_{k-1} + \cdots + a_1 + a_0,$$

Now using equation (4) and Proposition 7.21, we obtain

$$\begin{aligned}
[n] &= ([a_k] \odot [1]) \oplus ([a_{k-1}] \odot [1]) \oplus \cdots \oplus ([a_1] \odot [1]) \oplus ([a_0] \odot [1]) \\
&= [a_k] \oplus [a_{k-1}] \oplus \cdots \oplus [a_1] \oplus [a_0] \\
&= [a_k + a_{k-1} + \cdots + a_1 + a_0]. \\
&= [s(n)].
\end{aligned}$$

This completes the proof of Theorem 7.22.

Theorem 7.22. *Let $n \in \mathbb{N}$ and let $s(n)$ denote the sum of the digits of n. Then*

1. *$[n] = [s(n)]$, using congruence classes modulo 9.*
2. *$n \equiv s(n) \pmod 9$.*
3. *$9 \mid n$ if and only if $9 \mid s(n)$.*

Part (3) of Theorem 7.22 is called a **divisibility test**. If gives a necessary and sufficient condition for a natural number to be divisible by 9. Other divisibility tests will be explored in the exercises. Most of these divisibility tests can be proved in a manner similar to the proof of the divisibility test for 9.

Exercises 7.4

1. ⋆ **(a)** Complete the addition and multiplication tables for $\mathbb{Z}_4$.

⋆ **(b)** Complete the addition and multiplication tables for $\mathbb{Z}_7$.

(c) Complete the addition and multiplication tables for $\mathbb{Z}_8$.

2. The set $\mathbb{Z}_n$ contains n elements. One way to solve an equation in $\mathbb{Z}_n$ is to substitute each of these n elements in the equation to check which ones are solutions. In $\mathbb{Z}_n$, when parentheses are not used, we follow the usual order of operations, which means that multiplications are done first and then additions. Solve each of the following equations:

⋆ **(a)** $[x]^2 = [1]$ in $\mathbb{Z}_4$

(b) $[x]^2 = [1]$ in $\mathbb{Z}_8$

(c) $[x]^4 = [1]$ in $\mathbb{Z}_5$

(d) $[x]^2 \oplus [3] \odot [x] = [3]$ in $\mathbb{Z}_6$

⋆ **(e)** $[x]^2 \oplus [1] = [0]$ in $\mathbb{Z}_5$

(f) $[3] \odot [x] \oplus [2] = [0]$ in $\mathbb{Z}_5$

⋆ **(g)** $[3] \odot [x] \oplus [2] = [0]$ in $\mathbb{Z}_6$

(h) $[3] \odot [x] \oplus [2] = [0]$ in $\mathbb{Z}_9$

⋆ **3.** In each case, determine if the statement is true or false.

(**a**) For all $[a] \in \mathbb{Z}_6$, if $[a] \neq [0]$, then there exists a $[b] \in \mathbb{Z}_6$ such that $[a] \odot [b] = [1]$.

(**b**) For all $[a] \in \mathbb{Z}_5$, if $[a] \neq [0]$, then there exists a $[b] \in \mathbb{Z}_5$ such that $[a] \odot [b] = [1]$.

4. In each case, determine if the statement is true or false.

(**a**) For all $[a], [b] \in \mathbb{Z}_6$, if $[a] \neq [0]$ and $[b] \neq [0]$, then $[a] \odot [b] \neq [0]$.

(**b**) For all $[a], [b] \in \mathbb{Z}_5$, if $[a] \neq [0]$ and $[b] \neq [0]$, then $[a] \odot [b] \neq [0]$.

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

For each $[a] \in \mathbb{Z}_5$, if $[a] \neq [0]$, then $[a]^2 = [1]$ or $[a]^2 = [4]$.

(b) Does there exist an integer a such that $a^2 = 5, 158, 232, 468, 953, 153$? Use your work in Part (a) to justify your conclusion. Compare to Exercise (11) in Section 3.5.

6. Use mathematical induction to prove Proposition 7.21.

If n is a nonnegative integer, then $10^n \equiv 1 \pmod 9$, and hence for the equivalence relation of congruence modulo 9, $[10^n] = [1]$.

7. Use mathematical induction to prove that if n is a nonnegative integer, then $10^n \equiv 1 \pmod 3$. Hence, for congruence classes modulo 3, if n is a nonnegative integer, then $[10^n] = [1]$.

