2.1 THE DIVISION ALGORITHM

We have been exposed to the integers for several pages and as yet not a single divisibility property has been derived. It is time to remedy this situation. One theorem acts as the foundation stone upon which our whole development rests: the Division Algorithm. The result is familiar to most of us; roughly, it asserts that an integer a can be "divided" by a positive integer b in such a way that the remainder is smaller in size than b. The exact statement of this fact is

THEOREM 2-1 (Division Algorithm). *Given integers a and b, with $b > 0$, there exist unique integers q and r satisfying*

$$a = qb + r, \qquad 0 \leq r < b.$$

The integers q and r are called, respectively, the quotient and remainder in the division of a by b.

Proof: We begin by proving that the set

$$S = \{a - xb \mid x \text{ an integer}; a - xb \geq 0\}$$

is nonempty. For this, it suffices to exhibit a value of x making $a - xb$ nonnegative. Since the integer $b \geq 1$, we have $|a| b \geq |a|$ and so

$$a - (-|a|)b = a + |a| b \geq a + |a| \geq 0.$$

Hence, for the choice $x = -|a|$, $a - xb$ will lie in S. This paves the way for an application of the Well-Ordering Principle, from which we infer that the set S contains a smallest integer; call it r. By the definition of S, there exists an integer q satisfying

$$r = a - qb, \qquad 0 \leq r.$$

We argue that $r < b$. If this were not the case, then $r \geq b$ and

$$a - (q + 1)b = (a - qb) - b = r - b \geq 0.$$

The implication is that the integer $a-(q+1)b$ has the proper form to belong to the set S. But $a-(q+1)b=r-b<r$, leading to a contradiction of the choice of r as the smallest member of S. Hence, $r<b$.

We next turn to the task of showing the uniqueness of q and r. Suppose that a has two representations of the desired form; say

$$a=qb+r=q'b+r',$$

where $0\leq r<b$, $0\leq r'<b$. Then $r'-r=b(q-q')$ and, owing to the fact that the absolute value of a product is equal to the product of the absolute values,

$$|r'-r|=b\,|q-q'|\,.$$

Upon adding the two inequalities $-b<-r\leq 0$ and $0\leq r'<b$, we obtain $-b<r'-r<b$ or, in equivalent terms, $|r'-r|<b$. Thus, $b\,|q-q'|<b$, which yields

$$0\leq|q-q'|<1.$$

Since $|q-q'|$ is a nonnegative integer, the only possibility is that $|q-q'|=0$, whence $q=q'$; this in its turn gives $r=r'$, ending the proof.

A more general version of the Division Algorithm is obtained on replacing the restriction that b be positive by the simple requirement that $b\neq 0$.

COROLLARY. *If a and b are integers, with $b\neq 0$, then there exist unique integers q and r such that*

$$a=qb+r, \qquad 0\leq r<|b|.$$

Proof: It is enough to consider the case in which b is negative. Then $|b|>0$ and the theorem produces unique integers q' and r for which

$$a=q'\,|b|+r, \qquad 0\leq r<|b|.$$

Noting that $|b|=-b$, we may take $q=-q'$ to arrive at $a=qb+r$, with $0\leq r<|b|$.

To illustrate the Division Algorithm when $b < 0$, let us take $b = -7$. Then, for the choices of $a = 1, -2, 61$, and -59, one gets the expressions

$$\begin{aligned} 1 &= 0(-7) + 1, \\ -2 &= 1(-7) + 5, \\ 61 &= (-8)(-7) + 5, \\ -59 &= 9(-7) + 4. \end{aligned}$$

We wish to focus attention, not so much on the Division Algorithm, as on its applications. As a first example, note that with $b = 2$ the possible remainders are $r = 0$ and $r = 1$. When $r = 0$, the integer a has the form $a = 2q$ and is called *even*; when $r = 1$, the integer a has the form $a = 2q + 1$ and is called *odd*. Now a^2 is either of the form $(2q)^2 = 4k$ or $(2q + 1)^2 = 4(q^2 + q) + 1 = 4k + 1$. The point to be made is that the square of an integer leaves the remainder 0 or 1 upon division by 4.

