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

1.36 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.)

1.37** (Leibniz***) A function $f : \mathbb{R} \to \mathbb{R}$ is called a ***C^∞-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

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

1.38 **(i)** If $z = a + ib \neq 0$, prove that

$$\frac{1}{z} = \frac{a}{a^2+b^2} - i\frac{b}{a^2+b^2}.$$

(ii) If z lies on the unit circle, prove that $z^{-1} = \overline{z}$.

1.39 Find $\sqrt{i}$.

***1.40** **(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 $k = 0, 1, 2, \ldots, n-1$.

1.41 **(i)** Find $\sqrt{8+15i}$.

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

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

Proof. We will prove the theorem in the special case in which $a > 0$ and $b \geq 0$; Exercise 1.42 on page 51 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, $0 \leq r < a$.

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

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

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

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

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

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

Therefore, $(q - q')a \geq a$ 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 $a \neq 0$, then the integers q and r occurring in the division algorithm are called the ***quotient*** and the ***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.

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

Thus, the remainders after dividing 60 and -60 by 7 are different (see Exercise 1.77 on page 71).

The next result shows that there is no largest prime.

Corollary 1.30. *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. The appendix 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 ≥ a > 0
Output: q, r
q := 0;    r := b
WHILE r ≥ 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 $a \neq 0$, 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. 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 $a \leq m$. Since $0 < b$, we have $1 \leq b$, because b is an integer, and so $a \leq ab = m$. 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. It is easy to check that if at least one of a and b is nonzero, then $(a, b) > 0$.

Proposition 1.31. *If p is a prime and b is any integer, then*

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

Proof. A common divisor c of p and a is, of course, a divisor of p. But the only positive divisors of p are p and 1, and so $(p, a) = p$ or 1; it is p if $p \mid a$, 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 1.32. *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 theorem shows that more is true: $c \mid d$ for every common divisor c.

Corollary 1.33. *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 $\Rightarrow$) 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 1.32.

Sufficiency (i.e., the implication $\Leftarrow$) Let d denote the gcd of a and b, and let d' be a nonnegative common divisor divisible by every common divisor c. Thus,

$d' \le d$, because $c \le d$ is for every common divisor c. On the other hand, d itself is a common divisor, and so $d \mid d'$, by hypothesis. Hence, $d \le d'$, and so $d = d'$. •

The proof of Theorem 1.32 contains an idea that will be used again.

Corollary 1.34. *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 $0 \le r < d$. 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 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 1.35 (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 $a_1 a_2 \cdots a_n$, then it must divide at least one of the factors a_i. Conversely, if $m \ge 2$ 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 1.31. By Theorem 1.32, 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 $n \ge 2$.

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 $m \le a$). •

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 1.36. *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 1.37. *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 1.37 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 1.38. *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.

Proposition 1.39. *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. It suffices to prove that $e^{2\pi ik/n}$ is a primitive nth root of unity if and only if k and n are relatively prime.

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, suppose that $\zeta = e^{2\pi ik/n}$ is not a primitive nth root of unity. Lemma 1.26 says that ζ must be a dth root of unity for some divisor d of n with $d < n$; that is, there is $1 \leq m \leq d$ with

$$\zeta = e^{2\pi ik/n} = e^{2\pi im/d} = e^{2\pi imr/dr} = e^{2\pi imr/n}.$$

Since both k and mr are in the range between 1 and n, it follows that $k = mr$ (if $0 \leq x, y < 1$ and $e^{2\pi ix} = e^{2\pi iy}$, then $x = y$); that is, r is a divisor of k and of n, and so k and n are not relatively prime. •

Proposition 1.40. $\sqrt{2}$ *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[17], $2 \mid a$, 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 $(a, b) = 1$. •

[17]This proof can be made more elementary; one needs only Proposition 1.11.

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 BC), 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 numerical solution to the equation $x^2 = 2$, but there is a geometric solution. By the time of Euclid, (around 325 BC), 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 4.46), 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 the 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[18]. 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 1.41 (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 $(a, b) = (|a|, |b|)$. ◀

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 $a = r_1$.

[18]Every positive integer is a product of primes, and this is used, in Proposition 1.52, 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.

Repeated application of the division algorithm gives integers q_i, positive integers r_i, and equations:

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

(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 1.43 gives a smaller bound on the number of steps).

We use Corollary 1.33 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 upwards 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 $d = h - u''k$. Substituting in the next equation above,

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

so that 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 1.42.
Find $(326, 78)$, express it as a linear combination of 326 and 78, and write $78/326$ in lowest terms.

$$\boxed{326} = 4 \times \boxed{78} + \boxed{14} \tag{1}$$
$$\boxed{78} = 5 \times \boxed{14} + \boxed{8} \tag{2}$$
$$\boxed{14} = 1 \times \boxed{8} + \boxed{6} \tag{3}$$
$$\boxed{8} = 1 \times \boxed{6} + \boxed{2} \tag{4}$$
$$\boxed{6} = 3 \times \boxed{2}. \tag{5}$$

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 1.56 on page 52 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

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

Proposition 1.43 (Lamé's[19] Theorem). *Let $b \geq a$ be positive integers, and let $\delta(a)$ be the number of digits in the decimal expression of a. If n is the number of steps in the Euclidean algorithm computing the* gcd (b, a)*, then*

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

Proof. Let us denote b by r_0 and a by r_1 in the equations of the euclidean algorithm on page 44, 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 $r_{n-1} \leq q_n r_{n-1} = r_n$, 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 1.13, $F_{n+1} > \alpha^{n-1}$, where $\alpha = \frac{1}{2}(1+\sqrt{5})$, and so

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

[19]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 and P. Schreiber, respectively, in the journal *Historica Mathematica*.)

Now $\log_{10}\alpha \approx \log_{10}(1.62) \approx .208 > \frac{1}{5}$, so that

$$\log_{10} a > (n-1)\log_{10}\alpha > (n-1)/5;$$

that is,

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

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

For example, Lam´e's theorem guarantees there are at most 10 steps needed to compute (326, 78) (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 1.44. *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 $d_k \ne 0$.

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

Proof. Let m be a positive integer; since $b \ge 2$, there are powers of b larger than m. We prove, by induction on $k \ge 0$, that if $b^k \le m < b^{k+1}$, then m has an expression

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

in base b.

If $k = 0$, then $1 = b^0 \le m < b^1 = b$, and we may define $d_0 = m$. If $k > 0$, then the division algorithm gives integers d_k and r with $m = d_k b^k + r$, where $0 \le r < b^k$. Notice that $d_k < b$ (lest $m \ge b^{k+1}$) and $0 < d_k$ (lest $m < b^k$). If $r = 0$, define $d_0 = \cdots = d_{k-1} = 0$, and $m = d_k b^k$ is an expression in base b. If $r > 0$, then the inductive hypothesis shows that r and, hence, m has an expression in base b.

