Chapter 8

Topics in Number Theory

8.1 The Greatest Common Divisor

Preview Activity 1 (**The Greatest Common Divisor**)

1. Explain what it means to say that a nonzero integer m divides an integer n. Recall that we use the notation $m \mid n$ to indicate that the nonzero integer m divides the integer n.

2. Let m and n be integers with $m \neq 0$. Explain what it means to say that m does not divide n.

Definition. Let a and b be integers, not both 0. A **common divisor** of a and b is any nonzero integer that divides both a and b. The *largest* natural number that divides both a and b is called the **greatest common divisor** of a and b. The greatest common divisor of a and b is denoted by $\gcd(a, b)$.

3. Use the roster method to list the elements of the set that contains all the natural numbers that are divisors of 48.

4. Use the roster method to list the elements of the set that contains all the natural numbers that are divisors of 84.

5. Determine the intersection of the two sets in Parts (3) and (4). This set contains all the natural numbers that are common divisors of 48 and 84.

6. What is the greatest common divisor of 48 and 84?

7. Use the method suggested in Parts (3) through (6) to determine each of the following: $\gcd(8, -12)$, $\gcd(0, 5)$, $\gcd(8, 27)$, and $\gcd(14, 28)$.

8. If a and b are integers, make a conjecture about how the common divisors of a and b are related to the greatest common divisor of a and b.

Preview Activity 2 (The GCD and the Division Algorithm)
When we speak of the quotient and the remainder when we "divide an integer a by the positive integer b," we will always mean the quotient q and the remainder r guaranteed by the Division Algorithm. (See Section 3.5, page 143.)

1. Each row in the following table contains values for the integers a and b. In this table, the value of r is the remainder (from the Division Algorithm) when a is divided by b. Complete each row in this table by determining $\gcd(a, b)$, r, and $\gcd(b, r)$.

a	b	$\gcd(a, b)$	Remainder r	$\gcd(b, r)$
44	12			
75	21			
50	33			

2. Formulate a conjecture based on the results of the table in Part (1).

The System of Integers

Number theory is a study of the system of integers, $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ and the various properties of this set under the usual operations of addition and multiplication and under the usual ordering relation of "less than." The properties of the integers in Table 8.1 will be considered axioms in this text.

We will also assume the properties of the integers shown in Table 8.2. These properties can be proven from the properties in Table 8.1. (However, we will not do so here.)

	For all integers a, b, and c:
Closure Properties for Addition and Multiplication	$a + b \in \mathbb{Z}$ and $ab \in \mathbb{Z}$
Commutative Properties for Addition and Multiplication	$a + b = b + a$, and $ab = ba$
Associative Properties for Addition and Multiplication	$(a + b) + c = a + (b + c)$ and $(ab)\,c = a\,(bc)$
Distributive Properties of Multiplication over Addition	$a\,(b + c) = ab + ac$, and $(b + c)\,a = ba + ca$
Additive and Multiplicative Identity Properties	$a + 0 = 0 + a = a$, and $a \cdot 1 = 1 \cdot a = a$
Additive Inverse Property	$a + (-a) = (-a) + a = 0$

Table 8.1: Axioms for the Integers

Zero Property of Multiplication	If $a \in \mathbb{Z}$, then $a \cdot 0 = 0 \cdot a = 0$.
Cancellation Properties of Addition and Multiplication	If $a, b, c \in \mathbb{Z}$ and $a + b = a + c$, then $b = c$. If $a, b, c \in \mathbb{Z}$, $a \neq 0$ and $ac = bc$, then $b = c$.

Table 8.2: Properties of the Integers

We have already studied a good deal of number theory in this text in our discussion of proof methods. In particular, we have studied even and odd integers, divisibility of integers, congruence, and the Division Algorithm. See the summary for Chapter 3 on page 166 for a summary of results concerning even and odd integers as well as results concerning properties of divisors. We reviewed some of these properties and the Division Algorithm in the Preview Activities.

The Greatest Common Divisor

One of the most important concepts in elementary number theory is that of the greatest common divisor of two integers. The definition for the greatest common divisor of two integers (not both zero) was given in Preview Activity 1.

1. If $a, b \in \mathbb{Z}$ and a and b are not both 0, and if $d \in \mathbb{N}$, then $d = \gcd(a, b)$ provided that it satisfies all of the following properties:

- $d \mid a$ and $d \mid b$. That is, d is a common divisor of a and b.
- If k is a natural number such that $k \mid a$ and $k \mid b$, then $k \leq d$. That is, any other common divisor of a and b is less than or equal to d.

2. Consequently, a natural number d is not the greatest common divisor of a and b provided that it does not satisfy at least one of these properties. That is, d is not equal to $\gcd(a, b)$ provided that

- d does not divide a or d does not divide b; or
- There exists a natural number k such that $k \mid a$ and $k \mid b$ and $k > d$.

This means that d is not the greatest common divisor of a and b provided that it is not a common divisor of a and b or that there exists a common divisor of a and b that is greater than d.

In the preview activities, we determined the greatest common divisors for several pairs of integers. The process we used was to list all the divisors of both integers, then list all the common divisors of both integers and, finally, from the list of all common divisors, find the greatest (largest) common divisor. This method works reasonably well for small integers but can get quite cumbersome if the integers are large. Before we develop an efficient method for determining the greatest common divisor of two integers, we need to establish some properties of greatest common divisors.

One property was suggested in Preview Activity 1. If we look at the results in Part (7) of that preview activity, we should observe that any common divisor of a and b will divide $\gcd(a, b)$. In fact, the primary goals of the remainder of this section are

1. To find an efficient method for determining $\gcd(a, b)$, where a and b are integers.

2. To prove that the natural number $\gcd(a, b)$ is the only natural number d that satisfies the following properties:

- d divides a and d divides b; and
- if k is a natural number such that $k \mid a$ and $k \mid b$, then $k \mid d$.

The second goal is only slightly different from the definition of the greatest common divisor. The only difference is in the second condition where $k \leq d$ is replaced by $k \mid d$.

We will first consider the case where a and b are integers with $a \neq 0$ and $b > 0$. The proof of the result stated in the second goal contains a method (called the Euclidean Algorithm) for determining the greatest common divisors of the two integers a and b. The main idea of the method is to keep replacing the pair of integers (a, b) with another pair of integers (b, r), where $0 \leq r < b$ and $\gcd(b, r) = \gcd(a, b)$. This idea was explored in Preview Activity 2. Lemma 8.1 is a conjecture that could have been formulated in Preview Activity 2.

Lemma 8.1. *Let c and d be integers, not both equal to zero. If q and r are integers such that $c = d \cdot q + r$, then $\gcd(c, d) = \gcd(d, r)$.*

Proof. Let c and d be integers, not both equal to zero. Assume that q and r are integers such that $c = d \cdot q + r$. For ease of notation, we will let

$$m = \gcd(c, d) \text{ and } n = \gcd(d, r).$$

Now, m divides c and m divides d. Consequently, there exist integers x and y such that $c = mx$ and $d = my$. Hence,

$$\begin{aligned} r &= c - d \cdot q \\ r &= mx - (my)q \\ r &= m(x - yq). \end{aligned}$$

But this means that m divides r. Since m divides d and m divides r, m is less than or equal to $\gcd(d, r)$. Thus, $m \leq n$.

Using a similar argument, we see that n divides d and n divides r. Since $c = d \cdot q + r$, we can prove that n divides c. Hence, n divides c and n divides d. Thus, $n \leq \gcd(c, d)$ or $n \leq m$. We now have $m \leq n$ and $n \leq m$. Hence, $m = n$ and $\gcd(c, d) = \gcd(d, r)$. ■

Progress Check 8.2 (Illustrations of Lemma 8.1)
We completed several examples illustrating Lemma 8.1 in Preview Activity 2. For another example, let $c = 56$ and $d = 12$. The greatest common divisor of 56 and 12 is 4.

1. According to the Division Algorithm, what is the remainder r when 56 is divided by 12?

2. What is the greatest common divisor of 12 and the remainder r?

The key to finding the greatest common divisor (in more complicated cases) is to use the Division Algorithm again, this time with 12 and r. We now find integers q_2 and r_2 such that

$$12 = r \cdot q_2 + r_2.$$

3. What is the greatest common divisor of r and r_2?

The Euclidean Algorithm

The example in Progress Check 8.2 illustrates the main idea of the **Euclidean Algorithm** for finding $\gcd(a, b)$, which is explained in the proof of the following theorem.

Theorem 8.3. *Let a and b be integers with $a \neq 0$ and $b > 0$. Then $\gcd(a, b)$ is the only natural number d such that*

*(**a**) d divides a and d divides b, and*

*(**b**) if k is an integer that divides both a and b, then k divides d.*

Proof. Let a and b be integers with $a \neq 0$ and $b > 0$, and let $d = \gcd(a, b)$. By the Division Algorithm, there exist integers q_1 and r_1 such that

$$a = b \cdot q_1 + r_1, \text{ and } 0 \leq r_1 < b. \tag{1}$$

If $r_1 = 0$, then equation (1) implies that b divides a. Hence, $b = d = \gcd(a, b)$ and this number satisfies Conditions (a) and (b).