8. Let $n \in \mathbb{N}$ and let $s(n)$ denote the sum of the digits of n. So if we write

$$n = \left(a_k \times 10^k\right) + \left(a_{k-1} \times 10^{k-1}\right) + \cdots + \left(a_1 \times 10^1\right) + \left(a_0 \times 10^0\right),$$

then $s(n) = a_k + a_{k-1} + \cdots + a_1 + a_0$. Use the result in Exercise (7) to help prove each of the following:

(**a**) $[n] = [s(n)]$, using congruence classes modulo 3.

(**b**) $n \equiv s(n) \pmod 3$.

(**c**) $3 \mid n$ if and only if $3 \mid s(n)$.

9. Use mathematical induction to prove that if n is an integer and $n \geq 1$, then $10^n \equiv 0 \pmod 5$. Hence, for congruence classes modulo 5, if n is an integer and $n \geq 1$, then $[10^n] = [0]$.

10. Let $n \in \mathbb{N}$ and assume

$$n = \left(a_k \times 10^k\right) + \left(a_{k-1} \times 10^{k-1}\right) + \cdots + \left(a_1 \times 10^1\right) + \left(a_0 \times 10^0\right).$$

Use the result in Exercise (9) to help prove each of the following:

(**a**) $[n] = [a_0]$, using congruence classes modulo 5.

(**b**) $n \equiv a_0 \pmod 5$.

(**c**) $5 \mid n$ if and only if $5 \mid a_0$.

11. Use mathematical induction to prove that if n is an integer and $n \geq 2$, then $10^n \equiv 0 \pmod 4$. Hence, for congruence classes modulo 4, if n is an integer and $n \geq 2$, then $[10^n] = [0]$.

12. Let $n \in \mathbb{N}$ and assume

$$n = \left(a_k \times 10^k\right) + \left(a_{k-1} \times 10^{k-1}\right) + \cdots + \left(a_1 \times 10^1\right) + \left(a_0 \times 10^0\right).$$

Use the result in Exercise (11) to help prove each of the following:

(**a**) $[n] = [10a_1 + a_0]$, using congruence classes modulo 4.

(**b**) $n \equiv (10a_1 + a_0) \pmod 4$.

(**c**) $4 \mid n$ if and only if $4 \mid (10a_1 + a_0)$.

13. Use mathematical induction to prove that if n is an integer and $n \geq 3$, then $10^n \equiv 0 \pmod 8$. Hence, for congruence classes modulo 8, if n is an integer and $n \geq 3$, then $[10^n] = [0]$.

14. Let $n \in \mathbb{N}$ and assume

$$n = \left(a_k \times 10^k\right) + \left(a_{k-1} \times 10^{k-1}\right) + \cdots + \left(a_1 \times 10^1\right) + \left(a_0 \times 10^0\right).$$

Use the result in Exercise (13) to help develop a divisibility test for 8. Prove that your divisibility test is correct.

15. Use mathematical induction to prove that if n is a nonnegative integer then $10^n \equiv (-1)^n \pmod{11}$. Hence, for congruence classes modulo 11, if n is a nonnegative integer, then $[10^n] = [(-1)^n]$.

16. Let $n \in \mathbb{N}$ and assume

$$n = \left(a_k \times 10^k\right) + \left(a_{k-1} \times 10^{k-1}\right) + \cdots + \left(a_1 \times 10^1\right) + \left(a_0 \times 10^0\right).$$

Use the result in Exercise (15) to help prove each of the following:

(**a**) $n \equiv \sum_{j=0}^{k} (-1)^j a_j \pmod{11}$.

(**b**) $[n] = [\sum_{j=0}^{k} (-1)^j a_j]$, using congruence classes modulo 11.

(**c**) 11 divides n if and only if 11 divides $\sum_{j=0}^{k} (-1)^j a_j$.

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

For all $[a], [b] \in \mathbb{Z}_3$, if $[a]^2 + [b]^2 = [0]$, then $[a] = 0$ and $[b] = [0]$.

(b) Use Exercise (17a) to prove the following proposition:

Let $a, b \in \mathbb{Z}$. If $\left(a^2 + b^2\right) \equiv 0 \pmod 3$, then $a \equiv 0 \pmod 3$ and $b \equiv 0 \pmod 3$.

(c) Use Exercise (17b) to prove the following proposition:

For all $a, b \in \mathbb{Z}$, if 3 divides $\left(a^2 + b^2\right)$, then 3 divides a and 3 divides b.

18. Prove the following proposition:

For each $a \in \mathbb{Z}$, if there exist integers b and c such that $a = b^4 + c^4$, then the units digit of a must be 0, 1, 2, 5, 6, or 7.

