2

Divisibility and Modular Arithmetic

In this chapter we start with some basic concepts of divisibility and primes and then move on to introduce the systems of modular integers and their associated arithmetic. Some cryptographic applications of modular arithmetic will be shown beginning with the next chapter. The modular integers are prototypical abstract number systems on which cryptosystems can be built, and they are used as the underpinnings of several more advanced systems that will be introduced in later chapters. The chapter contains a good number of important theorems and propositions; readers with less theoretical backgrounds may wish to skip some of the longer, more technical proofs. Additional topics in number theory are covered in Chapter 8.

As children, our first experience with numbers involved the set of **positive integers**

$$\mathbb{Z}_+ = \{1, 2, 3, 4, 5, \cdots\}$$

If we expand this set to include zero and negative integers, we arrive at the set of **integers**

$$\mathbb{Z} = \{\cdots -3, -2, -1, 0, 1, 2, 3, \cdots\}$$

which is simply the set of all real numbers (the numbers on the number line) that have nothing after their decimal points. There is a rich theory and structure concerning the set of positive integers (and less specifically the set of integers) called **number theory**, but many mysteries, unsolved problems, and problems that can be solved only very inefficiently remain and make the integers a virtual goldmine for building cryptosystems.

Divisibility

One of the most fundamental concepts of the integers is that of divisibility, which is first learned in grade school. Here is the formal definition:

Definition 2.1

Suppose that a and b are integers with $a \neq 0$. We say that a **divides** b (written $a \mid b$) if there is an integer c such that $b = ac$. This can also be expressed by saying a is a **factor** of b, or b is a **multiple** of a. If a does not divide b, we write $a \nmid b$.

Here are some simple examples: $3 \mid 6$, since $6 = 3 \cdot 2$. Also, $-5 \mid 15$, since $15 = (-5) \cdot (-3)$. But $8 \nmid 20$, because $20/8$ is not an integer. Notice also that for any nonzero integer a, we have $a \mid a$ (since $a = a \cdot 1$), and $a \mid 0$ (since $0 = a \cdot 0$). The following theorem contains some basic yet very useful properties of divisibility.

Theorem 2.1

Let a, b, and c be integers.

(a) *Divisibility is transitive.* If $a \mid b$ and $b \mid c$, then $a \mid c$.

(b) If $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$ for any integers x and y.

Proof: Part (a): Since $a \mid b$ we can write $b = ae$ for some integer e. Similarly, since $b \mid c$, we can write $c = bf$ for some integer f. Substituting the former into the latter gives $c = (ae)f = a(ef)$. Since ef is an integer, we conclude that $a \mid c$.

Part (b): The hypotheses allow us to write $b = ae$ and $c = af$ for some integers e and f. Substituting these gives us $bx + cy = aex + afy = a(ex + fy)$. Since $ex + fy$ is an integer, we conclude that $a \mid (bx + cy)$. □

Primes

Definition 2.2

An integer $p > 1$ is called **prime** if the only positive factors of p are 1 and itself. An integer $a > 1$ that is not prime is called **composite**.

The first few primes are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, ... Prime numbers are the building blocks of the integers because any integer greater than 1 can always be uniquely factored into primes. This is the so-called *fundamental theorem of arithmetic*. We state this important theorem here but postpone its proof until we have developed some additional needed concepts.

Theorem 2.2: Fundamental Theorem of Arithmetic

Every positive integer $a > 1$ can be uniquely expressed as the product of primes. In other words, there exist unique prime numbers $p_1 < p_2 < \cdots < p_n$ and corresponding positive exponents $\alpha_1, \alpha_2, \cdots, \alpha_n \in \mathbb{Z}_+$ such that $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$.*

In general, it becomes difficult to verify whether or not a positive integer is prime for larger integers. If a positive integer a has a nontrivial

* This important theorem is the reason why the number 1 is not considered to be prime. If 1 were prime, we would no longer have unique factorization; for example, $18 = 2 \cdot 3^2 = 1^3 \cdot 2 \cdot 3^2 = 1^{12} \cdot 2 \cdot 3^2$, and so forth.

factorization $a = bc$, with $b, c > 1$, then one of b or c must be $\leq \sqrt{a}$ (otherwise we would have the contradiction $a = bc > \sqrt{a}\sqrt{a} = a$). This means that to check if a given positive integer a is prime, we need only look for (prime) factors that are at most equal to $\sqrt{a}$. But testing primality and, more generally, determining the prime factorization of large positive integers can take an inordinate amount of time, even with the best computers and algorithms.*

Example 2.1

Find the prime factorizations of each of the following integers:

(a) 847
(b) 4808
(c) 6177

Solution: Part (a) Using the basic principle mentioned above, we begin checking, in order, for prime factors of 847 (knowing that we can stop after we check primes up to $\sqrt{847} = 29.1033$). Certainly $2 \nmid 847$ (since the latter is odd), and also since $847/3 = 282\ 1/3 \notin \mathbb{Z}$, we know that $3 \nmid 847$. Since 847 does not end in 0 or 5, $5 \nmid 847$. But $847/7 = 121$, and we are now reduced to looking for prime factors of 121, so we can stop when we get to $\sqrt{121} = 11$. The following diagram is often used when such factorizations are done by hand. The resulting prime factorization is thus $847 = 7 \cdot 11^2$.

$$\begin{array}{r} 11 \\ 11\overline{)121} \\ 7\overline{)847} \end{array}$$

Parts (b) and (c): Going through the same procedure, the corresponding prime factorizations are $4808 = 2^3 \cdot 601$ and $6177 = 3 \cdot 29 \cdot 71$.

One natural question arises: How many primes are there (infinitely many, or does the list eventually end)? This question was resolved a very long time ago by Euclid, the Greek mathematician who lived 325 b.c.–265 b.c. and is most famous for his timeless geometry book *The Elements*; he proved that there are infinitely many primes. This never-ending supply of primes that are as large as we could possibly want has, as we will see later, important

* To illustrate this, we point out that RSA Security (a high-tech cryptographic security company) offered a number of challenges on their company Web site that were open to the public. One of these offered a $100,000 prize to the first person to factor a certain 304-digit number (larger prizes were available for factoring larger integers). This particular challenge remained open for several years. Such challenges actually benefit the company by helping to test the security of some of its secret codes (that rest on the infeasibility of being able to factor such large or even larger integers) against potential hackers. We discuss such topics in greater detail in Chapter 9.

ramifications in cryptography. Euclid's elegant proof uses the fundamental theorem of arithmetic.*

Theorem 2.3: Euclid

There are infinitely many primes.

Proof: Suppose the assertion were false. Then the list of all primes would be finite: $p_1 < p_2 < \cdots < p_M$. Consider the integer $N = p_1 \cdot p_2 \cdot \cdots \cdot p_M + 1$. By the fundamental theorem of arithmetic, N can be factored (uniquely) into primes. Let p_i be (any) one of the prime factors of N. Then, since $p_i \mid p_1 \cdot p_2 \cdot \cdots \cdot p_M$, and $p_i \mid N$, it follows from Theorem 2.1(b) that $p_i \mid (N - p_1 \cdot p_2 \cdot \cdots \cdot p_M)$, that is, $p_i \mid 1$. But this is a contradiction since no prime can divide 1. □

Greatest Common Divisors and Relatively Prime Integers

Definition 2.3

Suppose that a and b are integers not both equal to zero. The **greatest common divisor** of a and b, denoted $\gcd(a,b)$, is the largest integer d that divides both a and b. We say that a and b are **relatively prime** if $\gcd(a,b) = 1$.

For a simple example, since the common factors of 12 and 20 are 1, 2, and 4, we have $\gcd(12,20) = 4$. Similarly, since the only common (positive) factor of 8 and 15 is 1, $\gcd(8,15) = 1$, and 8 and 15 are relatively prime. For integers of moderate size that can be readily factored into primes, the greatest common divisor can be easily read from the prime factorizations—simply take all common prime factors and use the corresponding minimum exponents of each prime. It is routine to verify that this product of common prime powers is the desired gcd (see Exercise for the Reader 2.2). This method is illustrated in the following example.

Example 2.2

Find $\gcd(50,165)$, and $\gcd(1960,10800)$.