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

$$\sum_{i=0}^{k} d_i b^i < b^{k+1}: \tag{6}$$

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

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 1.45.
Let us follow the steps in the proof of Proposition 1.44 to write 12345 in base 7. First write the powers of 7 until 12345 is exceeded: 7; $7^2 = 49$; $7^3 = 343$; $7^4 = 2401$; $7^5 = 16807$. Repeated use of the division algorithm gives

$$\begin{aligned}
12345 &= 5 \times 7^4 + 340 \quad \text{and} \quad 340 < 7^4 = 2401;\\
340 &= 0 \times 7^3 + 340 \quad \text{and} \quad 340 < 7^3 = 343;\\
340 &= 6 \times 7^2 + 46 \quad \text{and} \quad 46 < 7^2 = 49;\\
46 &= 6 \times 7 + 4 \quad \text{and} \quad 4 < 7;\\
4 &= 4 \times 1.
\end{aligned}$$

The 7-adic digits of 12345 are thus 50664.

In short, the first 7-adic digit (on the left) is the quotient q (here, it is 5) after dividing by 7^k, where $7^k \le m < 7^{k+1}$. The second digit is the quotient after dividing the remainder $m - q7^k$ by 7^{k-1}. And so on; the 7-adic digits are the successive quotients. ◀

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 1.46.
Here is a problem of Bachet de M´eziriac 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 $\square$ by putting 1 and $\square$ on one pan and 3 on the other pan.

A solution to Bachet's problem is 1, 3, 9, 27. If $\square$ 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 $\square$. The reader should note that Proposition 1.44 gives the uniqueness of the weights used in the pans.

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

The reader may complete this table for $\square \leq 40$. ◀

Example 1.47.
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 1.46. If $\square$ 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 $\square$, 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

***1.42** 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 $0 \le r < |a|$.

1.43 Prove that $\sqrt{2}$ is irrational using Proposition 1.11 instead of Euclid's lemma.

1.44 Let $p_1, p_2, p_3, \ldots$ be the list of the primes in ascending order: $p_1 = 2$, $p_2 = 3$, $p_3 = 5, \ldots$ 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.

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

1.46 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 $d \mid k$.

1.47 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.

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

1.49** **(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.

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

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

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

(iii) Find gcd $d = (7404621, 73122)$ and write it as a linear combination; that is, find integers s and t with $d = 7404621s + 73122t$.

***1.51** 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.

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

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

1.54 Assume that $d = sa + tb$ is a linear combination of integers a and b. Find infinitely many pairs of integers (s_k, t_k) with