If $r_1 > 0$, then by Lemma 8.1, $\gcd(a, b) = \gcd(b, r_1)$. We use the Division Algorithm again to obtain integers q_2 and r_2 such that

$$b = r_1 \cdot q_2 + r_2, \text{ and } 0 \leq r_2 < r_1. \tag{2}$$

If $r_2 = 0$, then equation (2) implies that r_1 divides b. This means that $r_1 = \gcd(b, r_1)$. But we have already seen that $\gcd(a, b) = \gcd(b, r_1)$. Hence, $r_1 = \gcd(a, b)$. In addition, if k is an integer that divides both a and b, then, using equation (1), we see that $r_1 = a - b \cdot q_1$ and, hence k divides r_1. This shows that $r_1 = \gcd(a, b)$ satisfies Conditions (a) and (b).

If $r_2 > 0$, then by Lemma 8.1, $\gcd(b, r_1) = \gcd(r_1, r_2)$. But we have already seen that $\gcd(a, b) = \gcd(b, r_1)$. Hence, $\gcd(a, b) = \gcd(r_1, r_2)$. We now continue to apply the Division Algorithm to produce a sequence of pairs of integers

(all of which have the same greatest common divisor). This is summarized in the following table:

Original Pair	**Equation from Division Algorithm**	**Inequality from Division Algorithm**	**New Pair**
(a, b)	$a = b \cdot q_1 + r_1$	$0 \leq r_1 < b$	(b, r_1)
(b, r_1)	$b = r_1 \cdot q_2 + r_2$	$0 \leq r_2 < r_1$	(r_1, r_2)
(r_1, r_2)	$r_1 = r_2 \cdot q_3 + r_3$	$0 \leq r_3 < r_2$	(r_2, r_3)
(r_2, r_3)	$r_2 = r_3 \cdot q_4 + r_4$	$0 \leq r_4 < r_3$	(r_3, r_4)
(r_3, r_4)	$r_3 = r_4 \cdot q_5 + r_5$	$0 \leq r_5 < r_4$	(r_4, r_5)
$\vdots$	$\vdots$	$\vdots$	$\vdots$

From the inequalities in the third column of this table, we have a strictly decreasing sequence of nonnegative integers $(b > r_1 > r_2 > r_3 > r_4 \cdots)$. Consequently, a term in this sequence must eventually be equal to zero. Let p be the smallest natural number such that $r_{p+1} = 0$. This means that the last two rows in the preceding table will be

Original Pair	**Equation from Division Algorithm**	**Inequality from Division Algorithm**	**New Pair**
(r_{p-2}, r_{p-1})	$r_{p-2} = r_{p-1} \cdot q_p + r_p$	$0 \leq r_p < r_{p-1}$	(r_{p-1}, r_p)
(r_{p-1}, r_p)	$r_{p-1} = r_p \cdot q_{p+1} + 0$		

Remember that this table was constructed by repeated use of Lemma 8.1 and that the greatest common divisor of each pair of integers produced equals $\gcd(a, b)$. Also, the last row in the table indicates that r_p divides r_{p-1}. This means that $\gcd(r_{p-1}, r_p) = r_p$ and hence $r_p = \gcd(a, b)$.

This proves that $r_p = \gcd(a, b)$ satisfies Condition (a) of this theorem. Now assume that k is an integer such that k divides a and k divides b. We proceed through the table row by row. First, since $r_1 = a - b \cdot q$, we see that

$$k \text{ must divide } r_1.$$

The second row tells us that $r_2 = b - r_1 \cdot q_2$. Since k divides b and k divides r_1, we conclude that

$$k \text{ divides } r_2.$$

Continuing with each row, we see that k divides each of the remainders r_1, r_2, r_3, $\ldots$, r_p. This means that $r_p = \gcd(a, b)$ satisfies Condition (b) of the theorem. ■

Progress Check 8.4 (Using the Euclidean Algorithm)

1. Use the Euclidean Algorithm to determine gcd(180, 126). Notice that we have deleted the third column (Inequality from Division Algorithm) from the following table. It is not needed in the computations.

Original Pair	**Equation from Division Algorithm**	**New Pair**
(180, 126)	$180 = 126 \cdot 1 + 54$	(126, 54)
(126, 54)	$126 =$	

Consequently, gcd(180, 126) = _____.

2. Use the Euclidean Algorithm to determine gcd(4208, 288).

Original Pair	**Equation from Division Algorithm**	**New Pair**
(4208, 288)	$4208 = 288 \cdot 14 + 176$	(288,)

Consequently, gcd(4208, 288) = _____.

Some Remarks about Theorem 8.3

Theorem 8.3 was proven with the assumptions that $a, b \in \mathbb{Z}$ with $a \neq 0$ and $b > 0$. A more general version of this theorem can be proven with $a, b \in \mathbb{Z}$ and $b \neq 0$. This can be proven using Theorem 8.3 and the results in the following lemma.

Lemma 8.5. *Let $a, b \in \mathbb{Z}$ with $b \neq 0$. Then*

1. $\gcd(0, b) = |b|$.
2. *If* $\gcd(a, b) = d$, *then* $\gcd(a, -b) = d$.

The proofs of these results are in Exercise (4). An application of this result is given in the next example.

Example 8.6 (**Using the Euclidean Algorithm**)
Let $a = 234$ and $b = -42$. We will use the Euclidean Algorithm to determine $\gcd(234, 42)$.

Step	Original Pair	Equation from Division Algorithm	New Pair
1	$(234, 42)$	$234 = 42 \cdot 5 + 24$	$(42, 24)$
2	$(42, 24)$	$42 = 24 \cdot 1 + 18$	$(24, 18)$
3	$(24, 18)$	$24 = 18 \cdot 1 + 6$	$(18, 6)$
4	$(18, 6)$	$18 = 6 \cdot 3$	

So $\gcd(234, 42) = 6$ and hence $\gcd(234, -42) = 6$.

Writing $\gcd(a, b)$ in Terms of a and b

We will use Example 8.6 to illustrate another use of the Euclidean Algorithm. It is possible to use the steps of the Euclidean Algorithm in reverse order to write $\gcd(a, b)$ in terms of a and b. We will use these steps in reverse order to find integers m and n such that $\gcd(234, 42) = 234m + 42n$. The idea is to start with the row with the last nonzero remainder and work backward as shown in the following table:

Explanation	Result
First, use the equation in Step 3 to write 6 in terms of 24 and 18.	$6 = 24 - 18 \cdot 1$
Use the equation in Step 2 to write $18 = 42 - 24 \cdot 1$. Substitute this into the preceding result and simplify.	$6 = 24 - 18 \cdot 1$ $= 24 - (42 - 24 \cdot 1)$ $= 42 \cdot (-1) + 24 \cdot 2$
We now have written 6 in terms of 42 and 24. Use the equation in Step 1 to write $24 = 234 - 42 \cdot 5$. Substitute this into the preceding result and simplify.	$6 = 42 \cdot (-1) + 24 \cdot 2$ $= 42 \cdot (-1) + (234 - 42 \cdot 5) \cdot 2$ $= 234 \cdot 2 + 42 \cdot (-11)$

Hence, we can write

$$\gcd(234, 42) = 234 \cdot 2 + 42 \cdot (-11).$$

(Check this with a calculator.) In this case, we say that we have written $\gcd(234, 42)$ as a linear combination of 234 and 42. More generally, we have the following definition.

Definition. Let a and b be integers. A **linear combination** of a and b is an integer of the form $ax + by$, where x and y are integers.

Progress Check 8.7 (**Writing the gcd as a Linear Combination**)
Use the results from Progress Check 8.4 to

1. Write $\gcd(180, 126)$ as a linear combination of 180 and 126.
2. Write $\gcd(4208, 288)$ as a linear combination of 4208 and 288.

The previous example and progress check illustrate the following important result in number theory, which will be used in the next section to help prove some other significant results.

Theorem 8.8. *Let a and b be integers, not both 0. Then $\gcd(a, b)$ can be written as a linear combination of a and b. That is, there exist integers u and v such that $\gcd(a, b) = au + bv$.*

We will not give a formal proof of this theorem. Hopefully, the examples and activities provide evidence for its validity. The idea is to use the steps of the Euclidean Algorithm in reverse order to write $\gcd(a, b)$ as a linear combination of a and b. For example, assume the completed table for the Euclidean Algorithm is

Step	Original Pair	Equation from Division Algorithm	New Pair
1	(a, b)	$a = b \cdot q_1 + r_1$	(b, r_1)
2	(b, r_1)	$b = r_1 \cdot q_2 + r_2$	(r_1, r_2)
3	(r_1, r_2)	$r_1 = r_2 \cdot q_3 + r_3$	(r_2, r_3)
4	(r_2, r_3)	$r_2 = r_3 \cdot q_4 + 0$	(r_3, r_4)

We can use Step 3 to write $r_3 = \gcd(a, b)$ as a linear combination of r_1 and r_2. We can then solve the equation in Step 2 for r_2 and use this to write $r_3 = \gcd(a, b)$ as a linear combination of r_1 and b. We can then use the equation in Step 1 to solve for r_1 and use this to write $r_3 = \gcd(a, b)$ as a linear combination of a and b.

