Chapter 1

INTEGERS

In this chapter we will develop some of the properties of the set of integers

$$\mathbf{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

that are needed in our later work. The use of $\mathbf{Z}$ for the integers reflects the strong German influence on the modern development of algebra; $\mathbf{Z}$ comes from the German word for numbers, "Zahlen." Some of the computational techniques we study here will reappear numerous times in later chapters. Furthermore, we will construct some concrete examples that will serve as important building blocks for later work on groups, rings, and fields.

To give a simple illustration of how we will use elementary number theory, consider the matrix $A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$. The powers of A are $A^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$, $A^3 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, $A^4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $A^5 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, etc. Since A^4 is the identity matrix I, the powers begin to repeat at A^5, as we can see by writing

$$\begin{aligned} A^5 &= A^4A = IA = A, \\ A^6 &= A^4A^2 = IA^2 = A^2, \\ A^7 &= A^4A^3 = IA^3 = A^3, \qquad \text{etc.} \end{aligned}$$

How can we find A^{231}, for example? If we divide 231 by 4, we get 57, with remainder 3, so $231 = 4 \cdot 57 + 3$. This provides our answer, since

$$A^{231} = A^{4\cdot 57+3} = A^{4\cdot 57}A^3 = (A^4)^{57}A^3 = I^{57}A^3 = IA^3 = A^3 .$$

We can see that two powers A^j and A^k are equal precisely when j and k differ by a multiple of 4. Altogether there are only the following four powers:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

A very similar situation occurs when we analyze the positive powers of the complex number i. We have $i^1 = i$, $i^2 = -1$, $i^3 = -i$, and $i^4 = 1$. As before, we see that $i^j = i^k$ if and only if j and k differ by a multiple of 4.

As a slightly different example, consider the positive powers of the complex number

$$\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i \, .$$

There are only three distinct powers of ω, as shown below:

$$\begin{aligned}
\omega &= -\frac{1}{2} + \frac{\sqrt{3}}{2}i \, , \\
\omega^2 &= \left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)\left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right) = \frac{1}{4} - \frac{2\sqrt{3}}{4}i + \frac{3}{4}i^2 = -\frac{1}{2} - \frac{\sqrt{3}}{2}i \, , \\
\omega^3 &= \omega^2\omega = \left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i\right)\left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right) = \frac{1}{4} - \frac{3}{4}i^2 = 1 \, .
\end{aligned}$$

From this point on, the positive powers begin to repeat, and $\omega^j = \omega^k$ if and only if j and k differ by a multiple of 3.

To give a unified approach to situations analogous to the ones above, in which we need to consider numbers that exhibit similar behavior when they differ by a multiple of a number n, we will develop the notion of congruence modulo n. The notion of a congruence class will enable us to think of the collection of numbers that behave in the same way as a single entity. The simplest example is congruence modulo 2. When we consider two numbers to be similar if they differ by a multiple of 2, we are just saying that the two numbers are similar if they have the same parity (both are even, or both are odd). Another familiar situation of this type occurs when telling time, since on a clock we do not distinguish between times that differ by a multiple of 12 (or 24 if you are in Europe or the military).

In this chapter we will develop only enough number theory to be of use in later chapters, when we study groups, rings, and fields. Historically, almost all civilizations have developed the integers (at least the positive ones) for use in agriculture, commerce, etc. After the elementary operations (addition, subtraction, multiplication, and division) have been understood, human curiosity has taken over and individuals have begun to look for deeper properties that the integers may possess.

Nonmathematicians are often surprised that research is currently being done in mathematics. They seem to believe that all possible questions have already been answered. At this point an analogy may be useful. Think of all that is known as being contained in a ball. Adding knowledge enlarges the ball, and this means that the surface of the ball—the interface between known and unknown where research occurs—also becomes larger. In short, the more we know, the more questions there are to ask. In number theory, perhaps more than in any other branch of mathematics,

there are still many unanswered questions that can easily be posed. In fact, it seems that often the simplest sounding questions require the deepest tools to resolve.

One aspect of number theory that has particular applications in algebra is the one that concerns itself with questions of divisibility and primality. Fortunately for our study of algebra, this part of number theory is easily accessible, and it is with these properties of integers that we will deal in this chapter. Number theory got its start with Euclid and much of what we do in the first two sections appears in his book *Elements*.

Our approach to number theory will be to study it as a tool for later use. In the notes at the end of this chapter, we mention several important problems with which number theorists are concerned. You can read the notes at this point, before studying the material in the chapter. In fact, we suggest that you read them now, because we hope to indicate why number theory is so interesting in its own right.

1.1 Divisors

Obviously, at the beginning of the book we must decide where to start mathematically. We would like to give a careful mathematical development, including proofs of virtually everything we cover. However, that would take us farther into the foundations of mathematics than we believe is profitable in a beginning course in abstract algebra. As a compromise, we have chosen to assume a knowledge of basic set theory and some familiarity with the set of integers.

For the student who is concerned about how the integers can be described formally and how the basic properties of the integers can be deduced, we have provided some very sketchy information in the appendix. Even there we have taken a naive approach, rather than formally treating the basic notions of set theory as undefined terms and giving the axioms that relate them. We have included a list of the Peano postulates, which use concepts and axioms of set theory to characterize the natural numbers. We then give an outline of the logical development of the set of integers, and larger sets of numbers.

In the beginning sections of this chapter we will assume some familiarity with the set of integers, and we will simply take for granted some of the basic arithmetic and order properties of the integers. (These properties should be familiar from elementary school arithmetic. They are listed in detail in Section A.3 of the appendix.) The set $\{0, \pm 1, \pm 2, \ldots\}$ of **integers** will be denoted by $\mathbf{Z}$ throughout the text, while we will use $\mathbf{N}$ for the set $\{0, 1, 2, \ldots\}$ of **natural numbers**.

Our first task is to study divisibility. We will then develop a theory of prime numbers based on our work with greatest common divisors. The fact that exact division is not always possible within the set of integers should not be regarded as a deficiency. Rather, it is one source of the richness of the subject of number theory and leads to many interesting and fundamental propositions about the integers.

1.1.1 Definition. *An integer a is called a* ***multiple*** *of an integer b if $a = bq$ for some integer q. In this case we also say that b is a* ***divisor*** *of a, and we use the notation $b \mid a$.*

In the above case we can also say that b is a **factor** of a, or that a is **divisible** by b. If b is not a divisor of a, meaning that $a \neq bq$ for any $q \in \mathbf{Z}$, then we write $b \nmid a$. The set of all multiples of an integer a will be denoted by $a\mathbf{Z}$.

Be careful when you use the notation $b \mid a$. It describes a relationship between integers a and b and does *not* represent a fraction. Furthermore, a handwritten vertical line $\mid$ can easily be confused with the symbol /. The statement $2 \mid 6$ is a true statement; $6 \mid 2$ is a statement that is false. On the other hand, the equation $6/2 = 3$ is written correctly, since the fraction $6/2$ *does* represent the number 3. We have at least three different uses for a vertical line: for "such that" in the "set-builder" notation $\{ \mid \}$, when talking about the absolute value of a number, and to indicate that one integer is a divisor of another.

We note some elementary facts about divisors. If $a \neq 0$ and $b \mid a$, then $|b| \leq |a|$ since $|b| \leq |b||q| = |a|$ for some nonzero integer q. It follows from this observation that if $b \mid a$ and $a \mid b$, then $|b| = |a|$ and so $b = \pm a$. Therefore, if $b \mid 1$, then since it is always true that $1 \mid b$, we must have $b = \pm 1$.

Note that the only multiple of 0 is 0 itself. On the other hand, for any integer a we have $0 = a \cdot 0$, and thus 0 is a multiple of any integer. With the notation we have introduced, the set of all multiples of 3 is $3\mathbf{Z} = \{0, \pm 3, \pm 6, \pm 9, \ldots\}$. To describe $a\mathbf{Z}$ precisely, we can write

$$a\mathbf{Z} = \{m \in \mathbf{Z} \mid m = aq \text{ for some } q \in \mathbf{Z}\}.$$

Suppose that a is a multiple of b. Then every multiple of a is also a multiple of b, and in fact we can say that a is a multiple of b if and only if every multiple of a is also a multiple of b. In symbols we can write $b \mid a$ if and only if $a\mathbf{Z} \subseteq b\mathbf{Z}$. Exercise 15 asks for a more detailed proof of this statement.

Before we study divisors and multiples of a fixed integer, we need to state an important property of the set of natural numbers, which we will take as an axiom.

1.1.2 Axiom (Well-Ordering Principle). *Every nonempty set of natural numbers contains a smallest element.*

The well-ordering principle is often used in arguments by contradiction. If we want to show that all natural numbers have some property, we argue that if the set of natural numbers not having the property were nonempty, it would have a least member, and then we deduce a contradiction from this, using the particular facts of the situation. The theory of mathematical induction (see Appendix A.4) formalizes that sort of argument.

Let S be a nonempty set of integers that has a lower bound. That is, there is an integer b such that $b \leq n$ for all $n \in S$. If $b \geq 0$, then S is actually a set of natural

numbers, so it contains a smallest element by the well-ordering principle. If $b < 0$, then adding $|b|$ to each integer in S produces a new set T of natural numbers, since $n + |b| \geq 0$ for all $n \in S$. The set T must contain a smallest element, say t, and it is easy to see that $t - |b|$ is the smallest element of S. This allows us to use, if necessary, a somewhat stronger version of the well-ordering principle: every set of integers that is bounded below contains a smallest element.

The first application of the well-ordering principle will be to prove the division algorithm. In familiar terms, the division algorithm states that dividing an integer a by a positive integer b gives a quotient q and nonnegative remainder r, such that r is less than b. You could write this as

$$\frac{a}{b} = q + \frac{r}{b},$$

but since we are studying properties of the set of integers, we will avoid fractions and write this equation in the form

$$a = bq + r.$$

For example, if $a = 29$ and $b = 8$, then

$$29 = 8 \cdot 3 + 5,$$

so the quotient q is 3 and the remainder r is 5. You must be careful when a is a negative number, since the remainder must be nonnegative. Simply changing signs in the previous equation, we have

$$-29 = (8)(-3) + (-5),$$

which does not give an appropriate remainder. Rewriting this in the form

$$-29 = (8)(-4) + 3$$

gives the correct quotient $q = -4$ and remainder $r = 3$.

Solving for r in the equation $a = bq + r$ shows that $r = a - bq$, and that r must be the smallest nonnegative integer that can be written in this form, since $0 \leq r < b$. This observation clarifies the relationship between the quotient and remainder, and forms the basis of our proof that the division algorithm can be deduced from the well-ordering principle. Another way to see this relationship is to notice that you could find the remainder and quotient by repeatedly subtracting b from a and noting that you have the remainder in the required form when you obtain a nonnegative integer less than b.

The next theorem on "long division with remainder" has traditionally been called the "division algorithm".

1.1.3 Theorem (Division Algorithm). *For any integers a and b, with $b > 0$, there exist unique integers q (the **quotient**) and r (the **remainder**) such that*

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

Proof. Consider the set $R = \{a - bq : q \in \mathbf{Z}\}$. The elements of R are the potential remainders, and among these we need to find the smallest nonnegative one. We want to apply the well-ordering principle to the set R^+ of nonnegative integers in R, so we must first show that R^+ is nonempty. Since $b \geq 1$, the number $a - b(-|a|) = a + b \cdot |a|$ is nonnegative and belongs to R^+, so R^+ is nonempty.

Now by the well-ordering principle, R^+ has a smallest element, and we will call this element r. We will show that $a = bq + r$, with $0 \leq r$ and $r < b$. By definition, $r \geq 0$, and since $r \in R^+$, we must have $r = a - bq$ for some integer q. We cannot have $r \geq b$, since if we let $s = r - b$ we would have $s \geq 0$ and $s = a - b(q + 1) \in R^+$. Since $s < r$, this would contradict the way r was defined, and therefore we must have $r < b$. We have now proved the existence of r and q satisfying the conditions $a = bq + r$ and $0 \leq r < b$.

To show that q and r are unique, suppose that we can also write $a = bp + s$ for integers p and s with $0 \leq s < b$. We have $0 \leq r < b$ and $0 \leq s < b$, and this implies that $|s - r| < b$. But $bp + s = bq + r$ and so $s - r = b(q - p)$, which shows that $b \mid (s - r)$. The only way that b can be a divisor of a number with smaller absolute value is if that number is 0, and so we must have $s - r = 0$, or $s = r$. Then $bp = bq$, which implies that $p = q$ since $b > 0$. Thus the quotient and remainder are unique, and we have completed the proof of the theorem. □

Given integers a and b, with $b > 0$, we can use the division algorithm to write $a = bq + r$, with $0 \leq r < b$. Since $b \mid a$ if and only if there exists $q \in \mathbf{Z}$ such that $a = bq$, we see that $b \mid a$ if and only if $r = 0$. This simple observation gives us a useful tool in doing number theoretic proofs. To show that $b \mid a$ we can use the division algorithm to write $a = bq + r$ and then show that $r = 0$. This technique makes its first appearance in the proof of Theorem 1.1.4.

A set of multiples $a\mathbf{Z}$ has the property that the sum or difference of two integers in the set is again in the set, since $aq_1 \pm aq_2 = a(q_1 \pm q_2)$. We say that the set $a\mathbf{Z}$ is **closed under addition and subtraction**. This will prove to be a very important property in our later work. The next theorem shows that this property characterizes sets of multiples, since a nonempty set of integers is closed under addition and subtraction if and only if it is a set of the form $a\mathbf{Z}$, for some nonnegative integer a.

1.1.4 Theorem. *Let I be a nonempty set of integers that is closed under addition and subtraction. Then I either consists of zero alone or else contains a smallest positive element, in which case I consists of all multiples of its smallest positive element.*

Proof. Since I is nonempty, either it consists of 0 alone, or else it contains a nonzero integer a. In the first case we are done. In the second case, if I contains the nonzero integer a, then it must contain the difference $a - a = 0$, and hence the difference $0 - a = -a$, since I is assumed to be closed under subtraction. Now either a or $-a$ is positive, so I contains at least one positive integer. Having shown that the set of positive integers in I is nonempty, we can apply the well-ordering principle to guarantee that it contains a smallest member, say b.

Next we want to show that I is equal to the set $b\mathbf{Z}$ of all multiples of b. To show that $I = b\mathbf{Z}$, we will first show that $b\mathbf{Z} \subseteq I$, and then show that $I \subseteq b\mathbf{Z}$.

Any nonzero multiple of b is given by just adding b (or $-b$) to itself a finite number of times, so since I is closed under addition, it must contain all multiples of b. Thus $b\mathbf{Z} \subseteq I$.

On the other hand, to show that $I \subseteq b\mathbf{Z}$ we must take any element c in I and show that it is a multiple of b, or equivalently, that $b \mid c$. (Now comes the one crucial idea in the proof.) Using the division algorithm we can write $c = bq + r$, for some integers q and r with $0 \leq r < b$. Since I contains bq and is closed under subtraction, it must also contain $r = c - bq$. But this is a contradiction unless $r = 0$, because b was chosen to be the smallest positive integer in I and yet $r < b$ by the division algorithm. We conclude that $r = 0$, and therefore $c = bq$, so $b \mid c$ and we have shown that $I \subseteq b\mathbf{Z}$.