$$d = s_k a + t_k b.$$

***1.55** If a and b are relatively prime and if each divides an integer n, then their product ab also divides n.

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

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

1.58 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
```

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

Definition. A ***common divisor*** of integers $a_1, a_2, \ldots, a_n$ 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***.

***1.60** **(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 $1 \leq i \leq n$.

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

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

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

1.62 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, prove 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 1.11 by showing that the primes in such a factorization and the number of times each of them occurs are uniquely determined by a.

Theorem 1.48 (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 prove the theorem by induction on ℓ, the larger of m and n.

Base step. If $\ell = 1$, 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 1.35, 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. •

Corollary 1.49. *If $a \geq 2$ is an integer, then there are distinct primes p_i, unique up to indexing, and unique integers $e_i > 0$ with*

$$a = p_1^{e_1} \cdots p_n^{e_n}.$$

Proof. Just collect like terms in a prime factorization. •

The uniqueness in the Fundamental Theorem of Arithmetic says that the exponents $e_1, \ldots, e_n$ in the prime factorization $a = p_1^{e_1} \cdots p_n^{e_n}$ are well-defined integers determined by a.

It is sometimes convenient to allow factorizations $p_1^{e_1} \cdots p_n^{e_n}$ having some zero exponents, for this device allows us to use the same primes when factoring two given numbers. For example, $168 = 2^3 3^1 7^1$ and $60 = 2^2 3^1 5^1$ may be rewritten as $168 = 2^3 3^1 5^0 7^1$ and $60 = 2^2 3^1 5^1 7^0$.

Corollary 1.50. *Every positive rational number $r \neq 1$ has a unique factorization*

$$r = p_1^{g_1} \cdots p_n^{g_n}$$

where the p_i are distinct primes and the g_i are nonzero integers. Moreover, r is an integer if and only if $g_i > 0$ for all i.

Proof. There are positive integers a and b with $r = a/b$. If $a = p_1^{e_1} \cdots p_n^{e_n}$ and $b = p_1^{f_1} \cdots p_n^{f_n}$, then $r = p_1^{g_1} \cdots p_n^{g_n}$, where $g_i = e_i - f_i$ (we may assume that the same primes appear in both factorizations by allowing zero exponents). The desired factorization is obtained if one deletes those factors $p_i^{g_i}$, if any, with $g_i = 0$.

Suppose there were another such factorization

$$r = p_1^{h_1} \cdots p_n^{h_n}$$

(by allowing zero exponents, we may again assume that the same primes occur in each factorization). Suppose that $g_j \neq h_j$ for some j; reindexing if necessary, we may assume that $j = 1$ and that $g_1 > h_1$. Therefore,

$$p_1^{g_1 - h_1} p_2^{g_2} \cdots p_n^{g_n} = p_2^{h_2} \cdots p_n^{h_n}.$$

This is an equation of rational numbers, for some of the exponents may be negative. Cross-multiplying gives an equation in $\mathbb{Z}$ whose left side involves the prime p_1 and whose right side does not; this contradicts the fundamental theorem of arithmetic.

If all the exponents in the factorization of r are positive, then r is an integer because it is a product of integers. Conversely, if r is an integer, then it has a prime factorization in which all exponents are positive. •

Lemma 1.51. *Let positive integers a and b have prime factorizations*

$$a = p_1^{e_1} \cdots p_n^{e_n} \text{ and } b = p_1^{f_1} \cdots p_n^{f_n},$$

where $e_i,\ f_i \geq 0$ for all i. Then $a \mid b$ if and only if $e_i \leq f_i$ for all i.

Proof. If $e_i \leq f_i$ for all i, then $b = ac$, where $c = p_1^{f_1 - e_1} \cdots p_n^{f_n - e_n}$. The number c is an integer because $f_i - e_i \geq 0$ for all i. Therefore, $a \mid b$.

Conversely, if $b = ac$, let the prime factorization of c be $c = p_1^{g_1} \cdots p_n^{g_n}$, where $g_i \geq 0$ for all i. It follows from the Fundamental Theorem of Arithmetic that $e_i + g_i = f_i$ for all i, and so $f_i - e_i = g_i \geq 0$ for all i. •

Definition. A ***common multiple*** of a, b is an integer m with $a \mid m$ and $b \mid m$. The ***least common multiple***, denoted by $\operatorname{lcm}(a, b)$ (or, more briefly, by $[a, b]$), is the smallest positive common multiple if all $a, b \neq 0$, and it is 0 otherwise.

More generally, if $n \geq 2$, a ***common multiple*** of $a_1, a_2, \ldots, a_n$ is an integer m with $a_i \mid m$ for all i. The ***least common multiple***, denoted by $[a_1, a_2, \ldots, a_n]$, is the smallest positive common multiple if all $a_i \neq 0$, and it is 0 otherwise.

We can now give a new description of gcd's.

Proposition 1.52. *Let $a = p_1^{e_1} \cdots p_n^{e_n}$ and let $b = p_1^{f_1} \cdots p_n^{f_n}$, where $e_i,\ f_i \geq 0$ for all i; define*

$$m_i = \min\{e_i,\ f_i\} \quad \text{and} \quad M_i = \max\{e_i,\ f_i\}.$$

Then

$$\gcd(a, b) = p_1^{m_1} \cdots p_n^{m_n} \quad \text{and} \quad \operatorname{lcm}(a, b) = p_1^{M_1} \cdots p_n^{M_n}.$$

Proof. Define $d = p_1^{m_1} \cdots p_n^{m_n}$. Lemma 1.51 shows that d is a (positive) common divisor of a and b; moreover, if c is any (positive) common divisor, then $c = p_1^{g_1} \cdots p_n^{g_n}$, where $0 \leq g_i \leq \min\{e_i,\ f_i\} = m_i$ for all i. Therefore, $c \mid d$.

A similar argument shows that $D = p_1^{M_1} \cdots p_n^{M_n}$ is a common multiple that divides every other such. •

For small numbers a and b, using their prime factorizations is a more efficient way to compute their gcd than using the Euclidean algorithm. For example, since $168 = 2^3 3^1 5^0 7^1$ and $60 = 2^2 3^1 5^1 7^0$, we have $(168, 60) = 2^2 3^1 5^0 7^0 = 12$ and $[168, 60] = 2^3 3^1 5^1 7^1 = 840$. As we mentioned when we introduced the Euclidean algorithm, finding the prime factorization of a large integer is very inefficient.

Proposition 1.53. *If a and b are positive integers, then*

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

Proof. The result follows from Proposition 1.52 if one uses the identity

$$m_i + M_i = e_i + f_i,$$

where $m_i = \min\{e_i, f_i\}$ and $M_i = \max\{e_i, f_i\}$. •

Of course, this proposition allows us to compute the lcm as $ab/(a, b)$.

EXERCISES

1.63 **(i)** Find gcd(210, 48) using factorizations into primes.

(ii) Find gcd(1234, 5678).

***1.64** **(i)** Prove that an integer $m \geq 2$ is a perfect square if and only if each of its prime factors occurs an even number of times.

(ii) Prove that if m is a positive integer for which $\sqrt{m}$ is rational, then m is a perfect square. Conclude that if m is not a perfect square, then $\sqrt{m}$ is irrational.

1.65 If a and b are positive integers with $(a, b) = 1$, and if ab is a square, prove that both a and b are squares.