In general, if we can write $r_p = \gcd(a, b)$ as a linear combination of a pair in a given row, then we can use the equation in the preceding step to write $r_p = \gcd(a, b)$ as a linear combination of the pair in this preceding row.

The notational details of this induction argument get quite involved. Many mathematicians prefer to prove Theorem 8.8 using a property of the natural numbers called the Well-Ordering Principle. **The Well-Ordering Principle** for the

natural numbers states that any nonempty set of natural numbers must contain a least element. It can be proven that the Well-Ordering Principle is equivalent to the Principle of Mathematical Induction.

Exercises 8.1

1. Find each of the following greatest common divisors by listing all of the positive common divisors of each pair of integers.

⋆ **(a)** $\gcd(21, 28)$ ⋆ **(c)** $\gcd(58, 63)$ **(e)** $\gcd(110, 215)$

⋆ **(b)** $\gcd(-21, 28)$ ⋆ **(d)** $\gcd(0, 12)$ **(f)** $\gcd(110, -215)$

2. ⋆ **(a)** Let $a \in \mathbb{Z}$ and let $k \in \mathbb{Z}$ with $k \neq 0$. Prove that if $k \mid a$ and $k \mid (a + 1)$, then $k \mid 1$, and hence $k = \pm 1$.

(b) Let $a \in \mathbb{Z}$. Find the greatest common divisor of the consecutive integers a and $a + 1$. That is, determine $\gcd(a, a + 1)$.

3. **(a)** Let $a \in \mathbb{Z}$ and let $k \in \mathbb{Z}$ with $k \neq 0$. Prove that if $k \mid a$ and $k \mid (a + 2)$, then $k \mid 2$.

(b) Let $a \in \mathbb{Z}$. What conclusions can be made about the greatest common divisor of a and $a + 2$?

⋆ **4.** Let $a, b \in \mathbb{Z}$ with $b \neq 0$. Prove each of the following:

(a) $\gcd(0, b) = |b|$

(b) If $\gcd(a, b) = d$, then $\gcd(a, -b) = d$. That is, $\gcd(a, -b) = \gcd(a, b)$.

5. For each of the following pairs of integers, use the Euclidean Algorithm to find $\gcd(a, b)$ and to write $\gcd(a, b)$ as a linear combination of a and b. That is, find integers m and n such that $d = am + bn$.

⋆ **(a)** $a = 36, b = 60$ **(d)** $a = 12628, b = 21361$

⋆ **(b)** $a = 901, b = 935$ ⋆ **(e)** $a = 901, b = -935$

(c) $a = 72, b = 714$ **(f)** $a = -36, b = -60$

6. ⋆ **(a)** Find integers u and v such that $9u + 14v = 1$ or explain why it is not possible to do so. Then find integers x and y such that $9x + 14y = 10$ or explain why it is not possible to do so.

(b) Find integers x and y such that $9x + 15y = 10$ or explain why it is not possible to do so.

(c) Find integers x and y such that $9x + 15y = 3162$ or explain why it is not possible to do so.

7. ⋆ **(a)** Notice that $\gcd(11, 17) = 1$. Find integers x and y such that $11x + 17y = 1$.

⋆ **(b)** Let $m, n \in \mathbb{Z}$. Write the sum $\frac{m}{11} + \frac{n}{17}$ as a single fraction.

(c) Find two rational numbers with denominators of 11 and 17, respectively , whose sum is equal to $\frac{10}{187}$. **Hint**: Write the rational numbers in the form $\frac{m}{11}$ and $\frac{n}{17}$, where $m, n \in \mathbb{Z}$. Then write

$$\frac{m}{11} + \frac{n}{17} = \frac{10}{187}.$$

Use Exercises (7a) and (7b) to determine m and n.

(d) Find two rational numbers with denominators 17 and 21, respectively, whose sum is equal to $\frac{326}{357}$ or explain why it is not possible to do so.

(e) Find two rational numbers with denominators 9 and 15, respectively, whose sum is equal to $\frac{10}{225}$ or explain why it is not possible to do so.

Explorations and Activities

8. Linear Combinations and the Greatest Common Divisor

(a) Determine the greatest common divisor of 20 and 12?

(b) Let $d = \gcd(20, 12)$. Write d as a linear combination of 20 and 12.

(c) Generate at least six different linear combinations of 20 and 12. Are these linear combinations of 20 and 12 multiples of $\gcd(20, 12)$?

(d) Determine the greatest common divisor of 21 and -6 and then generate at least six different linear combinations of 21 and -6. Are these linear combinations of 21 and -6 multiples of $\gcd(21, -6)$?

(e) The following proposition was first introduced in Exercise (18) on page 243 in Section 5.2. Complete the proof of this proposition if you have not already done so.

Proposition 5.16 *Let a, b, and t be integers with $t \neq 0$. If t divides a and t divides b, then for all integers x and y, t divides (ax + by).*

Proof. Let a, b, and t be integers with $t \neq 0$, and assume that t divides a and t divides b. We will prove that for all integers x and y, t divides $(ax + by)$.

So let $x \in \mathbb{Z}$ and let $y \in \mathbb{Z}$. Since t divides a, there exists an integer m such that . . . .

(f) Now let a and b be integers, not both zero and let $d = \gcd(a, b)$. Theorem 8.8 states that d is a linear combination of a and b. In addition, let S and T be the following sets:

$$S = \{ax + by \mid x, y \in \mathbb{Z}\} \qquad \text{and} \qquad T = \{kd \mid k \in \mathbb{Z}\}.$$

That is, S is the set of all linear combinations of a and b, and T is the set of all multiples of the greatest common divisor of a and b. Does the set S equal the set T? If not, is one of these sets a subset of the other set? Justify your conclusions.

Note: In Parts (c) and (d), we were exploring special cases for these two sets.

8.2 Prime Numbers and Prime Factorizations

Preview Activity 1 (Exploring Examples where *a* Divides *b* · *c*)

1. Find at least three different examples of nonzero integers a, b, and c such that $a \mid (bc)$ but a does not divide b and a does not divide c. In each case, compute $\gcd(a, b)$ and $\gcd(a, c)$.
2. Find at least three different examples of nonzero integers a, b, and c such that $\gcd(a, b) = 1$ and $a \mid (bc)$. In each example, is there any relation between the integers a and c?
3. Formulate a conjecture based on your work in Parts (1) and (2).

Preview Activity 2 (Prime Factorizations)

Recall that a natural number p is a **prime number** provided that it is greater than 1 and the only natural numbers that divide p are 1 and p. A natural number other than 1 that is not a prime number is a **composite number**. The number 1 is neither prime nor composite. (See Exercise 13 from Section 2.4 on page 78.)

1. Give examples of four natural numbers that are prime and four natural numbers that are composite.

Theorem 4.9 in Section 4.2 states that every natural number greater than 1 is either a prime number or a product of prime numbers.

When a composite number is written as a product of prime numbers, we say that we have obtained a **prime factorization** of that composite number. For example, since $60 = 2^2 \cdot 3 \cdot 5$, we say that $2^2 \cdot 3 \cdot 5$ is a prime factorization of 60.

2. Write the number 40 as a product of prime numbers by first writing $40 = 2 \cdot 20$ and then factoring 20 into a product of primes. Next, write the number 40 as a product of prime numbers by first writing $40 = 5 \cdot 8$ and then factoring 8 into a product of primes.

3. In Part (2), we used two different methods to obtain a prime factorization of 40. Did these methods produce the same prime factorization or different prime factorizations? Explain.

4. Repeat Parts (2) and (3) with 150. First, start with $150 = 3 \cdot 50$, and then start with $150 = 5 \cdot 30$.

Greatest Common Divisors and Linear Combinations

In Section 8.1, we introduced the concept of the greatest common divisor of two integers. We showed how the Euclidean Algorithm can be used to find the greatest common divisor of two integers, a and b, and also showed how to use the results of the Euclidean Algorithm to write the greatest common divisor of a and b as a linear combination of a and b.

In this section, we will use these results to help prove the so-called Fundamental Theorem of Arithmetic, which states that any natural number greater than 1 that is not prime can be written as product of primes in "essentially" only one way. This means that given two prime factorizations, the prime factors are exactly the same, and the only difference may be in the order in which the prime factors are written. We start with more results concerning greatest common divisors. We first prove Proposition 5.16, which was part of Exercise (18) on page 243 in Section 5.2 and Exercise (8) on page 425in Section 8.1.

Proposition 5.16 *Let a, b, and t be integers with $t \neq 0$. If t divides a and t divides b, then for all integers x and y, t divides $(ax + by)$.*

Proof. Let a, b, and t be integers with $t \neq 0$, and assume that t divides a and t divides b. We will prove that for all integers x and y, t divides $(ax + by)$.