This completes the proof that $I = b\mathbf{Z}$. □

One of the main goals of Chapter 1 is to develop some properties of prime numbers, which we will do in Section 1.2. Before discussing prime numbers themselves, we will introduce the notion of relatively prime numbers, and this definition in turn depends on the notion of the greatest common divisor of two numbers. Our definition of the greatest common divisor is given in terms of divisibility, rather than in terms of size, since it is this form that is most useful in writing proofs. Exercise 20 gives an equivalent formulation that focuses on size.

1.1.5 Definition. *Let a and b be integers, not both zero. A positive integer d is called the* ***greatest common divisor*** *of a and b if*

(i) *d is a divisor of both a and b, and*

(ii) *any divisor of both a and b is also a divisor of d.*

The greatest common divisor of a and b will be denoted by $\gcd(a, b)$ *or* (a, b).

Our first observation is that $\gcd(0, 0)$ is undefined, but if a is any nonzero integer, then $\gcd(a, 0)$ is defined and equal to $|a|$. The definition of the greatest common divisor can be shortened by using our notation for divisors. If a and b are integers, not both zero, and d is a positive integer, then $d = \gcd(a, b)$ if

(i) $d \mid a$ and $d \mid b$, and

(ii) if $c \mid a$ and $c \mid b$, then $c \mid d$.

The fact that we have written down a definition of the greatest common divisor does not guarantee that there is such a number. Furthermore, the use of the word "the" has to be justified, since it implies that there can be only one greatest common divisor. The next theorem will guarantee the existence of the greatest common divisor, and the question of uniqueness is easily answered: if d_1 and d_2 are greatest common divisors of a and b, then the definition requires that $d_1 \mid d_2$ and $d_2 \mid d_1$, so $d_1 = \pm d_2$. Since both d_1 and d_2 are positive, we have $d_1 = d_2$.

If a and b are integers, then we will refer to any integer of the form $ma + nb$, where $m, n \in \mathbf{Z}$, as a **linear combination** of a and b. The next theorem gives a very useful connection between greatest common divisors and linear combinations.

1.1.6 Theorem. *Let a and b be integers, not both zero. Then a and b have a greatest common divisor, which can be expressed as the smallest positive linear combination of a and b.*

Moreover, an integer is a linear combination of a and b if and only if it is a multiple of their greatest common divisor.

Proof. Let I be the set of all linear combinations of a and b, that is,

$$I = \{x \in \mathbf{Z} \mid x = ma + nb \text{ for some } m, n \in \mathbf{Z}\}.$$

The set I is nonempty since it contains $a = 1 \cdot a + 0 \cdot b$ and $b = 0 \cdot a + 1 \cdot b$. It is closed under addition and subtraction since if $k_1, k_2 \in I$, then $k_1 = m_1 a + n_1 b$ and $k_2 = m_2 a + n_2 b$ for some integers m_1, m_2, n_1, n_2. Thus

$$k_1 \pm k_2 = (m_1 a + n_1 b) \pm (m_2 a + n_2 b) = (m_1 \pm m_2)a + (n_1 \pm n_2)b$$

also belong to I. By Theorem 1.1.4, the set I consists of all multiples of the smallest positive integer it contains, say d. Since $d \in I$, $d = ma + nb$ for some integers m and n.

Since we already know that d is positive, to show that $d = (a, b)$ we must show that (i) $d \mid a$ and $d \mid b$ and (ii) if $c \mid a$ and $c \mid b$, then $c \mid d$. First, d is a divisor of every element in I, so $d \mid a$ and $d \mid b$ since $a, b \in I$. Secondly, if $c \mid a$ and $c \mid b$, say $a = cq_1$ and $b = cq_2$, then

$$d = ma + nb = m(cq_1) + n(cq_2) = c(mq_1 + nq_2),$$

which shows that $c \mid d$.

The second assertion follows from the fact that I, the set of all linear combinations of a and b, is equal to $d\mathbf{Z}$, the set of all multiples of d. □

You are probably used to finding the greatest common divisor of a and b by first finding their prime factorizations. This is an effective technique for small numbers, but we must postpone a discussion of this method until after we have studied prime factorizations in Section 1.2. In practice, for large numbers it can be very difficult

to find prime factors, whereas the greatest common divisor can be found in many fewer steps by using the method we discuss next.

The greatest common divisor of two numbers can be computed by using a procedure known as the *Euclidean algorithm*. (Our proof of the existence of the greatest common divisor did not include an explicit method for finding it.) Before discussing the Euclidean algorithm, we need to note some properties of the greatest common divisor. First, if a and b are not both zero, then it is not difficult to see that $\gcd(a, b) = \gcd(|a|, |b|)$. Furthermore, if $b > 0$ and $b \mid a$, then $(a, b) = b$.

The next observation provides the basis for the Euclidean algorithm. If $b \neq 0$ and $a = bq + r$, then $(a, b) = (b, r)$. This can be shown by noting first that a is a multiple of (b, r) since it is a linear combination of b and r. Then $(b, r) \mid (a, b)$ since b is also a multiple of (b, r). A similar argument using the equality $r = a - bq$ shows that $(a, b) \mid (b, r)$, and it follows that $(a, b) = (b, r)$.

Given integers $a > b > 0$, the **Euclidean algorithm** uses the division algorithm repeatedly to obtain

$$\begin{array}{rcll} a & = & bq_1 + r_1 & \text{with} \quad 0 \leq r_1 < b \\ b & = & r_1 q_2 + r_2 & \text{with} \quad 0 \leq r_2 < r_1 \\ r_1 & = & r_2 q_3 + r_3 & \text{with} \quad 0 \leq r_3 < r_2 \\ & & & \text{etc.} \end{array}$$

If $r_1 = 0$, then $b \mid a$, and so $(a, b) = b$. Since $r_1 > r_2 > \ldots$, the remainders get smaller and smaller, and after a finite number of steps we obtain a remainder $r_{n+1} = 0$. The algorithm ends with the equation

$$r_{n-1} = r_n q_{n+1} + 0.$$

This gives us the greatest common divisor:

$$(a, b) = (b, r_1) = (r_1, r_2) = \ldots = (r_{n-1}, r_n) = (r_n, 0) = r_n \, .$$

Example 1.1.1.

In showing that $(24, 18) = 6$, we have $(24, 18) = (18, 6)$ since $24 = 18 \cdot 1 + 6$, and $(18, 6) = 6$ since $6 \mid 18$. Thus $(24, 18) = (18, 6) = 6$. □

Example 1.1.2.

To show that $(126, 35) = 7$, we first have $(126, 35) = (35, 21)$ since $126 = 35 \cdot 3 + 21$. Then $(35, 21) = (21, 14)$ since $35 = 21 \cdot 1 + 14$, and $(21, 14) = (14, 7)$ since $21 = 14 \cdot 1 + 7$. Finally, $(14, 7) = 7$ since $14 = 7 \cdot 2$. Thus $(126, 35) = (35, 21) = (21, 14) = (14, 7) = 7$. □

Example 1.1.3.

In finding (83, 38), we can arrange the work in the following manner:

$$\begin{aligned} 83 &= 38 \cdot 2 + 7 \\ 38 &= 7 \cdot 5 + 3 \\ 7 &= 3 \cdot 2 + 1 \\ 3 &= 3 \cdot 1 \end{aligned} \qquad \begin{aligned} (83, 38) &= (38, 7) \\ (38, 7) &= (7, 3) \\ (7, 3) &= (3, 1) \\ (3, 1) &= 1 . \end{aligned}$$

If you only need to find the greatest common divisor, stop as soon as you can compute it in your head. In showing that $(83, 38) = 1$, note that since 7 has no positive divisors except 1 and 7 and is not a divisor of 38, it is clear immediately that $(38, 7) = 1$. □

Example 1.1.4.

Sometimes it is necessary to find the linear combination of a and b that gives (a, b). In finding (126, 35) in Example 1.1.2 we had the following equations:

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1 q_2 + r_2 \\ r_1 &= r_2 q_3 + d \\ r_2 &= d q_4 + 0 \end{aligned} \qquad \begin{aligned} 126 &= 35 \cdot 3 + 21 \\ 35 &= 21 \cdot 1 + 14 \\ 21 &= 14 \cdot 1 + 7 \\ 14 &= 7 \cdot 2 + 0 . \end{aligned}$$

The next step is to solve for the nonzero remainder in each of the equations (omitting the last equation):

$$\begin{aligned} r_1 &= a + (-q_1)b \\ r_2 &= b + (-q_2)r_1 \\ d &= r_1 + (-q_3)r_2 \end{aligned} \qquad \begin{aligned} 21 &= 1 \cdot 126 + (-3) \cdot 35 \\ 14 &= 1 \cdot 35 + (-1) \cdot 21 \\ 7 &= 1 \cdot 21 + (-1) \cdot 14 . \end{aligned}$$

We then work with the last equation $d = r_1 + (-q_3)r_2$, which contains the greatest common divisor, as desired, but may not be a linear combination of the original integers a and b. We can obtain the desired linear combination by substituting for the intermediate remainders, one at a time. Our first equation is

$$7 = 1 \cdot 21 + (-1) \cdot 14 .$$

We next substitute for the previous remainder 14, using the equation $14 = 1 \cdot 35 + (-1) \cdot 21$. This gives the following equation, involving a linear combination of 35 and 21:

$$\begin{aligned} 7 &= 1 \cdot 21 + (-1) \cdot [1 \cdot 35 + (-1) \cdot 21] \\ &= (-1) \cdot 35 + 2 \cdot 21 . \end{aligned}$$

Finally, we use the first equation $21 = 1 \cdot 126 + (-3) \cdot 35$ to substitute for the remainder 21. This allows us to represent the greatest common divisor 7 as a linear combination of 126 and 35:

$$\begin{aligned} 7 &= (-1) \cdot 35 + 2 \cdot [1 \cdot 126 + (-3) \cdot 35] \\ &= 2 \cdot 126 + (-7) \cdot 35 \,. \end{aligned}$$ □

The technique introduced in the previous example can easily be extended to the general situation in which it is desired to express (a, b) as a linear combination of a and b. After solving for the remainder in each of the relevant equations, we obtain

$$\begin{aligned} r_1 &= a + (-q_1)b \\ r_2 &= b + (-q_2)r_1 \\ r_3 &= r_1 + (-q_3)r_2 \\ r_4 &= r_2 + (-q_4)r_3 \\ &\vdots \end{aligned}$$

At each step, the expression for the remainder depends upon the previous two remainders. By substituting into the successive equations and then rearranging terms, it is possible to express each remainder (in turn) as a linear combination of a and b. The final step is to express (a, b) as a linear combination of a and b.

The Euclidean algorithm can be put into a convenient matrix format that keeps track of the remainders and linear combinations at the same time. To find (a, b), the idea is to start with the following system of equations:

$$\begin{aligned} x &= a \\ y &= b \end{aligned}$$

and find, by using elementary row operations, an equivalent system of the following form:

$$\begin{aligned} m_1 x + n_1 y &= (a, b) \\ m_2 x + n_2 y &= 0 \,. \end{aligned}$$

Beginning with the matrix

$$\begin{bmatrix} 1 & 0 & a \\ 0 & 1 & b \end{bmatrix},$$

we use the division algorithm to write $a = bq_1 + r_1$. We then subtract q_1 times the bottom row from the top row, to get

$$\begin{bmatrix} 1 & -q_1 & r_1 \\ 0 & 1 & b \end{bmatrix}.$$

We next write $b = r_1q_2 + r_2$, and subtract q_2 times the top row from the bottom row. This gives the matrix

$$\begin{bmatrix} 1 & -q_1 & r_1 \\ -q_2 & 1+q_1q_2 & r_2 \end{bmatrix}$$

and it can be checked that this algorithm produces rows in the matrix that give each successive remainder, together with the coefficients of the appropriate linear combination of a and b. The procedure is continued until one of the entries in the right-hand column is zero. Then the other entry in this column is the greatest common divisor, and its row contains the coefficients of the desired linear combination.

Example 1.1.5.

In using the matrix form of the Euclidean algorithm to compute $(126, 35)$ we begin with the equations $x = 126$ and $y = 35$. We have the following matrices:

$$\begin{bmatrix} 1 & 0 & 126 \\ 0 & 1 & 35 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -3 & 21 \\ 0 & 1 & 35 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -3 & 21 \\ -1 & 4 & 14 \end{bmatrix} \rightsquigarrow$$

$$\begin{bmatrix} 2 & -7 & 7 \\ -1 & 4 & 14 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 2 & -7 & 7 \\ -5 & 18 & 0 \end{bmatrix},$$

ending with the equations $2x-7y = 7$ and $-5x+18y = 0$. Thus $(126, 35) = 7$, and substituting $x = 126$ and $y = 35$ in the equation $2x - 7y = 7$ gives us a linear combination $7 = 2 \cdot 126 + (-7) \cdot 35$.

Substituting into the second equation $-5x + 81y = 0$ also gives us some interesting information. Any multiple of the linear combination $0 = (-5) \cdot 126 + 18 \cdot 35$ can be added to the above representation of the greatest common divisor. Thus, for example, we also have $7 = (-3) \cdot 126 + 11 \cdot 35$ and $7 = (-8) \cdot 126 + 29 \cdot 35$. □

Example 1.1.6.

In matrix form, the solution for $(83, 38)$ is the following:

$$\begin{bmatrix} 1 & 0 & 83 \\ 0 & 1 & 38 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -2 & 7 \\ 0 & 1 & 38 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -2 & 7 \\ -5 & 11 & 3. \end{bmatrix} \rightsquigarrow$$

$$\begin{bmatrix} 11 & -24 & 1 \\ -5 & 11 & 3 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 11 & -24 & 1 \\ -38 & 83 & 0 \end{bmatrix}.$$

Thus $(83, 38) = 1$ and $(11)(83) + (-24)(38) = 1$. □

The number (a, b) can be written in many different ways as a linear combination of a and b. The matrix method gives a linear combination with $0 = m_1a + n_1b$, so if $(a, b) = ma + nb$, then adding the previous equation gives $(a, b) = (m + m_1)a + (n + n_1)b$. In fact, any multiple of the equation $0 = m_1a + n_1b$ could have been added, so there are infinitely many linear combinations of a and b that give (a, b).

EXERCISES: SECTION 1.1

Before working on the exercises, you must make sure that you are familiar with all of the definitions and theorems of this section. You also need to be familiar with the techniques of proof that have been used in the theorems and examples in the text. As a reminder, we take this opportunity to list several useful approaches.

—When working questions involving divisibility you may find it useful to go back to the definition. If you rewrite $b \mid a$ as $a = bq$ for some $q \in \mathbf{Z}$, then you have an equation involving integers, something concrete and familiar to work with.

—To show that $b \mid a$, try to write down an expression for a that has b as a factor.

