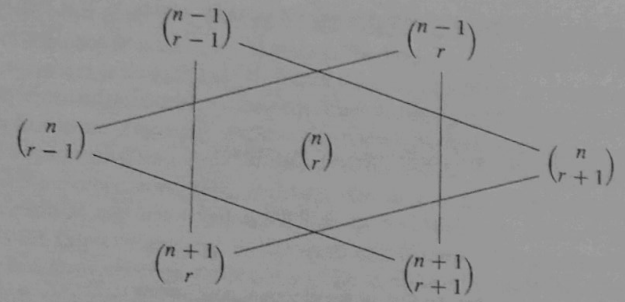

*H **1.37** For all odd $n \geq 1$, prove that there is a polynomial $g_n(x)$, all of whose coefficients are integers, such that

$$\sin(nx) = g_n(\sin x).$$

1.38 (i) What is the coefficient of x^{16} in $(1+x)^{20}$?

H (ii) How many ways are there to choose 4 colors from a palette containing paints of 20 different colors?

1.39 Give at least two different proofs that a set X with n elements has exactly 2^n subsets.

H **1.40** A weekly lottery asks you to select 5 different numbers between 1 and 45. At the week's end, 5 such numbers are drawn at random, and you win the jackpot if all your numbers match the drawn numbers. What is your chance of winning?

Definition. Define the ***n*th derivative** $f^{(n)}(x)$ of a function $f(x)$ inductively: set $f^{(0)}(x)$ to be $f(x)$ and, if $n \geq 0$, define $f^{(n+1)}(x) = (f^{(n)})'(x)$.

1.41 Assume that "term-by-term" differentiation holds for power series: if $f(x) = c_0 + c_1x + c_2x^2 + \cdots + c_nx^n + \cdots$, then the power series for the derivative $f'(x)$ is

$$f'(x) = c_1 + 2c_2x + 3c_3x^2 + \cdots + nc_nx^{n-1} + \cdots.$$

(i) Prove that $f(0) = c_0$.

(ii) Prove, for all $n \geq 0$, that

$$f^{(n)}(x) = n!c_n + (n+1)!c_{n+1}x + x^2g_n(x),$$

where $g_n(x)$ is some power series .

(iii) Prove that $c_n = f^{(n)}(x)(0)/n!$ for all $n \geq 0$. (Of course, this is Taylor's formula.)

*H **1.42** (*Leibniz*) A function $f : \mathbb{R} \to \mathbb{R}$ is called a ***C*$^\infty$-function** if it has an nth derivative $f^{(n)}(x)$ for every $n \geq 0$. Prove that if f and g are C^∞-functions, then

$$(fg)^{(n)}(x) = \sum_{k=0}^{n} \binom{n}{k} f^{(k)}(x) \cdot g^{(n-k)}(x).$$

1.43 Find $\sqrt{i}$.

***1.44** (i) If $z = r[\cos\theta + i\sin\theta]$, show that

$$w = \sqrt[n]{r}\,[\cos(\theta/n) + i\sin(\theta/n)]$$

is an nth root of z, where $r \geq 0$.

(ii) Show that every nth root of z has the form $\zeta^k w$, where ζ is a primitive nth root of unity and $k = 0, 1, 2, \ldots, n-1$.

1.45 H (i) Find $\sqrt{8 + 15i}$.

H (ii) Find all the fourth roots of $8 + 15i$.

→ 1.3 GREATEST COMMON DIVISORS

This is an appropriate time to introduce notation for some popular sets of numbers other than $\mathbb{Z}$ (denoting the integers) and $\mathbb{N}$ (denoting the natural numbers).

$\mathbb{Q} =$ the set of all rational numbers (or fractions), that is, all numbers of the form a/b, where a and b are integers and $b \neq 0$ (after the word *quotient*)

$\mathbb{R} =$ the set of all real numbers

$\mathbb{C} =$ the set of all complex numbers

Long division involves dividing an integer b by a nonzero integer a, giving

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

where q is an integer and $0 \leq r/a < 1$. We clear denominators to get a statement wholly in $\mathbb{Z}$.

→ **Theorem 1.32 (Division Algorithm).** *Given integers a and b with $a \neq 0$, there exist unique integers q and r with*

$$b = qa + r \quad \textit{and} \quad 0 \leq r < |a|.$$

Proof. We will prove the theorem in the special case in which $a > 0$ and $b \geq 0$; Exercise 1.47 on page 53 asks the reader to complete the proof. Long division involves finding the largest integer q with $qa \leq b$, which is the same thing as finding the smallest nonnegative integer of the form $b - qa$. We formalize this.

The set C of all nonnegative integers of the form $b - na$, where $n \geq 0$, is not empty because it contains $b = b - 0a$ (we are assuming that $b \geq 0$). By the Least Integer Axiom, C contains a smallest element, say, $r = b - qa$ (for some $q \geq 0$); of course, $r \geq 0$, by its definition. If $r \geq a$, then

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

Hence, $r - a = b - (q + 1)a$ is an element of C that is smaller than r, contradicting r being the smallest integer in C. Therefore, $0 \le r < a$.

It remains to prove the uniqueness of q and r. Suppose that $b = qa + r = q'a + r'$, where $0 \le r, r' < a$, so that

$$(q - q')a = r' - r.$$

We may assume that $r' \ge r$, so that $r' - r \ge 0$ and hence $q - q' \ge 0$. If $q \ne q'$, then $q - q' \ge 1$ (for $q - q'$ is an integer); thus, since $a > 0$,

$$(q - q')a \ge a.$$

On the other hand, since $r' < a$, Proposition A.2 gives

$$r' - r < a - r \le a.$$

Therefore, $(q - q')a \ge a$ and $r' - r < a$, contradicting the given equation $(q - q')a = r' - r$. We conclude that $q = q'$ and hence $r = r'$. •

→ **Definition.** If a and b are integers with $a \ne 0$, then the integers q and r occurring in the division algorithm are called the ***quotient*** and ***remainder*** after dividing b by a.

For example, there are only two possible remainders after dividing by 2, namely, 0 and 1. A number m is even if the remainder is 0; m is odd if the remainder is 1. Thus, either $m = 2q$ or $m = 2q + 1$.