Solution: The prime factorizations of the first pair of numbers are $50 = 2 \cdot 5^2$ and $165 = 3 \cdot 5 \cdot 11$; therefore, $\gcd(50,165) = 5$. Similarly, after computing the prime factorizations of $1960 = 2^3 \cdot 5 \cdot 7^2$ and $10800 = 2^4 \cdot 3^3 \cdot 5^2$, we conclude that $\gcd(1960, 10800) = 2^3 \cdot 5 = 40$.

* By contrast, the problem of whether there are infinitely many prime pairs has not yet been resolved. A prime pair consists of two primes whose difference is two; for example, 3 and 5, 5 and 7, 11 and 13, and 17 and 19 are the first few prime pairs.

Exercise 2.1

(a) Find the prime factorizations of 16000 and 42757.
(b) Compute gcd(100, 76), gcd(16000, 960).

Exercise 2.2

For a pair of nonzero integers a and b, the **least common multiple** of a and b, denoted lcm(a,b), is the smallest integer m that is divisible by both a and b.

(a) Find lcm(12, 28), and lcm(100, 76).
(b) Show that if $p_1 < p_2 < \cdots < p_n$ are the distinct primes appearing in the prime factorizations of either a or b, if $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ and if $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}$, then $\text{lcm}(a,b) = p_1^{\mu_1} p_2^{\mu_2} \cdots p_n^{\mu_n}$, where $\mu_i = \max(\alpha_i, \beta_i)$, and $\gcd(a,b) = p_1^{\sigma_1} p_2^{\sigma_2} \cdots p_n^{\sigma_n}$, where $\sigma_i = \min(\alpha_i, \beta_i)$.
(c) Show that $\text{lcm}(a,b) \cdot \gcd(a,b) = ab$.

For pairs of large integers, the above procedure for finding greatest common divisors is very slow (because there is no known fast algorithm for prime factorization); a much more efficient method circumvents the need to factor by using the so-called *Euclidean algorithm*. This simple yet very useful procedure in number theory is also due to Euclid. We first formalize the procedure of dividing one integer by another nonzero integer.

The Division Algorithm

Proposition 2.4: The Division Algorithm

If a is an integer and d is any positive integer, then there exist unique integers q and r satisfying $0 \le r < d$, such that $a = dq + r$. Here, a is called the **dividend**, d is called the **divisor**, q is called the **quotient**, and r is called the **remainder**.

Finding q and r is really just the "long division" problem $a \div d$ that one learns about in grade school, but Exercise for the Reader 2.3 shows how to quickly compute q and r, if one is using a calculator (or computer). The uniqueness proof of Proposition 2.4 is routine and is left as an exercise. Although the proposition is not really an algorithm, the terminology is nonetheless standard in number theory, so we will adhere to it. In the language of modular arithmetic that we introduce later in this chapter, the result of the division algorithm can be expressed as $a \equiv r \pmod{d}$. Given the integers a and d, the dividend d is most easily expressed in terms of the following "floor" function. The floor function inputs any real number and outputs the first integer below the number. The formal

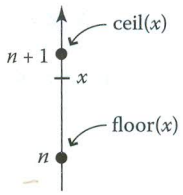

Figure 2.1 Illustration of the floor and ceiling functions.

definition of the floor function and the corresponding ceiling function are as follows.

Definition 2.4 The Floor and Ceiling Functions

The **floor function** is a function from the set of real numbers to the set of integers, defined by

floor(x) = $\lfloor x \rfloor$ = the greatest integer k that is less than or equal to x

The **ceiling function** has the same domain and codomain and is defined by

ceil(x) = $\lceil x \rceil$ = the least integer k that is greater than or equal to x

It is helpful to visualize the actions of these two functions using a vertical number line; see Figure 2.1. Notice that there are two different notations in use for the floor and ceiling functions; the abbreviated word *notation* is more natural and common in many computing platforms, while the symbolized notation is more compact and often used in mathematical developments. Here are some simple examples of some floors and ceilings: floor(4.75) = $\lfloor 4.75 \rfloor = 4$, ceil(4.75) = $\lceil 4.75 \rceil = 5$, $\lfloor -4.75 \rfloor = -5$, ceil(−4.75) = −4. Notice that when n is an integer, floor(n) = n = ceil(n), and conversely, if either of these two equations holds, n must be an integer.

Exercise for the Reader 2.3

(a) Show that if the division algorithm is applied to an integer division $a \div d$, where (as usual) $d > 0$, then the quotient and remainder are given as follows: $q = \lfloor a/d \rfloor$ and $r = a - qd$.

(b) Use part (a) to find the quotient and remainder when the division algorithm is applied to the following integer divisions:
(a) $123 \div 5$
(b) $-874 \div 15$.

The Euclidean Algorithm

The Euclidean algorithm consists of repeatedly applying the division algorithm. It is based on the following simple property:

Proposition 2.5

If a, d, q, and r are as in the division algorithm, then $\gcd(a, d) = \gcd(d, r)$.

Proof: From the equation $a = dq + r$, and Theorem 2.1(b), we see that if $e \mid r$ and $e \mid d$, then $e \mid a$. If we rewrite the equation as $r = a - dq$, then by the same token we get that if $e \mid a$ and $e \mid d$, then $e \mid r$. We have proved that the set of all common divisors of r and d equals the set of all common divisors of a and d, from which the result of the theorem directly follows. □

For the pair of integers (100,76) let us observe what happens when we repeatedly apply the division algorithm by dividing all new remainders into the previous divisors:

$$\begin{aligned} 100 &= 1 \cdot 76 + 24 \\ 76 &= 3 \cdot 24 + 4 \\ 24 &= 6 \cdot 4 + 0 \end{aligned}$$

From Proposition 2.5, we see that $\gcd(100,76) = \gcd(76,24) = \gcd(24, 4) = \gcd(4,0) = 4$. In general, this procedure will always stop since the sequence of remainders is strictly decreasing. (By the division algorithm, the new remainder must be less than the previous one because the previous remainder has become the divisor.) The last nonzero remainder will be the gcd of the two starting integers. This procedure is the Euclidean algorithm. We now make a formal statement of it.

Algorithm 2.1: The Euclidean Algorithm

Input: A pair of integers a and b, not both equal to zero.
Output: The greatest common divisor, $\gcd(a,b)$.

We may assume that $a \geq b$ (if not, switch a and b). Apply the division algorithm to write $a = q_0 b + r_1$. If $r_1 = 0$, then $\gcd(a,b) = b$; otherwise, continue by dividing successive divisors by successive remainders until a zero remainder is reached:

$$\begin{aligned} b &= q_1 r_1 + r_2, & 0 \leq r_2 < r_1 \\ r_1 &= q_2 r_2 + r_3, & 0 \leq r_3 < r_2 \\ &\cdots \\ r_{n-2} &= q_{n-1} r_{n-1} + r_n, & 0 \leq r_n < r_{n-1} \\ r_{n-1} &= q_n r_n + 0 \end{aligned}$$

The last nonzero remainder r_n is $\gcd(a,b)$.

Since the sequence of successive remainders is strictly decreasing, $b > r_1 > r_2 > \cdots > r_n > 0$, the algorithm must eventually terminate (at most

b steps). Since Proposition 2.5 implies that $\gcd(a,b) = \gcd(b,r_1) = \gcd(r_1,r_2) = \gcd(r_2,r_3) = \cdots = \gcd(r_{n-1},r_n) = \gcd(r_n,0) = r_n$, it follows that $\gcd(a,b) = r_n$, the last nonzero remainder that is encountered in this process.

We summarize how the division algorithm data is used in going from one round to the next:

$$\text{remainder} \rightarrow \text{divisor} \rightarrow \text{dividend} \rightarrow \text{not used}$$

In practice, the Euclidean algorithm is a very efficient method for computing greatest common divisors, and it does not require any factorizations. As we will soon discover, it can also be used to solve other interesting problems, and it is readily translated into computer programs.

Exercise for the Reader 2.4

Use the Euclidean algorithm to compute gcd(65, 91) and gcd(1665, 910).