So let $x \in \mathbb{Z}$ and let $y \in \mathbb{Z}$. Since t divides a, there exists an integer m such that $a = mt$ and since t divides b, there exists an integer n such that $b = nt$. Using substitution and algebra, we then see that

$$\begin{aligned} ax + by &= (mt)x + (nt)y \\ &= t(mx + ny) \end{aligned}$$

Since $(mx + ny)$ is an integer, the last equation proves that t divides $ax + by$ and this proves that for all integers x and y, t divides $(ax + by)$. ■

We now let $a, b \in \mathbb{Z}$, not both 0, and let $d = \gcd(a, b)$. Theorem 8.8 states that d can be written as a linear combination of a and b. Now, since $d \mid a$ and $d \mid b$, we can use the result of Proposition 5.16 to conclude that for all $x, y \in \mathbb{Z}$, $d \mid (ax + by)$. This means that d divides every linear combination of a and b. In addition, this means that d must be the smallest positive number that is a linear combination of a and b. We summarize these results in Theorem 8.9.

Theorem 8.9. *Let $a, b \in \mathbb{Z}$, not both 0.*

1. *The greatest common divisor, d, is a linear combination of a and b. That is, there exist integers m and n such that $d = am + bn$.*
2. *The greatest common divisor, d, divides every linear combination of a and b. That is, for all $x, y \in \mathbb{Z}$, $d \mid (ax + by)$.*
3. *The greatest common divisor, d, is the smallest positive number that is a linear combination of a and b.*

Relatively Prime Integers

In Preview Activity 1, we constructed several examples of integers a, b, and c such that $a \mid (bc)$ but a does not divide b and a does not divide c. For each example, we observed that $\gcd(a, b) \neq 1$ and $\gcd(a, c) \neq 1$.

We also constructed several examples where $a \mid (bc)$ and $\gcd(a, b) = 1$. In all of these cases, we noted that a divides c. Integers whose greatest common divisor is equal to 1 are given a special name.

Definition. Two nonzero integers a and b are **relatively prime** provided that $\gcd(a, b) = 1$.

Progress Check 8.10 (Relatively Prime Integers)

1. Construct at least three different examples where p is a prime number, $a \in \mathbb{Z}$, and $p \mid a$. In each example, what is $\gcd(a, p)$? Based on these examples, formulate a conjecture about $\gcd(a, p)$ when $p \mid a$.

2. Construct at least three different examples where p is a prime number, $a \in \mathbb{Z}$, and p does not divide a. In each example, what is $\gcd(a, p)$? Based on these examples, formulate a conjecture about $\gcd(a, p)$ when p does not divide a.

3. Give at least three different examples of integers a and b where a is not prime, b is not prime, and $\gcd(a, b) = 1$, or explain why it is not possible to construct such examples.

Theorem 8.11. *Let a and b be nonzero integers, and let p be a prime number.*

1. *If a and b are relatively prime, then there exist integers m and n such that $am + bn = 1$. That is, 1 can be written as linear combination of a and b.*

2. *If $p \mid a$, then $\gcd(a, p) = p$.*

3. *If p does not divide a, then $\gcd(a, p) = 1$.*

Part (1) of Theorem 8.11 is actually a corollary of Theorem 8.9. Parts (2) and (3) could have been the conjectures you formulated in Progress Check 8.10. The proofs are included in Exercise (1).

Given nonzero integers a and b, we have seen that it is possible to use the Euclidean Algorithm to write their greatest common divisor as a linear combination of a and b. We have also seen that this can sometimes be a tedious, time-consuming process, which is why people have programmed computers to do this. Fortunately, in many proofs of number theory results, we do not actually have to construct this linear combination since simply knowing that it exists can be useful in proving results. This will be illustrated in the proof of Theorem 8.12, which is based on work in Preview Activity 1.

Theorem 8.12. *Let a, b, be nonzero integers and let c be an integer. If a and b are relatively prime and $a \mid (bc)$, then $a \mid c$.*

The explorations in Preview Activity 1 were related to this theorem. We will first explore the forward-backward process for the proof. The goal is to prove that $a \mid c$. A standard way to do this is to prove that there exists an integer q such that

$$c = aq. \tag{1}$$

Since we are given that $a \mid (bc)$, there exists an integer k such that

$$bc = ak. \tag{2}$$

It may seem tempting to divide both sides of equation (2) by b, but if we do so, we run into problems with the fact that the integers are not closed under division. Instead, we look at the other part of the hypothesis, which is that a and b are relatively prime. This means that $\gcd(a, b) = 1$. How can we use this? This means that a and b have no common factors except for 1. In light of equation (2), it seems reasonable that any factor of a must also be a factor of c. But how do we formalize this?

One conclusion that we can use is that since $\gcd(a, b) = 1$, by Theorem 8.11, there exist integers m and n such that

$$am + bn = 1. \tag{3}$$

We may consider solving equation (3) for b and substituting this into equation (2). The problem, again, is that in order to solve equation (3) for b, we need to divide by n.

Before doing anything else, we should look at the goal in equation (1). We need to introduce c into equation (3). One way to do this is to multiply both sides of equation (3) by c. (This keeps us in the system of integers since the integers are closed under multiplication.) This gives

$$\begin{aligned} (am + bn)\, c &= 1 \cdot c \\ acm + bcn &= c. \end{aligned} \tag{4}$$

Notice that the left side of equation (4) contains a term, bcn, that contains bc. This means that we can use equation (2) and substitute $bc = ak$ in equation (4). After doing this, we can factor the left side of the equation to prove that $a \mid c$.

Progress Check 8.13 (Completing the Proof of Theorem 8.12)
Write a complete proof of Theorem 8.12.

Corollary 8.14.

1. *Let $a, b \in \mathbb{Z}$, and let p be a prime number. If $p \mid (ab)$, then $p \mid a$ or $p \mid b$.*
2. *Let p be a prime number, let $n \in \mathbb{N}$, and let $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. If $p \mid (a_1 a_2 \cdots a_n)$, then there exists a natural number k with $1 \leq k \leq n$ such that $p \mid a_k$.*

Part (1) of Corollary 8.14 is a corollary of Theorem 8.12. Part (2) is proved using mathematical induction. The basis step is the case where $n = 1$, and Part (1) is the case where $n = 2$. The proofs of these two results are included in Exercises (2) and (3).

Historical Note

Part (1) of Corollary 8.14 is known as **Euclid's Lemma**. Most people associate geometry with *Euclid's Elements*, but these books also contain many basic results in number theory. Many of the results that are contained in this section appeared in *Euclid's Elements*.

Prime Numbers and Prime Factorizations

We are now ready to prove the Fundamental Theorem of Arithmetic. The first part of this theorem was proved in Theorem 4.9 in Section 4.2. This theorem states that each natural number greater than 1 is either a prime number or is a product of prime numbers. Before we state the Fundamental Theorem of Arithmetic, we will discuss some notational conventions that will help us with the proof. We start with an example.

We will use $n = 120$. Since $5 \mid 120$, we can write $120 = 5 \cdot 24$. In addition, we can factor 24 as $24 = 2 \cdot 2 \cdot 2 \cdot 3$. So we can write

$$\begin{aligned} 120 &= 5 \cdot 24 \\ &= 5\,(2 \cdot 2 \cdot 2 \cdot 3)\,. \end{aligned}$$

This is a prime factorization of 120, but it is not the way we usually write this factorization. Most often, we will write the prime number factors in ascending order. So we write

$$120 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 \text{ or } 120 = 2^3 \cdot 3 \cdot 5.$$

Now, let $n \in \mathbb{N}$. To write the prime factorization of n with the prime factors in ascending order requires that if we write $n = p_1 p_2 \cdots p_r$, where $p_1, p_2, \cdots p_r$ are prime numbers, we will have $p_1 \leq p_2 \leq \cdots \leq p_r$.

Theorem 8.15 (**The Fundamental Theorem of Arithmetic**).

1. *Each natural number greater than 1 is either a prime number or is a product of prime numbers.*

2. *Let $n \in \mathbb{N}$ with $n > 1$. Assume that*

$$n = p_1 p_2 \cdots p_r \text{ and that } n = q_1 q_2 \cdots q_s,$$

where $p_1, p_2, \cdots p_r$ and $q_1, q_2, \cdots q_s$ are primes with $p_1 \leq p_2 \leq \cdots \leq p_r$ and $q_1 \leq q_2 \leq \cdots \leq q_s$. Then $r = s$, and for each j from 1 to r, $p_j = q_j$.

Proof. The first part of this theorem was proved in Theorem 4.9. We will prove the second part of the theorem by induction on n using the Second Principle of Mathematical Induction. (See Section 4.2.) For each natural number n with $n > 1$, let $P(n)$ be

> If $n = p_1 p_2 \cdots p_r$ and $n = q_1 q_2 \cdots q_s$, where $p_1, p_2, \cdots p_r$ and $q_1, q_2, \cdots q_s$ are primes with $p_1 \leq p_2 \leq \cdots \leq p_r$ and $q_1 \leq q_2 \leq \cdots \leq q_s$, then $r = s$, and for each j from 1 to r, $p_j = q_j$.