Warning! The division algorithm makes sense, in particular, when b is negative. A careless person may assume that b and $-b$ leave the same remainder after dividing by a, and this is usually false. For example, let us divide 60 and -60 by 7.

$$60 = 7 \cdot 8 + 4 \quad \text{and} \quad -60 = 7 \cdot (-9) + 3.$$

Thus, the remainders after dividing 60 and -60 by 7 are different (see Exercise 1.84 on page 75).

The next result shows that there is no largest prime.

→ **Corollary 1.33.** *There are infinitely many primes.*

Proof. (***Euclid***) Suppose, on the contrary, that there are only finitely many primes. If $p_1, p_2, \ldots, p_k$ is the complete list of all the primes, define $M = (p_1 \cdots p_k) + 1$. By Theorem 1.2, M is either a prime or a product of primes. But M is neither a prime ($M > p_i$ for every i) nor does it have any prime divisor p_i, for dividing M by p_i gives remainder 1 and not 0. For example, dividing M by p_1 gives $M = p_1(p_2 \cdots p_k) + 1$, so that the quotient and remainder are $q = p_2 \cdots p_k$ and $r = 1$; dividing M by p_2 gives $M = p_2(p_1 p_3 \cdots p_k) + 1$, so that $q = p_1 p_3 \cdots p_k$ and $r = 1$; and so forth. The assumption that there are only finitely many primes leads to a contradiction, and so there must be an infinite number of them. •

An *algorithm* solving a problem is a set of directions which gives the correct answer after a finite number of steps, never at any stage leaving the user in doubt as to what to do next. The division algorithm is an algorithm in this sense: one starts with a and b and ends with q and r. Appendix B at the end of the book treats algorithms more formally, using ***pseudocodes***, which are general directions that can easily be translated into a programming language. For example, here is a pseudocode for the division algorithm.

```
Input: $b \ge a > 0$
Output: $q, r$
$q := 0$;    $r := b$
WHILE $r \ge a$ DO
    $r := r - a$
    $q := q + 1$
END WHILE
```

→ **Definition.** If a and b are integers, then a is a ***divisor*** of b if there is an integer d with $b = ad$ (synonyms are a ***divides*** b and also b is a ***multiple*** of a). We denote this by

$$a \mid b.$$

Note that $3 \mid 6$, because $6 = 3 \times 2$, but that $3 \nmid 5$ (that is, 3 does not divide 5): even though $5 = 3 \times \frac{5}{3}$, the fraction $\frac{5}{3}$ is not an integer. The numbers ± 1 and $\pm b$ are divisors of any integer b. We always have $b \mid 0$ (because $0 = b \times 0$); on the other hand, if $0 \mid b$, then $b = 0$ (because there is some d with $b = 0 \times d = 0$).

If a and b are integers with $a \ne 0$, then a is a divisor of b if and only if the remainder r given by the division algorithm is 0. If a is a divisor of b, then the remainder r given by the division algorithm is 0; conversely, if the remainder r is 0, then a is a divisor of b.

→ **Definition.** A ***common divisor*** of integers a and b is an integer c with $c \mid a$ and $c \mid b$. The ***greatest common divisor*** of a and b, denoted by $\gcd(a, b)$ [or, more briefly, by (a, b)], is defined by

$$\gcd(a, b) = \begin{cases} 0 & \text{if } a = 0 = b \\ \text{the largest common divisor of } a \text{ and } b & \text{otherwise.} \end{cases}$$

The notation (a, b) for the gcd is, obviously, the same notation used for the ordered pair, but the reader should have no difficulty understanding the intended meaning from the context in which the symbol occurs.

If a and m are positive integers with $a \mid m$, say, $m = ab$, we claim that $a \le m$. Since $0 < b$, we have $1 \le b$, because b is an integer, and so $a \le ab = m$. It follows that gcd's always exist.

If c is a common divisor of a and b, then so is $-c$. Since one of $\pm c$ is nonnegative, the gcd is always nonnegative. If at least one of a and b is nonzero, then $(a, b) > 0$.

Proposition 1.34. *If p is a prime and b is any integer, then*

$$\gcd(p, b) = \begin{cases} p & \text{if } p \mid b \\ 1 & \text{otherwise.} \end{cases}$$

Proof. A common divisor c of p and b is, of course, a divisor of p. But the only positive divisors of p are p and 1, and so $(p, b) = p$ or 1; it is p if $p \mid b$, and it is 1 otherwise. •

→ **Definition.** A ***linear combination*** of integers a and b is an integer of the form

$$sa + tb,$$

where s and t are integers.

The next result is one of the most useful properties of gcd's.

→ **Theorem 1.35.** *If a and b are integers, then $\gcd(a, b)$ is a linear combination of a and b.*

Proof. We may assume that at least one of a and b is not zero (otherwise, the gcd is 0 and the result is obvious). Consider the set I of all the linear combinations:

$$I = \{sa + tb : s, t \text{ in } \mathbb{Z}\}.$$

Both a and b are in I (take $s = 1$ and $t = 0$ or vice versa). It follows that I contains positive integers (if $a \neq 0$, then I contains $\pm a$), and hence the set P of all those positive integers that lie in I is nonempty. By the Least Integer Axiom, P contains a smallest positive integer, say, d, which we claim is the gcd.

Since d is in I, it is a linear combination of a and b: there are integers s and t with

$$d = sa + tb.$$

Let us show that d is a common divisor by trying to divide each of a and b by d. The division algorithm gives $a = qd + r$, where $0 \leq r < d$. If $r > 0$, then

$$r = a - qd = a - q(sa + tb) = (1 - qs)a + (-qt)b \text{ is in } P,$$

contradicting d being the smallest element of P. Hence $r = 0$ and $d \mid a$; a similar argument shows that $d \mid b$.

Finally, if c is a common divisor of a and b, then $a = ca'$ and $b = cb'$, so that c divides d, for $d = sa + tb = c(sa' + tb')$. But if $c \mid d$, then $|c| \leq d$, and so d is the gcd of a and b. •

If $d = \gcd(a, b)$ and if c is a common divisor of a and b, then $c \leq d$. The next corollary shows that more is true: $c \mid d$ for every common divisor c.