One very useful consequence of the Euclidean algorithm can be previewed by looking at the preceding example where we used it to find gcd(100, 76) = 4. If we start with the second-to-last equation where this gcd(4) appeared as the remainder and work our way up, we will be able to express 4 in the form of $100x + 76y$ for some integers x and y, that is, as an *integer combination* of 100 and 76 (the integers for which we wanted to find the gcd). Here are the steps: we start with $76 = 3 \cdot 24 + 4$ and isolate the gcd(= 4) to write it as an integer combination of the two previous remainders: $4 = 3 \cdot 24 - 1 \cdot 76$. We then use the next equation up, $100 = 1 \cdot 76 + 24$, solve it for 24, and substitute the result into what we had just previously obtained: $4 = 3 \cdot 24 - 1 \cdot 76 = 3 \cdot (100 - 1 \cdot 76) - 1 \cdot 76 = 3 \cdot 100 - 4 \cdot 76$. The following theorem contains the general result.

Theorem 2.6

Suppose that a and b are integers not both equal to zero, and let $d = \gcd(a,b)$. Then there exist integers x and y such that $d = ax + by$. In the special case in which a and b are relatively prime, we can write $1 = ax + by$.

Proof: The proof is a constructive one in that it provides an algorithm for finding such an x and y. If we set $r_0 = b$ and $r_{-1} = a$, then the Euclidean algorithm consists of $n + 1$ applications of the division algorithm, and these can all be expressed as $r_{i-1} = q_i r_i + r_{i+1}$ $(i = 0,2,\cdots n)$. Each of these is then rewritten to be solved for the last remainder: $r_{i+1} = q_i r_i - r_{i-1}$ $(i = 0,2,\cdots n)$. Since $d = r_n$, we will start with the second-to-last equation $(i = n - 1)$ and rewrite it as $d = x_n r_{n-2} + y_n r_{n-1}$. Thus d is expressed as an integer combination of r_{n-2} and r_{n-1}. If we substitute the next equation up $(i = n - 2)$ $r_{n-1} = r_{n-3} - q_{n-2} r_{n-2}$ into our expression for d, we arrive at $d = x_n r_{n-2} + y_n r_{n-1} = x_n r_{n-2} + y_n (r_{n-3} - q_{n-2} r_{n-2}) = y_n r_{n-3} + (x_n - q_{n-2}) r_{n-2} =: x_{n-1} r_{n-3} + y_{n-1} r_{n-2}$. We continue this process of

successively moving up the list of division algorithm equations and substituting them into our existing integer combination of d. At the kth step ($i = n - k$), we will have obtained an expression for d as an integer combination $x_{n-k+1}r_{n-k-1} + y_{n-k+1}r_{n-k}$. At the final step ($k = n$; $i = 0$), we will have $d = x_1r_{-1} + y_1r_0 = x_1a + y_1b$, as desired. □

Although the proof is a bit technical, the idea is simple enough, and the whole scheme is nicely amenable to translate into a computer program. Later in the section we provide a very efficient implementation of this algorithm (that can be directly translated into a computer program).

Exercise for the Reader 2.5

(a) Use the procedure described in the proof of Theorem 2.6 to express gcd(65, 91) as an integer combination of 91 and 65. Similarly, express gcd(1665, 910) as an integer combination of 1165 and 910.

(b) Explain why the integers x and y in Theorem 2.6 are not unique.

Aside from its practical applications, Theorem 2.6 turns out to be very useful for obtaining new theoretical results. We demonstrate this by using it to prove the following result, which, in turn, will allow us to prove the fundamental theorem of arithmetic.

Proposition 2.7: Euclid's Lemma

(a) Suppose that p is a prime and that a and b are integers. If $p \mid ab$, then either $p \mid a$ or $p \mid b$.

(b) Suppose that p is a prime and that $a_1, a_2, \cdots, a_n$ are integers. If $p \mid a_1a_2 \cdots a_n$, then p must divide at least one of the factors $a_1, a_2, \cdots, a_n$.

Proof: (a) Assuming that $p \mid ab$, if also $p \mid a$, we are done; so assume that $p \nmid a$. We need to show that $p \mid b$. Since p is a prime and $p \nmid a$, it follows that $\gcd(a,p) = 1$. Theorem 2.6 thus allows us to write $1 = ax + py$ for some integers x and y. We multiply this equation by b to obtain $b = (ab)x + pyb$. But since $p \mid ab$, and certainly $p \mid p$, it follows from Theorem 2.1(b) that $p \mid b$, as desired.

(b) We can achieve the proof of part (b) by using the just proved special case of part (a) (when $n = 2$) to repeatedly chip away at it. Assuming that $p \mid a_1(a_2 \cdots a_n)$, part (a) tells us that either $p \mid a_1$, in which case we are done, or we get that $p \mid a_2 \cdots a_n$, which involves one less factor. Applying part (a) again to this smaller case $p \mid a_2(a_3 \cdots a_n)$, we find that either $p \mid a_2$, in which case we are done, or we get that $p \mid a_3 \cdots a_n$. If we continue this process, we will either be done or we arrive at a division involving the final two factors $p \mid a_{n-1}a_n$, to which one final application of part (a) will complete the proof. □

We are now nicely poised to prove the fundamental theorem of arithmetic.

Proof of Theorem 2.2. Part I: *Existence.* Suppose that there were positive integers greater than 1 that were not expressible as a product of primes. Let n be the smallest such integer. Since n cannot be prime (because a single prime is a product of primes), it must be composite, so we can write $n = ab$, where a and b are smaller integers with $1 < a, b < n$. But since n was chosen to be the smallest integer that cannot be written as a product of primes, both a and b must be expressible as a product of primes. Since $n = ab$, we can multiply prime factorizations of a and b to obtain a prime factorization of n. With this contradiction, the existence proof is complete.

Part II: *Uniqueness.* Suppose that a positive integer n had two different prime factorizations:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = q_1^{\beta_1} q_2^{\beta_2} \cdots q_\ell^{\beta_\ell}$$

where $p_1 < p_2 < \cdots < p_k$ and $q_1 < q_2 < \cdots < q_\ell$ are primes, and $\alpha_1, \alpha_2, \cdots, \alpha_k$ and $\beta_1, \beta_2, \cdots, \beta_\ell$ are positive exponents. If there are any primes among the p's and q's that are common, they can be divided through (cancelled) on both sides of the equation so that the lists $p_1 < p_2 < \cdots < p_k$ and $q_1 < q_2 < \cdots < q_\ell$ can be assumed to have no primes in common, and we assume that this is indeed the case. Now, since $p_1 \mid p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = q_1^{\beta_1} q_2^{\beta_2} \cdots q_\ell^{\beta_\ell}$, it follows from Euclid's lemma [Proposition 2.7(b)] that $p_1 \mid q_j$ for some index j. But since p_1 and q_j are both primes, it follows that $p_1 = q_j$, which contradicts the assumption that the p's and q's have no primes in common. This completes the uniqueness proof. □

Modular Arithmetic and Congruences

Among his numerous contributions to mathematics and science, the illustrious mathematician Carl Friedrich Gauss* (Figure 2.2) developed the extremely useful number–theoretic concepts of congruences and modular arithmetic. These concepts led to an infinite supply of abstract number systems that have turned out to play a pivotal role in an assortment

* Carl F. Gauss is widely considered to be the greatest mathematician who ever lived. His potential was discovered early, and his mathematical aptitude was astounding. While he was in second grade, his teacher, needing to keep him occupied for a while, asked him to perform the addition of the first 100 integers: $S = 1 + 2 + \cdots + 100$. Two minutes later, Gauss gave the teacher the answer. He did it by rewriting the sum in the reverse order $S = 100 + 99 + \cdots + 1$, adding vertically to the original to get $2S = 101 + 101 + \cdots + 101 = 100 \cdot 101$, so $S = 50 \cdot 101 = 5050$. This idea yields a general proof of an important mathematical series identity. Apart from his numerous groundbreaking contributions to mathematics, Gauss did significant work in physics and astronomy, as well as in other sciences. His brilliant ideas came to him so rapidly that he had a file cabinet full of them waiting to be written up for formal publication. He would often receive visits from other prominent international mathematicians who would proudly share with Gauss recent discoveries, and very often Gauss would simply reach into his file cabinet to pull out his ideas on the topic that frequently eclipsed those of the visitor. For many years until the inception of the Euro, Germany had honored Gauss by placing his image on the very common 10 Deutsche mark banknote (the value was approximately US$5). Figure 2.2 is an image of this banknote, with a drawing of Gauss's important normal (bell-shaped) curve, a cornerstone of statistics.