***1.66** Let $n = p^r m$, where p is a prime not dividing an integer $m \geq 1$. Prove that $p \nmid \binom{n}{p^r}$.

1.67 **Definition.** If p is a prime, define the ***p-adic norm*** of a rational number a as follows: $\|0\|_p = 0$; if $a \neq 0$, then $a = p^e p_1^{e_1} \cdots p_n^{e_n}$, where $p, p_1, \ldots, p_n$ are distinct primes, and we set $\|a\|_p = p^{-e}$.

(i) For all rationals a and b, prove that

$$\|ab\|_p = \|a\|_p\|b\|_p \text{ and } \|a + b\|_p \leq \max\{\|a\|_p, \|b\|_p\}.$$

(ii) Define $\delta_p(a, b) = \|a - b\|_p$.

(i) For all rationals a, b, prove $\delta_p(a, b) \geq 0$ and $\delta_p(a, b) = 0$ if and only if $a = b$;

(ii) For all rationals a, b, prove that $\delta_p(a, b) = \delta_p(b, a)$;

(iii) For all rationals a, b, c, prove $\delta_p(a, b) \leq \delta_p(a, c) + \delta_p(c, b)$.

(iii) If a and b are integers and $p^n \mid (a - b)$, then $\delta_p(a, b) \leq p^{-n}$. (Thus, a and b are "close" if $a - b$ is divisible by a "large" power of n.)

1.68 Let a and b be in $\mathbb{Z}$. Prove that if $\delta_p(a, b) \leq p^{-n}$, then a and b have the same first n p-adic digits, $d_0, \ldots, d_{n-1}$.

1.69 Prove that an integer $M \geq 0$ is the lcm of $a_1, a_2, \ldots, a_n$ if and only if it is a common multiple of $a_1, a_2, \ldots, a_n$ which divides every other common multiple.

***1.70** **(i)** Give another proof of Proposition 1.53, $[a, b](a, b) = |ab|$, without using the Fundamental Theorem of Arithmetic.

(ii) Find [1371, 123].

1.5 CONGRUENCES

When first learning long division, one emphasizes the quotient q; the remainder r is merely the fragment left over. There is now going to be a shift in viewpoint: we are interested in whether or not a given number b is a multiple of a number a, but we are not so interested in which multiple it may be. Hence, from now on, we will emphasize the remainder.

Two integers a and b are said to have the ***same parity*** if they are both even or both odd. If a and b have the same parity, then $a - b$ is even: this is surely true if a and b are both even; if a and b are both odd, then $a = 2m + 1$, $b = 2n + 1$, and $a - b = 2(m - n)$ is even. Conversely, if $a - b$ is even, then we cannot have one of them even and the other odd lest $a - b$ be odd. The next definition generalizes this notion of parity, letting any positive integer m play the role of 2.

Definition. If $m \geq 0$ is fixed, then integers a and b are ***congruent modulo m***, denoted by

$$a \equiv b \bmod m,$$

if $m \mid (a - b)$.

Usually, one assumes that the ***modulus*** $m \geq 2$ because the cases $m = 0$ and $m = 1$ are not very interesting: if a and b are integers, then $a \equiv b \bmod 0$ if and only if $0 \mid (a - b)$, that is, $a = b$, and so congruence mod 0 is ordinary equality. The congruence $a \equiv b \bmod 1$ is true for every pair of integers a and b because $1 \mid (a - b)$ always. Hence, every two integers are congruent mod 1.

The word "modulo" is usually abbreviated to "mod." The Latin root of this word means a standard of measure. Thus, the term *modular unit* is used today in architecture: a fixed length m is chosen, say, $m = 1$ foot, and plans are drawn so that the dimensions of every window, door, wall, etc., are integral multiples of m.

If a and b are positive integers, then $a \equiv b \bmod 10$ if and only if they have the same last digit; more generally, $a \equiv b \bmod 10^n$ if and only if they have same last n digits. For example, $526 \equiv 1926 \bmod 100$.

London time is 6 hours later than Chicago time. What time is it in London if it is 10:00 A.M. in Chicago? Since clocks are set up with 12 hour cycles, this is really a problem about congruence mod 12. To solve it, note that

$$10 + 6 = 16 \equiv 4 \bmod 12,$$

and so it is 4:00 P.M. in London.

The next theorem shows that congruence mod m behaves very much like equality.

Proposition 1.54. *If $m \geq 0$ is a fixed integer, then for all integers a, b, c,*

(i) $a \equiv a \bmod m$;

(ii) *if* $a \equiv b \bmod m$, *then* $b \equiv a \bmod m$;

(iii) *if* $a \equiv b \bmod m$ *and* $b \equiv c \bmod m$, *then* $a \equiv c \bmod m$.

Remark. (i) says that congruence is ***reflexive,*** (ii) says it is ***symmetric,*** and (iii) says it is ***transitive.*** ◀

Proof.
(i) Since $m \mid (a - a) = 0$, we have $a \equiv a \bmod m$.
(ii) If $m \mid (a - b)$, then $m \mid -(a - b) = b - a$ and so $b \equiv a \bmod m$.
(iii) If $m \mid (a - b)$ and $m \mid (b - c)$, then $m \mid [(a - b) + (b - c)] = a - c$, and so $a \equiv c \bmod m$. •

We now generalize the observation that $a \equiv 0 \bmod m$ if and only if $m \mid a$.

Proposition 1.55. *Let $m \geq 0$ be a fixed integer.*

(i) *If* $a = qm + r$, *then* $a \equiv r \bmod m$.

(ii) *If* $0 \leq r' < r < m$, *then r and r' are not congruent* $\bmod m$; *in symbols,* $r \not\equiv r' \bmod m$.

(iii) $a \equiv b \bmod m$ *if and only if a and b leave the same remainder after dividing by m.*

Proof.
(i) The equation $a - r = qm$ (from the division algorithm $a = qm + r$) shows that $m \mid (a - r)$.
(ii) If $r \equiv r' \bmod m$, then $m \mid (r - r')$ and $m \leq r - r'$. But $r - r' \leq r < m$, a contradiction.
(iii) If $a = qm + r$ and $b = q'm + r'$, where $0 \leq r < m$ and $0 \leq r' < m$, then $a - b = (q - q')m + (r - r')$; that is,

$$a - b \equiv r - r' \bmod m.$$

Therefore, if $a \equiv b \bmod m$, then $a - b \equiv 0 \bmod m$, hence $r - r' \equiv 0 \bmod m$, and $r \equiv r' \bmod m$; by (ii), $r = r'$.

Conversely, if $r = r'$, then $a = qm + r$ and $b = q'm + r$, so that $a - b = (q' - q)m$ and $a \equiv b \bmod m$. •

Corollary 1.56. *Given $m \geq 2$, every integer a is congruent* $\bmod m$ *to exactly one of* $0, 1, \ldots, m - 1$.

Proof. The division algorithm says that $a \equiv r \bmod m$, where $0 \leq r < m$; that is, r is an integer on the list 0, 1,..., $m-1$. If a were congruent to two integers on the list, say, r and r', then $r \equiv r' \bmod m$, contradicting part (ii) of Proposition 1.55. Therefore, a is congruent to a unique such r. •

We know that every integer a is either even or odd; that is, a has the form $2k$ or $1+2k$. We now see that if $m \geq 2$, then every integer a has exactly one of the forms $km = 0 + km$, $1 + km$, $2 + km$, ..., $(m-1) + km$; thus, congruence mod m generalizes the even/odd dichotomy from $m = 2$ to $m \geq 2$. Notice how we continue to focus on the remainder in the division algorithm and not upon the quotient.

Congruence is compatible with addition and multiplication.

Proposition 1.57. *Let $m \geq 0$ be a fixed integer.*

(i) *If $a_i \equiv a_i' \bmod m$ for $i = 1, 2, \ldots, n$, then*

$$a_1 + \cdots + a_n \equiv a_1' + \cdots + a_n' \bmod m.$$

In particular, if $a \equiv a' \bmod m$ and $b \equiv b' \bmod m$, then

$$a + b \equiv a' + b' \bmod m.$$

(ii) *If $a_i \equiv a_i' \bmod m$ for $i = 1, 2, \ldots, n$, then*

$$a_1 \cdots a_n \equiv a_1' \cdots a_n' \bmod m.$$

In particular, if $a \equiv a' \bmod m$ and $b \equiv b' \bmod m$, then

$$ab \equiv a'b' \bmod m.$$