We can also show the following: The square of any odd integer is of the form $8k + 1$. For, by the Division Algorithm, any integer is representable as one of the four forms $4q$, $4q + 1$, $4q + 2$, $4q + 3$. In this classification, only those integers of the forms $4q + 1$ and $4q + 3$ are odd. When the latter are squared, we find that

$$(4q + 1)^2 = 8(2q^2 + q) + 1 = 8k + 1$$

and similarly

$$(4q + 3)^2 = 8(2q^2 + 3q + 1) + 1 = 8k + 1.$$

As examples, the square of the odd integer 7 is $7^2 = 49 = 8 \cdot 6 + 1$, while the square of 13 is $13^2 = 169 = 8 \cdot 21 + 1$.

PROBLEMS 2.1

1. Prove that if a and b are integers, with $b > 0$, then there exist unique integers q and r satisfying $a = qb + r$, where $2b \leq r < 3b$.
2. Show that any integer of the form $6k + 5$ is also of the form $3k + 2$, but not conversely.
3. Use the Division Algorithm to establish that
   (a) every odd integer is either of the form $4k + 1$ or $4k + 3$;
   (b) the square of any integer is either of the form $3k$ or $3k + 1$;
   (c) the cube of any integer is either of the form $9k$, $9k + 1$, or $9k + 8$.

4. For $n \geq 1$, prove that $n(n+1)(2n+1)/6$ is an integer. [*Hint:* By the Division Algorithm, n has one of the forms $6k$, $6k+1$, $\ldots$, $6k+5$; establish the result in each of these six cases.]
5. Verify that if an integer is simultaneously a square and a cube (as is the case with $64 = 8^2 = 4^3$), then it must be either of the form $7k$ or $7k+1$.
6. Obtain the following version of the Division Algorithm: For integers a and b, with $b \neq 0$, there exist unique integers q and r satisfying $a = qb + r$, where $-\frac{1}{2}|b| < r \leq \frac{1}{2}|b|$. [*Hint:* First write $a = q'b + r'$, where $0 \leq r' < |b|$. When $0 \leq r' \leq \frac{1}{2}|b|$, let $r = r'$ and $q = q'$; when $\frac{1}{2}|b| < r' < |b|$, let $r = r' - |b|$ and $q = q' + 1$ if $b > 0$ or $q = q' - 1$ if $b < 0$.]
7. Prove that no integer in the sequence

$$11, 111, 1111, 11111, \ldots$$

is a perfect square. [*Hint:* A typical term $111 \cdots 111$ can be written as $111 \cdots 111 = 111 \cdots 108 + 3 = 4k + 3$.]

2.2 THE GREATEST COMMON DIVISOR

Of special significance is the case in which the remainder in the Division Algorithm turns out to be zero. Let us look into this situation now.

> DEFINITION 2-1. An integer b is said to be *divisible* by an integer $a \neq 0$, in symbols $a \mid b$, if there exists some integer c such that $b = ac$. We write $a \nmid b$ to indicate that b is not divisible by a.

Thus, for example, -12 is divisible by 4, since $-12 = 4(-3)$. However, 10 is not divisible by 3; for there is no integer c which makes the statement $10 = 3c$ true.

There is other language for expressing the divisibility relation $a \mid b$. One could say that a is a *divisor* of b, that a is a *factor* of b or that b is a *multiple* of a. Notice that, in Definition 2-1, there is a restriction on the divisor a: whenever the notation $a \mid b$ is employed, it is understood that a is different from zero.

If a is a divisor of b, then b is also divisible by $-a$ (indeed, $b = ac$ implies that $b = (-a)(-c)$), so that the divisors of an integer always occur in pairs. In order to find all the divisors of a given integer, it is sufficient to obtain the positive divisors and then adjoin to them the corresponding negative integers. For this reason, we shall usually limit ourselves to a consideration of positive divisors.