→ **Corollary 1.36.** *Let a and b be integers. A nonnegative common divisor d is their gcd if and only if $c \mid d$ for every common divisor c.*

Proof. *Necessity* (i.e., the implication ⇒) That every common divisor c of a and b is a divisor of $d = sa+tb$, has already been proved at the end of the proof of Theorem 1.35.

Sufficiency (i.e., the implication ⇐) Let d denote the gcd of a and b, and let d' be a nonnegative common divisor divisible by every common divisor c. Thus, $d' \leq d$, because $c \leq d$ is for every common divisor c. On the other hand, d itself is a common divisor, and so $d \mid d'$, by hypothesis. Hence, $d \leq d'$, and so $d = d'$. •

The proof of Theorem 1.35 contains an idea that will be used again.

→ **Corollary 1.37.** *Let I be a subset of $\mathbb{Z}$ such that*

(i) *0 is in I;*

(ii) *if a and b are in I, then $a - b$ is in I;*

(iii) *if a is in I and q is in $\mathbb{Z}$, then qa is in I.*

Then there is a nonnegative integer d in I with I consisting precisely of all the multiples of d.

Proof. If I consists of only the single integer 0, take $d = 0$. If I contains a nonzero integer a, then $(-1)a = -a$ is in I, by (iii). Thus, I contains $\pm a$, one of which is positive. By the Least Integer Axiom, I contains a smallest positive integer; call it d.

We claim that every element a in I is a multiple of d. The division algorithm gives integers q and r with $a = qd + r$, where $0 \leq r < d$. Since d is in I, so is qd, by (iii), and so (ii) gives $r = a - qd$ in I. But $r < d$, the smallest positive element of I, and so $r = 0$: thus, a is a multiple of d. •

The next result, called *Euclid's lemma*, is of great interest, for it gives one of the most important characterizations of prime numbers. Euclid's lemma is used frequently (at least ten times in this chapter alone), and an analog of it for irreducible polynomials is equally important. Looking further ahead, this lemma motivates the notion of *prime ideal*.

→ **Theorem 1.38 (Euclid's Lemma).** *If p is a prime and $p \mid ab$, then $p \mid a$ or $p \mid b$. More generally, if a prime p divides a product $a_1a_2 \cdots a_n$, then it must divide at least one of the factors a_i. Conversely, if $m \geq 2$ is an integer such that $m \mid ab$ always implies $m \mid a$ or $m \mid b$, then m is a prime.*

Proof. Assume that $p \nmid a$; that is, p does not divide a; we must show that $p \mid b$. Now the gcd $(p, a) = 1$, by Proposition 1.34. By Theorem 1.35, there are integers s and t with $1 = sp + ta$, and so

$$b = spb + tab.$$

Since $p \mid ab$, we have $ab = pc$ for some integer c, so that $b = spb + tpc = p(sb + tc)$ and $p \mid b$. The second statement now follows easily by induction on $n \geq 2$.

We prove the contrapositive: if m is composite, then there is a product ab divisible by m, yet neither factor is divisible by m. Since m is composite, $m = ab$, where $a < m$ and $b < m$. Thus, m divides ab, but m divides neither factor (if $m \mid a$, then $m \leq a$). •

Here is a concrete illustration showing that Euclid's lemma is not true in general: $6 \mid 12 = 4 \times 3$, but $6 \nmid 4$ and $6 \nmid 3$.

→ **Proposition 1.39.** *If p is a prime, then $p \mid \binom{p}{j}$ for $0 < j < p$.*

Proof. Recall that

$$\binom{p}{j} = \frac{p!}{j!(p-j)!} = \frac{p(p-1)\cdots(p-j+1)}{j!}.$$

Cross multiplying gives

$$j!\binom{p}{j} = p(p-1)\cdots(p-j+1),$$

so that $p \mid j!\binom{p}{j}$. If $p \mid j!$, then Euclid's lemma says that p would have to divide some factor $1, 2, \ldots, j$ of $j!$. Since $0 < j < p$, each factor of $j!$ is strictly less than p, and so p is not a divisor of any of them. Therefore, $p \nmid j!$. As $p \mid j!\binom{p}{j}$, Euclid's lemma now shows that p must divide $\binom{p}{j}$. •

Notice that the assumption that p is prime is needed; for example, $\binom{4}{2} = 6$, but $4 \nmid 6$.

→ **Definition.** Call integers a and b ***relatively prime*** if their gcd is 1.

Thus, a and b are relatively prime if their only common divisors are ± 1; moreover, 1 is a linear combination of a and b. For example, 2 and 3 are relatively prime, as are 8 and 15.

Here is a generalization of Euclid's lemma having the same proof.

→ **Corollary 1.40.** *Let a, b, and c be integers. If c and a are relatively prime and if $c \mid ab$, then $c \mid b$.*

Proof. By hypothesis, $ab = cd$ for some integer d. There are integers s and t with $1 = sc + ta$, and so $b = scb + tab = scb + tcd = c(sb + td)$. •

We see that it is important to know proofs: Corollary 1.40 does not follow from the statement of Euclid's lemma, but it does follow from its proof.

Definition. An expression a/b for a rational number (where a and b are integers) is in ***lowest terms*** if a and b are relatively prime.

Lemma 1.41. *Every nonzero rational number r has an expression in lowest terms.*

Proof. Since r is rational, $r = a/b$ for integers a and b. If $d = (a, b)$, then $a = a'd$, $b = b'd$, and $a/b = a'd/b'd = a'/b'$. But $(a', b') = 1$, for if $d' > 1$ is a common divisor of a' and b', then $d'd > d$ is a larger common divisor of a and b. •

Here is a description of the Euler ϕ-function that does not mention cyclotomic polynomials. Recall that $\phi(n)$ was defined as the number of *primitive* nth roots of unity ζ; that is, $\zeta^n = 1$, but $\zeta^d \neq 1$ for $1 \leq d < n$.

→ **Proposition 1.42.** *If $n \geq 1$ is an integer, then $\phi(n)$ is the number of integers k with $1 \leq k \leq n$ and $(k, n) = 1$.*

Proof. Since every nth root of unity has the form $\zeta = e^{2\pi ik/n}$, by Corollary 1.28, it suffices to prove that ζ is primitive if and only if $(k, n) = 1$.