Figure 2.2 Carl Friedrich Gauss (1777–1855), German mathematician.

of cryptosystems. The entire framework is based on the following very simple definition.

Definition 2.5

Let m be a positive integer. We say that two integers a and b are **congruent mod(ulo) m**, and denote this as $a \equiv b \pmod{m}$, if $m \mid (a-b)$. The number m is called the **modulus** of the congruency. If $m \nmid (a-b)$, we say that a and b are **incongruent mod m**, and write this as $a \not\equiv b \pmod{m}$.

Example 2.3: Two Familiar Moduli

(a) Notice that $15 \equiv 3 \pmod{12}$, since $15 - 3 = 12$; similarly, since $27 - 3 = 24 = 2 \cdot 12$, we have $27 \equiv 3 \pmod{12}$. The reader can similarly check that $3 \equiv -9 \equiv -21 \equiv -33 \cdots \pmod{12}$. Congruences mod 12 can be visualized by means of a traditional (as opposed to a digital) clock; see Figure 2.3. Two times are congruent in the clock if one can be made into the other by turning the (hour) hand of the clock a complete number of revolutions either clockwise (corresponding to adding 12) or counterclockwise (corresponding to subtracting 12).

(b) Anyone who has studied angles or trigonometry will already be familiar with 360 as a modulus, since 360° corresponds to a complete revolution angle (so adding any multiple of it results in the same angle as wherever we started). Thus the angular equalities: $-90° = 270° = 630° = \cdots$ correspond to the congruences $-90 \equiv 270 \equiv 630 \cdots \pmod{360}$. To see that $-90 \equiv 630 \pmod{360}$, for example, we note that $-90 - 630 = -720 = -2 \cdot 360$.

If we rewrite the condition $m \mid (a-b)$ for $a \equiv b \pmod{m}$ as $a - b = km$ (for some integer k), we then obtain $a = b + km$. We summarize this alternate formulation:

$$a \equiv b \pmod{m} \iff a = b + km, \text{ for some } k \in \mathbb{Z} \qquad (2.1)$$

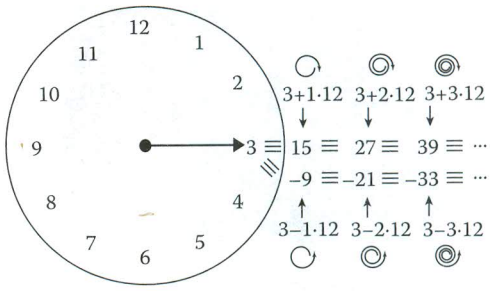

Figure 2.3 Congruence modulo 12 is like clockwork; two integers are congruent mod 12 if one can be obtained from the other by adding or subtracting a multiple of 12, corresponding to making an integral number of revolutions around the clock.

This formula is illustrated in Figure 2.3, showing how to get all of the integers that are congruent to 3 (mod 12). Congruences satisfy three basic properties that will be tacitly used throughout the remainder of this book.

Proposition 2.8: Basic Properties of Congruences

The three properties of this proposition—reflexivity, symmetry, and transitivity—can be applied to any relation between pairs of objects of a set, and if they are satisfied together the relation is called an *equivalence relation*. Thus congruence mod m is an equivalence relation.

If m is a positive integer, then congruence mod m satisfies the following properties:

(a) *Reflexivity.* $a \equiv a \pmod{m}$ for any integer a.
(b) *Symmetry.* If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$ for any integers a, b.
(c) *Transitivity.* If $a \equiv b \pmod{m}$ and $b \equiv a \pmod{m}$, then $a \equiv c \pmod{m}$ for any integers a, b, c.

Proof: Part (a): Since $m \mid 0 = (a - a)$, we obtain that $a \equiv a \pmod{m}$.

Part (b): Using Equation 2.1, from $a \equiv b \pmod{m}$, we can write that $a - b = km$ for some integer k. Negating both sides of this equation produces $b - a = -(a - b) = (-k)m$, which by Equation 2.1 is equivalent to $b \equiv a \pmod{m}$.

Part (c): Applying Equation 2.1 to the assumptions $a \equiv b \pmod{m}$ and $b \equiv a \pmod{m}$, we may write $a - b = km$ and $b - c = \ell m$ for some integers k, ℓ. Adding these two equations leads us to $a - c = (a - b) + (b - c) = mk + m\ell = m(k + \ell)$, which by Equation 2.1 is equivalent to $a \equiv c \pmod{m}$. □

One important consequence of Proposition 2.8 is that for any positive integer m, the integers can be broken down into m *congruence classes* of integers that are mutually congruent mod m. For example,

for congruences mod 12 (clockwork), the 12 congruence classes are as follows:

$$\cdots -36 \equiv -24 \equiv -12 \equiv 0 \equiv 12 \equiv 24 \equiv 36 \cdots \pmod{12}$$
$$\cdots -35 \equiv -23 \equiv -11 \equiv 1 \equiv 13 \equiv 25 \equiv 37 \cdots \pmod{12}$$
$$\cdots -34 \equiv -22 \equiv -10 \equiv 2 \equiv 14 \equiv 26 \equiv 38 \cdots \pmod{12}$$
$$\cdots$$
$$\cdots -25 \equiv -13 \equiv -1 \equiv 11 \equiv 23 \equiv 35 \equiv 47 \cdots \pmod{12}$$

The reader should observe that (i) the sets are disjoint, (ii) all integers are accounted for (read from top to bottom, proceed to next column left or right), and (iii) the gap between successive integers in any row is always 12. In terms of the clock (Figure 2.3), this means that the rows are obtained by starting at any given hour on the clock and successively adding/subtracting 12 (corresponding to complete revolutions on the clock).

Exercise for the Reader 2.6

Show that $a \equiv b \pmod 2$ if, and only if, a and b have the **same parity**, that is, a and b are both even or both odd. Describe the congruence classes mod 2.

The following simple proposition gives yet another useful way to view the relation of congruence mod m.

Proposition 2.9: Congruences and Remainders

If m is a positive integer and a, b are integers, then $a \equiv b \pmod m$ if, and only if, a and b both have the same remainder $r \in \{0,1,2,\cdots,n-1\}$ when they are divided by m using the division algorithm (Proposition 2.4).

Proof: We use the division algorithm (Proposition 2.4) to write $a = mq + r$ and $b = mq' + r'$, where q, r, q', r' are uniquely determined integers with $0 \le r, r' < m$.

Now, if the remainders are the same, that is, $r = r'$, then we have:

$$a - b = mq + r - mq' - r' = m(q - q') + \underbrace{(r - r')}_{=0} = m(q - q')$$

so $m \mid (a - b)$, which means that $a \equiv b \pmod m$.

Conversely, if we start with $a \equiv b \pmod m$, this means that $m \mid (a - b)$, and substituting the above expressions for a and b, we obtain $m \mid (mq + r - mq' - r')$ or $m \mid (m[q - q'] + r - r')$. Since m certainly divides $m[q - q']$, it follows [from Theorem 2.1(b)] that $m \mid (r - r')$. But since the remainders r, r' lie in the range $\{0,1,2,\cdots,m-1\}$, their difference $r - r'$ must lie in the range $\{-(m-1), \cdots, -2, -1, 0, 1, 2, \cdots, m-1\}$, and the only possible way to have $m \mid (r - r')$, would be if $r - r' = 0$, that is, the remainders are the same. □

For the clockwork example, the 12 possible remainders, 0, 1, 2, …, 11, correspond to the 12 congruence classes. Except for the fact that 0 represents 12, these numbers represent the hours on the clock. In fact, any member of a congruence class can be used to represent the whole class. What makes this concept so powerful is that the *answers we get with arithmetic operations on any integers will land in the same congruence class mod m, regardless which integers in a congruence class we use.* Before formally enunciating this important fact, we provide a motivating example.

Example 2.4

Compare the answers (mod 12) of the following arithmetic operations with the corresponding answers using instead the representatives of the integers taken from the set of possible remainders {0, 1, 2, ⋯, 11}.

(a) $56 + 81$
(b) $-23 \cdot 187 \cdot 38^4$

Solution: Part (a): $56 + 81 = 137 = 11 \cdot 12 + 5$, so $(56 + 81) \equiv 5 \pmod{12}$. On the other hand, since $56 = 4 \cdot 12 + 8$ and $81 = 6 \cdot 12 + 9$, we have (by Equation 2.1) $56 \equiv 8$ and $81 \equiv 9 \pmod{12}$. Performing the addition of the remainders gives $8 + 9 = 17 = 1 \cdot 12 + 5$, so $(8 + 9) \equiv 5 \pmod{12}$—the same answer (mod 12).