(iii) *If $a \equiv b \bmod m$, then $a^n \equiv b^n \bmod m$ for all $n \geq 1$.*

Proof.
(i) The proof is by induction on $n \geq 2$. For the base step, if $m \mid (a - a')$ and $m \mid (b - b')$, then $m \mid (a - a' + b - b') = (a + b) - (a' + b')$. Therefore, $a + b \equiv a' + b' \bmod m$. The proof of the inductive step is routine.
(ii) The proof is by induction on $n \geq 2$. For the base step, we must show that if $m \mid (a - a')$ and $m \mid (b - b')$, then $m \mid (ab - a'b')$, and this follows from the identity

$$\begin{aligned} ab - a'b' &= (ab - a'b) + (a'b - a'b') \\ &= (a - a')b + a'(b - b'). \end{aligned}$$

Therefore, $ab \equiv a'b' \bmod m$. The proof of the inductive step is routine.
(iii) This is the special case of (ii) when $a_i = a$ and $a_i' = b$ for all i. •

Let us repeat a warning given on page 36. A number and its negative usually have different remainders after being divided by a number m. For example, $60 = 7 \cdot 8 + 4$ and $-60 = 7 \cdot (-9) + 3$. In terms of congruences,

$$60 \equiv 4 \bmod 7 \qquad \text{while} \qquad -60 \equiv 3 \bmod 7.$$

In light of Proposition 1.55(i), if the remainder after dividing b by m is r and the remainder after dividing $-b$ by m is s, then $b \equiv r \bmod m$ and $-b \equiv s \bmod m$. Therefore, Proposition 1.57(i) gives

$$r + s \equiv b - b \equiv 0 \bmod m.$$

Thus, $r + s = m$, for $0 \le r, s < m$. For example, we have just seen that the remainders after dividing 60 and -60 by 7 are 4 and 3, respectively. If both a and $-a$ have the same remainder r after dividing by m, then $-r \equiv r \bmod m$; that is, $2r \equiv 0 \bmod m$. Exercise 1.77 on page 71 asks you to solve this last congruence.

The next example shows how one can use congruences. In each case, the key idea is to solve a problem by replacing numbers by their remainders.

Example 1.58.

(i) Prove that if a is in $\mathbb{Z}$, then $a^2 \equiv 0$, 1, or 4 mod 8.

If a is an integer, then $a \equiv r \bmod 8$, where $0 \le r \le 7$; moreover, by Proposition 1.57(iii), $a^2 \equiv r^2 \bmod 8$, and so it suffices to look at the squares of the remainders.

r	0	1	2	3	4	5	6	7
r^2	0	1	4	9	16	25	36	49
$r^2 \bmod 8$	0	1	4	1	0	1	4	1

Table 1.1. Squares mod 8

We see in Table 1.1 that only 0, 1, or 4 can be a remainder after dividing a perfect square by 8.

(ii) Prove that $n = 1003456789$ is not a perfect square.

Since $1000 = 8 \cdot 125$, we have $1000 \equiv 0 \bmod 8$, and so

$$1003456789 = 1003456 \cdot 1000 + 789 \equiv 789 \bmod 8.$$

Dividing 789 by 8 leaves remainder 5; that is, $n \equiv 5 \bmod 8$. Were n a perfect square, then $n \equiv 0$, 1, or 4 mod 8.

(iii) If m and n are positive integers, are there any perfect squares of the form $3^m + 3^n + 1$?

Again, let us look at remainders mod 8. Now $3^2 = 9 \equiv 1 \bmod 8$, and so we can evaluate $3^m \bmod 8$ as follows: if $m = 2k$, then $3^m = 3^{2k} = 9^k \equiv 1 \bmod 8$; if $m = 2k + 1$, then $3^m = 3^{2k+1} = 9^k \cdot 3 \equiv 3 \bmod 8$. Thus,

$$3^m \equiv \begin{cases} 1 \bmod 8 & \text{if } m \text{ is even;} \\ 3 \bmod 8 & \text{if } m \text{ is odd.} \end{cases}$$

Replacing numbers by their remainders after dividing by 8, we have the following possibilities for the remainder of $3^m + 3^n + 1$, depending on the parities of m and n:

$$\begin{aligned} 3 + 1 + 1 &\equiv 5 \bmod 8 \\ 3 + 3 + 1 &\equiv 7 \bmod 8 \\ 1 + 1 + 1 &\equiv 3 \bmod 8 \\ 1 + 3 + 1 &\equiv 5 \bmod 8. \end{aligned}$$

In no case is the remainder 0, 1, or 4, and so no number of the form $3^m + 3^n + 1$ can be a perfect square, by part (i). ◀

Every positive integer is congruent to either 0, 1, or 2 mod 3; hence, if $p \neq 3$ is a prime, then either $p \equiv 1 \bmod 3$ or $p \equiv 2 \bmod 3$. For example, 7, 13, and 19 are congruent to 1 mod 3, while 2, 5, 11, and $17 \equiv 2 \bmod 3$. The next theorem is another illustration of the fact that a proof of one theorem may be adapted to prove another theorem.

Proposition 1.59. *There are infinitely many primes p with $p \equiv 2 \bmod 3$.*

Remark. This proposition is a special case of a beautiful theorem of Dirichlet about primes in arithmetic progressions: If a, b in $\mathbb{N}$ are relatively prime, then there are infinitely many primes of the form $a + bn$. In this proposition, we show that there are infinitely many primes of the form $2 + 3n$. Even though the proof of this special case is not difficult, the proof of Dirichlet's theorem uses complex analysis and it is deep. ◀

Proof. We mimic Euclid's proof that there are infinitely many primes. Suppose, on the contrary, that there are only finitely many primes congruent to 2 mod 3; let them be $p_1, \ldots, p_s$. Consider the number

$$m = 1 + p_1^2 \cdots p_s^2.$$

Now $p_i \equiv 2 \bmod 3$ implies $p_i^2 \equiv 4 \equiv 1 \bmod 3$, and so $m \equiv 1 + 1 = 2 \bmod 3$. Since $m > p_i$ for all i, the number m is not prime, for it is not one of the p_i.

Actually, none of the p_i divide m: if we define $Q_i = p_1^2 \cdots p_{i-1}^2 p_i p_{i+1}^2 \cdots p_s^2$, then the uniqueness part of the division algorithm coupled with the equation $m = p_i Q_i + 1$ shows that m leaves remainder 1 after dividing by p_i. Hence, the prime factorization of m is $m = q_1 \cdots q_t$, where, for each j, either $q_j = 3$ or $q_j \equiv 1 \bmod 3$. Thus, $m = q_1 \cdots q_t \equiv 0 \bmod 3$ or $m = q_1 \cdots q_t \equiv 1 \bmod 3$, contradicting $m \equiv 2 \bmod 3$. •

The next result shows how congruence can simplify complicated expressions.

Proposition 1.60. *If p is a prime and a and b are integers, then*

$$(a+b)^p \equiv a^p + b^p \bmod p.$$

Proof. The binomial theorem gives

$$(a+b)^p = a^p + b^p + \sum_{r=1}^{p-1} \binom{p}{r} a^{p-r} b^r.$$

But Proposition 1.36 gives $\binom{p}{r} \equiv 0 \bmod p$ for $0 < r < p$, and so Proposition 1.57 gives $(a+b)^p \equiv a^p + b^p \bmod p$. •

Theorem 1.61 (*Fermat*).

(i) *If p is a prime, then*

$$a^p \equiv a \bmod p$$

for every a in $\mathbb{Z}$.

(ii) *If p is a prime, then*

$$a^{p^k} \equiv a \bmod p$$

for every a in $\mathbb{Z}$ and every integer $k \geq 1$.

Proof.
(i) Assume first that $a \geq 0$; we proceed by induction on a. The base step $a = 0$ is plainly true. For the inductive step, observe that

$$(a+1)^p \equiv a^p + 1 \bmod p,$$

by Proposition 1.60. The inductive hypothesis gives $a^p \equiv a \bmod p$, and so $(a+1)^p \equiv a^p + 1 \equiv a + 1 \bmod p$, as desired.

Now consider $-a$, where $a \geq 0$. If $p = 2$, then $-a \equiv a$; hence, $(-a)^2 = a^2 \equiv a \equiv -a \bmod 2$. If p is an odd prime, then $(-a)^p = (-1)^p a^p \equiv (-1)^p a \equiv -a \bmod p$, as desired.

(ii) A straightforward induction on $k \geq 1$; the base step is part (i). •

Corollary 1.62. *A positive integer a is divisible by* 3 *if and only if the sum of its* (*decimal*) *digits is divisible by* 3.

Proof. If the decimal form of a is $d_k \dots d_1 d_0$, then

$$a = d_k 10^k + \cdots + d_1 10 + d_0.$$