—Another approach to proving that $b \mid a$ is to use the division algorithm to write $a = bq + r$, where $0 \leq r < b$, and show that $r = 0$.

—Theorem 1.1.6 is extremely useful in questions involving greatest common divisors. Remember that finding *some* linear combination of a and b is not necessarily good enough to determine $\gcd(a, b)$. You must show that the linear combination you believe is equal to $\gcd(a, b)$ is actually the *smallest* positive linear combination of a and b.

Exercises for which a solution is given in the answer key are marked by the symbol †.

1. A number n is called **perfect** if it is equal to the sum of its proper positive divisors (those divisors different from n). The first perfect number is 6 since $1 + 2 + 3 = 6$. For each number between 6 and the next perfect number, make a list containing the number, its proper divisors, and their sum.

   Note: If you reach 40, you have missed the next perfect number.

2. Find the quotient and remainder when a is divided by b.
   (a) $a = 99$, $b = 17$
   (b) $a = -99$, $b = 17$
   (c) $a = 17$, $b = 99$
   (d) $a = -1017$, $b = 99$

3. Use the Euclidean algorithm to find the following greatest common divisors.
   †(a) (35, 14)
   (b) (15, 11)
   †(c) (252, 180)
   (d) (513, 187)
   †(e) (7655, 1001)

4. Use the Euclidean algorithm to find the following greatest common divisors.
   (a) (6643, 2873)
   (b) (7684, 4148)
   (c) (26460, 12600)
   (d) (6540, 1206)
   (e) (12091, 8439)

5.† For each part of Exercise 3, find integers m and n such that (a, b) is expressed in the form $ma + nb$.

6. For each part of Exercise 4, find integers m and n such that (a, b) is expressed in the form $ma + nb$.

7. Let a, b, c be integers. Give a proof for these facts about divisors:
   (a) If $b \mid a$, then $b \mid ac$.
   (b) If $b \mid a$ and $c \mid b$, then $c \mid a$.
   (c) If $c \mid a$ and $c \mid b$, then $c \mid (ma + nb)$ for any integers m, n.

8. Let a, b, c be integers such that $a + b + c = 0$. Show that if n is an integer which is a divisor of two of the three integers, then it is also a divisor of the third.

9. Let a, b, c be integers.
   (a) Show that if $b \mid a$ and $b \mid (a + c)$, then $b \mid c$.
   (b) Show that if $b \mid a$ and $b \nmid c$, then $b \nmid (a + c)$.

10. Let a, b, c be integers, with $c \neq 0$. Show that $bc \mid ac$ if and only if $b \mid a$.

11. Show that if $a > 0$, then $(ab, ac) = a(b, c)$.

12. Show that if n is any integer, then $(10n + 3, 5n + 2) = 1$.

13. Show that if n is any integer, then $(a + nb, b) = (a, b)$.

14. For what positive integers n is it true that $(n, n + 2) = 2$? Prove your claim.

15. Give a detailed proof of the statement in the text that if a and b are integers, then $b \mid a$ if and only if $a\mathbb{Z} \subseteq b\mathbb{Z}$.

16. Let a, b, c be integers, with $b > 0, c > 0$, and let q be the quotient and r the remainder when a is divided by b.
   (a) Show that q is the quotient and rc is the remainder when ac is divided by bc.
   (b) Show that if q' is the quotient when q is divided by c, then q' is the quotient when a is divided by bc. (Do not assume that the remainders are zero.)

17. Let a, b, n be integers with $n > 1$. Suppose that $a = nq_1 + r_1$ with $0 \leq r_1 < n$ and $b = nq_2 + r_2$ with $0 \leq r_2 < n$. Prove that $n \mid (a - b)$ if and only if $r_1 = r_2$.

18. Show that any nonempty set of integers that is closed under subtraction must also be closed under addition. (Thus part of the hypothesis of Theorem 1.1.4 is redundant.)

19. Let a, b, q, r be integers such that $b \neq 0$ and $a = bq + r$. Prove that $(a, b) = (b, r)$ by showing that (b, r) satisfies the definition of the greatest common divisor of a and b.

20. Perhaps a more natural definition of the greatest common divisor is the following: Let a and b be integers, not both zero. An integer d is called the greatest common divisor of the nonzero integers a and b if (i) $d \mid a$ and $d \mid b$, and (ii) $c \mid a$ and $c \mid b$ implies $d \geq c$. Show that this definition is equivalent to Definition 1.1.5.

21. Prove that the sum of the cubes of any three consecutive positive integers is divisible by 3.

22.†Find all integers x such that $3x + 7$ is divisible by 11.

23. Develop a theory of integer solutions x, y of equations of the form $ax + by = c$, where a, b, c are integers. That is, when can an equation of this form be solved, and if it can be solved, how can all solutions be found? Test your theory on these equations:

$$60x + 36y = 12, \qquad 35x + 6y = 8, \qquad 12x + 18y = 11.$$

Finally, give conditions on a and b under which $ax + by = c$ has solutions for every integer c.

24. Formulate a definition of the greatest common divisor of three integers a, b, c (not all zero). With the appropriate definition you should be able to prove that the greatest common divisor is a linear combination of a, b and c.

1.2 Primes

The main focus of this section is on prime numbers. Our method will be to investigate the notion of two integers which are relatively prime, that is, those which have no common divisors except ± 1. Using some facts which we will prove about them, we will be able to prove the prime factorization theorem, which states that every nonzero integer can be expressed as a product of primes. Finally, we will be able to use prime factorizations to learn more about greatest common divisors and least common multiples.

1.2.1 Definition. *The nonzero integers a and b are said to be* ***relatively prime*** *if* $(a, b) = 1$.

1.2.2 Proposition. *Let a, b be nonzero integers. Then $(a, b) = 1$ if and only if there exist integers m, n such that $ma + nb = 1$.*

Proof. If a and b are relatively prime, then by Theorem 1.1.6 integers m and n can be found for which $ma+nb = 1$. To prove the converse, we only need to note that if there exist integers m and n with $ma + nb = 1$, then 1 must be the smallest positive linear combination of a and b, and thus $(a, b) = 1$, again by Theorem 1.1.6. □

Proposition 1.2.2 will be used repeatedly in the proof of the next result. A word of caution—it is often tempting to jump from the equation $d = ma + nb$ to the conclusion that $d = (a, b)$. For example, $16 = 2 \cdot 5 + 3 \cdot 2$, but obviously $(5, 2) \neq 16$. The most that it is possible to say (using Theorem 1.1.6) is that d is a multiple of (a, b). Of course, if $ma + nb = 1$, then Proposition 1.2.2 implies that $(a, b) = 1$.

1.2.3 Proposition. *Let a, b, c be integers, where $a \neq 0$ or $b \neq 0$.*

(a) *If $b \mid ac$, then $b \mid (a, b) \cdot c$.*

(b) *If $b \mid ac$ and $(a, b) = 1$, then $b \mid c$.*

(c) *If $b \mid a$, $c \mid a$ and $(b, c) = 1$, then $bc \mid a$.*

(d) *$(a, bc) = 1$ if and only if $(a, b) = 1$ and $(a, c) = 1$.*

Proof. (a) Assume that $b \mid ac$. To show that $b \mid (a, b) \cdot c$, we will try to find an expression for $(a, b) \cdot c$ that has b as an obvious factor. We can write $(a, b) = ma+nb$ for some $m, n \in \mathbb{Z}$, and then multiplying by c gives

$$(a, b) \cdot c = mac + nbc .$$

Now b is certainly a factor of nbc, and by assumption it is also a factor of ac, so it is a factor of mac and therefore of the sum $mac + nbc$. Thus $b \mid (a, b) \cdot c$.

(b) Simply letting $(a, b) = 1$ in part (a) gives the result immediately.

(c) If $b \mid a$, then $a = bq$ for some integer q. If $c \mid a$, then $c \mid bq$, so if $(b, c) = 1$, it follows from part (b) that $c \mid q$, say with $q = cq_1$. Substituting for q in the equation $a = bq$ gives $a = bcq_1$, and thus $bc \mid a$.

(d) Suppose that $(a, bc) = 1$. Then $ma + n(bc) = 1$ for some integers m and n, and by viewing this equation as $ma + (nc)b = 1$ and $ma + (nb)c = 1$ we can see that $(a, b) = 1$ and $(a, c) = 1$.

Conversely, suppose that $(a, b) = 1$ and $(a, c) = 1$. Then $m_1a + n_1b = 1$ for some integers m_1 and n_1, and $m_2a + n_2c = 1$ for some integers m_2 and n_2. Multiplying these two equations gives

$$(m_1m_2a + m_1n_2c + m_2n_1b)a + (n_1n_2)bc = 1,$$

which shows that $(a, bc) = 1$. □

1.2.4 Definition. *An integer $p > 1$ is called a* ***prime number*** *if its only divisors are ± 1 and $\pm p$. An integer $a > 1$ is called* ***composite*** *if it is not prime.*

To determine whether or not a given integer $n > 1$ is prime, we could just try to divide n by each positive integer less than n. This method of trial division is very inefficient, and for this reason various sophisticated methods of "primality testing" have been developed. The need for efficient tests has become particularly apparent recently, because of applications to computer security that make use of cryptographic algorithms. To determine the complete list of all primes up to some bound, there is a useful procedure handed down from antiquity.

Example 1.2.1 (Sieve of Eratosthenes).

The primes less than a fixed positive integer a can be found by the following procedure. List all positive integers less than a (except 1), and cross off every even number except 2. Then go to the first number that has not been crossed off, which will be 3, and cross off all higher multiples of 3. Continue this process to find all primes less than a. You can stop after you have crossed off all proper multiples of primes p for which $p < \sqrt{a}$, since you will have crossed off every number less than a that has a proper factor. (If b is composite, say $b = b_1 b_2$, then either $b_1 \leq \sqrt{b}$ or $b_2 \leq \sqrt{b}$.) For example, we can find all primes less than 20 by just crossing off all multiples of 2 and 3, since $5 > \sqrt{20}$:

	~~2~~	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	.

This method is attributed to the Greek mathematician Eratosthenes, and is called the **sieve of Eratosthenes**.

Similarly, the integers less than a and relatively prime to a can be found by crossing off the prime factors of a and all of their multiples. For example, the prime divisors of 36 are 2 and 3, and so the positive integers less than 36 and relatively prime to it can be found as follows:

1	~~2~~	~~3~~	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~	11	~~12~~
13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~	~~21~~	~~22~~	23	~~24~~
25	~~26~~	~~27~~	~~28~~	29	~~30~~	31	~~32~~	~~33~~	~~34~~	35	.

□

Euclid's lemma, the next step in our development of the fundamental theorem of arithmetic, is the one that requires our work on relatively prime numbers. We will use Proposition 1.2.3 (b) in a crucial way.

1.2.5 Lemma (Euclid). *An integer $p > 1$ is prime if and only if it satisfies the following property: for all integers a and b, if $p \mid ab$, then either $p \mid a$ or $p \mid b$.*

Proof. Suppose that p is prime and $p \mid ab$. We know that either $(p, a) = p$ or $(p, a) = 1$, since (p, a) is always a divisor of p and p is prime. In the first

case $p \mid a$ and we are done. In the second case, since $(p, a) = 1$, we can apply Proposition 1.2.3 (b) to show that $p \mid ab$ implies $p \mid b$. Thus we have shown that if $p \mid ab$, then either $p \mid a$ or $p \mid b$.

Conversely, suppose that p satisfies that given condition. If p were composite, then we could write $p = ab$ for some positive integers smaller than p. The condition would imply that either $p \mid a$ or $p \mid b$, which would be an obvious contradiction. □

The following corollary extends Euclid's lemma to the product of more than two integers. In the proof we will use mathematical induction, which we hope is familiar to you. If you do not remember how to use induction, you should read the discussion in Appendix A.4.

1.2.6 Corollary. *If p is a prime number, and $p \mid a_1 a_2 \cdots a_n$ for integers $a_1, a_2, \ldots, a_n$, then $p \mid a_i$ for some i with $1 \leq i \leq n$.*

Proof. In order to use the principle of mathematical induction, let P_n be the following statement: if $p \mid a_1 a_2 \cdots a_n$, then $p \mid a_i$ for some $1 \leq i \leq n$. The statement P_1 is clearly true. Next, assume that the statement P_k is true, that is, if $p \mid a_1 a_2 \cdots a_k$, then $p \mid a_i$ for some $1 \leq i \leq k$. If $p \mid a_1 a_2 \cdots a_k a_{k+1}$, for integers $a_1, a_2, \ldots, a_k, a_{k+1}$, then applying Euclid's lemma to $a = a_1 a_2 \cdots a_k$ and $b = a_{k+1}$ yields that $p \mid a_1 a_2 \cdots a_k$ or $p \mid a_{k+1}$. In case $p \mid a_1 a_2 \cdots a_k$, the truth of the statement P_k implies that $p \mid a_i$ for some $1 \leq i \leq k$. Thus, in either case, $p \mid a_i$ for some $1 \leq i \leq k+1$, and hence the statement P_{k+1} is true. By the principle of mathematical induction (as stated in Theorem A.4.2 of Appendix A.4), the statement P_n holds for all positive integers n. □

The next theorem, on prime factorization, is sometimes called the fundamental theorem of arithmetic. The naive way to prove that an integer a can be written as a product of primes is to note that either a is prime and we are done, or else a is composite, say $a = bc$. Then the same argument can be applied to b and c, and continued until a has been broken up into a product of primes. (This process must stop after a finite number of steps because of the well-ordering principle.) We also need to prove that any two factorizations of a number are in reality the same. The idea of the proof is to use Euclid's lemma to pair the primes in one factorization with those in the other. In fact, the proof of the uniqueness of the factorization requires a more delicate argument than the proof of the existence of the factorization.

1.2.7 Theorem (Fundamental Theorem of Arithmetic). *Any integer $a > 1$ can be factored uniquely as a product of prime numbers, in the form*

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n},$$

where $p_1 < p_2 < \ldots < p_n$ and the exponents $\alpha_1, \alpha_2, \ldots, \alpha_n$ are all positive.

Proof. Suppose that there is some integer that cannot be written as a product of primes. Then the set of all integers $a > 1$ that have no prime factorization must be nonempty, so as a consequence of the well-ordering principle it must have a smallest member, say b. Now b cannot itself be a prime number since then it would have a prime factorization. Thus b is composite, and we can write $b = cd$ for positive integers c, d that are smaller than b. Since b was assumed to be the smallest positive integer not having a factorization into primes, and c and d are smaller, then both c and d must have factorizations into products of primes. This shows that b also has such a factorization, which is a contradiction. Since multiplication is commutative, the prime factors can be ordered in the desired manner.