If k and n are not relatively prime, then $n = dr$ and $k = ds$, where d, r, and s are integers, and $d > 1$; it follows that $r < n$. Hence, $\frac{k}{n} = \frac{ds}{dr} = \frac{s}{r}$, so that $(e^{2\pi ik/n})^r = (e^{2\pi is/r})^r = 1$, and hence $e^{2\pi ik/n}$ is not a primitive nth root of unity.

Conversely, assume that $(k, n) = 1$. Write $\zeta = e^{2\pi ik/n}$ and $\eta = e^{2\pi i/n}$. There are integers s and t with $sk + tn = 1$. Hence,

$$\eta = e^{2\pi i/n} = e^{2\pi iks/n}e^{2\pi int/n} = e^{2\pi iks/n} = \zeta^s.$$

If there is d with $1 \leq d < n$, then $\zeta^d = 1$ and $\eta^d = 1$, contradicting η being a primitive nth root of unity. Therefore, no such d exists, and ζ is a primitive nth root of unity. •

Proposition 1.43. *$\sqrt{2}$ is irrational.*

Proof. Suppose, on the contrary, that $\sqrt{2}$ is rational; that is, $\sqrt{2} = a/b$. We may assume that a/b is in lowest terms; that is, $(a, b) = 1$. Squaring, $a^2 = 2b^2$. By Euclid's lemma,[16] $2 \mid a$, so that $2m = a$, hence $4m^2 = a^2 = 2b^2$, and $2m^2 = b^2$. Euclid's lemma now gives $2 \mid b$, contradicting $(a, b) = 1$. •

This last result is significant in the history of mathematics. The ancient Greeks defined *number* to mean "positive integer," while (positive) rational numbers were viewed as "ratios" $a : b$ (which we can interpret as fractions a/b). That $\sqrt{2}$ is irrational was a shock to the Pythagoreans (around 600 B.C.), for it told them that $\sqrt{2}$ could not be defined in terms of numbers (positive integers) alone. On the other hand, they knew that the diagonal of a square having sides of length 1 has length $\sqrt{2}$. Thus, there is no

[16] This proof can be made more elementary; one needs only Proposition 1.14.

numerical solution to the equation $x^2 = 2$, but there is a geometric solution. By the time of Euclid (around 325 B.C.), this problem was resolved by splitting mathematics into two different disciplines: algebra and geometry. This resolution is probably one of the main reasons that the golden age of classical mathematics declined in Europe after the rise of the Roman Empire. For example, there were geometric ways of viewing addition, subtraction, multiplication, and division of segments (see Theorem 4.47), but it was virtually impossible to do any algebra. A sophisticated geometric argument (due to Eudoxus and given in Euclid's *Elements*) was needed to prove the version of cross-multiplication saying that if $a : b = c : d$, then $a : c = b : d$.

We quote van der Waerden, *Science Awakening*, page 125:

> Nowadays we say that the length of the diagonal is the "irrational number" $\sqrt{2}$, and we feel superior to the poor Greeks who "did not know irrationals." But the Greeks knew irrational ratios very well . . . That they did not consider $\sqrt{2}$ as a number was not a result of ignorance, but of strict adherence to the definition of number. *Arithmos* means quantity, therefore whole number. Their logical rigor did not even allow them to admit fractions; they replaced them by ratios of integers.
>
> For the Babylonians, every segment and every area simply represented a number . . . When they could not determine a square root exactly, they calmly accepted an approximation. Engineers and natural scientists have always done this. But the Greeks were concerned with exact knowledge, with "the diagonal itself," as Plato expresses it, not with an acceptable approximation.
>
> In the domain of numbers (positive integers), the equation $x^2 = 2$ cannot be solved, not even in that of ratios of numbers. But it is solvable in the domain of segments; indeed the diagonal of the unit square is a solution. Consequently, in order to obtain exact solutions of quadratic equations, we have to pass from the domain of numbers (positive integers) to that of geometric magnitudes. Geometric algebra is valid also for irrational segments and is nevertheless an exact science. It is therefore logical necessity, not the mere delight in the visible, which compelled the Pythagoreans to transmute their algebra into a geometric form.

Even though the Greek definition of number is no longer popular, their dichotomy still persists. For example, almost all American high schools teach one year of algebra followed by one year of geometry, instead of two years in which both subjects are developed together. The problem of defining *number* has arisen several times since the classical Greek era. In the 1500s, mathematicians had to deal with negative numbers and with complex numbers (see our discussion of cubic polynomials in Chapter 5); the description of real numbers generally accepted today dates from the late 1800s. There are echos of ancient Athens in our time. L. Kronecker (1823–1891) wrote,

> Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk. (God created the integers; everything else is the work of Man.)

Even today some logicians argue for a new definition of number.

Our discussion of gcd's is incomplete. What is $\gcd(12327, 2409)$? To ask the question another way, is the expression 2409/12327 in lowest terms? The next result not only enables one to compute gcd's efficiently, it also allows one to compute integers s and t expressing the gcd as a linear combination.[17] Before giving the theorem, consider the following example. Since $(2, 3) = 1$, there are integers s and t with $1 = 2s + 3t$. A moment's thought gives $s = -1$ and $t = 1$; but another moment's thought gives $s = 2$ and $t = -1$. We conclude that the coefficients s and t expressing the gcd as a linear combination are not uniquely determined. The algorithm below, however, always picks out a particular pair of coefficients.