Now $10 \equiv 1 \bmod 3$, so that Proposition 1.57(iii) gives $10^i \equiv 1^i = 1 \bmod 3$ for all i; thus Proposition 1.57(i) gives $a \equiv d_k + \cdots + d_1 + d_0 \bmod m$. Therefore, a is divisible by 3 if and only if $a \equiv 0 \bmod 3$ if and only if $d_k + \cdots + d_1 + d_0 \equiv 0 \bmod 3$. •

Remark. Since $10 \equiv 1 \bmod 9$, the same result holds if we replace 3 by 9 (it is often called ***casting out 9's***): a positive integer a is divisible by 9 if and only if the sum of its (decimal) digits is divisible by 9. ◀

Corollary 1.63. *Let p be a prime and let n be a positive integer. If $m \geq 0$ and if Σ is the sum of the p-adic digits of m, then*

$$n^m \equiv n^\Sigma \bmod p.$$

Proof. Let $m = d_k p^k + \cdots + d_1 p + d_0$ be the expression of m in base p. By Fermat's theorem, Theorem 1.61(ii), $n^{p^i} \equiv n \bmod p$ for all i; thus, $n^{d_i p^i} = (n^{d_i})^{p^i} \equiv n^{d_i} \bmod p$. Therefore,

$$\begin{aligned} n^m &= n^{d_k p^k + \cdots + d_1 p + d_0} \\ &= n^{d_k p^k} n^{d_{k-1} p^{k-1}} \cdots n^{d_1 p} n^{d_0} \\ &\equiv n^{d_k} n^{d_{k-1}} \cdots n^{d_1} n^{d_0} \bmod p \\ &\equiv n^{d_k + \cdots + d_1 + d_0} \bmod p \\ &\equiv n^\Sigma \bmod p. \quad \bullet \end{aligned}$$

Example 1.64.
What is the remainder after dividing 3^{12345} by 7? By Example 1.45, the 7-adic digits of 12345 are 50664. Therefore, $3^{12345} \equiv 3^{21} \bmod 7$ (because $5 + 0 + 6 + 6 + 4 = 21$). The 7-adic digits of 21 are 30 (because $21 = 3 \times 7$), and so $3^{21} \equiv 3^3 \bmod 7$ (because 3 + 0 = 3). We conclude that $3^{12345} \equiv 3^3 = 27 \equiv 6 \bmod 7$. ◀

Theorem 1.65. *If $(a, m) = 1$, then, for every integer b, the congruence*

$$ax \equiv b \bmod m$$

can be solved for x; in fact, $x = sb$, where $sa \equiv 1 \bmod m$. Moreover, any two solutions are congruent mod m.

Remark. We consider the case $(a, m) \neq 1$ in Exercise 1.82 on page 71. ◀

Proof. Since $(a, m) = 1$, there is an integer s with $as \equiv 1 \bmod m$ (because there is a linear combination $1 = sa + tm$). It follows that $b = sab + tmb$ and $asb \equiv b \bmod m$, so that $x = sb$ is a solution. (Note that Proposition 1.55(i) allows us to take s with $1 \leq s < m$.)

If y is another solution, then $ax \equiv ay \bmod m$, and so $m \mid a(x - y)$. Since $(a, m) = 1$, Corollary 1.37 gives $m \mid (x - y)$; that is, $x \equiv y \bmod m$. •

Corollary 1.66. *If p is prime, the congruence $ax \equiv b \bmod p$ is always solvable if a is not divisible by p.*

Proof. Since p is a prime, $p \nmid a$ implies $(a, p) = 1$. •

Example 1.67.
When $(a, m) = 1$, Theorem 1.65 says that the solutions to $ax \equiv b \bmod m$ are precisely those integers of the form $sb + km$ for k in $\mathbb{Z}$, where $sa \equiv 1 \bmod m$; that is, where $sa + tm = 1$. Thus, s can always be found by the Euclidean algorithm. However, when m is small, it is easier to find such an integer s by trying each of $ra = 2a, 3a, \ldots, (m-1)a$ in turn, at each step checking whether $ra \equiv 1 \bmod m$.

For example, let us find all the solutions to

$$2x \equiv 9 \bmod 13.$$

Considering the products $2 \cdot 2, 3 \cdot 2, 4 \cdot 2, \ldots \bmod 13$ quickly leads to $7 \times 2 = 14 \equiv 1 \bmod 13$; that is, $s = 7$ and $x = 7 \cdot 9 = 63 \equiv 11 \bmod 13$. Therefore,

$$x \equiv 11 \bmod 13.$$

Thus, the solutions are $\ldots, -15, -2, 11, 24, \ldots$. ◀

Example 1.68.
Find all the solutions to $51x \equiv 10 \bmod 94$.

Since 94 is large, seeking an integer s with $51s \equiv 1 \bmod 94$, as in Example 1.67, can be tedious. The Euclidean algorithm gives $1 = -35 \cdot 51 + 19 \cdot 94$, and so $s = -35$. Therefore, the solutions consist of all those numbers congruent to $(-35) \times 10 \bmod 94$; that is, numbers of the form $-350 + 94k$. ◀

There are problems solved in ancient Chinese manuscripts that involve simultaneous congruences with relatively prime moduli.

Theorem 1.69 (Chinese Remainder Theorem). *If m and m' are relatively prime, then the two congruences*

$$x \equiv b \bmod m$$
$$x \equiv b' \bmod m'$$

have a common solution, and any two solutions are congruent mod mm'.

Proof. Every solution of the first congruence has the form $x = b + km$ for some integer k; hence, we must find k such that $b + km \equiv b' \bmod m'$; that is, $km \equiv b' - b \bmod m'$. Since $(m, m') = 1$, however, Theorem 1.65 applies at once to show that such an integer k does exist.

If y is another common solution, then both m and m' divide $x - y$; by Exercise 1.55 on page 52, $mm' \mid (x - y)$, and so $x \equiv y \bmod mm'$. •

Example 1.70.
Find all the solutions to the simultaneous congruences

$$x \equiv 7 \bmod 8$$
$$x \equiv 11 \bmod 15.$$

Every solution to the first congruence has the form

$$x = 7 + 8k,$$

for some integer k. Substituting, $x = 7 + 8k \equiv 11 \bmod 15$, so that

$$8k \equiv 4 \bmod 15.$$

But $2 \cdot 8 = 16 \equiv 1 \bmod 15$, so that multiplying by 2 gives

$$16k \equiv k \equiv 8 \bmod 15.$$

We conclude that $x = 7 + 8 \cdot 8 = 71$ is a solution, and the Chinese Remainder Theorem says that every solution has the form $71 + 120n$ for n in $\mathbb{Z}$. ◀

Example 1.71.
Solve the simultaneous congruences

$$x \equiv 2 \bmod 5$$
$$3x \equiv 5 \bmod 13.$$

Every solution to the first congruence has the form $x = 5k + 2$ for k in $\mathbb{Z}$. Substituting into the second congruence, we have

$$3(5k + 2) \equiv 5 \bmod 13.$$

Therefore,

$$\begin{aligned} 15k + 6 &\equiv \quad 5 \bmod 13 \\ 2k &\equiv -1 \bmod 13. \end{aligned}$$

Now $7 \times 2 \equiv 1 \bmod 13$, and so multiplying by 7 gives

$$k \equiv -7 \equiv 6 \bmod 13.$$

By the Chinese Remainder Theorem, all the simultaneous solutions x have the form

$$x \equiv 5k + 2 \equiv 5 \cdot 6 + 2 = 32 \bmod 65;$$

that is, the solutions are

$$\ldots, -98, -33, 32, 97, 162, \ldots. \quad \blacktriangleleft$$

Example 1.72 (A Mayan Calendar).
A congruence arises whenever there is cyclic behavior. For example, suppose we choose some particular Sunday as time zero and enumerate all the days according to the time elapsed since then. Every date now corresponds to some integer (which is negative if it occurred before time zero), and, given two dates t_1 and t_2, we ask for the number $x = t_2 - t_1$ of days from one to the other. If, for example, t_1 falls on a Thursday and t_2 falls on a Tuesday, then $t_1 \equiv 4 \bmod 7$ and $t_2 \equiv 2 \bmod 7$, and so $x = t_2 - t_1 = -2 \equiv 5 \bmod 7$. Thus, $x = 7k + 5$ for some k.

About 2500 years ago, the Maya of Central America and Mexico developed three calendars (each having a different use). Their religious calendar, called *tzolkin*, consisted of 20 "months," each having 13 days (so that the tzolkin "year" had 260 days). The months were

1. Imix	6. Cimi	11. Chuen	16. Cib
2. Ik	7. Manik	12. Eb	17. Caban
3. Akbal	8. Lamat	13. Ben	18. Etznab
4. Kan	9. Muluc	14. Ix	19. Cauac
5. Chicchan	10. Oc	15. Men	20. Ahau