Part (b): Computing this large quantity and then applying the division algorithm leads us to

$-23 \cdot 187 \cdot 38^4 = -23 \cdot 187 \cdot 2085136 = -8968169936 = -747347495 \cdot 12 + 4$, so that $(-23 \cdot 187 \cdot 38^4) \equiv 4 \pmod{12}$.

On the other hand, since $-23 \equiv 1$, $187 \equiv 7$ and $38 \equiv 2 \pmod{12}$ when we compute the same operations with these much less unwieldy remainders, we obtain $1 \cdot 7 \cdot 2^4 = 7 \cdot 16$; if we replace, in turn, 16 with 4 (its remainder mod 12), we get $7 \cdot 4 = 28 = 4 \pmod{12}$—once again, the same answer that we obtained with the larger numbers (mod 12).

The results of the above example are not coincidental; the next result confirms this good news, establishing that modular arithmetic is easier than ordinary arithmetic.

Proposition 2.10: Validity of Congruent Substitutions in Modular Arithmetic

Suppose that m is a positive integer and that a, b, a', b' are integers with $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$. The following congruences are then valid:

(a) $a + a' \equiv b + b' \pmod{m}$
(b) $-a \equiv -a' \pmod{m}$
(c) $a \cdot b \equiv a' \cdot b' \pmod{m}$
(d) $a - a' \equiv b - b' \pmod{m}$
(e) $a^k \equiv (a')^k \pmod{m}$, for any positive integer k

We will prove this result momentarily, but let us first relish some of its ramifications. In the motivating example, we previewed some of these consequences when we replaced each integer with its remainder (mod 12). Remainders are often convenient replacements, but the proposition tells us that we are free to use any replacements that we find convenient. As another example, consider the problem of computing (mod 12) the power 47^{129}. If we computed this integer directly, it would have nearly 500 digits! But since $47 \equiv 11 \pmod{12}$ (its remainder), part (e) of the proposition tells us we could instead compute 11^{129} and will get the same answer (mod 12). This number still has about 300 digits, but if we notice that $11 \equiv -1 \pmod{12}$, the proposition would tell us that we could simply compute $(-1)^{129}$, which we immediately see (by hand) is -1 (as is any odd power of -1). So, we may conclude that $47^{129} \equiv -1 \equiv 11 \pmod{12}$. In Chapter 6, we will develop an efficient scheme of computing any powers in modular arithmetic. This algorithm, known as *fast exponentiation*, will be a vital component of certain public key cryptosystems that will be considered later.

Exercise for the Reader 2.7

Working in mod 10 arithmetic, compute each of the following quantities, using representatives in $\{0, 1, 2, \cdots, 9\}$ for your final answers.

(a) $88 + 1234 + 82645$
(b) $(11!)^2$

Explain why the answers to these (and any arithmetic computations mod 10) will simply be the one's (final) digit of the corresponding answer in (ordinary) integer arithmetic.

Proof of Proposition 2.10. We begin by recasting the assumptions $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$ as $a - a' = km$, and $b - b' = \ell m$, for some integers k, ℓ.

Part (a): Since $a + a' - (b + b') = (a - b) + (a' - b') = km + \ell m = (k + \ell)m$, it follows that $a + a' \equiv b + b' \pmod{m}$.

Part (b): Since $-a - (-a') = -a + a' = -(a - a') = (-k)m$, it follows that $-a \equiv -a' \pmod{m}$.

Part (c): Since $a \cdot b - a' \cdot b' = a \cdot b - a \cdot b' + a \cdot b' - a' \cdot b' = a(b - b') + (a - a')b = a(\ell m) + (km)b = [a\ell + kb]m$, it follows that $a \cdot b \equiv a' \cdot b' \pmod{m}$.

Part (d): This part follows from parts (a) and (b), since $a - b = a + (-b)$.

Part (e): This part follows from part (c), since exponentiation is a sequence of multiplications. □

Note: Students familiar with computer platforms might be familiar with the **mod function**, which depends on a parameter m (the modulus). This is a function from the set of integers $\mathbb{Z}$ to the set of possible remainders mod m: $\{0, 1, 2, \cdots, m-1\}$, for any inputted integer a, this mod function outputs its remainder when a is divided by m. It is usually denoted as `mod(a,m)`. Thus, the output of `mod(33, 12)` would be 9, since 9 is the remainder when 33 is divided by 12.

Exercise for the Reader 2.8

For a given modulus m, a positive integer, is the mod function that is described in the above note a one-to-one function? Is it an onto function? Explain your answers.

Having established some basic properties of congruences and modular arithmetic, we are now poised to introduce the abstract number systems that are known as modular integers. In contrast with the system $\mathbb{Z}$ of integers, which is an infinite set, all modular integer systems are finite sets.

Modular Integer Systems

Definition 2.6

If m is a positive integer, the set of **integers modulo m**, denoted by $\mathbb{Z}_m$, is the set of possible remainders when dividing by m:

$$\mathbb{Z}_m = \{0, 1, 2, \cdots, m-1\}$$

We define the arithmetic operations of addition, subtraction, multiplication, and exponentiation on $\mathbb{Z}_m$ by performing the corresponding arithmetic operations on the integers, converting, whenever convenient, in the final answer to an element of $\mathbb{Z}_m$.*

Proposition 2.10 assures us that the results of such operations will always be consistent. Our next example will look at addition and multiplication tables for $\mathbb{Z}_m$ for two small values of m. Although such tables are usually not constructed in practice, examination of the tables in these small cases will help to enlighten some general properties of modular integer systems.

Example 2.5

Create addition and multiplication tables for $\mathbb{Z}_5$ and $\mathbb{Z}_6$. Do you notice any similarities or differences in the corresponding tables?

Solution: In Table 2.1 and Table 2.2, we construct addition and multiplication tables for $\mathbb{Z}_5$, and Table 2.3 and Table 2.4 give the corresponding tables for $\mathbb{Z}_6$.

Exercise for the Reader 2.9

Perform the following operations in $\mathbb{Z}_{12}$: $11+8$, $5 \cdot 8$, 11^2. Is there an element $b \in \mathbb{Z}_{12}$ such that $5b = 1$ in $\mathbb{Z}_{12}$?

* With its addition and multiplication operations, the system $\mathbb{Z}_m$ of integers modulo m inherits almost all of the nice properties of arithmetic that the system $\mathbb{Z}$ of integers possess, such as commutativity of addition and multiplication: $a+b=b+c$ and $ab=ba$, associativity of addition and multiplication: $(a+b)+c=a+(b+c)$ and $(ab)c=a(bc)$, and the distributive law: $a(b+c)=ab+ac$. The modular integers are examples of what are called *commutative rings* in abstract algebra.

TABLE 2.1 Addition Table for $\mathbb{Z}_5$

+	**0**	**1**	**2**	**3**	**4**
0	0	1	2	3	**4**
1	1	2	3	4	**0**
2	2	3	4	0	**1**
3	3	4	0	1	**2**
4	**4**	**0**	**1**	**2**	**3**

TABLE 2.2 Multiplication Table for $\mathbb{Z}_5$

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

The addition tables for $\mathbb{Z}_5$ and $\mathbb{Z}_6$ are quite similar in structure. The row for 0 is simply a copy of the row of the second numbers (upper column) corresponding to the fact that 0 is the *additive identity*: $0 + a = a$. The remaining rows are simply cyclic shifts of the first row; each time we shift to the left by 1 (with wraparound) from the previous row, corresponding to the next higher number being added. This simple structure is common to addition tables for any $\mathbb{Z}_m$. There is a stark difference, though, in the multiplication tables. Notice that each nonzero row (or column) of the multiplication table for $\mathbb{Z}_5$ contains each of the elements of $\mathbb{Z}_5$ (as is the case for the addition tables), but this is not the case for the multiplication table for $\mathbb{Z}_6$. For example, in $\mathbb{Z}_6$, we can get 0

TABLE 2.3 Addition Table for $\mathbb{Z}_6$

+	**0**	**1**	**2**	**3**	**4**	**5**
0	0	1	2	3	4	**5**
1	1	2	3	4	5	**0**
2	2	3	4	5	0	**1**
3	3	4	5	0	1	**2**
4	4	5	0	1	2	**3**
5	**5**	**0**	**1**	**2**	**3**	**4**

TABLE 2.4 Multiplication Table for $\mathbb{Z}_6$

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

by multiplying the two nonzero numbers 2 and 3. This sort of problem generally occurs in any $\mathbb{Z}_m$ when m is composite but never occurs in $\mathbb{Z}_p$ for a prime modulus p (Why?). Furthermore, when p is prime, any nonzero row in the multiplication table of $\mathbb{Z}_p$ will always contain all of the elements of $\mathbb{Z}_p$. In order to elaborate on these concepts, we first need a definition.