If there exists an integer > 1 for which the factorization is not unique, then by the well-ordering principle there exists a smallest such integer, say a. Assume that a has two factorizations $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ and $a = q_1^{\beta_1} q_2^{\beta_2} \cdots q_m^{\beta_m}$, where $p_1 < p_2 < \ldots < p_n$, and $q_1 < q_2 < \ldots < q_m$, with $\alpha_i > 0$ for $i = 1, \ldots, n$, and $\beta_i > 0$ for $i = 1, \ldots, m$. By Corollary 1.2.6 of Euclid's lemma, $q_1 \mid p_k$ for some k with $1 \leq k \leq n$ and $p_1 \mid q_j$ for some j with $1 \leq j \leq m$. Since all of the numbers p_i and q_i are prime, we must have $q_1 = p_k$ and $p_1 = q_j$. Then $p_1 = q_1$ since $q_1 \leq q_j = p_1 \leq p_k = q_1$. Hence we can let

$$s = \frac{a}{p_1} = \frac{a}{q_1} = p_1^{\alpha_1 - 1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} = q_1^{\beta_1 - 1} q_2^{\beta_2} \cdots q_m^{\beta_m} .$$

If $s = 1$ then $a = p_1$ has a unique factorization, contrary to the choice of a. If $s > 1$, then since $s < a$ and s has two factorizations, we again have a contradiction to the choice of a. □

If the prime factorization of an integer is known, then it is easy to list all of its divisors. If $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, then b is a divisor of a if and only if $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}$, where $\beta_i \leq \alpha_i$ for all i. Thus we can list all possible divisors of a by systematically decreasing the exponents of each of its prime divisors.

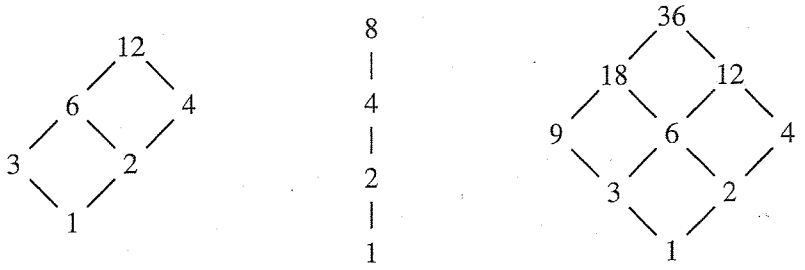
Example 1.2.2.

The positive divisors of 12 are 1, 2, 3, 4, 6, 12; the positive divisors of 8 are 1, 2, 4, 8; and the positive divisors of 36 are 1, 2, 3, 4, 6, 9, 12, 18, 36. In Figure 1.2.1, we have arranged the divisors so as to show the divisibility relations among them. There is a path (moving upward only) from a to b if and only if $a \mid b$.

In constructing the first diagram in Figure 1.2.1, it is easiest to use the prime factorization of 12. Since $12 = 2^2 3$, we first divide 12 by 2 to get 6 and then divide again by 2 to get 3. This gives the first side of the diagram, and to construct the opposite side of the diagram we divide each number by 3.

If the number has three different prime factors, then we would need a three-dimensional diagram. (Visualize the factors as if on the edges of a box.) With more than three distinct prime factors, the diagrams lose their clarity. □

Figure 1.2.1:



The following proof, although easy to follow, is an excellent example of the austere beauty of mathematics.

1.2.8 Theorem (Euclid). *There exist infinitely many prime numbers.*

Proof. Suppose that there were only finitely many prime numbers, say p_1, p_2, $\ldots$, p_n. Then consider the number $a = p_1 p_2 \cdots p_n + 1$. By Theorem 1.2.7, the number a has a prime divisor, say p. Now p must be one of the primes we listed, so $p \mid (p_1 p_2 \cdots p_n)$, and since $p \mid a$, it follows that $p \mid (a - p_1 p_2 \cdots p_n)$. This is a contradiction since p cannot be a divisor of 1. □

Example 1.2.3.

Consider the numbers $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^4 - 1 = 15$, $2^5 - 1 = 31$, and $2^6 - 1 = 63$. The prime exponents each give rise to a prime, while the composite exponents each give a composite number. Is this true in general? Continuing to investigate prime exponents gives $2^7 - 1 = 127$, which is prime, but $2^{11} - 1 = 2047 = 23 \cdot 89$. Thus a prime exponent may or may not yield a prime number.

On the other hand, it is always true that a composite exponent yields a composite number. To prove this, let n be composite, say $n = qm$ (where q and m are integers greater than 1), and consider $2^n - 1 = 2^{qm} - 1$. We need to find a nontrivial factorization of $2^{qm} - 1 = (2^q)^m - 1$. We can look at this as $x^m - 1$, and then we have the familiar factorization

$$x^m - 1 = (x - 1)(x^{m-1} + x^{m-2} + \ldots + x^2 + x + 1) .$$

Substituting $x = 2^q$ shows that $2^q - 1$ is a factor of $2^n - 1$. Now $1 < 2^q - 1 < 2^n - 1$ since both q and m are greater than 1, and so we have found a nontrivial factorization of $2^n - 1$. □

The final concept we study in this section is the least common multiple of two integers. Its definition is parallel to that of the greatest common divisor. We can characterize it in terms of the prime factorizations of the two numbers, or by the fact that the product of two numbers is equal to the product of their least common multiple and greatest common divisor.

1.2.9 Definition. *A positive integer m is called the* ***least common multiple*** *of the nonzero integers a and b if*

(i) *m is a multiple of both a and b, and*

(ii) *any multiple of both a and b is also a multiple of m.*

We will use the notation $\text{lcm}[a, b]$ *or* $[a, b]$ *for the least common multiple of a and b.*

When written out in symbols, the definition of the least common multiple looks like this: $m = \text{lcm}[a, b]$ if (i) $a \mid m$ and $b \mid m$, and (ii) if $a \mid c$ and $b \mid c$, then $m \mid c$.

There are times, as in next proposition, when it is convenient to allow the prime factorization of a number to include primes with exponent 0. This leads to a representation that is no longer unique, but it is particularly useful to be able to write the prime factorizations of two different integers in terms of the *same* primes.

1.2.10 Proposition. *Let a and b be positive integers with prime factorizations $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ and $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}$, where $\alpha_i \geq 0$ and $\beta_i \geq 0$ for all i.*

(a) *Then $a \mid b$ if and only if $\alpha_i \leq \beta_i$ for $1 = 1, 2, \ldots, n$.*

(b) *For each i, let $\delta_i = \min\{\alpha_i, \beta_i\}$ and $\mu_i = \max\{\alpha_i, \beta_i\}$. Then*

$$\gcd(a, b) = p_1^{\delta_1} p_2^{\delta_2} \cdots p_n^{\delta_n} \quad \textit{and} \quad \text{lcm}[a, b] = p_1^{\mu_1} p_2^{\mu_2} \cdots p_n^{\mu_n} .$$

Proof. (a) Suppose that $\alpha_i \leq \beta_i$ for $i = 1, 2, \ldots, n$. Let $\gamma_i = \beta_i - \alpha_i$, for $i = 1, 2, \ldots, n$, and set $c = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_n^{\gamma_n}$ (note that $\gamma_i \geq 0$ for $i = 1, 2, \ldots, n$). Then

$$\begin{aligned} ac &= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_n^{\gamma_n} = p_1^{\alpha_1+\gamma_1} p_2^{\alpha_2+\gamma_2} \cdots p_n^{\alpha_n+\gamma_n} \\ &= p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n} = b . \end{aligned}$$

Since $b = ac$, we have $a \mid b$.

Conversely, suppose that $a \mid b$. Then there exists $c \in \mathbf{Z}$ such that $b = ac$. For any prime p such that $p \mid c$, we have $p \mid b$, and so $p = p_j$ for some j with $1 \leq j \leq n$.

Thus c has a factorization $c = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_n^{\gamma_n}$, where $\gamma_i \geq 0$ for $i = 1, 2, \ldots, n$. Since $b = ac$, we have

$$p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n} = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_n^{\gamma_n} = p_1^{\alpha_1+\gamma_1} p_2^{\alpha_2+\gamma_2} \cdots p_n^{\alpha_n+\gamma_n} ,$$

where $\beta_i = \alpha_i + \gamma_i$ for $i = 1, 2, \ldots, n$. Because $\gamma_i \geq 0$, we have $\alpha_i \leq \beta_i$ for $i = 1, 2, \ldots, n$.

(b) The proof follows immediately from part (a) and the definitions of the least common multiple and greatest common divisor. □

As a corollary of Proposition 1.2.10, it is clear that

$$\gcd(a, b) \cdot \operatorname{lcm}[a, b] = ab .$$

This can also be shown directly from the definitions, as we have noted in Exercise 15.

For small numbers it is probably easiest to use their prime factorizations to find their greatest common divisor and least common multiple. It takes a great deal of work to find the prime factors of a large number, even on a computer making use of sophisticated algorithms. In contrast, the Euclidean algorithm is much faster, so its use is more efficient for finding the greatest common divisor of large numbers.

Example 1.2.4.

In the previous section we computed $(126, 35)$. To do this using Proposition 1.2.10 we need the factorizations $126 = 2^1 \cdot 3^2 \cdot 7^1$ and $35 = 5^1 \cdot 7^1$. We then add terms so that we have the same primes in each case, to get $126 = 2^1 \cdot 3^2 \cdot 5^0 \cdot 7^1$ and $35 = 2^0 \cdot 3^0 \cdot 5^1 \cdot 7^1$. Thus we obtain $(126, 35) = 2^0 \cdot 3^0 \cdot 5^0 \cdot 7^1 = 7$ and $[126, 35] = 2^1 \cdot 3^2 \cdot 5^1 \cdot 7^1 = 630$. □

EXERCISES: SECTION 1.2

When proving results in these exercises, we recommend that you first try to use Proposition 1.2.2, Proposition 1.2.3, or Lemma 1.2.5, before trying to use the very powerful Fundamental Theorem of Arithmetic.

1. Find the prime factorizations of each of the following numbers, and use them to compute the greatest common divisor and least common multiple of the given pairs of numbers.

   †(a) 35, 14

   (b) 15, 11

   †(c) 252, 180

   (d) 7684, 4148

   †(e) 6643, 2873

2. Use the sieve of Eratosthenes to find all prime numbers less than 200.

3.†For each composite number a, with $4 \leq a \leq 20$, find all positive numbers less than a that are relatively prime to a.

4. Find all positive integers less than 60 and relatively prime to 60.

   Hint: Use techniques similar to the sieve of Eratosthenes.

5.†For each of the numbers 9, 15, 20, 24 and 100, give a diagram of all divisors of the number, showing the divisibility relationships. (See Example 1.2.2.)

6. For each of the following numbers, give a diagram of all divisors of the number, showing the divisibility relationships.

   (a) 60

   (b) 1575

7. Let m and n be positive integers such that $m + n = 57$ and $[m, n] = 680$. Find m and n.

8. Let a, b be positive integers, and let $d = (a, b)$. Since $d \mid a$ and $d \mid b$, there exist integers h, k such that $a = dh$ and $b = dk$. Show that $(h, k) = 1$.

9. Let a, b, c be positive integers, and let $d = (a, b)$. Since $d \mid a$, there exists an integer h with $a = dh$. Show that if $a \mid bc$, then $h \mid c$.

10. Show that $a\mathbf{Z} \cap b\mathbf{Z} = [a, b]\mathbf{Z}$.

11. Let a, b be nonzero integers, and let p be a prime. Show that if $p \mid [a, b]$, then either $p \mid a$ or $p \mid b$.

12. Let a, b, c be nonzero integers. Show that $(a, b) = 1$ and $(a, c) = 1$ if and only if $(a, [b, c]) = 1$.

13. Let a, b be nonzero integers. Prove that $(a, b) = 1$ if and only if $(a + b, ab) = 1$.

14. Let a, b be nonzero integers with $(a, b) = 1$. Compute $(a + b, a - b)$.

15. Let a and b be positive integers, and let m be an integer such that $ab = m(a, b)$. Without using the prime factorization theorem, prove that $(a, b)[a, b] = ab$ by verifying that m satisfies the necessary properties of $[a, b]$.

16. A positive integer a is called a **square** if $a = n^2$ for some $n \in \mathbf{Z}$. Show that the integer $a > 1$ is a square if and only if every exponent in its prime factorization is even.

17. Show that if the positive integer a is not a square, then $a \neq b^2/c^2$ for integers b, c. Thus any positive integer that is not a square must have an irrational square root.

    Hint: Use Exercise 16 to show that $ac^2 \neq b^2$.

18. Show that if a, b are positive integers such that $(a, b) = 1$ and ab is a square, then a and b are also squares.

19. Let p and q be prime numbers. Prove that $pq + 1$ is a square if and only if p and q are twin primes.

20. A positive integer is called **square-free** if it is a product of distinct primes. Prove that every positive integer can be written uniquely as a product of a square and a square-free integer.

21. Prove that if $a > 1$, then there is a prime p with $a < p \leq a! + 1$.

22. Show that for any $n > 0$, there are n consecutive composite numbers.

23. Show that if n is a positive integer such that $2^n + 1$ is prime, then n is a power of 2.

24. Show that $\log 2 / \log 3$ is not a rational number.

25. If a, b, c are positive integers such that $a^2 + b^2 = c^2$, then (a, b, c) is called a **Pythagorean triple**. For example, (3, 4, 5) and (5, 12, 13) are Pythagorean triples. Assume that (a, b, c) is a Pythagorean triple in which the only common divisors of a, b, c are ± 1.

    (a) Show that a and b cannot both be odd.

    (b) Assume that a is even. Show that there exist relatively prime integers m and n such that $a = 2mn$, $b = m^2 - n^2$, and $c = m^2 + n^2$.

    Hint: Factor $a^2 = c^2 - b^2$ after showing that $(c + b, c - b) = 2$.

1.3 Congruences

For many problems involving integers, all of the relevant information is contained in the remainders obtained by dividing by some fixed integer n. Since only n different remainders are possible $(0, 1, \ldots, n - 1)$, having only a finite number of cases to deal with can lead to considerable simplifications. For small values of n it even becomes feasible to use trial-and-error methods.

Example 1.3.1.

A famous theorem of Lagrange states that every positive integer can be written as sum of four squares. (See the notes at the end of this chapter for a short discussion of this problem.) To illustrate the use of remainders in solving a number theoretic problem, we will show that any positive integer whose remainder is 7 when divided by 8 cannot be written as the sum of three squares. Therefore this theorem of Lagrange is as sharp as possible.

If $n = a^2 + b^2 + c^2$, then when both sides are divided by 8, the remainders must be the same. It will follow from Proposition 1.3.3 that we can compute the remainder of $n = a^2 + b^2 + c^2$ by adding the remainders of a^2, b^2, and c^2 (and subtracting a multiple of 8 if necessary). By the same proposition, we can

compute the remainders of a^2, b^2, and c^2 by squaring the remainders of a, b, and c (and subtracting a multiple of 8 if necessary). The possible remainders for a, b, and c are 0, 1, ..., 7, and squaring and taking remainders yields only the values 0, 1, and 4. To check the possible remainders for $a^2 + b^2 + c^2$ we only need to add together three such terms. (If we get a sum larger than 7 we subtract 8.) A careful analysis of all of the cases shows that we cannot obtain 7 as a remainder for $a^2 + b^2 + c^2$. Thus we cannot express any integer n whose remainder is 7 when divided by 8 in the form $n = a^2 + b^2 + c^2$. □

Trial and error techniques similar to those of Example 1.3.1 can sometimes be used to show that a polynomial equation has no integer solution. For example, if $x = c$ is a solution of the equation $a_k x^k + \ldots + a_1 x + a_0 = 0$, then $a_k c^k + \ldots + a_1 c + a_0$ must be divisible by every integer n. If some n can be found for which $a_k x^k + \ldots + a_1 x + a_0$ is never divisible by n, then this can be used to prove that the equation has no integer solutions. For example, $x^3 + x + 1 = 0$ has no integer solutions since $c^3 + c + 1$ is odd for all integers c, and thus is never divisible by 2.