Let us describe a tzolkin date by an ordered pair $\{m, d\}$, where $1 \le m \le 20$ and $1 \le d \le 13$ (thus, m denotes the month and d denotes the day). Instead of enumerating as we do (so that Imix 1 is followed by Imix 2, then by Imix 3, and so forth), the Maya let both month and day cycle simultaneously; that is, the days proceed as follows:

Imix 1, Ik 2, Akbal 3,..., Ben 13, Ix 1, Men 2,...,
Cauac 6, Ahau 7, Imix 8, Ik 9,....

We now ask how many days have elapsed between Oc 11 and Etznab 5. More generally, let us find the number x of days that have elapsed from tzolkin $\{m, d\}$ to tzolkin $\{m', d'\}$. As we remarked at the beginning of this example, the cyclic behavior of the days gives the congruence

$$x \equiv d' - d \bmod 13$$

(e.g., there are 13 days between Imix 1 and Ix 1; here, $x \equiv 0 \bmod 13$), while the cyclic behavior of the months gives the congruence

$$x \equiv m' - m \bmod 20$$

(e.g., there are 20 days between Imix 1 and Imix 8; here, $x \equiv 0 \bmod 20$). To answer the original question, Oc 11 corresponds to the ordered pair $\{10, 11\}$ and Etznab 5 corresponds to $\{18, 5\}$. The simultaneous congruences are thus

$$\begin{aligned} x &\equiv -6 \bmod 13 \\ x &\equiv \ \ 8 \bmod 20. \end{aligned}$$

Since $(13, 20) = 1$, we can solve this system as in the proof of the Chinese Remainder Theorem. The first congruence gives

$$x = 13k - 6,$$

and the second gives

$$13k - 6 \equiv 8 \bmod 20;$$

that is,

$$13k \equiv 14 \bmod 20.$$

Since $13 \times 17 = 221 \equiv 1 \bmod 20$,[20] we have $k \equiv 17 \times 14 \bmod 20$, that is,

$$k \equiv 18 \bmod 20,$$

and so the Chinese Remainder Theorem gives

$$x = 13k - 6 \equiv 13 \times 18 - 6 \equiv 228 \bmod 260.$$

It is not clear whether Oc 11 precedes Etznab 5 in a given year (one must look). If it does, then there are 228 days between them; otherwise, there are $32 = 260 - 228$ days between them. ◀

[20] One finds 17 either by trying each number between 1 and 19 or by using the Euclidean algorithm.

Example 1.73 (Public Key Cryptography).
In a war between A and B, spies for A learn of a surprise attack being planned by B, and so they must send an urgent message back home. If B learns that its plans are known to A, it will, of course, change them, and so A's spies put the message in code before sending it.

It is no problem to convert a message in English into a number. Make a list of the 52 English letters (lower case and upper case) together with a space and the 11 punctuation marks

$$\texttt{, . ; : ! ? - ' " ( )}$$

In all, there are 64 symbols. Assign a two-digit number to each symbol. For example,

$$\begin{aligned} &\text{a} \mapsto 01, \ldots, \text{z} \mapsto 26, \text{A} \mapsto 27, \ldots, \text{Z} \mapsto 52 \\ &\text{space} \mapsto 53, \ . \mapsto 54, \ , \mapsto 55, \ldots, (\mapsto 63,) \mapsto 64. \end{aligned}$$

A *cipher* is a code in which distinct letters in the original message are replaced by distinct symbols. It is not difficult to decode any cipher; indeed, many newspapers print daily cryptograms to entertain their readers. In the cipher we have just described, "I love you." is encoded

$$\text{I love you.} = 3553121522055325152154.$$

Notice that each coded message in this cipher has an even number of digits, and so decoding, converting the number into English, is a simple matter. Thus,

$$\begin{aligned} 3553121522055325152154 &= (35)(53)(12)(15)(22)(05)(53)(25)(15)(21)(54) \\ &= \text{I love you.} \end{aligned}$$

What makes a good code? If a message is a natural number x (and this is no loss in generality), we need a way to encode x (in a fairly routine way so as to avoid introducing any errors into the coded message), and we need a (fairly routine) method for the recipient to decode the message. Of utmost importance is security: an unauthorized reader of the (coded) message should not be able to decode it. An ingenious way to find a code with these properties, now called *RSA public key cryptography*, was found in 1978 by R. Rivest, A. Shamir, and L. Adleman; they received the 2002 Turing Award for their discovery.

Given natural numbers N, s, and t, suppose that $x^{st} \equiv x \bmod N$ for every natural number x. We can encode any natural number $x < N$ as $[x^s]_N$, the remainder of $x^s \bmod N$, and we can decode this if we know the number t, for

$$(x^s)^t = x^{st} \equiv x \bmod N.$$

It remains to find numbers N, s, and t satisfying the several criteria for a good code.

I : ***Ease of Encoding and Decoding.***

Suppose that N has d (decimal) digits. It is enough to show how to encode a number x with at most d digits, for we can subdivide a longer number into blocks each having at most d digits. An efficient computation of $x^s \bmod N$ is based on the fact that computing $x^2 \bmod N$ is an easy task for a computer. Since computing x^{2^i} is just computing i squares, this, too, is an easy task. Now write the exponent s in base 2, so that computing x^s is the same as multiplying several squares. If $m = 2^i + 2^j + \cdots + 2^z$, then $x^m = x^{2^i+2^j+\cdots+2^z} = x^{2^i}x^{2^j}\cdots x^{2^z}$. In short, computers can encode a message in this way with no difficulty.

Decoding involves computing $(x^s)^t \bmod N$, and this is also an easy task (assuming t is known) if, as above, we write t in base 2.

II : ***Constructing N and m = st.***

Choose distinct primes p and q, both congruent to 2 mod 3, and define $N = pq$. If $m \geq p$, then

$$x^m = x^{m-p}x^p \equiv x^{m-p}x = x^{m-(p-1)} \bmod p,$$

by Fermat's theorem. If $m - (p-1) \geq p$, we may repeat this, continuing until we have

$$\begin{aligned} x^{m-(p-1)} &= x^{m-(p-1)-p}x^p \\ &\equiv x^{m-(p-1)-p}x \\ &= x^{m-2(p-1)} \\ &\vdots \\ &\equiv x^{m-h(p-1)} \bmod p, \end{aligned}$$

where h is the largest integer for which $m - h(p-1) \geq 0$. But this is just the division algorithm: $m = h(p-1) + r$, where r is the remainder after dividing m by $p-1$. Hence, for all x,

$$x^m \equiv x^r \bmod p.$$

Therefore, if $m \equiv 1 \bmod (p-1)$, then

$$x^m \equiv x \bmod p \quad \text{for all } x.$$

Similarly, if $m \equiv 1 \bmod (q-1)$, then $x^m \equiv x \bmod (q-1)$ for all x. Therefore, if m is chosen such that

$$m \equiv 1 \bmod (p-1)(q-1),$$

then $x^m \equiv x \bmod p$ and $x^m \equiv x \bmod q$; that is, $p \mid (x^m - x)$ and $q \mid (x^m - x)$. As p and q are distinct primes, they are relatively prime, and so $pq \mid (x^m - x)$, by Exercise 1.55 on page 52. Since $N = pq$, we have shown that if $m \equiv 1 \bmod (p-1)(q-1)$, then

$$x^m \equiv x \bmod N \quad \text{for all } x.$$

It remains to find such a number m and a factorization $m = st$. We claim that there is a factorization with $s = 3$. Let us first show that $\big(3, (p-1)(q-1)\big) = 1$. Since $p \equiv 2 \bmod 3$ and $q \equiv 2 \bmod 3$, we have $p - 1 \equiv 1 \bmod 3$ and $q - 1 \equiv 1 \bmod 3$; hence, $(p-1)(q-1) \equiv 1 \bmod 3$, so that 3 and $(p-1)(q-1)$ are relatively prime [Proposition 1.31]. Thus, there are integers t and u with $1 = 3t + (p-1)(q-1)u$, so that $3t \equiv 1 \bmod (p-1)(q-1)$. To sum up, $x^{3t} \equiv x \bmod N$ for all x with this choice of t. Choosing $m = 3t$ completes the construction of the ingredients of the code.