Modular Inverses

Definition 2.7

For any $a \in \mathbb{Z}_m$, we say that a is **invertible** (or has an inverse) if there exists another element $a^{-1} \in \mathbb{Z}_m$ such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$. The element a^{-1}, if it exists, is called the **(multiplicative) inverse** of a.

If we have the multiplication table available, it can be determined whether an element $a \in \mathbb{Z}_m$ has an inverse simply by checking if the row of this element in the table contains a 1. For example, from Table 2.2 (multiplication table for $\mathbb{Z}_5$), we see that in $\mathbb{Z}_5$ we have $1^{-1} = 1$, $2^{-1} = 3$, $3^{-1} = 2$, and $4^{-1} = 4$. (In any $\mathbb{Z}_m$, the element 1 will always be its own inverse, and the element 0 will never have an inverse—why?) From Table 2.4, we see that in $\mathbb{Z}_6$, $1^{-1} = 1$, $5^{-1} = 5$, and no other elements have inverses. We point out that since multiplication in $\mathbb{Z}_m$ is commutative (that is, $ab = ba$ for all $a, b \in \mathbb{Z}_m$), only one of the two conditions for inverses ($a \cdot a^{-1} = 1$, or $a^{-1} \cdot a = 1$) needs to be checked. Also, there can be only one inverse of any element $a \in \mathbb{Z}_m$. [*Proof*: Suppose that both b and $a^{-1} \in \mathbb{Z}_m$ were inverses of $a \in \mathbb{Z}_m$. Then $b = b \cdot 1 = b \cdot (a \cdot a^{-1}) = (b \cdot a) \cdot a^{-1} = 1 \cdot a^{-1} = a^{-1}$. □] Inverses are important for an assortment of reasons, some of which we will discuss shortly. The following result provides a simple criterion to determine whether an element $a \in \mathbb{Z}_m$ has an inverse.

Proposition 2.11: Inverses in $\mathbb{Z}_m$

An element $a \in \mathbb{Z}_m$ is invertible precisely when $\gcd(a, m) = 1$, that is, when it is relatively prime to m. Moreover, the inverse a^{-1} can be obtained from the integer equation $1 = ax + my$ (recall Theorem 2.6), as $a^{-1} \equiv x \pmod{m}$. In particular, all nonzero elements of $\mathbb{Z}_m$ are invertible precisely when $m = p$ is prime.

Proof: If $\gcd(a, m) = 1$, then by Theorem 2.6, there exist integers x and y such that $1 = ax + my$. If we rewrite this as $1 - ax = my$, we see that $m \mid (1 - ax)$, and so $ax \equiv 1 \pmod{m}$. This implies (resetting x to be its mod m representative between 1 and $m - 1$) that $x = a^{-1}$ in $\mathbb{Z}_m$. Conversely, if a has an inverse a^{-1} in $\mathbb{Z}_m$, then $a \cdot a^{-1} \equiv 1 \pmod{m}$, or $m \mid (1 - a \cdot a^{-1})$. It follows (from the definition of divisibility) that $1 - a \cdot a^{-1} = mk$, or $mk + a \cdot a^{-1} = 1$, for some $k \in \mathbb{Z}$. From this latter equation, it readily follows that $\gcd(a, m) = 1$, because any (prime) factor

of both a and m would also [by Theorem 2.1(b)] necessarily have to be a (prime) factor of 1 (which has no prime factors). The last statement easily follows from the criterion since any prime number p is relative prime to all positive integers that are less than p, that is, to all nonzero elements in $\mathbb{Z}_p$.□

One important task relating to modular arithmetic concerns *solving congruences*. For example, a simple congruence such as $x + 5 \equiv 2 \pmod{12}$ can easily be solved by subtracting 5 from both sides (just like in basic algebra): $x \equiv 2 - 5 \equiv -3 \equiv 9 \pmod{12}$. From Proposition 2.10 we can always add or multiply both sides of a congruence by any number (or an equivalent representative of that number, mod m). Dividing both sides of a congruence is more difficult; in general, to divide both sides of a congruence by a number a, a needs to be invertible in $\mathbb{Z}_m$; that is (from Proposition 2.11), we must have $\gcd(a, m) = 1$. Furthermore, once it is ascertained that we can divide both sides by a, we will actually be multiplying both sides by a^{-1} rather than dividing (with real numbers) by a. This is where modular arithmetic and ordinary arithmetic are very different (unlike with multiplication and addition). This process is illustrated in the following example.

Example 2.6

Solve each of the following congruences for x:

(a) $3x + 2 \equiv 1 \pmod{5}$.

(b) $5x - 4 \equiv 4 \pmod{6}$.

Solution: Part (a): From Table 2.2 (or by simple trial and error multiplying 3 by each of the four nonzero elements of $\mathbb{Z}_5$ until we get 1), we see that $3^{-1} = 2$ in $\mathbb{Z}_5$. Thus, when we need to divide the congruence by 3, we will be multiplying both sides by 2: $3x + 2 \equiv 1 \Rightarrow 3x \equiv 1 - 2 \equiv -1 \equiv 4 \Rightarrow x (= 2 \cdot 3x) = 2 \cdot 4 \equiv 8 \equiv 3 \pmod{5}$. This answer is easily checked in the original congruence: $3 \cdot 3 + 2 \equiv 11 \equiv 1 \pmod{5}$.

Part (b): In $\mathbb{Z}_6$, 5 is invertible since it is relatively prime to 6, so we will be able to perform the necessary division by 5 to solve this congruence. From Table 2.4 (or by simple trial and error), we find that $5^{-1} = 5$, so when we need to divide this congruence by 5, we will multiply both sides by (its inverse) 5: $5x - 4 \equiv 4 \Rightarrow 5x \equiv 4 + 4 \equiv 8 \equiv 2 \Rightarrow x = 5 \cdot 2 \equiv 10 \equiv 4 \pmod{6}$. Once again, this answer is easily checked.

Extended Euclidean Algorithm

We will discuss more general congruences shortly, but first we provide an algorithm for computing the inverse of an invertible integer a mod m. From Proposition 2.11, we know that a must satisfy $\gcd(a,m) = 1$, which means that there exist integers x and y, such that $1 = ax + my$. As shown in the proof of Proposition 2.11, a^{-1} can be taken to be the

integer x (mod m) in this equation. We explained earlier how these integers x and y can be computed by working backwards through the intermediate steps of the Euclidean algorithm. The algorithm below is an extended version of the Euclidean algorithm that works in a more organized fashion to output the numbers x and y, along with the greatest common divisor d. The algorithm operates on ordered lists (vectors) with three components. The components of such an ordered list V will be denoted (in order) as $V(1)$, $V(2)$, $V(3)$. Thus, for example, if $V = [2, 4, 6]$, then $V(1) = 2$, $V(2) = 4$, $V(3) = 6$. The algorithm will also be multiplying ordered lists by numbers, and this is done by multiplying each of the components by the number, for example: 5 [2, 4, 6] = [10, 20, 30].

Algorithm 2.2: The Extended Euclidean Algorithm

Input: A pair of positive integers a and b, with $a \geq b$.
Output: Three integers, $d = \gcd(a,b)$, x, and y, that satisfy the equation $d = ax + by$.

Step 1. Set $U = [a, 1, 0]$, $V = [b, 0, 1]$ (Initialize recordkeeping vectors)
Step 2. WHILE $V(1) > 0$

(Tasks below will be repeated while first component of V is positive)

$W = U - \text{floor}\,(U(1)/V(1))V$
Update: $U = V$
Update: $V = W$
END (WHILE)*

Step 3. Output: $d = U(1)$, $x = U(2)$, $y = U(3)$

The ordinary Euclidean algorithm (Algorithm 2.1) had the same inputs but outputted only d. It is not so obvious that this algorithm actually does what is claimed; we will explain it and prove that it does indeed work after the following illustrative example.