A more familiar situation in which we carry out arithmetic after dividing by a fixed integer is the addition of hours on a clock (where the fixed integer is 12). Another example is given by the familiar rules "even plus even is even," "even times even is even," etc., which are useful in other circumstances (where the fixed integer is 2). Gauss introduced the following congruence notation, which simplifies computations of this sort.

1.3.1 Definition. *Let n be a positive integer. Integers a and b are said to be* ***congruent modulo*** *n if they have the same remainder when divided by n. This is denoted by writing $a \equiv b \pmod{n}$.*

If we use the division algorithm to write $a = nq + r$, where $0 \leq r < n$, then $r = n \cdot 0 + r$. It follows immediately from the previous definition that $a \equiv r \pmod{n}$. In particular, any integer is congruent modulo n to one of the integers $0, 1, 2, \ldots, n-1$.

We feel that the definition we have given provides the best intuitive understanding of the notion of congruence, but in almost all proofs it will be easiest to use the characterization given by the next proposition. Using this characterization makes it possible to utilize the facts about divisibility that we have developed in the preceding sections of this chapter.

1.3.2 Proposition. *Let a, b, and $n > 0$ be integers. Then $a \equiv b \pmod{n}$ if and only if $n \mid (a - b)$.*

Proof. If $a \equiv b \pmod{n}$, then a and b have the same remainder when divided by n, so the division algorithm gives $a = nq_1 + r$ and $b = nq_2 + r$. Solving for the common remainder gives $a - nq_1 = b - nq_2$. Thus $a - b = n(q_1 - q_2)$, and so $n \mid (a - b)$.

To prove the converse, assume that $n \mid (a - b)$. Then there exists $k \in \mathbf{Z}$ with $a - b = nk$, and hence $b = a - nk$. If upon applying the division algorithm we have $a = nq + r$, with $0 \leq r < n$, then $b = a - nk = (nq + r) - nk = n(q - k) + r$. Since $0 \leq r < n$, division of b by n also yields the remainder r. Hence $a \equiv b \pmod{n}$. □

When working with congruence modulo n, the integer n is called the **modulus**. By the preceding proposition, $a \equiv b \pmod{n}$ if and only if $a - b = nq$ for some integer q. We can write this in the form $a = b + nq$, for some integer q. This observation gives a very useful method of replacing a congruence with an equation (over $\mathbf{Z}$). On the other hand, Proposition 1.3.3 shows that any equation can be converted to a congruence modulo n by simply changing the $=$ sign to $\equiv$. In doing so, any term congruent to 0 can simply be omitted. Thus the equation $a = b + nq$ would be converted back to $a \equiv b \pmod{n}$.

Congruence behaves in many ways like equality. The following properties, which are obvious from the definition of congruence modulo n, are a case in point. Let a, b, c be integers. Then

(i) $a \equiv a \pmod{n}$;

(ii) if $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$;

(iii) if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

The following theorem carries this analogy even further. Perhaps its most important consequence is that when adding, subtracting, or multiplying congruences you may substitute any congruent integer. For example, to show that $99^2 \equiv 1 \pmod{100}$, it is easier to substitute -1 for 99 and just show that $(-1)^2 = 1$.

1.3.3 Proposition. *Let $n > 0$ be an integer. Then the following conditions hold for all integers a, b, c, d:*

(a) *If $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$, then $a \pm b \equiv c \pm d \pmod{n}$, and $ab \equiv cd \pmod{n}$.*

(b) *If $a + c \equiv a + d \pmod{n}$, then $c \equiv d \pmod{n}$. If $ac \equiv ad \pmod{n}$ and $(a, n) = 1$, then $c \equiv d \pmod{n}$.*

Proof. (a) If $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$, then $n \mid (a - c)$ and $n \mid (b - d)$. Adding shows that $n \mid ((a + b) - (c + d))$, and subtracting shows that $n \mid ((a - b) - (c - d))$. Thus $a \pm b \equiv c \pm d \pmod{n}$.

Since $n \mid (a - c)$, we have $n \mid (ab - cb)$, and since $n \mid (b - d)$, we have $n \mid (cb - cd)$. Adding shows that $n \mid (ab - cd)$ and thus $ab \equiv cd \pmod{n}$.

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

If $ac \equiv ad \pmod{n}$, then $n \mid (ac - ad)$, and since $(n, a) = 1$, it follows from Proposition 1.2.3 (b) that $n \mid (c - d)$. Thus $c \equiv d \pmod{n}$. □

The consequences of Proposition 1.3.3 can be summarized as follows.

(i) For any number in the congruence, you can substitute any congruent integer.

(ii) You can add or subtract the same integer on both sides of a congruence.

(iii) You can multiply both sides of a congruence by the same integer.

(iv) Canceling, or dividing both sides of a congruence by the same integer, must be done very carefully. You may divide both sides of a congruence by an integer a only if $(a, n) = 1$. For example, $30 \equiv 6 \pmod 8$, but dividing both sides by 6 gives $5 \equiv 1 \pmod 8$, which is certainly false. On the other hand, since 3 is relatively prime to 8, we may divide both sides by 3 to get $10 \equiv 2 \pmod 8$.

Proposition 1.3.3 shows that the remainder upon division by n of $a+b$ or ab can be found by adding or multiplying the remainders of a and b when divided by n and then dividing by n again if necessary. For example, if $n = 8$, then 101 has remainder 5 and 142 has remainder 6 when divided by 8. Thus $101 \cdot 142 = 14,342$ has the same remainder as 30 (namely, 6) when divided by 8. Formally, $101 \equiv 5 \pmod 8$ and $142 \equiv 6 \pmod 8$, so it follows that $101 \cdot 142 \equiv 5 \cdot 6 \equiv 6 \pmod 8$.

As a further example, we compute the powers of 2 modulo 7. Rather than computing each power and then dividing by 7, we reduce modulo 7 at each stage of the computations:

$$\begin{aligned} 2^2 &\equiv 4 \pmod 7, \\ 2^3 &\equiv 2^2 2 \equiv 4 \cdot 2 \equiv 1 \pmod 7, \\ 2^4 &\equiv 2^3 2 \equiv 1 \cdot 2 \equiv 2 \pmod 7, \\ 2^5 &\equiv 2^4 2 \equiv 2 \cdot 2 \equiv 4 \pmod 7. \end{aligned}$$

From the way in which we have done the computations, it is clear that the powers will repeat. In fact, since there are only finitely many remainders modulo n, the powers of any integer will eventually begin repeating modulo n.

1.3.4 Proposition. *Let a and $n > 1$ be integers. There exists an integer b such that $ab \equiv 1 \pmod n$ if and only if $(a, n) = 1$.*

Proof. If there exists an integer b such that $ab \equiv 1 \pmod n$, then we have $ab = 1 + qn$ for some integer q. This can be rewritten to give a linear combination of a and n equal to 1, and so $(a, n) = 1$.

Conversely, if $(a, n) = 1$, then there exist integers s, t such that $sa + tn = 1$. Letting $b = s$ and reducing the equation to a congruence modulo n gives $ab \equiv 1 \pmod n$. □

We are now ready to present a systematic study of linear congruences that involve unknowns. The previous proposition shows that the congruence

$$ax \equiv 1 \pmod n$$

has a solution if and only if $(a, n) = 1$. In fact, the proof of the proposition shows that the solution can be obtained by using the Euclidean algorithm to write $1 = ab + nq$ for some $b, q \in \mathbf{Z}$, since then $1 \equiv ab \pmod n$.

The next theorem determines all solutions of a linear congruence of the form

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

Of course, if the numbers involved are small, it may be simplest just to use trial and error. For example, to solve $3x \equiv 2 \pmod{5}$, we only need to substitute $x = 0, 1, 2, 3, 4$. Thus by trial and error we can find the solution $x \equiv 4 \pmod{5}$.

In many ways, solving congruences is like solving equations. There are a few important differences, however. A linear equation over the integers (an equation of the form $ax = b$, where $a \neq 0$) has at most one solution. On the other hand, the linear congruence $2x \equiv 2 \pmod{4}$ has the two solutions $x \equiv 1 \pmod{4}$ and $x \equiv 3 \pmod{4}$.

For linear equations, it may happen that there is no solution. The same is true for linear congruences. For example, trial and error shows that the congruence $3x \equiv 2 \pmod{6}$ has no solution. Thus the first step in solving a linear congruence is to use the theorem to determine whether or not a solution exists.

We say that two solutions r and s to the congruence $ax \equiv b \pmod{n}$ are **distinct solutions modulo** n if r and s are not congruent modulo n. Thus in the next theorem the statement "d distinct solutions modulo n" means that there are d solutions $s_1, s_2, \ldots, s_d$ such that if $i \neq j$, then s_i and s_j are not congruent modulo n. This terminology is necessary in order to understand what we mean by "solving" the congruence $ax \equiv b \pmod{n}$. In the next section, we will introduce the concept of a "congruence class" to clarify the situation.

1.3.5 Theorem. *Let a, b and $n > 1$ be integers. The congruence $ax \equiv b \pmod{n}$ has a solution if and only if b is divisible by d, where $d = (a, n)$. If $d \mid b$, then there are d distinct solutions modulo n, and these solutions are congruent modulo n/d.*

Proof. To prove the first statement, observe that $ax \equiv b \pmod{n}$ has a solution if and only if there exist integers s and q such that $as = b + nq$, or, equivalently, $as + (-q)n = b$. Thus there is a solution if and only if b can be expressed as a linear combination of a and n. By Theorem 1.1.6 the linear combinations of a and n are precisely the multiples of d, so there is a solution if and only if $d \mid b$.

To prove the second statement, assume that $d \mid b$, and let $m = n/d$. Suppose that x_1 and x_2 are solutions of the congruence $ax \equiv b \pmod{n}$, giving $ax_1 \equiv ax_2 \pmod{n}$. Then $n \mid a(x_1 - x_2)$, and so it follows from Proposition 1.2.3 (a) that $n \mid d(x_1 - x_2)$. Thus $m \mid (x_1 - x_2)$, and so $x_1 \equiv x_2 \pmod{m}$. On the other hand, if $x_1 \equiv x_2 \pmod{m}$, then $m \mid (x_1 - x_2)$, and so $n \mid d(x_1 - x_2)$ since $n = dm$. Then since $d \mid a$ we can conclude that $n \mid a(x_1 - x_2)$, and so $ax_1 \equiv ax_2 \pmod{n}$.

We can choose the distinct solutions from among the n remainders $0, 1, \ldots, n-1$. Given one such solution, we can find all others in the set by adding multiples of n/d, giving a total of d distinct solutions. □

We now describe an algorithm for solving linear congruences of the form

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

We first compute $d = (a, n)$, and if $d \mid b$, then we write the congruence $ax \equiv b \pmod{n}$ as an equation $ax = b + qn$. Since d is a common divisor of a, b, and n, we can write $a = da_1$, $b = db_1$, and $n = dm$. Thus we get $a_1x = b_1 + qm$, which yields the congruence

$$a_1x \equiv b_1 \pmod{m} ,$$

where $a_1 = a/d$, $b_1 = b/d$, and $m = n/d$.

It follows immediately from Proposition 1.2.10 that since $d = (a, n)$, the numbers a_1 and m must be relatively prime. Thus by Proposition 1.3.4 we can apply the Euclidean algorithm to find an integer c such that $ca_1 \equiv 1 \pmod{m}$. Multiplying both sides of the congruence $a_1x \equiv b_1 \pmod{m}$ by c gives the solution

$$x \equiv cb_1 \pmod{m} .$$

Finally, since the original congruence was given modulo n, we should give our answer modulo n instead of modulo m. The congruence $x \equiv cb_1 \pmod{m}$ can be converted to the equation $x = cb_1 + mk$, which yields the solution $x \equiv cb_1 + mk \pmod{n}$. The solution modulo m determines d distinct solutions modulo n. The solutions have the form $s_0 + km$, where s_0 is any particular solution of $x \equiv b_1c \pmod{m}$ and k is any integer.

Example 1.3.2 (Homogeneous linear congruences).

In this example we consider the special case of a linear homogeneous congruence

$$ax \equiv 0 \pmod{n} .$$

In this case there always exists a solution, namely $x \equiv 0 \pmod{n}$, but this may not be the only solution modulo n.

As the first step in the solution we obtain $a_1x \equiv 0 \pmod{n_1}$, where $a = da_1$ and $n = dn_1$. Since a_1 and n_1 are relatively prime, by part (b) of Proposition 1.3.3 we can cancel a_1, to obtain

$$x \equiv 0 \pmod{n_1} , \qquad \text{with } n_1 = \frac{n}{\gcd(a, n)} .$$

We have d distinct solutions modulo n.

For example, $28x \equiv 0 \pmod{48}$ reduces to $x \equiv 0 \pmod{12}$, and $x \equiv 0$, 12, 24, 26 are the four distinct solutions modulo 48. □

Example 1.3.3.

To solve the congruence

$$60x \equiv 90 \pmod{105} ,$$

we first note that $(60, 105) = 15$, and then check that $15 \mid 90$, so that there will indeed be a solution. Dividing the corresponding equation $60x = 90 + 105q$ by 15, we obtain the equation $4x = 6 + 7q$, which reduces to the congruence

$$4x \equiv 6 \pmod{7} .$$

To solve this congruence, we need an integer c with $c \cdot 4 \equiv 1 \pmod{7}$, so in effect we must solve another congruence, $4z \equiv 1 \pmod{7}$. We could use the Euclidean algorithm, but with such a small modulus, trial and error is quicker, and it is easy to see that $c = 2$ will work.

We now multiply both sides of the congruence $4x \equiv 6 \pmod{7}$ by 2, to obtain $8x \equiv 12 \pmod{7}$, which reduces to

$$x \equiv 5 \pmod{7} .$$

Writing the solution in the form of an equation, we have $x = 5 + 7k$, so $x \equiv 5 + 7k \pmod{105}$. By adding multiples of 7 to the particular solution $x_0 = 5$, we obtain the solutions $\ldots, -2, 5, 12, 19, \ldots$. There are 15 distinct solutions modulo 105, so we have

$$x \equiv 5, 12, 19, 26, 33, 40, 47, 54, 61, 68, 75, 82, 89, 96, 103 \pmod{105} . \quad \square$$

In the next theorem we show how to solve two simultaneous congruences over moduli that are relatively prime. The motivation for the proof of the next theorem is as follows. Assume that the congruences $x \equiv a \pmod{n}$ and $x \equiv b \pmod{m}$ are given. If we can find integers y and z with

$$y \equiv 1 \pmod{n} \qquad y \equiv 0 \pmod{m}$$

$$z \equiv 0 \pmod{n}. \qquad z \equiv 1 \pmod{m}$$

then $x = ay + bz$ will be a solution to the pair of simultaneous congruences $x \equiv a \pmod{n}$ and $x \equiv b \pmod{m}$. This can be seen by reducing modulo n and then modulo m.