For the basis step, we notice that since 2 is a prime number, its only factorization is $2 = 1 \cdot 2$. This means that the only equation of the form $2 = p_1 p_2 \cdots p_r$, where $p_1, p_2, \cdots p_r$ are prime numbers, is the case where $r = 1$ and $p_1 = 2$. This proves that $P(2)$ is true.

For the inductive step, let $k \in \mathbb{N}$ with $k \geq 2$. We will assume that $P(2), P(3), \ldots, P(k)$ are true. The goal now is to prove that $P(k+1)$ is true. To prove this, we assume that $(k+1)$ has two prime factorizations and then prove that these prime factorizations are the same. So we assume that

> $k + 1 = p_1 p_2 \cdots p_r$ and that $k + 1 = q_1 q_2 \cdots q_s$, where $p_1, p_2, \cdots p_r$ and $q_1, q_2, \cdots q_s$ are primes with $p_1 \leq p_2 \leq \cdots \leq p_r$ and $q_1 \leq q_2 \leq \cdots \leq q_s$.

We must now prove that $r = s$, and for each j from 1 to r, $p_j = q_j$. We can break our proof into two cases: (1) $p_1 \leq q_1$; and (2) $q_1 \leq p_1$. Since one of these must be true, and since the proofs will be similar, we can assume, without loss of generality, that $p_1 \leq q_1$.

Since $k + 1 = p_1 p_2 \cdots p_r$, we know that $p_1 \mid (k + 1)$, and hence we may conclude that $p_1 \mid (q_1 q_2 \cdots q_s)$. We now use Corollary 8.14 to conclude that there exists a j with $1 \leq j \leq s$ such that $p_1 \mid q_j$. Since p_1 and q_j are primes, we conclude that

$$p_1 = q_j .$$

We have also assumed that $q_1 \leq q_j$ for all j and, hence, we know that $q_1 \leq p_1$. However, we have also assumed that $p_1 \leq q_1$. Hence,

$$p_1 = q_1 .$$

We now use this and the fact that $k + 1 = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$ to conclude that

$$p_2 \cdots p_r = q_2 \cdots q_s .$$

The product in the previous equation is less that $k + 1$. Hence, we can apply our induction hypothesis to these factorizations and conclude that $r = s$, and for each j from 2 to r, $p_j = q_j$.

This completes the proof that if $P(2), P(3), \ldots, P(k)$ are true, then $P(k + 1)$ is true. Hence, by the Second Principle of Mathematical Induction, we conclude that $P(n)$ is true for all $n \in \mathbb{N}$ with $n \geq 2$. This completes the proof of the theorem. ■

Note: : We often shorten the result of the Fundamental Theorem of Arithmetic by simply saying that each natural number greater than one that is not a prime has a **unique factorization** as a product of primes. This simply means that if $n \in \mathbb{N}$, $n > 1$, and n is not prime, then no matter how we choose to factor n into a product of primes, we will always have the same prime factors. The only difference may be in the order in which we write the prime factors.

Further Results and Conjectures about Prime Numbers

1. **The Number of Prime Numbers**
   Prime numbers have fascinated mathematicians for centuries. For example, we can easily start writing a list of prime numbers in ascending order. Following is a list of the prime numbers less than 100.

   2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97

This list contains the first 25 prime numbers. Does this list ever stop? The question was answered in *Euclid's Elements*, and the result is stated in Theorem 8.16. The proof of this theorem is considered to be one of the classical proofs by contradiction.

Theorem 8.16. *There are infinitely many prime numbers.*

Proof. We will use a proof by contradiction. We assume that there are only finitely many primes, and let

$$p_1, p_2, \ldots, p_m$$

be the list of all the primes. Let

$$M = p_1 p_2 \cdots p_m + 1. \tag{1}$$

Notice that $M \neq 1$. So M is either a prime number or, by the Fundamental Theorem of Arithmetic, M is a product of prime numbers. In either case, M has a factor that is a prime number. Since we have listed all the prime numbers, this means that there exists a natural number j with $1 \leq j \leq m$ such that $p_j \mid M$. Now, we can rewrite equation (1) as follows:

$$1 = M - p_1 p_2 \cdots p_m. \tag{2}$$

We have proved $p_j \mid M$, and since p_j is one of the prime factors of $p_1 p_2 \cdots p_m$, we can also conclude that $p_j \mid (p_1 p_2 \cdots p_m)$. Since p_j divides both of the terms on the right side of equation (2), we can use this equation to conclude that p_j divides 1. This is a contradiction since a prime number is greater than 1 and cannot divide 1. Hence, our assumption that there are only finitely many primes is false, and so there must be infinitely many primes. ■

2. The Distribution of Prime Numbers

There are infinitely many primes, but when we write a list of the prime numbers, we can see some long sequences of consecutive natural numbers that contain no prime numbers. For example, there are no prime numbers between 113 and 127. The following theorem shows that there exist arbitrarily long sequences of consecutive natural numbers containing no prime numbers. A guided proof of this theorem is included in Exercise (15).

Theorem 8.17. *For any natural number n, there exist at least n consecutive natural numbers that are composite numbers.*

There are many unanswered questions about prime numbers, two of which will now be discussed.

3. The Twin Prime Conjecture

By looking at the list of the first 25 prime numbers, we see several cases where consecutive prime numbers differ by 2. Examples are: 3 and 5; 11 and 13; 17 and 19; 29 and 31. Such pairs of prime numbers are said to be **twin primes**. How many twin primes exist? The answer is not known. The **Twin Prime Conjecture** states that there are infinitely many twin primes. As of June 25, 2010, this is still a conjecture as it has not been proved or disproved.

For some interesting information on prime numbers, visit the Web site *The Prime Pages* (http://primes.utm.edu/), where there is a link to The Largest Known Primes Web site. According to information at this site as of June 25, 2010, the largest known twin primes are

$$\left(65516468355 \times 2^{333333} - 1\right) \text{ and } \left(65516468355 \times 2^{333333} + 1\right).$$

Each of these prime numbers contains 100355 digits.

4. Goldbach's Conjecture

Given an even natural number, is it possible to write it as a sum of two prime numbers? For example,

$$4 = 2 + 2 \qquad 6 = 3 + 3 \qquad 8 = 5 + 3$$
$$78 = 37 + 41 \qquad 90 = 43 + 47 \qquad 138 = 67 + 71$$

One of the most famous unsolved problems in mathematics is a conjecture made by Christian Goldbach in a letter to Leonhard Euler in 1742. The conjecture, now known as **Goldbach's Conjecture**, is as follows:

> Every even integer greater than 2 can be expressed as the sum of two (not necessarily distinct) prime numbers.

As of June 25, 2010, it is not known if this conjecture is true or false, although most mathematicians believe it to be true.

Exercises 8.2

⋆ **1.** Prove the second and third parts of Theorem 8.11.

(**a**) Let a be a nonzero integer, and let p be a prime number. If $p \mid a$, then $\gcd(a, p) = p$.

(**b**) Let a be a nonzero integer, and let p be a prime number. If p does not divide a, then $\gcd(a, p) = 1$.

⋆ **2.** Prove the first part of Corollary 8.14.

Let $a, b \in \mathbb{Z}$, and let p be a prime number. If $p \mid (ab)$, then $p \mid a$ or $p \mid b$. **Hint**: Consider two cases: (1) $p \mid a$; and (2) p does not divide a.

⋆ **3.** Use mathematical induction to prove the second part of Corollary 8.14.

Let p be a prime number, let $n \in \mathbb{N}$, and let $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. If $p \mid (a_1 a_2 \cdots a_n)$, then there exists a $k \in \mathbb{N}$ with $1 \leq k \leq n$ such that $p \mid a_k$.

⋆ **4.** (**a**) Let a and b be nonzero integers. If there exist integers x and y such that $ax + by = 1$, what conclusion can be made about $\gcd(a, b)$? Explain.

(**b**) Let a and b be nonzero integers. If there exist integers x and y such that $ax + by = 2$, what conclusion can be made about $\gcd(a, b)$? Explain.

5. (**a**) Let $a \in \mathbb{Z}$. What is $\gcd(a, a + 1)$? That is, what is the greatest common divisor of two consecutive integers? Justify your conclusion.

Hint: Exercise (4) might be helpful.

(**b**) Let $a \in \mathbb{Z}$. What conclusion can be made about $\gcd(a, a + 2)$? That is, what conclusion can be made about the greatest common divisor of two integers that differ by 2? Justify your conclusion.

6. (**a**) Let $a \in \mathbb{Z}$. What conclusion can be made about $\gcd(a, a + 3)$? That is, what conclusion can be made about the greatest common divisor of two integers that differ by 3? Justify your conclusion.

(**b**) Let $a \in \mathbb{Z}$. What conclusion can be made about $\gcd(a, a + 4)$? That is, what conclusion can be made about the greatest common divisor of two integers that differ by 4? Justify your conclusion.

7. ⋆ (**a**) Let $a = 16$ and $b = 28$. Determine the value of $d = \gcd(a, b)$, and then determine the value of $\gcd\left(\frac{a}{d}, \frac{b}{d}\right)$.