Example 2.7

(a) Use Algorithm 2.2 to compute $d = \gcd(148, 75)$ and integers x and y such that $d = 148x + 75y$.
(b) If it exists, compute the $75^{-1} \bmod 148$.

Solution: Part (a):

Step 1. We initialize $U = [148, 1, 0]$, $V = [75, 0, 1]$
Step 2. Since $V(1) = 75 > 0$

* This notation means that the operations after the WHILE instruction and before its END are to be executed repeatedly until the condition indicated after the WHILE—in this case, V(1) > 0—fails to be valid.

we set: $W = U - \text{floor}(U(1) / V(1))V$
$= [148, 1, 0] - \lfloor 148 / 75 \rfloor [75, 0, 1]$
$= [148, 1, 0] - 1 \cdot [75, 0, 1] = [73, 1, -1]$.

We update $U = V = [75, 0, 1]$, and $V = W = [73, 1, -1]$.

Since $V(1) = 73 > 0$, we repeat this with the updates:

$W = U - \text{floor}(U(1) / V(1))V = [75, 0, 1] - \lfloor 75 / 73 \rfloor [73, 1, -1]$
$= [75, 0, 1] - 1 \cdot [73, 1, -1] = [2, -1, 2]$.
$U = V = [73, 1, -1]$, and $V = W = [2, -1, 2]$.

Since $V(1) = 2 > 0$, we again repeat these updates:

$W = U - \text{floor}(U(1) / V(1))V = [73, 1, -1] - \lfloor 73 / 2 \rfloor [2, -1, 2]$
$= [73, 1, -1] - 36 \cdot [2, -1, 2] = [1, 37, -73]$.
$U = V = [2, -1, 1]$, and $V = W = [1, 37, -73]$.

Since $V(1) = 1 > 0$, we need one final updating:

$W = U - \text{floor}(U(1) / V(1))V = [2, -1, 1] - \lfloor 2 / 1 \rfloor [1, 37, -73]$
$= [2, -1, 1] - 2 \cdot [1, 37, -73] = [0, -75, 147]$.
$U = V = [1, 37, -73]$, and $V = W = [0, -75, 147]$.

Step 3. Output: $d = U(1) = 1$, $x = U(2) = 37$, $y = U(3) = -73$

The resulting relationship is easily checked: $1 = 37 \cdot 148 - 73 \cdot 75$.

Part (b): The result of part (a) tells us that $\gcd(148, 75) = 1$, so from Proposition 2.11 and the equation $1 = 37 \cdot 148 - 73 \cdot 75$, and since $-73 \equiv 75 \pmod{148}$, we get that $75^{-1} = 75$ in $\mathbb{Z}_{148}$.

Exercise for the Reader 2.10

(a) Use Algorithm 2.2 to compute $d = \gcd(1155, 862)$, and integers x and y such that $d = 1155x + 862y$.
(b) If it exists, compute 862^{-1} in $\mathbb{Z}_{1155}$.

Algorithm 2.2 is really just the Euclidean algorithm in disguise, with some additional recordkeeping (hence the three-element vectors). The proof below will use the notation of the Euclidean algorithm (Algorithm 1.1), so it might be helpful for the reader to review this algorithm before reading this proof.

Proof That the Outputs d, x, and y of Algorithm 1.2 Satisfy $d = \gcd(a, b)$ *and* $d = ax + by$. We first point out that throughout the algorithm, any of the length-3 vectors $Z = U$, V, or W always corresponds to a valid equation:

$$Z(1) = a \cdot Z(2) + b \cdot Z(3), \text{ where } Z = [Z(1), Z(2), Z(3)]$$

To see this, note first that it is clearly true for the initial vectors $U = [a, 1, 0]$ and $V = [b, 0, 1]$. (For example, for $Z = U$, the equation becomes $a = a \cdot 1 + b \cdot 0$.) All other vectors created or updated in the algorithm are either taken to be a previously constructed vector or (in the case of a W vector) taken as a vector of the form $U + \alpha V$, where α is an integer. It suffices to show if the vectors U and V both correspond to a valid equation with the above scheme, then so will the vector $U + \alpha V$. Indeed, from the corresponding equations for U and V: $U(1) = a \cdot U(2) + b \cdot U(3)$, $V(1) = a \cdot V(2) + b \cdot V(3)$, if we add α times the second to the first, we get $U(1) + \alpha V(1) = a \cdot [U(2) + \alpha V(2)] + b \cdot [U(3) + \alpha V(3)]$, which is the (valid) equation corresponding to the vector $U + \alpha V$. With this being done, it now suffices to show that the algorithm eventually terminates, and when it does, we have (the final value of) $U(1) = \gcd(a,b)$. As in the proof of Theorem 2.6, if we set $r_0 = b$ and $r_{-1} = a$, the Euclidean algorithm can be expressed as successive applications of the division algorithm, where each one defines the next element of the remainder sequence: $r_{i-1} = q_i r_i + r_{i+1}$ $(i = 0, 1, 2, \cdots n)$. Recall that the sequence of remainders is strictly decreasing and the final nonzero remainder (r_n) is $\gcd(a,b)$. If we look at the first component of the recursive formula of Algorithm 2.2, that is, $W(1) = U(1) - \text{floor}(U(1) / V(1)) \cdot V(1)$, we see that $W(1)$ is simply the remainder when the division algorithm is applied to the integer division of $U(1)$ by $V(1)$. Since $U(1)$ starts off at a, $V(1)$ starts off at b, and at each iteration, $U(1)$ is updated to $V(1)$ and $V(1)$ to (the new remainder) $W(1)$, we see that at the ith iteration of Algorithm 2.2, $W(1)$ is exactly the value of the new remainder in the ith iteration of the Euclidean algorithm. It follows that the values of $U(1)$ are strictly decreasing integers (so the algorithm terminates) whose last nonzero value is $\gcd(a,b)$, as claimed. □

Solving Linear Congruences

We have completely described an efficient method for solving any linear congruence:

$$ax + b \equiv c \pmod{m} \tag{2.2}$$

whenever $\gcd(a,m) = 1$, in which case there is always a unique solution. Since the first step of subtracting b from both sides (in modular arithmetic) is always easy, the heart of solving such a congruence is the (modular) division step, so we really can focus attention on the simpler equation (obtained by setting $b = 0$ in Equation 2.2):

$$ax \equiv c \pmod{m} \tag{2.3}$$

We complete our analysis of Equation 2.3 by moving to the remaining situation where $\gcd(a,m) = d > 1$. In order for a solution to exist, we must have $d \mid c$. [*Proof*: For any solution x, we would have $m \mid ax - c$, so since $d \mid m$, we get also that $d \mid ax - c$, and since $d \mid a$, it follows that $d \mid ax - (ax - c) = c$. □] In case $d \mid c$, it turns out that the congruence (Equation 2.3) will always have d distinct solutions (mod m).

***Algorithm 2.3* (*Procedure for Solving* $ax \equiv c \pmod{m}$ *in the Case* $d = \gcd(a,m) > 1$ *and* $d \mid c$)**

Recall that if $d \nmid c$, there are no solutions.

Step 1. Solve the modified congruence $(a/d)y \equiv (c/d) \pmod{m/d}$ as explained earlier in this section. This is possible, and there will be a unique solution y_0, since $\gcd(a/d, m/d) = 1$.

Step 2. The d solutions of the original congruence are $y_0, y_0 + m/d, y_0 + 2m/d, \cdots, y_0 + (d-1)m/d \pmod{m}$.

Before we explain why this algorithm works, we give an example to illustrate its use.

Example 2.8

Find all solutions of the following congruences:

(a) $2x \equiv 7 \pmod{10}$
(b) $6x \equiv 12 \pmod{21}$

Solution: Part (a): Since $d = \gcd(2, 10) = 2$ does not divide 7, there is no solution.