1.3.6 Theorem (Chinese Remainder Theorem). *Let n and m be positive integers, with $(n, m) = 1$. Then the system of congruences*

$$x \equiv a \ (mod\ n) \qquad x \equiv b \ (mod\ m)$$

has a solution. Moreover, any two solutions are congruent modulo mn.

Proof. Since $(n, m) = 1$, there exist integers r and s such that $rm + sn = 1$. Then $rm \equiv 1 \pmod{n}$ and $sn \equiv 1 \pmod{m}$. Following the suggestion in the preceding paragraph, we let $x = arm + bsn$. Then a direct computation verifies that $x \equiv arm \equiv a \pmod{n}$ and $x \equiv bsn \equiv b \pmod{m}$.

If x is a solution, then adding any multiple of mn is obviously still a solution. Conversely, if x_1 and x_2 are two solutions of the given system of congruences, then they must be congruent modulo n and modulo m. Thus $x_1 - x_2$ is divisible by both n and m, so it is divisible by mn since by assumption $(n, m) = 1$. Therefore $x_1 \equiv x_2 \pmod{mn}$. □

Example 1.3.4.

The proof of Theorem 1.3.6 actually shows how to solve the given system of congruences. For example, if we wish to solve the system

$$x \equiv 7 \pmod{8} \qquad x \equiv 3 \pmod{5}$$

we first use the Euclidean algorithm to write $2 \cdot 8 - 3 \cdot 5 = 1$. Then $x = 7(-3)(5) + 3(2)(8) = -57$ is a solution, and the general solution is $x = -57 + 40t$. The smallest nonnegative solution is therefore 23, so we have

$$x \equiv 23 \pmod{40}\ .\ \square$$

Another proof of the existence of a solution in Theorem 1.3.6 can be given as follows. In some respects this method of solution is more intuitive and provides a convenient algorithm for solving the congruences. Given the congruences

$$x \equiv a \pmod{n} \qquad x \equiv b \pmod{m}$$

we can rewrite the first congruence as an equation in the form $x = a + qn$ for some $q \in \mathbf{Z}$. To find a simultaneous solution, we only need to substitute this expression for x in the second congruence, giving $a + qn \equiv b \pmod{m}$, or

$$qn \equiv b - a \pmod{m}\ .$$

Since $(n, m) = 1$, we can solve the congruence $nz \equiv 1 \pmod{m}$, and using this solution we can solve for q in the congruence $qn \equiv b - a \pmod{m}$.

Recall that we converted the first congruence $x \equiv a \pmod{m}$ to the equation $x = a + qn$. Now that we have a value for q, we can substitute, and so this gives the simultaneous solutions to the two congruences in the form $x = a + qn$. We can choose as a particular solution the smallest positive integer in this form. The general solution is obtained by adding multiples of mn.

Example 1.3.5.

To illustrate the second method of solution, again consider the system

$$x \equiv 7 \pmod{8} \qquad x \equiv 3 \pmod{5}\ .$$

The first congruence gives us the equation $x = 7+8q$, and then substituting we obtain $7 + 8q \equiv 3 \pmod{5}$, or equivalently, $3q \equiv -4 \pmod{5}$. Multiplying by 2, since $2 \cdot 3 \equiv 1 \pmod{5}$, gives $q \equiv -8 \pmod{5}$ or $q \equiv 2 \pmod{5}$. This yields the particular solution $x = 7 + 2 \cdot 8 = 23$. □

EXERCISES: SECTION 1.3

1. Solve the following congruences.
   †(a) $4x \equiv 1 \pmod{7}$
   (b) $2x \equiv 1 \pmod{9}$
   †(c) $5x \equiv 1 \pmod{32}$
   (d) $19x \equiv 1 \pmod{36}$
2. Write n as a sum of four squares for $1 \leq n \leq 20$.
3. Solve the following congruences.
   †(a) $10x \equiv 5 \pmod{21}$
   (b) $10x \equiv 5 \pmod{15}$
   †(c) $10x \equiv 4 \pmod{15}$
   (d) $10x \equiv 4 \pmod{14}$
4. Solve the following congruence. $20x \equiv 12 \pmod{72}$
5. †Solve the following congruence. $25x \equiv 45 \pmod{60}$
6. Find all integers x such that $3x + 7$ is divisible by 11.
   (New techniques are available for this problem, which was Exercise 22 in Section 1.1)

7. The smallest positive solution of the congruence $ax \equiv 0 \pmod{n}$ is called the **additive order** of a modulo n. Find the additive orders of each of the following elements, by solving the appropriate congruences.

   †(a) 8 modulo 12

   (b) 7 modulo 12

   †(c) 21 modulo 28

   (d) 12 modulo 18

8. Prove that if p is a prime number and a is any integer such that $p \nmid a$, then the additive order of a modulo p is equal to p.

9. Prove that if $n > 1$ and $a > 0$ are integers and $d = (a, n)$, then the additive order of a modulo n is n/d.

10. Let a, b, n be positive integers. Prove that if $a \equiv b \pmod{n}$, then $(a, n) = (b, n)$.

11. Show that 7 is a divisor of $(6! + 1)$, 11 is a divisor of $(10! + 1)$, and 19 is a divisor of $(18! + 1)$.

12. Show that $4 \cdot (n^2 + 1)$ is never divisible by 11.

13. Prove that the sum of the cubes of any three consecutive positive integers is divisible by 9. (Compare Exercise 21 of Section 1.1.)

14. Find the units digit of $3^{29} + 11^{12} + 15$.

    Hint: Choose an appropriate modulus n, and then reduce modulo n.

15. Solve the following congruences by trial and error.

    †(a) $x^2 \equiv 1 \pmod{16}$

    (b) $x^3 \equiv 1 \pmod{16}$

    †(c) $x^4 \equiv 1 \pmod{16}$

    (d) $x^8 \equiv 1 \pmod{16}$

16. Solve the following congruences by trial and error.

    (a) $x^3 + 2x + 2 \equiv 0 \pmod{5}$

    (b) $x^4 + x^3 + x^2 + x + 1 \equiv 0 \pmod{2}$

    (c) $x^4 + x^3 + 2x^2 + 2x \equiv 0 \pmod{3}$

17. List and solve all quadratic congruences modulo 3. That is, list and solve all congruences of the form $ax^2 + bx + c \equiv 0 \pmod{3}$. The only coefficients you need to consider are 0, 1, 2.

18. Solve the following system of congruences.

$$x \equiv 15 \pmod{27} \qquad x \equiv 16 \pmod{20}$$

19.† Solve the following system of congruences.

$$x \equiv 11 \pmod{16} \qquad x \equiv 18 \pmod{25}$$

20. Solve the following system of congruences.

$$2x \equiv 5 \pmod{7} \qquad 3x \equiv 4 \pmod{8}$$

Hint: First reduce to the usual form.

21. Solve the following system of congruences.

$$x \equiv a \pmod{n} \qquad x \equiv b \pmod{n+1}$$

22. Extend the techniques of the Chinese remainder theorem to solve the following system of congruences.

$$2x \equiv 3 \pmod{7} \qquad x \equiv 4 \pmod{6} \qquad 5x \equiv 50 \pmod{55}$$

23. This exercise extends the Chinese remainder theorem. Let m, n be positive integers, with $(m, n) = d$ and $[m, n] = k$. Prove that the system of congruences

$$x \equiv a \pmod{n} \qquad x \equiv b \pmod{m}$$

has a solution if and only if $a \equiv b \pmod{d}$, and in this case any two solutions are congruent modulo k.

24. (Casting out nines) Show that the remainder of an integer n when divided by 9 is the same as the remainder of the sum of its digits when divided by 9.

Hint: For example, $7862 \equiv 7 + 8 + 6 + 2 \pmod{9}$. How you can use the digits of 7862 to express it in terms of powers of 10?

Note: "Casting out nines" is a traditional method for checking a sum of a long column of large numbers by reducing each of the numbers modulo 9 and checking the sum modulo 9. This exercise shows that the method is practical, because it provides a quick algorithm for reducing an integer modulo 9.

25. Find a result similar to casting out nines for the integer 11.

26. Let p be a prime number and let a, b be any integers. Prove that

$$(a+b)^p \equiv a^p + b^p \pmod{p}\,.$$

27. Prove that in any Pythagorean triple (a, b, c), either a or b is divisible by 3, and one of a, b, c is divisible by 5.

28. Prove that there exist infinitely many prime numbers of the form $4m + 3$ (where m is an integer).

1.4 Integers Modulo n

In working with congruences, we have established that in computations involving addition, subtraction, and multiplication, we can consider congruent numbers to be interchangeable. In this section we will formalize this point of view. We will now consider entire congruence classes as individual entities, and we will work with these entities much as we do with ordinary numbers. The point of introducing the notation given below is to allow us to use our experience with ordinary numbers as a guide to working with congruence classes. Most of the laws of integer arithmetic hold for the arithmetic of congruence classes. The notable exception is that the product of two nonzero congruence classes may be zero.

1.4.1 Definition. *Let a and $n > 0$ be integers. The set of all integers which have the same remainder as a when divided by n is called the* ***congruence class of a modulo*** *n, and is denoted by $[a]_n$, where*

$$[a]_n = \{x \in \mathbf{Z} \mid x \equiv a \ (mod\ n)\} .$$

The collection of all congruence classes modulo n is called the ***set of integers modulo*** *n, denoted by $\mathbf{Z}_n$.*

Note that $[a]_n = [b]_n$ if and only if $a \equiv b \pmod{n}$. When the modulus is clearly understood from the context, the subscript n can be omitted and $[a]_n$ can be written simply as $[a]$.

A given congruence class can be denoted in many ways. For example, $x \equiv 5 \pmod{3}$ if and only if $x \equiv 8 \pmod{3}$, since $5 \equiv 8 \pmod{3}$. This shows that $[5]_3 = [8]_3$. We sometimes say that an element of $[a]_n$ is a **representative of the congruence class**. Each congruence class $[a]_n$ has a unique nonnegative representative that is smaller than n, namely, the remainder when a is divided by n. This shows that there are exactly n distinct congruence classes modulo n. For example, the congruence classes modulo 3 can be represented by 0, 1, and 2.

$$\begin{aligned} [0]_3 &= \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\} \\ [1]_3 &= \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\} \\ [2]_3 &= \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\} \end{aligned}$$

Each integer belongs to exactly one congruence class modulo 3, since the remainder on division by 3 is unique. In general, each integer belongs to a unique congruence class modulo n. Hence we have

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

The set $\mathbf{Z}_2$ consists of $[0]_2$ and $[1]_2$, where $[0]_2$ is the set of even numbers and $[1]_2$ is the set of odd numbers. With the new notation, the familiar rules

"even + even = even," "odd + even = odd," "odd + odd = even"

can be expressed as

$$[0]_2 + [0]_2 = [0]_2\,, \qquad [1]_2 + [0]_2 = [1]_2\,, \qquad [1]_2 + [1]_2 = [0]_2\,.$$

Similarly,

"even $\times$ even = even," "even $\times$ odd = even," "odd $\times$ odd = odd"

can be expressed as

$$[0]_2 \cdot [0]_2 = [0]_2\,, \qquad [0]_2 \cdot [1]_2 = [0]_2\,, \qquad [1]_2 \cdot [1]_2 = [1]_2\,.$$

These rules can be summarized by giving an addition table and a multiplication table (Table 1.4.1).

Table 1.4.1: Addition and Multiplication in $\mathbf{Z}_2$

+	[0]	[1]
[0]	[0]	[1]
[1]	[1]	[0]

·	[0]	[1]
[0]	[0]	[0]
[1]	[0]	[1]

To use the addition table, select an element a from the first column, and an element b from the top row. Read from left to right in the row to which a belongs, until reaching the column to which b belongs. The corresponding entry in the table is $a + b$. In this table, as we will sometimes do elsewhere, we have simplified our notation for congruence classes by omitting the subscript in $[a]_n$.

A similar addition and multiplication can be introduced in $\mathbf{Z}_n$, for any n. Given congruence classes in $\mathbf{Z}_n$, we add (or multiply) them by picking representatives of each congruence class. We then add (or multiply) the representatives, and find the congruence class to which the result belongs. This can be written formally as follows.

Addition: $[a]_n + [b]_n = [a + b]_n$

Multiplication: $[a]_n \cdot [b]_n = [ab]_n$

In $\mathbf{Z}_{12}$, for example, we have $[8]_{12} = [20]_{12}$ and $[10]_{12} = [34]_{12}$. Adding congruence classes gives the same answer, no matter which representatives we use: $[8]_{12} + [10]_{12} = [18]_{12} = [6]_{12}$ and also $[20]_{12} + [34]_{12} = [54]_{12} = [6]_{12}$.

1.4.2 Proposition. *Let n be a positive integer, and let a, b be any integers. Then the addition and multiplication of congruence classes given below are well-defined:*

$$[a]_n + [b]_n = [a+b]_n \ , \qquad [a]_n \cdot [b]_n = [ab]_n \ .$$

Proof. We must show that the given formulas do not depend on the integers a and b which have been chosen to represent the congruence classes with which we are concerned. Suppose that x and y are any other representatives of the congruence classes $[a]_n$ and $[b]_n$, respectively. Then $x \equiv a \pmod{n}$ and $y \equiv b \pmod{n}$, and so we can apply Proposition 1.3.3. It follows from that proposition that $x + y \equiv a + b \pmod{n}$ and $xy \equiv ab \pmod{n}$, and thus we have $[x]_n + [y]_n = [a+b]_n$ and $[x]_n \cdot [y]_n = [ab]_n$. Since the formulas we have given do not depend on the particular representatives chosen, we say that addition and multiplication are "well-defined." □

The familiar rules for addition and multiplication carry over from the addition and multiplication of integers. A complete discussion of these rules will be given in Chapter 5, when we study ring theory. If $[a]_n, [b]_n \in \mathbf{Z}_n$ and $[a]_n + [b]_n = [0]_n$, then $[b]_n$ is called an **additive inverse** of $[a]_n$. By Proposition 1.3.3 (b), additive inverses are unique. We will denote the additive inverse of $[a]_n$ by $-[a]_n$. It is easy to see that $-[a]_n$ is in fact equal to $[-a]_n$, since $[a]_n + [-a]_n = [a-a]_n = [0]_n$.

For any elements $[a]_n$, $[b]_n$, $[c]_n$ in $\mathbf{Z}_n$, the following laws hold.