⋆ (**b**) Repeat Exercise (7a) with $a = 10$ and $b = 45$.

(c) Let $a, b \in \mathbb{Z}$, not both equal to 0, and let $d = \gcd(a, b)$. Explain why $\frac{a}{d}$ and $\frac{b}{d}$ are integers. Then prove that $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. **Hint**: Start by writing d as a linear combination of a and b.

This says that if you divide both a and b by their greatest common divisor, the result will be two relatively prime integers.

8. Are the following propositions true or false? Justify your conclusions.

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

(b) For all integers $a, b,$ and c, if $a \mid c$, $b \mid c$ and $\gcd(a, b) = 1$, then $(ab) \mid c$.

⋆ **9.** In Exercise (17) in Section 3.5, it was proved that if n is an odd integer, then $8 \mid (n^2 - 1)$. (This result was also proved in Exercise (19) in Section 7.4.) Now, prove the following proposition:

If n is an odd integer and 3 does not divide n, then $24 \mid (n^2 - 1)$.

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

For all $a, b, c \in \mathbb{Z}$, $\gcd(a, bc) = 1$ if and only if $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$.

(b) Use mathematical induction to prove the following proposition:

Let $n \in \mathbb{N}$ and let $a, b_1, b_2, \ldots, b_n \in \mathbb{Z}$. If $\gcd(a, b_i) = 1$ for all $i \in \mathbb{N}$ with $1 \leq i \leq n$, then $\gcd(a, b_1 b_2 \cdots b_n) = 1$.

⋆ **11.** Is the following proposition true or false? Justify your conclusion.

For all integers $a, b,$ and c, if $\gcd(a, b) = 1$ and $c \mid (a + b)$, then $\gcd(a, c) = 1$ and $\gcd(b, c) = 1$.

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

If $n \in \mathbb{N}$, then $\gcd(5n + 2, 12n + 5) = 1$.

13. Let $y \in \mathbb{N}$. Use the Fundamental Theorem of Arithmetic to prove that there exists an odd natural number x and a nonnegative integer k such that $y = 2^k x$.

14. **(a)** Determine five different primes that are congruent to 3 modulo 4.

(b) Prove that there are infinitely many primes that are congruent to 3 modulo 4.

15. **(a)** Let $n \in \mathbb{N}$. Prove that 2 divides $[(n + 1)! + 2]$.

(**b**) Let $n \in \mathbb{N}$ with $n \geq 2$. Prove that 3 divides $[(n+1)! + 3]$.

(**c**) Let $n \in \mathbb{N}$. Prove that for each $k \in \mathbb{N}$ with $2 \leq k \leq (n+1)$, k divides $[(n+1)! + k]$.

(**d**) Use the result of Exercise (15c) to prove that for each $n \in \mathbb{N}$, there exist at least n consecutive composite natural numbers.

16. The Twin Prime Conjecture states that there are infinitely many twin primes, but it is not known if this conjecture is true or false. The answers to the following questions, however, can be determined.

(**a**) How many pairs of primes p and q exist where $q - p = 3$? That is, how many pairs of primes are there that differ by 3? Prove that your answer is correct. (One such pair is 2 and 5.)

(**b**) How many triplets of primes of the form p, $p+2$, and $p+4$ are there? That is, how many triplets of primes exist where each prime is 2 more than the preceding prime? Prove that your answer is correct. Notice that one such triplet is 3, 5, and 7.

Hint: Try setting up cases using congruence modulo 3.

17. Prove the following proposition:

Let $n \in \mathbb{N}$. For each $a \in \mathbb{Z}$, if $\gcd(a, n) = 1$, then for every $b \in \mathbb{Z}$, there exists an $x \in \mathbb{Z}$ such that $ax \equiv b \pmod{n}$.

Hint: One way is to start by writing 1 as a linear combination of a and n.

18. Prove the following proposition:

For all natural numbers m and n, if m and n are twin primes other than the pair 3 and 5, then 36 divides $mn+1$ and $mn+1$ is a perfect square.

Hint: Look at several examples of twin primes. What do you notice about the number that is between the two twin primes? Set up cases based on this observation.

Explorations and Activities

19. Square Roots and Irrational Numbers. In Chapter 3, we proved that some square roots (such as $\sqrt{2}$ and $\sqrt{3}$) are irrational numbers. In this activity, we will use the Fundamental Theorem of Arithmetic to prove that if a natural number is not a perfect square, then its square root is an irrational number.

(**a**) Let n be a natural number. Use the Fundamental Theorem of Arithmetic to explain why if n is composite, then there exist prime numbers $p_1, p_2, \ldots, p_r$ and natural numbers $\alpha_1, \alpha_2, \ldots, \alpha_r$ such that

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}. \tag{1}$$

Then, if we use $r = 1$ and $\alpha_1 = 1$ for a prime number, explain why we can write any natural number in the form given in equation (1).

(**b**) A natural number b is a **perfect square** if and only if there exists a natural number a such that $b = a^2$. Explain why 36, 400, and 15876 are perfect squares. Then determine the prime factorization of these perfect squares. What do you notice about these prime factorizations?

(**c**) Let n be a natural number written in the form given in equation (1) in part (a). Prove that n is a perfect square if and only if for each natural number k with $1 \leq k \leq r$, α_k is even.

(**d**) Prove that for all natural numbers n, if n is not a perfect square, then $\sqrt{n}$ is an irrational number. **Hint**: Use a proof by contradiction.

8.3 Linear Diophantine Equations

Preview Activity 1 (Integer Solutions for Linear Equations in One Variable)

1. Does the linear equation $6x = 42$ have a solutions that is an integer? Explain.

2. Does the linear equation $7x = -21$ have a solution that is an integer? Explain.

3. Does the linear equation $4x = 9$ have a solution that is an integer? Explain.

4. Does the linear equation $-3x = 20$ have a solution that is an integer? Explain.

5. Prove the following theorem:

Theorem 8.18. *Let $a, b \in \mathbb{Z}$ with $a \neq 0$.*

- *If a divides b, then the equation $ax = b$ has exactly one solution that is an integer.*

- *If a does not divide b, then the equation $ax = b$ has no solution that is an integer.*

Preview Activity 2 (Linear Equations in Two Variables)

1. Find integers x and y so that $2x + 6y = 25$ or explain why it is not possible to find such a pair of integers.

2. Find integers x and y so that $6x - 9y = 100$ or explain why it is not possible to find such a pair of integers.

3. Notice that $x = 2$ and $y = 1$ is a solution of the equation $3x + 5y = 11$, and that $x = 7$ and $y = -2$ is also a solution of the equation $3x + 5y = 11$.

(**a**) Find two pairs of integers x and y so that $x > 7$ and $3x + 5y = 11$. (Try to keep the integer values of x as small as possible.)

(**b**) Find two pairs of integers x and y so that $x < 2$ and $3x + 5y = 11$. (Try to keep the integer values of x as close to 2 as possible.)

(**c**) Determine formulas (one for x and one for y) that will generate pairs of integers x and y so that $3x + 5y = 11$.

Hint: The two formulas can be written in the form $x = 2 + km$ and $y = 1 + kn$, where k is an arbitrary integer and m and n are specific integers.

4. Notice that $x = 4$ and $y = 0$ is a solution of the equation $4x + 6y = 16$, and that $x = 7$ and $y = -2$ is a solution of the equation $4x + 6y = 16$.

(**a**) Find two pairs of integers x and y so that $x > 7$ and $4x + 6y = 16$. (Try to keep the integer values of x as small as possible.)

(**b**) Find twopairs of integers x and y so that $x < 4$ and $4x + 6y = 16$. (Try to keep the integer values of x as close to 4 as possible.)

(**c**) Determine formulas (one for x and one for y) that will generate pairs of integers x and y so that $4x + 6y = 16$.

Hint: The two formulas can be written in the form $x = 4 + km$ and $y = 0 + kn$, where k is an arbitrary integer and $m$and n are specific integers.

In the two preview activities, we were interested only in integer solutions for certain equations. In such instances, we give the equation a special name.

Definition. An equation whose solutions are required to be integers is called a **Diophantine equation**.

Diophantine equations are named in honor of the Greek mathematician Diophantus of Alexandria (circa 300 C.E.). Very little is known about Diophantus' life except that he probably lived in Alexandria in the early part of the fourth century C.E. and was probably the first to use letters for unknown quantities in arithmetic problems. His most famous work, *Arithmetica*, consists of approximately 130 problems and their solutions. Most of these problems involved solutions of equations in various numbers of variables. It is interesting to note that Diophantus did not restrict his solutions to the integers but recognized rational number solutions as well. Today, however, the solutions for a so-called Diophantine equation must be integers.

Definition. If a and b are integers with $a \neq 0$, then the equation $ax = b$ is a **linear Diophantine equation in one variable**.

Theorem 8.18 in Preview Activity 1 provides us with results that allows us to determine which linear diophantine equations in one variable have solutions and which ones do not have a solution.