→ **Theorem 1.44 (Euclidean Algorithm).** *Let a and b be positive integers. There is an algorithm that finds the* gcd *$d = (a, b)$, and there is an algorithm that finds a pair of integers s and t with $d = sa + tb$.*

Remark. The general case for arbitrary a and b follows from this, for

$$(a, b) = (|a|, |b|). \quad ◀$$

Proof. The idea is to keep repeating the division algorithm (we will show where this idea comes from after the proof is completed). Let us set $b = r_0$ and $a = r_1$. Repeated application of the division algorithm gives integers q_i, positive integers r_i, and equations:

$$\begin{array}{rll}
b = & q_1 a + r_2, & r_2 < a \\
a = r_1 = & q_2 r_2 + r_3, & r_3 < r_2 \\
r_2 = & q_3 r_3 + r_4, & r_4 < r_3 \\
& \vdots & \vdots \\
r_{n-3} = & q_{n-2} r_{n-2} + r_{n-1}, & r_{n-1} < r_{n-2} \\
r_{n-2} = & q_{n-1} r_{n-1} + r_n, & r_n < r_{n-1} \\
r_{n-1} = & q_n r_n &
\end{array}$$

[17] Every positive integer is a product of primes, and this is used, in Proposition 1.55, to compute gcd's. However, finding prime factorizations of large numbers is notoriously difficult; indeed, it is the basic reason why public key cryptography is secure.

(remember that all q_j and r_j are explicitly known from the division algorithm). Notice that there is a last remainder; the procedure stops because the remainders form a strictly decreasing sequence of nonnegative integers (indeed, the number of steps needed is less than a. Proposition 1.46 gives a smaller bound on the number of steps).

We use Corollary 1.36 to show that the last remainder $d = r_n$ is the gcd. Let us rewrite the top equations of the Euclidean algorithm without subscripts.

$$\begin{aligned} b &= qa + r \\ a &= q'r + s. \end{aligned}$$

If c is a common divisor of a and b, then the first equation shows that $c \mid r$. Going down to the second equation, we now know that $c \mid a$ and $c \mid r$, and so $c \mid s$. Continuing down the list, we see that c divides every remainder; in particular, $c \mid d$.

Let us now rewrite the bottom equations of the Euclidean algorithm without subscripts.

$$\begin{aligned} f &= ug + h \\ g &= u'h + k \\ h &= u''k + d \\ k &= vd \end{aligned}$$

Going from the bottom up, we have $d \mid k$ and $d \mid d$, so that $d \mid h$; going up again, $d \mid h$ and $d \mid k$ imply $d \mid g$. Working upward ultimately gives $d \mid a$ and $d \mid b$. We conclude that d is a common divisor. But $d = (a, b)$ because we saw, in the preceding paragraph, that if c is any common divisor, then $c \mid d$.

We now find s and t, again working from the bottom up. Rewrite the equation $h = u'k + d$ as $d = h - u'k$, and substitute $k = g - u'h$ from the equation above it:

$$d = h - u''k = h - u''(g - u'h) = (1 + u''u')h - u''g.$$

Thus, d is a linear combination of g and h. Continue this procedure, replacing h by $f - ug$, and so on, until d is written as a linear combination of a and b. •

We say that n is the ***number of steps*** in the Euclidean algorithm, for one does not know whether r_n in the $(n-1)$st step

$$r_{n-2} = q_{n-1}r_{n-1} + r_n$$

is the gcd until the division algorithm is applied to r_{n-1} and r_n.

Example 1.45.
Find (326, 78), express it as a linear combination of 326 and 78, and write 78/326 in lowest terms.

$$\begin{aligned} \boxed{326} &= 4 \times \boxed{78} + \boxed{14} && (1) \\ \boxed{78} &= 5 \times \boxed{14} + \boxed{8} && (2) \\ \boxed{14} &= 1 \times \boxed{8} + \boxed{6} && (3) \\ \boxed{8} &= 1 \times \boxed{6} + \boxed{2} && (4) \\ \boxed{6} &= 3 \times \boxed{2}. && (5) \end{aligned}$$

The Euclidean algorithm gives (326, 78) = 2.

We now express 2 as a linear combination of 326 and 78, working from the bottom up using the equations above.

$$\begin{aligned} 2 &= \boxed{8} - 1\boxed{6} \quad \text{by Eq. (4)} \\ &= \boxed{8} - 1\left(\boxed{14} - 1\boxed{8}\right) \quad \text{by Eq. (3)} \\ &= 2\boxed{8} - 1\boxed{14} \\ &= 2\left(\boxed{78} - 5\boxed{14}\right) - 1\boxed{14} \quad \text{by Eq. (2)} \\ &= 2\boxed{78} - 11\boxed{14} \\ &= 2\boxed{78} - 11\left(\boxed{326} - 4\boxed{78}\right) \quad \text{by Eq. (1)} \\ &= 46\boxed{78} - 11\boxed{326}; \end{aligned}$$

thus, $s = 46$ and $t = -11$.

Dividing numerator and denominator by the gcd, namely, 2, gives $78/326 = 39/163$, and the last expression is in lowest terms. ◀

The Greek terms for the Euclidean algorithm are *antanairesis* or *anthyphairesis*, either of which may be freely translated as "back and forth subtraction." Exercise 1.61 on page 54 says that $(b, a) = (b-a, a)$. If $b-a \geq a$, repeat to get $(b, a) = (b-a, a) = (b-2a, a)$. Keep subtracting until a pair a and $b - qa$ (for some q) is reached with $b - qa < a$. Thus, if $r = b - qa$, where $0 \leq r < a$, then

$$(b, a) = (b - a, a) = (b - 2a, a) = \cdots = (b - qa, a) = (r, a).$$

Now change direction: repeat the procedure beginning with the pair $(r, a) = (a, r)$, for $a > r$; eventually one reaches $(d, 0) = d$.

For example, antanairesis computes the gcd (326, 78) as follows:

$$(326, 78) = (248, 78) = (170, 78) = (92, 78) = (14, 78).$$

So far, we have been subtracting 78 from the other larger numbers. At this point, we now subtract 14 (this is the reciprocal aspect of antanairesis), for 78 > 14.

$$(78, 14) = (64, 14) = (50, 14) = (36, 14) = (22, 14) = (8, 14).$$

Again we change direction:

$$(14, 8) = (6, 8).$$

Change direction once again to get $(8, 6) = (2, 6)$, and change direction one last time to get

$$(6, 2) = (4, 2) = (2, 2) = (0, 2) = 2.$$

Thus, $\gcd(326, 78) = 2$.