Associativity:
$$([a]_n + [b]_n) + [c]_n = [a]_n + ([b]_n + [c]_n)$$
$$([a]_n \cdot [b]_n) \cdot [c]_n = [a]_n \cdot ([b]_n \cdot [c]_n)$$

Commutativity:
$$[a]_n + [b]_n = [b]_n + [a]_n$$
$$[a]_n \cdot [b]_n = [b]_n \cdot [a]_n$$

Distributivity:
$$[a]_n \cdot ([b]_n + [c]_n) = [a]_n \cdot [b]_n + [a]_n \cdot [c]_n$$

Identities:
$$[a]_n + [0]_n = [a]_n$$
$$[a]_n \cdot [1]_n = [a]_n$$

Additive inverses:
$$[a]_n + [-a]_n = [0]_n$$

We will give a proof of the distributive law and leave the proofs of the remaining properties as an exercise. If $a, b, c \in \mathbf{Z}$, then

$$\begin{aligned} [a]_n \cdot ([b]_n + [c]_n) &= [a]_n \cdot [b+c]_n = [a(b+c)]_n \\ &= [ab+ac]_n = [ab]_n + [ac]_n \\ &= [a]_n \cdot [b]_n + [a]_n \cdot [c]_n \ . \end{aligned}$$

The steps in the proof depend on the definitions of addition and multiplication and the equality $a(b+c) = ab + ac$, which is the distributive law for $\mathbf{Z}$.

In doing computations in $\mathbf{Z}_n$, the one point at which particular care must be taken is the cancellation law, which no longer holds in general. Otherwise, in almost all cases your experience with integer arithmetic can be trusted when working with congruence classes. A quick computation shows that $[6]_8 \cdot [5]_8 = [6]_8 \cdot [1]_8$, but $[5]_8 \neq [1]_8$. It can also happen that the product of nonzero classes is equal to zero. For example, $[6]_8 \cdot [4]_8 = [0]_8$.

1.4.3 Definition. *If $[a]_n$ belongs to $\mathbf{Z}_n$, and $[a]_n[b]_n = [0]_n$ for some nonzero congruence class $[b]_n$, then $[a]_n$ is called a* ***divisor of zero.***

If $[a]_n$ is not a divisor of zero, then in the equation $[a]_n[b]_n = [a]_n[c]_n$ we may cancel $[a]_n$, to get $[b]_n = [c]_n$. To see this, if $[a]_n[b]_n = [a]_n[c]_n$, then $[a]_n([b]_n - [c]_n) = [a]_n[b-c]_n = [0]_n$, and so $[b]_n - [c]_n$ must be zero since $[a]_n$ is not a divisor of zero. This shows that $[b]_n = [c]_n$.

1.4.4 Definition. *If $[a]_n$ belongs to $\mathbf{Z}_n$, and $[a]_n[b]_n = [1]_n$, for some congruence class $[b]_n$, then $[b]_n$ is called a* ***multiplicative inverse*** *of $[a]_n$ and is denoted by $[a]_n^{-1}$.*

In this case, we say that $[a]_n$ is an ***invertible*** *element of $\mathbf{Z}_n$, or a* ***unit*** *of $\mathbf{Z}_n$.*

The next proposition (which is just a restatement of Proposition 1.3.4) shows that a has a multiplicative inverse modulo n if and only if $(a, n) = 1$. When a satisfies this condition, it follows from Proposition 1.3.3 (b) that any two solutions to $ax \equiv 1 \pmod{n}$ are congruent modulo n, and so we are justified in referring to *the* multiplicative inverse of $[a]_n$, whenever it exists.

In $\mathbf{Z}_7$, each nonzero congruence class contains representatives which are relatively prime to 7, and so each nonzero congruence class has a multiplicative inverse. We can list them as $[1]_7^{-1} = [1]_7$, $[2]_7^{-1} = [4]_7$, $[3]_7^{-1} = [5]_7$, and $[6]_7^{-1} = [6]_7$. We did not need to list $[4]_7^{-1}$ and $[5]_7^{-1}$ since, in general, if $[a]_n^{-1} = [b]_n$, then $[b]_n^{-1} = [a]_n$.

From this point on, if the meaning is clear from the context we will omit the subscript on congruence classes. Using this convention in $\mathbf{Z}_n$, we note that if $[a]$ has a multiplicative inverse, then it cannot be a divisor of zero, since $[a][b] = [0]$ implies $[b] = [a]^{-1}([a][b]) = [a]^{-1}[0] = [0]$.

1.4.5 Proposition. *Let n be a positive integer.*

(a) *The congruence class $[a]_n$ has a multiplicative inverse in $\mathbf{Z}_n$ if and only if $(a, n) = 1$.*

(b) *A nonzero element of $\mathbf{Z}_n$ either has a multiplicative inverse or is a divisor of zero.*

Proof. (a) If $[a]$ has a multiplicative inverse, say $[a]^{-1} = [b]$, then $[a][b] = [1]$. Therefore $ab \equiv 1 \pmod{n}$, which implies that $ab = 1 + qn$ for some integer q. Thus $ab + (-q)n = 1$, and so $(a, n) = 1$.

Conversely, if $(a, n) = 1$, then there exist integers b and q such that $ab+qn = 1$. Reducing modulo n shows that $ab \equiv 1 \pmod{n}$, and so $[b] = [a]^{-1}$.

(b) Assume that a represents a nonzero congruence class, so that $n \nmid a$. If $(a, n) = 1$, then $[a]$ has a multiplicative inverse. If not, then $(a, n) = d$, where $1 < d < n$. In this case, since $d \mid n$ and $d \mid a$, we can find integers k, b with $n = kd$ and $a = bd$. Then $[k]$ is a nonzero element of $\mathbf{Z}_n$, but

$$[a][k] = [ak] = [bdk] = [bn] = [0],$$

which shows that $[a]$ is a divisor of zero. □

1.4.6 Corollary. *The following conditions on the modulus $n > 0$ are equivalent.*

(1) *The number n is prime.*

(2) *$\mathbf{Z}_n$ has no divisors of zero, except $[0]_n$.*

(3) *Every nonzero element of $\mathbf{Z}_n$ has a multiplicative inverse.*

Proof. Since n is prime if and only if every positive integer less than n is relatively prime to n, Corollary 1.4.6 follows from Proposition 1.4.5. □

The proof of Proposition 1.4.5 (a) shows that if $(a, n) = 1$, then the multiplicative inverse of $[a]$ can be computed by using the Euclidean algorithm.

Example 1.4.1.

For example, to find $[11]^{-1}$ in $\mathbf{Z}_{16}$ using the matrix form of the Euclidean algorithm (see the discussion preceding Example 1.1.5) we have the following computation:

$$\begin{bmatrix} 1 & 0 & 16 \\ 0 & 1 & 11 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -1 & 5 \\ 0 & 1 & 11 \end{bmatrix} \rightsquigarrow$$

$$\begin{bmatrix} 1 & -1 & 5 \\ -2 & 3 & 1 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 11 & -16 & 0 \\ -2 & 3 & 1 \end{bmatrix}.$$

Thus $16(-2) + 11 \cdot 3 = 1$, which shows that $[11]_{16}^{-1} = [3]_{16}$.

When the numbers are small, as in this case, it is often easier to use trial and error. The positive integers less than 16 and relatively prime to 16 are $1, 3, 5, 7, 9, 11, 13, 15$. It is easier to use the representatives $\pm 1, \pm 3, \pm 5, \pm 7$ since if $[a][b] = [1]$, then $[-a][-b] = [1]$, and so $[-a]^{-1} = -[a]^{-1}$. Now we observe that $3 \cdot 5 = 15 \equiv -1 \pmod{16}$, so $3(-5) \equiv 1 \pmod{16}$. Thus $[3]_{16}^{-1} = [-5]_{16} = [11]_{16}$ and $[-3]_{16}^{-1} = [5]_{16}$. Finally, $7 \cdot 7 \equiv 1 \pmod{16}$, so $[7]_{16}^{-1} = [7]_{16}$ and $[-7]_{16}^{-1} = [-7]_{16} = [9]_{16}$. □

Another way to find the inverse of an element $[a] \in \mathbf{Z}_n$ is to take successive powers of $[a]$. If $(a, n) = 1$, then $[a]$ is not a zero divisor, and so no power of $[a]$ can be zero. We let $[a]^0 = [1]$. The set of powers $[1]$, $[a]$, $[a]^2$, $[a]^3$, ... must contain fewer than n distinct elements, so after some point there must be a repetition. Suppose that the first repetition occurs for the exponent m, say $[a]^m = [a]^k$, with $k < m$. Then $[a]^{m-k} = [a]^0 = [1]$ since we can cancel $[a]$ from both sides a total of k times. This shows that for the first repetition we must have had $k = 0$, so actually $[a]^m = [1]$. From this we can see that $[a]^{-1} = [a]^{m-1}$.

Example 1.4.2.

To find $[11]_{16}^{-1}$, we can list the powers of $[11]_{16}$. We have $[11]^2 = [-5]^2 = [9]$, $[11]^3 = [11]^2[11] = [99] = [3]$, and $[11]^4 = [11]^3[11] = [33] = [1]$. Thus again we see that $[11]_{16}^{-1} = [3]_{16}$. □

We are now ready to continue our study of equations in $\mathbf{Z}_n$. A linear congruence of the form $ax \equiv b \pmod{n}$ can be viewed as a linear equation $[a]_n[x]_n = [b]_n$ in $\mathbf{Z}_n$. If $[a]_n$ has a multiplicative inverse, then there is a unique congruence class $[x]_n = [a]_n^{-1}[b]_n$ that is the solution to the equation. Without the notation for congruence classes we would need to modify the statement regarding uniqueness to say that if x_0 is a solution of $ax \equiv b \pmod{n}$, then so is $x_0 + qn$, for any integer q.

It is considerably harder to solve nonlinear congruences of the form $a_k x^k + \ldots + a_1 x + a_0 \equiv 0 \pmod{n}$, where $a_k, \ldots, a_0 \in Z$. It can be shown that in solving congruences modulo n of degree greater than or equal to 1, the problem reduces to solving congruences modulo p^α for the prime factors of n. This question is usually addressed in a course on elementary number theory, where the Chinese remainder theorem is used to show how to determine the solutions modulo a prime power p^α (for integers $\alpha \geq 2$) from the solutions modulo p. Then to determine the solutions modulo p we can proceed by trial and error, simply substituting each of $0, 1, \ldots, p-1$ into the congruence. Fermat's theorem (Corollary 1.4.12) can be used to reduce the problem to considering polynomials of degree at most $p - 1$.

We will prove this theorem of Fermat as a special case of a more general theorem due to Euler. Another proof will also be given in Section 3.2, which takes advantage of the concepts we will have developed by then. The statement of Euler's theorem involves a function of paramount importance in number theory and algebra, which we now introduce.

1.4.7 Definition. *Let n be a positive integer. The number of positive integers less than or equal to n which are relatively prime to n will be denoted by $\varphi(n)$. This function is called* ***Euler's φ-function****, or the* ***totient function****.*

In Section 1.2 we gave a procedure for listing the positive integers less than n and relatively prime to n. However, in many cases we only need to determine the numerical value of $\varphi(n)$, without actually listing the numbers themselves. With the formula in Proposition 1.4.8, $\varphi(n)$ can be given in terms of the prime factorization of n. Note that $\varphi(1) = 1$.

1.4.8 Proposition. *If the prime factorization of n is $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, where $\alpha_i > 0$ for $1 \leq i \leq k$, then*

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right).$$

Proof. See Exercises 17, 29, and 30. A proof of this result will also be presented in Section 3.5. □

Example 1.4.3.

Using the formula in Proposition 1.4.8, we have

$$\varphi(10) = 10\left(\frac{1}{2}\right)\left(\frac{4}{5}\right) = 4 \qquad \text{and} \qquad \varphi(36) = 36\left(\frac{1}{2}\right)\left(\frac{2}{3}\right) = 12\,. \ \square$$

1.4.9 Definition. *The set of units of $\mathbf{Z}_n$, the congruence classes $[a]$ such that $(a, n) = 1$, will be denoted by $\mathbf{Z}_n^\times$.*

1.4.10 Proposition. *The set $\mathbf{Z}_n^\times$ of units of $\mathbf{Z}_n$ is closed under multiplication.*

Proof. This can be shown either by using Proposition 1.2.3 (d) or by using the formula $([a][b])^{-1} = [b]^{-1}[a]^{-1}$. □

The number of elements of $\mathbf{Z}_n^\times$ is given by $\varphi(n)$. The next theorem should be viewed as a result on powers of elements in $\mathbf{Z}_n^\times$, although it is phrased in the more familiar congruence notation.

1.4.11 Theorem (Euler). *If $(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

Proof. In the set $\mathbf{Z}_n$, there are $\varphi(n)$ congruence classes which are represented by an integer relatively prime to n. Let these representatives be $\{a_1, \ldots, a_{\varphi(n)}\}$. For the given integer a, consider the congruence classes represented by the products $\{aa_1, \ldots, aa_{\varphi(n)}\}$. By Proposition 1.3.3 (b) these are all distinct because $(a, n) = 1$.

Since each of the products is still relatively prime to n, we must have a representative from each of the $\varphi(n)$ congruence classes we started with. Therefore

$$a_1 a_2 \cdots a_{\varphi(n)} \equiv (aa_1)(aa_2)\cdots(aa_{\varphi(n)}) \equiv a^{\varphi(n)} a_1 a_2 \cdots a_{\varphi(n)} \pmod{n}.$$

Since the product $a_1 \cdots a_{\varphi(n)}$ is relatively prime to n, we can cancel it in the congruence

$$a_1 a_2 \cdots a_{\varphi(n)} \equiv a^{\varphi(n)} a_1 a_2 \cdots a_{\varphi(n)} \pmod{n},$$

and so we have $a^{\varphi(n)} \equiv 1 \pmod{n}$. □

1.4.12 Corollary (Fermat). *If p is a prime number, then for any integer a we have $a^p \equiv a \pmod{p}$.*

Proof. If $p \mid a$, then trivially $a^p \equiv a \equiv 0 \pmod{p}$. If $p \nmid a$, then $(a, p) = 1$ and Euler's theorem gives $a^{\varphi(p)} \equiv 1 \pmod{p}$. Then since $\varphi(p) = p - 1$, we have $a^p \equiv a \pmod{p}$. □

It is instructive to include another proof of Fermat's "little" theorem, one that does not depend on Euler's theorem. Expanding $(a + b)^p$ we obtain

$$(a+b)^p = a^p + pa^{p-1}b + \frac{p(p-1)}{1 \cdot 2} a^{p-2}b^2 + \ldots + pab^{p-1} + b^p.$$

For $k \neq 0, k \neq p$, each of the coefficients

$$\frac{p!}{k!(p-k)!}$$

is an integer and has p as a factor, since p is a divisor of the numerator but not the denominator. Therefore

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

Using induction, this can be extended to more terms, giving $(a + b + c)^p \equiv a^p + b^p + c^p \pmod{p}$, etc. Writing a as $(1 + 1 + \ldots + 1)$ shows that

$$a^p = (1 + 1 + \ldots + 1)^p \equiv 1^p + \ldots + 1^p \equiv a \pmod{p}.$$

As a final remark we note that if $(a, n) = 1$, then the multiplicative inverse of $[a]_n$ can be given explicitly as $[a]_n^{\varphi(n)-1}$, since by Euler's theorem, $a \cdot a^{\varphi(n)-1} \equiv 1 \pmod{n}$. Note also that for a given n the exponent $\varphi(n)$ in Euler's theorem may not be the smallest exponent possible. For example, in $\mathbf{Z}_8$ the integers $\pm 1, \pm 3$, are relatively prime to 8, and Euler's theorem states that $a^4 \equiv 1 \pmod{8}$ for each of these integers. In fact, $a^2 \equiv 1 \pmod{8}$ for $a = \pm 1, \pm 3$.