A linear Diophantine equation in two variables can be defined in a manner similar to the definition for a linear Diophantine equation in one variable.

Definition. Let a, b, and c be integers with $a \neq 0$ and $b \neq 0$. The Diophantine equation $ax + by = c$ is called a **linear Diophantine equation in two variables**.

The equations that were investigated in Preview Activity 2 were linear Diophantine equations in two variables. The problem of determining all the solutions of a linear Diophantine equation has been completely solved. Before stating the general result, we will provide a few more examples.

Example 8.19 (A Linear Diophantine Equation in Two Variables)
The following example is similar to the examples studied in Preview Activity 2.

We can use substitution to verify that $x = 2$ and $y = -1$ is a solution of the linear Diophantine equation

$$4x + 3y = 5.$$

The following table shows other solutions of this Diophantine equation.

x	y
2	-1
5	-5
8	-9
11	-13

x	y
-1	3
-4	7
-7	11
-10	15

It would be nice to determine the pattern that these solutions exhibit. If we consider the solution $x = 2$ and $y = -1$ to be the "starting point," then we can see that the other solutions are obtained by adding 3 to x and subtracting 4 from y in the previous solution. So we can write these solutions to the equation as

$$x = 2 + 3k \qquad \text{and} \qquad y = -1 - 4k,$$

where k is an integer. We can use substitution and algebra to verify that these expressions for x and y give solutions of this equation as follows:

$$\begin{aligned} 4x + 3y &= 4(2 + 3k) + 3(-1 - 4k) \\ &= (8 + 12k) + (-3 - 12k) \\ &= 5. \end{aligned}$$

We should note that we have not yet proved that these solutions are all of the solutions of the Diophantine equation $4x + 3y = 5$. This will be done later.

If the general form for a linear Diophantine equation is $ax + by = c$, then for this example, $a = 4$ and $b = 3$. Notice that for this equation, we started with one solution and obtained other solutions by adding $b = 3$ to x and subtracting $a = 4$ from y in the previous solution. Also, notice that $\gcd(3, 4) = 1$.

Progress Check 8.20 (An Example of a Linear Diophantine Equation)

1. Verify that the following table shows some solutions of the linear Diophantine equation $6x + 9y = 12$.

x	y
2	0
5	-2
8	-4
11	-6

x	y
-1	2
-4	4
-7	6
-10	8

2. Follow the pattern in this table to determine formulas for x and y that will generate integer solutions of the equation $6x + 9y = 12$. Verify that the formulas actually produce solutions for the equation $6x + 9y = 12$.

Progress Check 8.21 (Revisiting Preview Activity 2)
Do the solutions for the linear Diophantine equations in Preview Activity 2 show the same type of pattern as the solutions for the linear Diophantine equations in Example 8.19 and Progress Check 8.20? Explain.

The solutions for the linear Diophantine equations in Preview Activity 2, Example 8.19, and Progress Check 8.20 provide examples for the second part of Theorem 8.22.

Theorem 8.22. *Let a, b, and c be integers with $a \neq 0$ and $b \neq 0$, and let $d = \gcd(a, b)$.*

1. *If d does not divide c, then the linear Diophantine equation $ax + by = c$ has no solution.*
2. *If d divides c, then the linear Diophantine equation $ax + by = c$ has infinitely many solutions. In addition, if (x_0, y_0) is a particular solution of this equation, then all the solutions of this equation can be written in the form*

$$x = x_0 + \frac{b}{d}k \quad \text{and} \quad y = y_0 - \frac{a}{d}k,$$

for some integer k.

Proof. The proof of Part (1) is Exercise (1). For Part (2), we let a, b, and c be integers with $a \neq 0$ and $b \neq 0$, and let $d = \gcd(a, b)$. We also assume that $d \mid c$. Since $d = \gcd(a, b)$, Theorem 8.8 tells us that d is a linear combination of a and b. So there exist integers s and t such that

$$d = as + bt. \tag{1}$$

Since $d \mid c$, there exists an integer m such that $c = dm$. We can now multiply both sides of equation (1) by m and obtain

$$\begin{aligned} dm &= (as + bt)m \\ c &= a(sm) + b(tm). \end{aligned}$$

This means that $x = sm$, $y = tm$ is a solution of $ax + by = c$, and we have proved that the Diophantine equation $ax + by = c$ has at least one solution.

Now let $x = x_0$, $y = y_0$ be any particular solution of $ax + by = c$, let $k \in \mathbb{Z}$, and let

$$x = x_0 + \frac{b}{d}k \qquad y = y_0 - \frac{a}{d}k. \tag{2}$$

We now verify that for each $k \in \mathbb{Z}$, the equations in (2) produce a solution of $ax + by = c$.

$$\begin{aligned} ax + by &= a\left(x_0 + \frac{b}{d}k\right) + b\left(y_0 - \frac{a}{d}k\right) \\ &= ax_0 + \frac{ab}{d}k + by_0 - \frac{ab}{d}k \\ &= ax_0 + by_0 \\ &= c. \end{aligned}$$

This proves that the Diophantine equation $ax + by = c$ has infinitely many solutions.

We now show that every solution of this equation can be written in the form described in (2). So suppose that x and y are integers such that $ax + by = c$. Then

$$(ax + by) - (ax_0 + by_0) = c - c = 0,$$

and this equation can be rewritten in the following form:

$$a(x - x_0) = b(y_0 - y). \tag{3}$$

Dividing both sides of this equation by d, we obtain

$$\left(\frac{a}{d}\right)(x - x_0) = \left(\frac{b}{d}\right)(y_0 - y).$$

This implies that

$$\frac{a}{d} \text{ divides } \left(\frac{b}{d}\right)(y_0 - y).$$

However, by Exercise (7) in Section 8.2, $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, and so by Theorem 8.12, we can conclude that $\frac{a}{d}$ divides $(y_0 - y)$. This means that there exists an integer k such that $y_0 - y = \frac{a}{d}k$, and solving for y gives

$$y = y_0 - \frac{a}{d}k.$$

Substituting this value for y in equation (3) and solving for x yields

$$x = x_0 + \frac{b}{d}k.$$

This proves that every solution of the Diophantine equation $ax + by = c$ can be written in the form prescribed in (2). ■

The proof of the following corollary to Theorem 8.22 is Exercise (2).

Corollary 8.23. *Let a, b, and c be integers with $a \neq 0$ and $b \neq 0$. If a and b are relatively prime, then the linear Diophantine equation $ax + by = c$ has infinitely many solutions. In addition, if x_0, y_0 is a particular solution of this equation, then all the solutions of the equation are given by*

$$x = x_0 + bk \qquad y = y_0 - ak$$

where $k \in \mathbb{Z}$.

Progress Check 8.24 (Linear Diophantine Equations)

1. Use the Euclidean Algorithm to verify that $\gcd(63, 336) = 21$. What conclusion can be made about linear Diophantine equation $63x + 336y = 40$ using Theorem 8.22? If this Diophantine equation has solutions, write formulas that will generate the solutions.

2. Use the Euclidean Algorithm to verify that $\gcd(144, 225) = 9$. What conclusion can be made about linear Diophantine equation $144x + 225y = 27$ using Theorem 8.22? If this Diophantine equation has solutions, write formulas that will generate the solutions.

Exercises 8.3

1. Prove Part (1) of Theorem 8.22:

   Let a, b, and c be integers with $a \neq 0$ and $b \neq 0$, and let $d = \gcd(a, b)$. If d does not divide c, then the linear Diophantine equation $ax + by = c$ has no solution.

2. Prove Corollary 8.23.

   Let a, b, and c be integers with $a \neq 0$ and $b \neq 0$. If a and b are relatively prime, then the linear Diophantine equation $ax + by = c$ has infinitely many solutions. In addition, if (x_0, y_0) is a particular solution of this equation, then all the solutions of the equation are given by

   $$x = x_0 + bk \qquad y = y_0 - ak,$$

   where $k \in \mathbb{Z}$.

3. Determine all solutions of the following linear Diophantine equations.

⋆ **(a)** $9x + 14y = 1$

⋆ **(b)** $18x + 22y = 4$

⋆ **(c)** $48x - 18y = 15$

⋆ **(d)** $12x + 9y = 6$

(e) $200x + 49y = 10$

(f) $200x + 54y = 21$

(g) $10x - 7y = 31$

(h) $12x + 18y = 6$

⋆ **4.** A certain rare artifact is supposed to weigh exactly 25 grams. Suppose that you have an accurate balance scale and 500 each of 27 gram weights and 50 gram weights. Explain how to use Theorem 8.22 to devise a plan to check the weight of this artifact.

Hint: Notice that $\gcd(50, 27) = 1$. Start by writing 1 as a linear combination of 50 and 27.

⋆ **5.** On the night of a certain banquet, a caterer offered the choice of two dinners, a steak dinner for \$25 and a vegetarian dinner for \$16. At the end of the evening, the caterer presented the host with a bill (before tax and tips) for \$1461. What is the minimum number of people who could have attended the banquet? What is the maximum number of people who could have attended the banquet?