III : ***Security.***

Since $3t \equiv 1 \bmod (p-1)(q-1)$, he who knows the factorization $N = pq$ knows the number $(p-1)(q-1)$, and hence he can find t using the Euclidean algorithm. Unauthorized readers may know N, but without knowing its factorization, they do not know t and, hence, they cannot decode. This is why this code is secure today. For example, if both p and q have about 200 digits (and, for technical reasons, they are not too close together), then the fastest existing computers need two or three months to factor N. By Proposition 1.59, there are plenty of primes congruent to 2 mod 3, and so we may choose a different pair of primes p and q every month, say, thereby stymying the enemy. ◀

EXERCISES

1.71 Find all the integers x which are solutions to each of the following congruences:

- **(i)** $3x \equiv 2 \bmod 5$.
- **(ii)** $7x \equiv 4 \bmod 10$.
- **(iii)** $243x + 17 \equiv 101 \bmod 725$.
- **(iv)** $4x + 3 \equiv 4 \bmod 5$.
- **(v)** $6x + 3 \equiv 4 \bmod 10$.
- **(vi)** $6x + 3 \equiv 1 \bmod 10$.

1.72 Let m be a positive integer, and let m' be an integer obtained from m by rearranging its (decimal) digits (e.g., take $m = 314159$ and $m' = 539114$). Prove that $m - m'$ is a multiple of 9.

1.73 Prove that a positive integer n is divisible by 11 if and only if the alternating sum of its digits is divisible by 11 (if the digits of a are $d_k \ldots d_2 d_1 d_0$, then their ***alternating sum*** is $d_0 - d_1 + d_2 - \cdots$).

1.74 What is the remainder after dividing 10^{100} by 7? (The huge number 10^{100} is called a *googol* [21] in children's stories.)

***1.75** **(i)** Prove that $10q + r$ is divisible by 7 if and only if $q - 2r$ is divisible by 7.

(ii) Given an integer a with decimal digits $d_k d_{k-1} \ldots d_0$, define

$$a' = d_k d_{k-1} \cdots d_1 - 2d_0.$$

Show that a is divisible by 7 if and only if some one of a', a'', a''',... is divisible by 7. (For example, if $a = 65464$, then $a' = 6546 - 8 = 6538$, $a'' = 653 - 16 = 637$, and $a''' = 63 - 14 = 49$; we conclude that 65464 is divisible by 7.)

***1.76** **(i)** Show that $1000 \equiv -1 \bmod 7$.

(ii) Show that if $a = r_0 + 1000r_1 + 1000^2 r_2 + \cdots$, then a is divisible by 7 if and only if $r_0 - r_1 + r_2 - \cdots$ is divisible by 7.

Remark. Exercises 1.75 and 1.76 combine to give an efficient way to determine whether large numbers are divisible by 7. If $a = 33456789123987$, for example, then $a \equiv 0 \bmod 7$ if and only if $987 - 123 + 789 - 456 + 33 = 1230 \equiv 0 \bmod 7$. By Exercise 1.75 on page 71, $1230 \equiv 123 \equiv 6 \bmod 7$, and so a is not divisible by 7. ◀

***1.77** For a given positive integer m, find all integers r with $0 < r < m$ such that $2r \equiv 0 \bmod m$.

1.78 Prove that there are no integers x, y, and z such that

$$x^2 + y^2 + z^2 = 999.$$

1.79 Prove that there is no perfect square a^2 whose last two digits are 35.

1.80 If x is an odd number not divisible by 3, prove that $x^2 \equiv 1 \bmod 24$.

***1.81** Prove that if p is a prime and if $a^2 \equiv 1 \bmod p$, then $a \equiv \pm 1 \bmod p$.

***1.82** Consider the congruence $ax \equiv b \bmod m$ when $\gcd(a, m) = d$. Show that $ax \equiv b \bmod m$ has a solution if and only if $d \mid b$.

1.83 Solve the congruence $x^2 \equiv 1 \bmod 21$.

1.84 Solve the simultaneous congruences:

(i) $x \equiv 2 \bmod 5$ and $3x \equiv 1 \bmod 8$;

(ii) $3x \equiv 2 \bmod 5$ and $2x \equiv 1 \bmod 3$.

1.85 How many days are there between Akbal 13 and Muluc 8 in the Mayan tzolkin calendar?

1.86 **(i)** Show that $(a + b)^n \equiv a^n + b^n \bmod 2$ for all a and b and for all $n \geq 1$.

(ii) Show that $(a + b)^2 \not\equiv a^2 + b^2 \bmod 3$.

1.87 On a desert island, five men and a monkey gather coconuts all day, then sleep. The first man awakens and decides to take his share. He divides the coconuts into five equal shares, with one coconut left over. He gives the extra one to the monkey, hides his share, and goes to sleep. Later, the second man awakens and takes his

[21] This word was invented by a 9-year-old boy when his uncle asked him to think up a name for the number 1 followed by a hundred zeros. At the same time, the boy suggested *googolplex* for a 1 followed by a googol zeros.

fifth from the remaining pile; he too finds one extra and gives it to the monkey. Each of the remaining three men does likewise in turn. Find the minimum number of coconuts originally present.

1.6 DATES AND DAYS

Congruences can be used to determine on which day of the week a given date falls. For example, on what day of the week was July 4, 1776?

A ***year*** is the amount of time it takes the Earth to make one complete orbit around the Sun; a ***day*** is the amount of time it takes the Earth to make a complete rotation about the axis through its north and south poles. There is no reason why the number of days in a year should be an integer, and it is not; a year is approximately 365.2422 days long. In 46 B.C., Julius Caesar (and his scientific advisors) compensated for this by creating the ***Julian calendar***, containing a ***leap year*** every 4 years; that is, every fourth year has an extra day, namely, February 29, and so it contains 366 days (a ***common year*** is a year that is not a leap year). This would be fine if the year were exactly 365.25 days long, but it has the effect of making the year $365.25 - 365.2422 = .0078$ days (about 11 minutes and 14 seconds) too long. After 128 years, a full day was added to the calendar; that is, the Julian calendar overcounted the number of days. In the year 1582, the vernal equinox (the Spring day on which there are exactly 12 hours of daylight and 12 hours of night) occurred on March 11 instead of on March 21. Pope Gregory XIII (and his scientific advisors) then installed the ***Gregorian calendar*** by erasing 10 days that year; the day after October 4, 1582 was October 15, 1582, and this caused confusion and fear among the people. The Gregorian calendar modified the Julian calendar as follows. Call a year y ending in 00 a ***century year***. If a year y is not a century year, then it is a leap year if it is divisible by 4; if y is a century year, it is a leap year only if it is divisible by 400. For example, 1900 is not a leap year, but 2000 is a leap year. The Gregorian calendar is the one in common use today, but it was not uniformly adopted throughout Europe. For example, the British did not accept it until 1752, when 11 days were erased, and the Russians did not accept it until 1918, when 13 days were erased (thus, the Russians called their 1917 revolution the October Revolution, even though it occurred in November of the Gregorian calendar).

The true number of days in 400 years is about

$$400 \times 365.2422 = 146096.88 \text{ days.}$$

In this period, the Julian calendar has

$$400 \times 365 + 100 = 146,100 \text{ days,}$$