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 18 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*

$$a = bq + r\,,\ \textit{with}\ 0 \le r < b\,.$$

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 $b \ge 1$, 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 $0 \le r$ and $r < b$. By definition, $r \ge 0$, and since $r \in R^+$, we must have $r = a - bq$ for some integer q. We cannot have $r \ge b$, since if we let $s = r - b$ we would have $s \ge 0$ 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 $0 \le r < b$.

To show that q and r are unique, suppose that we can also write $a = bp + s$ for integers p and s with $0 \le s < b$. We have $0 \le r < b$ and $0 \le s < b$, and this implies that $|s - r| < b$. But $bp + s = bq + r$ and so $s - r = b(q - p)$, which shows that $b \,|\, (s - r)$. 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 $0 \le r < b$. Since $b \,|\, a$ if and only if there exists $q \in \mathbf{Z}$ such that $a = bq$, we see that $b \,|\, a$ if and only if $r = 0$. This simple observation gives us a useful tool in doing number theoretic proofs. To show that $b \,|\, a$ 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 $I = b\mathbf{Z}$. □

Looking ahead[1].

> *Theorem 1.1.4 will reappear in Chapter 3, when we study cyclic groups, and again in Chapter 5. when we show that* $\mathbf{Z}$ *is a principal ideal domain.*

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 23 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).

[1] See the related comments in the preface.

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 $d \in I$, we have $d = ma + nb$ 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:

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1q_2 + r_2 \\ r_1 &= r_2q_3 + d \\ r_2 &= dq_4 + 0 \end{aligned} \qquad \begin{aligned} 126 &= 35 \cdot 3 + 21 \\ 35 &= 21 \cdot 1 + 14 \\ 21 &= 14 \cdot 1 + 7 \\ 14 &= 7 \cdot 2 + 0 . \end{aligned}$$

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:

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

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 $0 = (-5) \cdot 126 + 18 \cdot 35$ 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 $0 = m_1 a + n_1 b$, so if $(a, b) = ma + nb$, then adding the previous equation yields $(a, b) = (m + m_1)a + (n + n_1)b$. In fact, any multiple of the equation $0 = m_1 a + n_1 b$ could have been added, so there are infinitely many linear combinations of a and b that give (a, b).

Example 1.1.7 (Difference of squares)**.**

We will prove that if m and n are odd integers, then $4 \mid (m^2 - n^2)$.

Proof: Since m and n are odd, we can write them in the form $m = 2r + 1$ and $n = 2s + 1$, for some integers r and s. Then we can factor $m^2 - n^2$ to get $(m + n)(m - n)$, so substituting for m and n gives us

$$m^2 - n^2 = (2r + 1 + 2s + 1)(2r + 1 - 2s - 1) = (2)(r + s + 1)(2)(r - s).$$

Thus $m^2 - n^2 = 4(r + s + 1)(r - s)$, so we have an expression for $m^2 - n^2$ that has 4 as a factor, showing that $4 \mid (m^2 - n^2)$.

Comments: To use the fact that m and n are odd, we needed to find a way to represent odd integers. Then since we may have $m \neq n$, we had to be careful to use two different variables (r and s) in describing them. Note that there is a sharper result in Exercise 17. □

Example 1.1.8 (Cube roots of unity)**.**

For the complex number $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$, we will prove that $\omega^n = 1$ if and only if $3 \mid n$, for any integer n.

Proof: Since $(a+bi)(c+di) = (ac-bd)+(ad+bd)i$, a short calculation shows that $\omega^2 = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$, and $\omega^3 = 1$. If $n \in \mathbf{Z}$, and $3 \mid n$, then $n = 3q$ for some $q \in \mathbf{Z}$. Then $\omega^n = \omega^{3q} = (\omega^3)^q = 1^q = 1$.

Conversely, if $n \in \mathbf{Z}$ and $\omega^n = 1$, we can use the division algorithm to write $n = q \cdot 3 + r$, where the remainder r satisfies $0 \leq r < 3$. Then $1 = \omega^n = \omega^{3q+r} = (\omega^3)^q \omega^r = \omega^r$. Since $r = 0, 1, 2$ and we have shown that $\omega \neq 1$ and $\omega^2 \neq 1$, the only possibility is $r = 0$, and therefore $3 \mid n$. □

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 with an answer in the text (see "Selected Answers") are marked by the symbol †, while ‡marks those that appear in the supplement "Selected Solutions for Students".

1. Let $m, n, r, s \in \mathbf{Z}$. If $m^2 + n^2 = r^2 + s^2 = mr + ns$, prove that $m = r$ and $n = s$.
2. 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.
3. 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) $a = -1017$, $b = 99$
4. 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)

5. 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)

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

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

8. 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.

9. 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.

10. 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 $b \nmid (a + c)$.

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

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

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

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

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

16. Show that the positive integer n is the difference of two squares if and only if n is odd or divisible by 4.

17.‡ Show that the positive integer k is the difference of two odd squares if and only if k is divisible by 8. (This sharpens the result in Example 1.1.7.)

18.‡ 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 $a\mathbf{Z} \subseteq b\mathbf{Z}$.

19. 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.)

20. 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 $r_1 = r_2$.

21. 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.)

22. 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.

23. 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.

24. Show that 3 divides the sum of the cubes of any three consecutive positive integers.

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

26. Prove the following proposition. Let $a, b, n \in \mathbf{Z}$ with $(a, b) = d$, and let x_0, y_0 be a particular solution to the equation $ax + by = n$. Then every solution to $ax + by = n$ has the form $x = x_0 + \frac{b}{d}t$, $y = y_0 - \frac{a}{d}t$, for some $t \in \mathbf{Z}$. Furthermore, for every $t \in Z$ the integers $x = x_0 + \frac{b}{d}t$, $y = y_0 - \frac{a}{d}t$, yield a solution to $ax + by = n$.

27. Prove the following proposition. Let $a, b \in \mathbf{Z}^+$ with $(a, b) = 1$. Then the equation $ax + by = n$ has solutions $x, y \in \mathbf{Z}$ with $x \geq 0$, $y \geq 0$ if $n > ab - a - b$. Moreover, if $n = ab - a - b$, then there are no such solutions.

28. 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* $(a, b) = 1$.