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

Let $n \in \mathbb{Z}$. If n is odd, then $8 \mid \left(n^2 - 1\right)$. **Hint**: What are the possible values of $n \pmod 8$?

20. Prove the following proposition:

Let $n \in \mathbb{N}$. If $n \equiv 7 \pmod 8$, then n is not the sum of three squares. That is, there do not exist natural numbers a, b, and c such that $n = a^2 + b^2 + c^2$.

Explorations and Activities

21. Using Congruence Modulo 4. The set $\mathbb{Z}_n$ is a finite set, and hence one way to prove things about $\mathbb{Z}_n$ is to simply use the n elements in $\mathbb{Z}_n$ as the n cases for a proof using cases. For example, if $n \in \mathbb{Z}$, then in $\mathbb{Z}_4$, $[n] = [0]$, $[n] = [1]$, $[n] = [2]$, or $[n] = [3]$.

(**a**) Prove that if $n \in \mathbb{Z}$, then in $\mathbb{Z}_4$, $[n]^2 = [0]$ or $[n]^2 = [1]$. Use this to conclude that in $\mathbb{Z}_4$, $[n^2] = [0]$ or $[n^2] = [1]$.

(**b**) Translate the equations $\left[n^2\right] = [0]$ and $\left[n^2\right] = [1]$ in $\mathbb{Z}_4$ into congruences modulo 4.

(**c**) Use a result in Exercise (12) to determine the value of r so that $r \in \mathbb{Z}$, $0 \leq r < 3$, and

$$104\,257\,833\,259 \equiv r \pmod 4.$$

That is, $[104\,257\,833\,259] = [r]$ in $\mathbb{Z}_4$.

(**d**) Is the natural number 104 257 833 259 a perfect square? Justify your conclusion.

7.5 Chapter 7 Summary

Important Definitions

- Relation from A to B, page 364
- Relation on A, page 364
- Domain of a relation, page 364
- Range of a relation, page 364
- Inverse of a relation, page 373
- Reflexive relation, page 375
- Symmetric relation, page 375
- Transitive relation, page 375
- Equivalence relation, page 378
- Equivalence class, page 391
- Congruence class, page 392
- Partition of a set, page 395
- Integers modulo n, page 402
- Addition in $\mathbb{Z}_n$, page 404
- Multiplication in $\mathbb{Z}_n$, page 404

Important Theorems and Results about Relations, Equivalence Relations, and Equivalence Classes

- **Theorem 7.6**. *Let R be a relation from the set A to the set B. Then*

  1. *The domain of R^{-1} is the range of R. That is, $dom(R^{-1}) = range(R)$.*
  2. *The range of R^{-1} is the domain of R. That is, $range(R^{-1}) = dom(R)$.*
  3. *The inverse of R^{-1} is R. That is, $\left(R^{-1}\right)^{-1} = R$.*

- **Theorem 7.10**. *Let $n \in \mathbb{N}$ and let $a, b \in \mathbb{Z}$. Then $a \equiv b \pmod{n}$ if and only if a and b have the same remainder when divided by n.*

- **Theorem 7.14**. *Let A be a nonempty set and let $\sim$ be an equivalence relation on A.*

  1. *For each $a \in A$, $a \in [a]$.*
  2. *For each $a, b \in A$, $a \sim b$ if and only if $[a] = [b]$.*
  3. *For each $a, b \in A$, $[a] = [b]$ or $[a] \cap [b] = \emptyset$.*

- **Corollary 7.16**. *Let $n \in \mathbb{N}$. For each $a \in \mathbb{Z}$, let $[a]$ represent the congruence class of a modulo n.*

  1. *For each $a \in \mathbb{Z}$, $a \in [a]$.*
  2. *For each $a, b \in \mathbb{Z}$, $a \equiv b \pmod{n}$ if and only if $[a] = [b]$.*
  3. *For each $a, b \in \mathbb{Z}$, $[a] = [b]$ or $[a] \cap [b] = \emptyset$.*

- **Corollary 7.17**. *Let $n \in \mathbb{N}$. For each $a \in \mathbb{Z}$, let $[a]$ represent the congruence class of a modulo n.*

  1. $\mathbb{Z} = [0] \cup [1] \cup [2] \cup \cdots \cup [n-1]$
  2. *For $j, k \in \{0, 1, 2, \ldots, n-1\}$, if $j \neq k$, then $[j] \cap [k] = \emptyset$.*

- **Theorem 7.18**. *Let $\sim$ be an equivalence relation on the nonempty set A. Then the collection $\mathcal{C}$ of all equivalence classes determined by $\sim$ is a partition of the set A.*