The division algorithm (which is just iterated subtraction!) is a more efficient way of performing antanairesis. There are four subtractions in the passage from $(326, 78)$ to $(14, 78)$; the division algorithm expresses this as

$$326 = 4 \times 78 + 14.$$

There are then five subtractions in the passage from $(78, 14)$ to $(8, 14)$; the division algorithm expresses this as

$$78 = 5 \times 14 + 8.$$

There is one subtraction in the passage from $(14, 8)$ to $(6, 8)$:

$$14 = 1 \times 8 + 6.$$

There is one subtraction in the passage from $(8, 6)$ to $(2, 6)$:

$$8 = 1 \times 6 + 2,$$

and there are three subtractions from $(6, 2)$ to $(0, 2) = 2$:

$$6 = 3 \times 2.$$

These are the steps in the Euclidean algorithm.

The Euclidean algorithm was one of the first algorithms for which an explicit bound on the number of its steps in a computation was given. The proof of this involves the Fibonacci sequence

$$F_0 = 0, \quad F_1 = 1, \quad F_n = F_{n-1} + F_{n-2} \quad \text{for all } n \geq 2.$$

Proposition 1.46 (Lamé's[18] Theorem). *Let $b \geq a$ be positive integers, and let $d(a)$ be the number of digits in the decimal expression of a. If n is the number of steps in the Euclidean algorithm computing $\gcd(b, a)$, then*

$$n \leq 5d(a).$$

Proof. Let us denote b by r_0 and a by r_1 in the equations of the Euclidean algorithm on page 45, so that every equation there has the form

$$r_j = r_{j+1}q_{j+1} + r_{j+2}$$

except the last one, which is

$$r_{n-1} = r_n q_n.$$

Note that $q_n \geq 2$: if $q_n \leq 1$, then $r_{n-1} \leq q_n r_n = r_n$, contradicting $r_n < r_{n-1}$. Similarly, all $q_1, q_2, \ldots, q_{n-1} \geq 1$: otherwise $q_j = 0$ for some $j \leq n-1$, and $r_{j-1} = r_{j+1}$, contradicting the strict inequalities $r_n < r_{n-1} < \cdots < r_1 = b$.

Now

$$r_n \geq 1 = F_2$$

and, since $q_n \geq 2$,

$$r_{n-1} = r_n q_n \geq 2r_n \geq 2F_2 \geq 2 = F_3.$$

More generally, let us prove, by induction on $j \geq 0$, that

$$r_{n-j} \geq F_{j+2}.$$

The inductive step is

$$\begin{aligned} r_{n-j-1} &= r_{n-j}q_{n-j} + r_{n-j+1} \\ &\geq r_{n-j} + r_{n-j+1} \qquad \text{(since } q_{n-j} \geq 1\text{)} \\ &\geq F_{j+2} + F_{j+1} = F_{j+3}. \end{aligned}$$

We conclude that $a = r_1 = r_{n-(n-1)} \geq F_{n-1+2} = F_{n+1}$. By Corollary 1.16, $F_{n+1} > \gamma^{n-1}$, where $\gamma = \frac{1}{2}(1 + \sqrt{5})$, and so

$$a > \gamma^{n-1}.$$

Now $\log_{10}\gamma > \log_{10}(1.6) > \frac{1}{5}$, so that

$$\log_{10} a > (n-1)\log_{10}\gamma > (n-1)/5.$$

[18] This is an example in which a theorem's name is not that of its discoverer. Lamé's proof appeared in 1844. The earliest estimate for the number of steps in the Euclidean algorithm can be found in a rare book by Simon Jacob, published around 1564. There were also estimates by T. F. de Lagny in 1733, A.-A.-L. Reynaud in 1821, E. Léger in 1837, and P.-J.-E. Finck in 1841. [This earlier work is described in articles of P. Shallit (1994) and P. Schreiber (1995), respectively, in the journal *Historia Mathematica*.]

Therefore,

$$n - 1 < 5\log_{10} a < 5d(a),$$

because $d(a) = \lfloor \log_{10} a \rfloor + 1$, and so $n \le 5d(a)$ since $d(a)$, hence $5d(a)$, is an integer. •

For example, Lamé's theorem guarantees there are at most 10 steps needed to compute (326, 78), for $d(78) = 2$; actually, there are 5 steps.

The usual notation for the integer 5754 is an abbreviation of

$$5 \times 10^3 + 7 \times 10^2 + 5 \times 10 + 4.$$

The next result shows that there is nothing special about the number 10; any integer $b \ge 2$ can be used instead of 10.

→ **Proposition 1.47.** *If $b \ge 2$ is an integer, then every positive integer m has an expression in **base b**: there are integers d_i with $0 \le d_i < b$ such that*

$$m = d_k b^k + d_{k-1} b^{k-1} + \cdots + d_0;$$

moreover, this expression is unique if $d_k \neq 0$.

Remark. The numbers $d_k, \ldots, d_0$ are called the ***b-adic digits*** of m. ◄

Proof. We iterate the division algorithm to define integers a_i and d_i as follows.

$$\begin{aligned} m &= a_0 b + d_0, & 0 &\le d_0 < b \\ a_0 &= a_1 b + d_1, & 0 &\le d_1 < b \\ a_1 &= a_2 b + d_2, & 0 &\le d_2 < b \\ &\vdots & &\vdots \end{aligned}$$

An easy induction shows that $m = b^{i+1}a_i + b^i d_i + b^{i-1} d_{i-1} + \cdots + bd_1 + d_0$. There is an integer k with $b^k \le m < b^{k+1}$; for this k, we have $a_k = 0$ (if $a_k \neq 0$, then $a_k \ge 1$ and $m \ge b^{k+1}a_k \ge b^{k+1}$). Hence

$$m = b^k d_k + b^{k-1} d_{k-1} + b^{k-2} d_{k-2} + \cdots + bd_1 + d_0$$

is an expression for m in base b.