EXERCISES: SECTION 1.4

1. Make addition and multiplication tables for the following sets.
   (a) $\mathbf{Z}_3$
   (b) $\mathbf{Z}_4$
   †(c) $\mathbf{Z}_{12}$
2. Make multiplication tables for the following sets.
   (a) $\mathbf{Z}_6$
   (b) $\mathbf{Z}_7$
   (c) $\mathbf{Z}_8$
3. Find the multiplicative inverses of the given elements (if possible).
   †(a) $[14]$ in $\mathbf{Z}_{15}$
   (b) $[38]$ in $\mathbf{Z}_{83}$
   †(c) $[351]$ in $\mathbf{Z}_{6669}$
   (d) $[91]$ in $\mathbf{Z}_{2565}$
4. Let a and b be integers.
   (a) Prove that $[a]_n = [b]_n$ if and only if $a \equiv b \pmod{n}$.
   (b) Prove that either $[a]_n \cap [b]_n = \emptyset$ or $[a]_n = [b]_n$.
5. Prove that each congruence class $[a]_n$ in $\mathbf{Z}_n$ has a unique representative r that satisfies $0 \leq r < n$.
6. Let m and n be positive integers such that $m \mid n$. Show that for any integer a, the congruence class $[a]_m$ is the union of the congruence classes $[a]_n$, $[a+m]_n$, $[a+2m]_n$, $\ldots$, $[a+n-m]_n$.
7. Prove that the associative and commutative laws hold for addition and multiplication of congruence classes, as defined in Proposition 1.4.2.
8. Use Proposition 1.3.3 (b) to show that if $[b]$ and $[c]$ are both multiplicative inverses of $[a]$ in $\mathbf{Z}_n$, then $b \equiv c \pmod{n}$.
9. Let $(a, n) = 1$. The smallest positive integer k such that $a^k \equiv 1 \pmod{n}$ is called the **multiplicative order** of $[a]$ in $\mathbf{Z}_n^\times$.
   †(a) Find the multiplicative orders of $[5]$ and $[7]$ in $\mathbf{Z}_{16}^\times$.
   (b) Find the multiplicative orders of $[2]$ and $[5]$ in $\mathbf{Z}_{17}^\times$.
10. Let $(a, n) = 1$. If $[a]$ has multiplicative order k in $\mathbf{Z}_n^\times$, show that $k \mid \varphi(n)$.
11. †In $\mathbf{Z}_9^\times$ each element is equal to a power of $[2]$. (Verify this.) Can you find a congruence class in $\mathbf{Z}_8^\times$ such that each element of $\mathbf{Z}_8^\times$ is equal to some power of that class? Answer the same question for $\mathbf{Z}_7^\times$.

12. Generalizing Exercise 11, we say that the set of units $\mathbf{Z}_n^\times$ of $\mathbf{Z}_n$ is **cyclic** if it has an element of multiplicative order $\varphi(n)$. Show that $\mathbf{Z}_{10}^\times$ and $\mathbf{Z}_{11}^\times$ are cyclic, but $\mathbf{Z}_{12}^\times$ is not.

13. An element $[a]$ of $\mathbf{Z}_n$ is said to be **idempotent** if $[a]^2 = [a]$.

    †(a) Find all idempotent elements of $\mathbf{Z}_6$ and $\mathbf{Z}_{12}$.

    (b) Find all idempotent elements of $\mathbf{Z}_{10}$ and $\mathbf{Z}_{30}$.

14. If p is a prime number, show that $[0]$ and $[1]$ are the only idempotent elements in $\mathbf{Z}_p$.

15. If n is not a prime power, show that $\mathbf{Z}_n$ has an idempotent element different from $[0]$ and $[1]$.

    Hint: Suppose that $n = bc$, with $(b, c) = 1$. Solve the simultaneous congruences $x \equiv 1 \pmod{b}$ and $x \equiv 0 \pmod{c}$.

16. An element $[a]$ of $\mathbf{Z}_n$ is said to be **nilpotent** if $[a]^k = [0]$ for some k. Show that $\mathbf{Z}_n$ has no nonzero nilpotent elements if and only if n has no factor that is a square (except 1).

17. Using the formula for $\varphi(n)$, compute $\varphi(27)$, $\varphi(81)$, and $\varphi(p^\alpha)$, where p is a prime number. Give a proof that the formula for $\varphi(n)$ is valid when $n = p^\alpha$, where p is a prime number.

18. Show that if a and b are positive integers such that $a \mid b$, then $\varphi(a) \mid \varphi(b)$.

19. Find all integers $n > 1$ such that $\varphi(n) = 2$.

20. Show that $\varphi(1)+\varphi(p)+\ldots+\varphi(p^\alpha) = p^\alpha$ for any prime number p and any positive integer α.

21. Show that if $n > 2$, then $\varphi(n)$ is even.

22. For $n = 12$ show that $\sum_{d|n} \varphi(d) = n$. Do the same for $n = 18$.

23. Show that if $n > 1$, then the sum of all positive integers less than n and relatively prime to n is $n\varphi(n)/2$. That is, $\sum_{0<a<n,\ (a,n)=1} a = n\varphi(n)/2$.

24. Show that if p is a prime number, then the congruence $x^2 \equiv 1 \pmod{p}$ has only the solutions $x \equiv 1$ and $x \equiv -1$.

25. Let a, b be integers, and let p be a prime number of the form $p = 2k+1$. Show that if $p \nmid a$ and $a \equiv b^2 \pmod{p}$, then $a^k \equiv 1 \pmod{p}$.

26. Let $p = 2k+1$ be a prime number. Show that if a is an integer such that $p \nmid a$, then either $a^k \equiv 1 \pmod{p}$ or $a^k \equiv -1 \pmod{p}$.

27. Prove Wilson's theorem, which states that if p is a prime number, then $(p-1)! \equiv -1 \pmod{p}$.

    Hint: $(p-1)!$ is the product of all elements of $\mathbf{Z}_p^\times$. Pair each element with its inverse, and use Exercise 24. For three special cases see Exercise 11 in Section 1.3.

28. Prove that if $(m, n) = 1$, then $n^{\varphi(m)} + m^{\varphi(n)} \equiv 1 \pmod{mn}$.

29. Prove that if m, n are positive integers with $(m, n) = 1$, then $\varphi(mn) = \varphi(m)\varphi(n)$.

    Hint: Use the Chinese remainder theorem to show that each pair of elements $[a]_m$ and $[b]_n$ (in $\mathbf{Z}_m$ and $\mathbf{Z}_n$ respectively) corresponds to a unique element $[x]_{mn}$ in $\mathbf{Z}_{mn}$. Then show that under this correspondence, $[a]$ and $[b]$ are units if and only if $[x]$ is a unit.

30. Use Exercise 17 and Exercise 29 to prove Proposition 1.4.8.

Notes

The prime numbers are the basic the basic building blocks in number theory, since every positive integer can be written (essentially uniquely) as a product of prime numbers. (If you are reading this before studying the chapter, perhaps we need to remind you that an integer $p > 1$ is called prime if its only positive divisors are 1 and p.) Euclid considered primes and proved that there are infinitely many. When we look at the sequence of primes

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \ldots$$

we observe that except for 2, all primes are odd. Any two odd primes on the list must differ by at least 2, but certain pairs of "twin primes" that differ by the minimal amount 2 do appear, for example,

$$(3, 5), (5, 7), (11, 13), (17, 19), (29, 31), (41, 43), \ldots.$$

Are there infinitely many "twin prime" pairs? The answer to this innocent question is unknown.

Although any positive integer is a product of primes, what about sums? Another open question is attributed to Christian Goldbach (1690–1764). He asked whether every even integer greater than 2 can be written as the sum of two primes. (Since the sum of two odd primes is even, the only way to write an odd integer as a sum of two primes is to use an odd prime added to 2. That means that the only odd primes that can be represented as a sum of two primes are the ones that occur as the larger prime in a pair of "twin primes.") We invite you to experiment in writing some even integers as sums of two primes.

A beautiful theorem proved by Joseph Louis Lagrange (1736–1813) in 1770 states that every positive integer can be written as the sum of four squares (where an integer of the form n^2 is called a square). Could we get by with fewer than four squares? The answer is no; try representing 7 as a sum of three squares. This naturally leads to the question of which positive integers can be written as the sum of three squares. The answer is that n can be written as a sum of three squares if and

ANSWERS TO SELECTED EXERCISES

Exercises for which a solution is given are marked in the text by the symbol †.

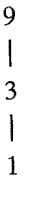
Chapter 1

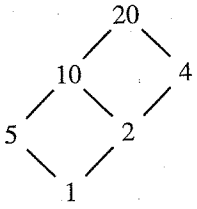
Section 1.1

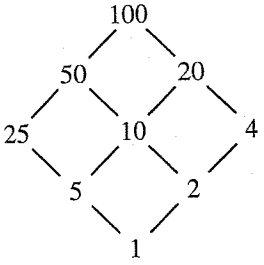
3. (a) $\gcd(35, 14) = 7$ (c) $\gcd(252, 180) = 36$ (e) $\gcd(7655, 1001) = 1$
5. (a) $7 = 1 \cdot 35 + (-2) \cdot 14$ (c) $36 = (-2) \cdot 252 + 3 \cdot 180$
   (e) $1 = (-397) \cdot 7655 + 3036 \cdot 1001$
22. The integer x must have remainder 5 when divided by 11.

Section 1.2

1. (a) $35 = 5^1 7^1$, $14 = 2^1 7^1$, $(35, 14) = 7$, $[35, 14] = 70$.
   (c) $252 = 2^2 3^2 7^1$, $180 = 2^2 3^2 5^1$, $(252, 180) = 36$, $[252, 180] = 1260$.
   (e) $6643 = 7^1 13^1 73^1$, $2873 = 13^2 17^1$, $(6643, 2873) = 13$, $[6643, 2873] = 1468103$.
3. for $a = 4$: $\{1, 3\}$; for $a = 6$: $\{1, 5\}$; ... for $a = 9$: $\{1, 2, 4, 5, 7, 8\}$; ...
   for $a = 15$: $\{1, 2, 4, 7, 8, 11, 13, 14\}$; etc.
5. Diagrams of divisors of 9, 20, and 100:







Section 1.3

1. (a) $x \equiv 2 \pmod 7$ (c) $x \equiv 13 \pmod{32}$
3. (a) $x \equiv 11 \pmod{21}$ (c) No solution
5. $x \equiv 9, 21, 33, 45, 57 \pmod{60}$
7. (a) 3 (c) 4
15. (a) $x \equiv 1, 7, 9, 15 \pmod{16}$ (c) $x \equiv 1, 3, 5, 7, 9, 11, 13, 15 \pmod{16}$
19. $x \equiv 43 \pmod{400}$

Section 1.4

1. Multiplication table for $\mathbf{Z}_{12}$:

·	0	1	2	3	4	5	6	7	8	9	10	11
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11
2	0	2	4	6	8	10	0	2	4	6	8	10
3	0	3	6	9	0	3	6	9	0	3	6	9
4	0	4	8	0	4	8	0	4	8	0	4	8
5	0	5	10	3	8	1	6	11	4	9	2	7
6	0	6	0	6	0	6	0	6	0	6	0	6
7	0	7	2	9	4	11	6	1	8	3	10	5
8	0	8	4	0	8	4	0	8	4	0	8	4
9	0	9	6	3	0	9	6	3	0	9	6	3
10	0	10	8	6	4	2	0	10	8	6	4	2
11	0	11	10	9	8	7	6	5	4	3	2	1

3. (a) [14] (c) Not invertible.
9. (a) The element [5] has multiplicative order 4, and [7] has multiplicative order 2.
11. There is no such congruence class in $\mathbf{Z}_8^\times$. In $\mathbf{Z}_7^\times$ each element is a power of [3] (or [5]).
13. (a) The idempotent elements of $\mathbf{Z}_6$ are [0], [1], [3], [4], and the idempotent elements of $\mathbf{Z}_{12}$ are [0], [1], [4], [9].

Chapter 2

Section 2.1

1. (a) The function f is one-to-one and onto.
   (c) The function f is one-to-one and onto if and only if $(m, n) = 1$.
3. (a) $f^{-1}(x) = x - 3$
   (c) If $(m, n) = 1$, and $km \equiv 1 \pmod{n}$, then $f^{-1}([x]_n) = [kx - kb]_n$, for all $[x]_n \in \mathbf{Z}_n$.
6. (a) There are 8 functions from S into T, and 9 from T into S.
8. The formula in (e) defines a function; the formulas in (a) and (c) do not.
10. (a) $f([8]_8) \neq f([0]_8)$ (c) $h([4]_4) \neq h([0]_4)$

Section 2.2

1. (a) We have $f(\mathbf{Z}) = \{1, i, -1, -i\}$, $\mathbf{Z}/f = \mathbf{Z}_4$, and the function $\bar{f} : \mathbf{Z}/f \to f(\mathbf{Z})$ is defined by $\bar{f}([n]_4) = i^n$.
   (c) We have $h(\mathbf{Z}_{12}) = \{[0]_{12}, [9]_{12}, [6]_{12}, [3]_{12}\}$ and $\mathbf{Z}_{12}/h = \{[[0]_{12}], [[1]_{12}], [[2]_{12}], [[3]_{12}]\}$, where $[[0]_{12}] = \{[0]_{12}, [4]_{12}, [8]_{12}\}$, $[[1]_{12}] = \{[1]_{12}, [5]_{12}, [9]_{12}\}$, $[[2]_{12}] = \{[2]_{12}, [6]_{12}, [10]_{12}\}$, $[[3]_{12}] = \{[3]_{12}, [7]_{12}, [11]_{12}\}$. The function $\bar{h} : \mathbf{Z}_{12}/h \to h(\mathbf{Z}_{12})$ is defined by $\bar{h}([[n]_{12}]) = h([n]_{12}) = [9n]_{12}$.
6. Define $\sim$ by $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$ if and only if $z_1 = z_2$.
8. (b) We have $[1] = \{\pm 1\}$ and $[6] = \{\pm 2^i 3^j \mid i \geq 1, j \geq 1\}$.

Section 2.3

1. (a) $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 6 & 7 & 4 & 1 & 5 \end{pmatrix}$ (c) $\tau^2\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 2 & 7 & 3 & 6 & 1 & 5 \end{pmatrix}$