6. The goal of this exercise is to determine all (integer) solutions of the linear Diophantine equation in three variables $12x_1 + 9x_2 + 16x_3 = 20$.

⋆ **(a)** First, notice that $\gcd(12, 9) = 3$. Determine formulas that will generate all solutions for the linear Diophantine equation $3y + 16x_3 = 20$.

⋆ **(b)** Explain why the solutions (for x_1 and x_2) of the Diophantine equation $12x_1 + 9x_2 = 3y$ can be used to generate solutions for $12x_1 + 9x_2 + 16x_3 = 20$.

⋆ **(c)** Use the general value for y from Exercise (6a) to determine the solutions of $12x_1 + 9x_2 = 3y$.

(d) Use the results from Exercises (6a) and (6c) to determine formulas that will generate all solutions for the Diophantine equation $12x_1 + 9x_2 + 16x_3 = 20$.

Note: These formulas will involve two arbitrary integer parameters. Substitute specific values for these integers and then check the resulting solution in the original equation. Repeat this at least three times.

(e) Check the general solution for $12x_1 + 9x_2 + 16x_3 = 20$ from Exercise (6d).

7. Use the method suggested in Exercise (6) to determine formulas that will generate all solutions of the Diophantine equation $8x_1 + 4x_2 - 6x_3 = 6$. Check the general solution.

8. Explain why the Diophantine equation $24x_1 - 18x_2 + 60x_3 = 21$ has no solution.

9. The purpose of this exercise will be to prove that the nonlinear Diophantine equation $3x^2 - y^2 = -2$ has no solution.

(**a**) Explain why if there is a solution of the Diophantine equation $3x^2 - y^2 = -2$, then that solution must also be a solution of the congruence $3x^2 - y^2 \equiv -2 \pmod 3$.

(**b**) If there is a solution to the congruence $3x^2 - y^2 \equiv -2 \pmod 3$, explain why there then must be an integer y such that $y^2 \equiv 2 \pmod 3$.

(**c**) Use a proof by contradiction to prove that the Diophantine equation $3x^2 - y^2 = -2$ has no solution.

10. Use the method suggested in Exercise (9) to prove that the Diophantine equation $7x^2 + 2 = y^3$ has no solution.

Explorations and Activities

11. Linear Congruences in One Variable. Let n be a natural number and let $a, b \in \mathbb{Z}$ with $a \neq 0$. A congruence of the form $ax \equiv b \pmod n$ is called a **linear congruence in one variable**. This is called a linear congruence since the variable x occurs to the first power.

A **solution of a linear congruence in one variable** is defined similarly to the solution of an equation. A solution is an integer that makes the resulting congruence true when the integer is substituted for the variable x. For example,

- The integer $x = 3$ is a solution for the congruence $2x \equiv 1 \pmod 5$ since $2 \cdot 3 \equiv 1 \pmod 5$ is a true congruence.
- The integer $x = 7$ is not a solution for the congruence $3x \equiv 1 \pmod 6$ since $3 \cdot 7 \equiv 1 \pmod 6$ is a not a true congruence.

(**a**) Verify that $x = 2$ and $x = 5$ are the only solutions the linear congruence $4x \equiv 2 \pmod 6$ with $0 \leq x < 6$.

(**b**) Show that the linear congruence $4x \equiv 3 \pmod 6$ has no solutions with $0 \leq x < 6$.

(**c**) Determine all solutions of the linear congruence $3x \equiv 7 \pmod 8$ with $0 \leq x < 8$.

The following parts of this activity show that we can use the results of Theorem 8.22 to help find all solutions of the linear congruence $6x \equiv 4 \pmod 8$.

(**d**) Verify that $x = 2$ and $x = 6$ are the only solutions for the linear congruence $6x \equiv 4 \pmod 8$ with $0 \leq x < 8$.

(**e**) Use the definition of "congruence" to rewrite the congruence $6x \equiv 4 \pmod 8$ in terms of "divides."

(**f**) Use the definition of "divides" to rewrite the result in part (11e) in the form of an equation. (An existential quantifier must be used.)

(**g**) Use the results of parts (11d) and (11f) to write an equation that will generate all the solutions of the linear congruence $6x \equiv 4 \pmod 8$.

Hint: Use Theorem 8.22. This can be used to generate solutions for x and the variable introduced in part (11f). In this case, we are interested only in the solutions for x.

Now let n be a natural number and let $a, c \in \mathbb{Z}$ with $a \neq 0$. A general linear congruence of the form $ax \equiv c \pmod n$ can be handled in the same way that we handled in $6x \equiv 4 \pmod 8$.

(**h**) Use the definition of "congruence" to rewrite $ax \equiv c \pmod n$ in terms of "divides."

(**i**) Use the definition of "divides" to rewrite the result in part (11h) in the form of an equation. (An existential quantifier must be used.)

(**j**) Let $d = \gcd(a, n)$. State and prove a theorem about the solutions of the linear congruence $ax \equiv c \pmod n$ in the case where d does not divide c.

Hint: Use Theorem 8.22.

(**k**) Let $d = \gcd(a, n)$. State and prove a theorem about the solutions of the linear congruence $ax \equiv c \pmod n$ in the case where d divides c.

8.4 Chapter 8 Summary

Important Definitions

- Greatest common divisor of two integers, page 414
- Linear combination of two integers, page 423
- Prime number, page 426
- Composite number, page 426
- Prime factorization, page 427
- Relatively prime integers, page 428
- Diophantine equation, page 441
- Linear Diophantine equation in two variables, page 441

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

- **Theorem 8.3**. *Let a and b be integers with $a \neq 0$ and $b > 0$. Then* $\gcd(a, b)$ *is the only natural number d such that*

  (a) *d divides a,*

  (b) *d divides b, and*

  (c) *if k is an integer that divides both a and b, then k divides d.*

- **Theorem 8.8**. *Let a and b be integers, not both 0. Then* $\gcd(a, b)$ *can be written as a linear combination of a and b. That is, there exist integers u and v such that* $\gcd(a, b) = au + bv$.

- **Theorem 8.9**.

  1. *The greatest common divisor, d, is a linear combination of a and b. That is, there exist integers m and n such that $d = am + bn$.*
  2. *The greatest common divisor, d, divides every linear combination of a and b. That is, for all $x, y \in \mathbb{Z}$, $d \mid (ax + by)$.*
  3. *The greatest common divisor, d, is the smallest positive number that is a linear combination of a and b.*

- **Theorem 8.11**. *Let a and b be nonzero integers, and let p be a prime number.*

  1. *If a and b are relatively prime, then there exist integers m and n such that $am + bn = 1$. That is, 1 can be written as linear combination of a and b.*
  2. *If $p \mid a$, then $\gcd(a, p) = p$.*
  3. *If p does not divide a, then $\gcd(a, p) = 1$.*

- **Theorem 8.12** *Let a, b, and c be integers. If a and b are relatively prime and $a \mid (bc)$, then $a \mid c$.*

- **Corollary 8.14**

  1. *Let $a, b \in \mathbb{Z}$, and let p be a prime number. If $p \mid (ab)$, then $p \mid a$ or $p \mid b$.*
  2. *Let p be a prime number, let $n \in \mathbb{N}$, and let $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. If $p \mid (a_1 a_2 \cdots a_n)$, then there exists a natural number k with $1 \leq k \leq n$ such that $p \mid a_k$.*

- **Theorem 8.15, The Fundamental Theorem of Arithmetic**

  1. *Each natural number greater than 1 is either a prime number or is a product of prime numbers.*
  2. *Let $n \in \mathbb{N}$ with $n > 1$. Assume that*

     $$n = p_1 p_2 \cdots p_r \text{ and that } n = q_1 q_2 \cdots q_s,$$

     where $p_1, p_2, \cdots p_r$ and $q_1, q_2, \cdots q_s$ are primes with $p_1 \leq p_2 \leq \cdots \leq p_r$ and $q_1 \leq q_2 \leq \cdots \leq q_s$. Then $r = s$, and for each j from 1 to r, $p_j = q_j$.

- **Theorem 8.16**. *There are infinitely many prime numbers.*

- **Theorem 8.22**. *Let a, b, and c be integers with $a \neq 0$ and $b \neq 0$, and let $d = gcd(a, b)$.*

  1. *If d does not divide c, then the linear Diophantine equation $ax + by = c$ has no solution.*

2. *If d divides c, then the linear Diophantine equation $ax + by = c$ has infinitely many solutions. In addition, if (x_0, y_0) is a particular solution of this equation, then all the solutions of the equation are given by*

$$x = x_0 + \frac{b}{d}k \quad \text{and} \quad y = y_0 - \frac{a}{d}k,$$

where $k \in \mathbb{Z}$.

- **Corollary 8.23**. *Let a, b, and c be integers with $a \neq 0$ and $b \neq 0$. If a and b are relatively prime, then the linear Diophantine equation $ax + by = c$ has infinitely many solutions. In addition, if x_0, y_0 is a particular solution of this equation, then all the solutions of the equation are given by*

$$x = x_0 + bk \quad \text{and} \quad y = y_0 - ak,$$

where $k \in \mathbb{Z}$.