Before proving uniqueness of the digits d_i, we first observe that if $0 \le d_i < b$ for all i, then

$$\sum_{i=0}^{k} d_i b^i \le \sum_{i=0}^{k} (b-1) b^i = \sum_{i=0}^{k} b^{i+1} - \sum_{i=0}^{k} b^i = b^{k+1} - 1 < b^{k+1}. \tag{6}$$

We now prove, by induction on $k \ge 0$, that if $b^k \le m < b^{k+1}$, then the b-adic digits d_i in the expression $m = \sum_{i=0}^{k} d_i b^i$ are uniquely determined by m. Let $m = \sum_{i=0}^{k} d_i b^i = \sum_{i=0}^{k} c_i b^i$, where $0 \le d_i < b$ and $0 \le c_i < b$ for all i. Subtracting, we obtain

$$0 = \sum_{i=0}^{k} (d_i - c_i) b^i.$$

Eliminate any zero coefficients, and transpose all negative coefficients $d_i - c_i$, if any, to obtain an equation in which all coefficients are positive and in which the index sets I and J are disjoint:

$$L = \sum_{i \text{ in } I} (d_i - c_i) b^i = \sum_{j \text{ in } J} (c_j - d_j) b^j = R.$$

Let p be the largest index in I and let q be the largest index in J. Since I and J are disjoint, we may assume that $q < p$. As the left side L involves b^p with a nonzero coefficient, we have $L \ge b^p$; but Eq. (6) shows that the right side $R < b^{q+1} \le b^p$, a contradiction. Therefore, the b-adic digits are uniquely determined. •

Example 1.48.
Let us follow the steps in the proof of Proposition 1.47 to write 12345 in base 7. Repeated use of the division algorithm gives

$$\begin{aligned} 12345 &= 1763 \cdot 7 + 4 \\ 1763 &= 251 \cdot 7 + 6 \\ 251 &= 35 \cdot 7 + 6 \\ 35 &= 5 \cdot 7 + 0 \\ 5 &= 0 \cdot 7 + 5. \end{aligned}$$

The 7-adic digits of 12345 are thus 50664. ◄

The most popular bases are $b = 10$ (giving everyday *decimal* digits), $b = 2$ (giving *binary* digits, useful because a computer can interpret 1 as "on" and 0 as "off"), and $b = 16$ (*hexadecimal*, also for computers), but let us see that other bases can also be useful.

Example 1.49.
Here is a problem of Bachet de Méziriac from 1624. A merchant had a 40-pound weight that broke into 4 pieces. When the pieces were weighed, it was found that each piece was a whole number of pounds and that the four pieces could be used to weigh every integral weight between 1 and 40 pounds. What were the weights of the pieces?

Weighing means using a balance scale having two pans, with weights being put on either pan. Thus, given weights of 1 and 3 pounds, one can weigh a 2-pound weight □ by putting 1 and □ on one pan and 3 on the other pan.

A solution to Bachet's problem is 1, 3, 9, 27. If □ denotes a given integral weight, let us write the weights on one pan to the left of the semicolon and the weights on the other pan to the right of the semicolon. The number in boldface is the weight of □. The reader should note that Proposition 1.47 gives the uniqueness of the weights used in the pans.

1	1 ; □	**9**	9 ; □
2	3 ; 1, □	**10**	9, 1 ; □
3	3 ; □	**11**	9, 3 ; 1, □
4	3, 1 ; □	**12**	9, 3 ; □
5	9 ; 3, 1, □	**13**	9, 3, 1 ; □
6	9 ; 3, □	**14**	27 ; 9, 3, 1, □
7	9, 1 ; 3, □	**15**	27 ; 9, 3, □
8	9 ; 1, □		

The reader may complete this table for □ ≤ 40. ◀

Example 1.50.
Given a balance scale, the weight (as an integral number of pounds) of any person weighing at most 364 pounds can be found using only six lead weights.

We begin by proving that every positive integer m can be written

$$m = e_k 3^k + e_{k-1} 3^{k-1} + \cdots + 3e_1 + e_0,$$

where $e_i = -1, 0$, or 1.

The idea is to modify the 3-adic expansion

$$m = d_k 3^k + d_{k-1} 3^{k-1} + \cdots + 3d_1 + d_0.$$

where $d_i = 0, 1, 2$, by "carrying." If $d_0 = 0$ or 1, set $e_0 = d_0$ and leave d_1 alone. If $d_0 = 2$, set $e_0 = -1$, and replace d_1 by $d_1 + 1$ (we have merely substituted $3 - 1$ for 2). Now $1 \le d_1 + 1 \le 3$. If $d_1 + 1 = 1$, set $e_1 = 1$, and leave d_2 alone; if $d_1 + 1 = 2$, set $e_1 = -1$, and replace d_2 by $d_2 + 1$; if $d_1 + 1 = 3$, define $e_1 = 0$ and replace d_2 by $d_2 + 1$. Continue in this way (the ultimate expansion of m may begin with either $e_k 3^k$ or $e_{k+1} 3^{k+1}$). Here is a table of the first few numbers in this new expansion (let us write $\bar{1}$ instead of -1).

1	1	**9**	100
2	$1\bar{1}$	**10**	101
3	10	**11**	$11\bar{1}$
4	11	**12**	110
5	$1\bar{1}\bar{1}$	**13**	111
6	$1\bar{1}0$	**14**	$1\bar{1}\bar{1}\bar{1}$
7	$1\bar{1}1$	**15**	$1\bar{1}\bar{1}0$
8	$10\bar{1}$		

The reader should now understand Example 1.49. If □ weighs m pounds, write $m = \sum e_i 3^i$, where $e_i = 1, 0$, or -1, and then transpose those terms having negative coefficients. Those weights with $e_i = -1$ go on the pan with □, while those weights with $e_i = 1$ go on the other pan.

The solution to the current weighing problem involves choosing as weights 1, 3, 9, 27, 81, and 243 pounds. One can find the weight of anyone under 365 pounds, because $1 + 3 + 9 + 27 + 81 = 364$. ◀

EXERCISES

H **1.46** True or false with reasons.

- **(i)** $6 \mid 2$.
- **(ii)** $2 \mid 6$.
- **(iii)** $6 \mid 0$.
- **(iv)** $0 \mid 6$.
- **(v)** $0 \mid 0$.
- **(vi)** $(n, n + 1) = 1$ for every natural number n.
- **(vii)** $(n, n + 2) = 2$ for every natural number n.
- **(viii)** If b and m are positive integers, then $b \mid m$ if and only if the last b-adic digit d_0 of m is 0.
- **(ix)** 113 is a sum of distinct powers of 2.
- **(x)** If a and b are natural numbers, there there are natural numbers s and t with $\gcd(a, b) = sa + tb$.

*H **1.47** Given integers a and b (possibly negative) with $a \neq 0$, prove that there exist unique integers q and r with $b = qa + r$ and $0 \le r < |a|$.

1.48 Prove that $\sqrt{2}$ is irrational using Proposition 1.14 instead of Euclid's lemma.

H **1.49** Let $p_1, p_2, p_3, \ldots$ be the list of the primes in ascending order: $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, and so forth. Define $f_k = p_1 p_2 \cdots p_k + 1$ for $k \ge 1$. Find the smallest k for which f_k is not a prime.

***1.50** Prove that if d and d' are nonzero integers, each of which divides the other, then $d' = \pm d$.

H **1.51** If ζ is a root of unity, prove that there is a positive integer d with $\zeta^d = 1$ such that whenever $\zeta^k = 1$, then $d \mid k$.

H **1.52** Show that every positive integer m can be written as a sum of distinct powers of 2; show, moreover, that there is only one way in which m can so be written.

1.53 Find the b-adic digits of 1000 for $b = 2, 3, 4, 5$, and 20.

1.54** H (i) Prove that if n is ***squarefree (i.e., $n > 1$ and n is not divisible by the square of any prime), then $\sqrt{n}$ is irrational.

H (ii) Prove that $\sqrt[3]{2}$ is irrational.

1.55 (i) Find $d = \gcd(12327, 2409)$, find integers s and t with $d = 12327s + 2409t$, and put the fraction 2409/12327 in lowest terms.

(ii) Find $d = \gcd(7563, 526)$, and express d as a linear combination of 7563 and 526.

(iii) Find $d = \gcd(73122, 7404621)$ and express d as a linear combination of 73122 and 7404621.

***1.56** Let a and b be integers, and let $sa + tb = 1$ for s, t in $\mathbb{Z}$. Prove that a and b are relatively prime.

***1.57** If $d = (a, b)$, prove that a/d and b/d are relatively prime.

*H **1.58** Prove that if $(r, m) = 1 = (r', m)$, then $(rr', m) = 1$.

H **1.59** Let a, b and d be integers. If $d = sa + tb$, where s and t are integers, find infinitely many pairs of integers (s_k, t_k) with $d = s_k a + t_k b$.

*H **1.60** If a and b are relatively prime and if each divides an integer n, prove that their product ab also divides n.

*H **1.61** Prove, for any (possibly negative) integers a and b, that $(b, a) = (b - a, a)$.

H **1.62** If $a > 0$, prove that $a(b, c) = (ab, ac)$. [One must assume that $a > 0$ lest $a(b, c)$ be negative.]

1.63 Prove that the following pseudocode implements the Euclidean algorithm.

```
Input: $a, b$
Output: $d$
$d := b$;   $s := a$
WHILE $s > 0$ DO
   rem := remainder after dividing $d$ by $s$
   $d := s$
   $s :=$ rem
END WHILE
```

H **1.64** If F_n denotes the nth term of the Fibonacci sequence $0, 1, 1, 2, 3, 5, 8, \ldots$, prove, for all $n \geq 1$, that F_{n+1} and F_n are relatively prime.

Definition. A ***common divisor*** of integers $a_1, a_2, \ldots, a_n$, where $n \geq 2$, is an integer c with $c \mid a_i$ for all i; the largest of the common divisors, denoted by $(a_1, a_2, \ldots, a_n)$, is called the ***greatest common divisor***.

***1.65** (i) Show that if d is the greatest common divisor of $a_1, a_2, \ldots, a_n$, then $d = \sum t_i a_i$, where t_i is in $\mathbb{Z}$ for all i with $1 \leq i \leq n$.

(ii) Prove that if c is a common divisor of $a_1, a_2, \ldots, a_n$, then $c \mid d$.

***1.66** (i) Show that (a, b, c), the gcd of a, b, c, is equal to $(a, (b, c))$.

(ii) Compute $(120, 168, 328)$.

1.67** A ***Pythagorean triple is a triple (a, b, c) of positive integers for which

$$a^2 + b^2 = c^2;$$

it is called ***primitive*** if the gcd $(a, b, c) = 1$.

(i) Consider a complex number $z = q + ip$, where $q > p$ are positive integers. Prove that

$$(q^2 - p^2, 2qp, q^2 + p^2)$$

is a Pythagorean triple by showing that $|z^2| = |z|^2$. [One can prove that every *primitive* Pythagorean triple (a, b, c) is of this type.]

(ii) Show that the Pythagorean triple $(9, 12, 15)$ (which is not primitive) is not of the type given in part (i).

(iii) Using a calculator which can find square roots but which can display only 8 digits, show that

$$(19597501, 28397460, 34503301)$$

is a Pythagorean triple by finding q and p.

→ 1.4 THE FUNDAMENTAL THEOREM OF ARITHMETIC

We have already seen, in Theorem 1.2, that every integer $a \geq 2$ is either a prime or a product of primes. We are now going to generalize Proposition 1.14 by showing that the primes in such a factorization and the number of times each of them occurs are uniquely determined by a.

→ **Theorem 1.51 (Fundamental Theorem of Arithmetic).** *Every integer $a \geq 2$ is a prime or a product of primes. Moreover, if a has factorizations*

$$a = p_1 \cdots p_m \text{ and } a = q_1 \cdots q_n,$$

where the p's and q's are primes, then $n = m$ and the q's may be reindexed so that $q_i = p_i$ for all i.

Proof. We may assume that $m \geq n$, and the proof is by induction on m.

Base step. If $m = 1$, then the given equation is $a = p_1 = q_1$, and the result is obvious.

Inductive step. The equation gives $p_m \mid q_1 \cdots q_n$. By Theorem 1.38, Euclid's lemma, there is some i with $p_m \mid q_i$. But q_i, being a prime, has no positive divisors other than 1 and itself, so that $q_i = p_m$. Reindexing, we may assume that $q_n = p_m$. Canceling, we have $p_1 \cdots p_{m-1} = q_1 \cdots q_{n-1}$. By the inductive hypothesis, $n - 1 = m - 1$ and the q's may be reindexed so that $q_i = p_i$ for all i. •