Part (b): Since $d = \gcd(6, 21) = 3$ does divide 12, there will be 3 (= d) distinct solutions (mod 21). We use Algorithm 2.3 to find them. The modified congruence from Step 1 is $(6/3)y \equiv (12/3) \pmod{21/3}$ or $2y \equiv 4 \pmod{7}$, which has the (unique) solution $y_0 = 2 \pmod{7}$.* Step 2 now gives us the set of two solutions of the original congruence: $\{2, 2 + 21/3, 2 + 2 \cdot 21/3\} = \{2, 9, 16\}$. These are easily checked to satisfy the original congruence.

Exercise for the Reader 2.11

Find all solutions of the following congruences:

(a) $123x \equiv 12 \pmod{456}$
(b) $15x + 4 \equiv 20 \pmod{25}$

We now explain why Algorithm 2.3 does its job.

Proof That Algorithm 2.3 Correctly Finds All Solutions of the Indicated Congruence. Since the d solutions indicated by the algorithm are distinct integers mod m, there are two things we need to do: (i) we must show that the d solutions indicated by the algorithm actually solve the original congruence, and (ii) there are no other solutions (mod m).

* Up to now, our method for solving the congruence $2y \equiv 4 \pmod{7}$ would be to first find that the inverse of 2 (mod 7) is 4 [since $2 \cdot 4 = 8 \equiv 1 \pmod{7}$], and then multiply both sides of the congruence to obtain $y \equiv 4 \cdot 4 \equiv 16 \equiv 2 \pmod{7}$. Whenever a congruence can be solved by ordinary integer arithmetic, the resulting solution will also be a valid one for the congruence. This is because if two real numbers are equal, then they will be congruent modulo any m. However, this method should not be applied directly to any congruence $ax \equiv b \pmod{m}$, where $d > 1$, and $d = \gcd(a,b) \mid c$, because it will give only one of the d solutions: For example, $5x \equiv 15 \pmod{25}$ has four solutions, but $x \equiv 3 \pmod{25}$ has only one!

Part (i): The fact that $(a/d)y_0 \equiv (c/d) \pmod{m/d}$ means that $(m/d) \mid [(a/d)y_0 - (c/d)]$. This divisibility relation implies that $m \mid [ay_0 - c]$, which is equivalent to the congruence $ay_0 \equiv c \pmod{m}$. Now, since $d \mid a$ for any integer i, we have $a(y_0 + im/d) \equiv ay_0 + (a/d)im \equiv c + 0 \equiv c \pmod{m}$, so $y_0 + im/d$ solves the indicated congruence. In particular, so do the d indicated solutions.

Part (ii): We first observe that there can be no other solutions of the original congruence of the form $y_0 + im/d$ $(i \in \mathbb{Z}) \pmod{m}$ other than the d solutions indicated by the algorithm. This is because for any integer i, if r is the remainder when i is divided by d, $y_0 + im/d \equiv y_0 + rm/d \pmod{m}$. It remains to show that there can be no solutions other than these of the original congruence. Indeed, suppose that there was a solution z_0, $az_0 \equiv c \pmod{m}$, which is not of this form. Therefore, there is a unique integer i_0, such that $y_0 + i_0\, m/d < z_0 < y_0 + (i_0 + 1)m/d$. If we rewrite this double inequality as $i_0\, m/d < z_0 - y_0 < (i_0 + 1)m/d$, it is clear that $z_0 \not\equiv y_0 \pmod{m/d}$. However, the argument in part (a) shows that since $az_0 \equiv c \pmod{m}$, we have $(a/d)z_0 \equiv c/d \pmod{m/d}$, and this contradicts the fact that y_0 was the unique solution of this latter congruence. □

We have thus completely described how to solve a single linear congruence of form Equation 2.3 (or Equation 2.2). We summarize the procedure:

Summary of Procedure for Solving the Single Linear Congruence (Equation 2.2)

$$ax + b \equiv c \pmod{m}$$

Step 1. Subtract b from both sides to obtain the equation $ax \equiv c - b \pmod{m}$.

Step 2. First compute $d = \gcd(a,m)$.

Case 1. $d = 1$. *Unique Solution.* Use the extended Euclidean Algorithm 2.2 to compute integers e and f such that $1 = ae + mf$, to obtain $a^{-1} \equiv e \pmod{m}$. The unique solution of Equation 2.2 is given by $x \equiv a^{-1} \cdot (c - b) \pmod{m}$.

Case 2. $d > 1$ and $d \nmid c$. *No Solution.* There are no solutions of the congruence Equation 2.2 $\pmod{m}$.

Case 3. $d > 1$ and $d \mid c$. *Multiple Solutions.* Use the extended Euclidean Algorithm 2.2 to compute integers e' and f' such that $1 = (a/d)e' + (m/d)f'$, to obtain $(a/d)^{-1} \equiv e' \pmod{m/d}$. Use this to find the unique solution of the modified congruence $(a/d)y \equiv ([c - b]/d)$: $y_0 \equiv (a/d)^{-1} \cdot ([c - b]/d) \pmod{m/d}$. The d solutions of the original congruence are y_0, $y_0 + m/d$, $y_0 + 2m/d, \cdots, y_0 + (d - 1)m/d \pmod{m}$.

Exercise for the Reader 2.12

Find all solutions of the following congruences:

(a) $6x + 2 \equiv 5 \pmod{9}$
(b) $6x + 2 \equiv 3 \pmod{9}$
(c) $5x + 2 \equiv 3 \pmod{9}$

The Chinese Remainder Theorem

In many applications, including some in cryptography that we will see later on, it is necessary to simultaneously solve a system of linear congruences of different moduli*:

$$\begin{cases} a_1 x \equiv c_1 \pmod{m_1} \\ a_2 x \equiv c_2 \pmod{m_2} \\ \quad \vdots \\ a_k x \equiv c_k \pmod{m_k} \end{cases} \tag{2.4}$$

More precisely, we would like to know when we find an integer x that solves each of the congruences in Equation 2.4. Furthermore, in cases where such a simultaneous integer solution exists, we would like to classify all of the solutions.

Puzzles that can be modeled by simultaneous congruences such as Equation 2.4 have appeared in various ancient mathematical documents, including those from the Greeks (dating back to the first century a.d.), the Chinese (dating to back to the third century a.d.), and the Hindus (dating back to the seventh century a.d.). The following is an example of such an ancient Hindu puzzle.

Example 2.9: A Hindu Puzzle from the Seventh Century a.d.

Determine a system of simultaneous congruences that models the following puzzle:

While a woman is on her way to the market, a horse steps on her basket and crushes all her eggs. The rider agrees to pay for the damage and asks how many eggs she had. She does not recall the exact number, but she knows that when she had taken them out two at a time, there was one egg left. The same thing happened when she removed them three, four, five, and six at a time, but when she took them out seven at a time, they all came out. What was the smallest number of eggs she could have had?

Solution: Letting x denote the (unknown) number of eggs that were in the woman's basket, the problem tells us that x must solve each of the following congruences:

$$\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 1 \pmod 3 \\ x \equiv 1 \pmod 4 \\ x \equiv 1 \pmod 5 \\ x \equiv 1 \pmod 6 \\ x \equiv 0 \pmod 7 \end{cases} \tag{2.5}$$

* Since the reduction from a more general linear congruence $ax + b \equiv c \pmod m$ is simple, it suffices to assume that our linear congruences are in the form $ax \equiv c \pmod m$.

The problem seeks the smallest positive solution of Equation 2.5. We point out one very simple observation about congruences that will sometimes help to simplify such systems.

Proposition 2.12

Suppose that m_1, m_2 are positive integers with $m_1 \mid m_2$. Any solution of a linear congruence $ax \equiv c \pmod{m_2}$ will also be a solution of the same congruence $\pmod{m_1}$.

Proof: By definition, x solves the first congruence means that $m_2 \mid (ax - c)$. Since we are assuming that $m_1 \mid m_2$, it follows by transitivity of divisibility [Theorem 2.1(a)] that $m_1 \mid (ax - c)$, which means that $ax \equiv c \pmod{m_1}$. □

If we apply this proposition to the Equation 2.5, since both 2 and 3 divide 6, the congruences $x \equiv 1 \pmod 2$, $x \equiv 1 \pmod 3$ are redundant consequences of the congruence $x \equiv 1 \pmod 6$. Thus, they can be safely removed from the system to produce the following simpler, but equivalent system*:

$$\begin{cases} x \equiv 1 \pmod 4 \\ x \equiv 1 \pmod 5 \\ x \equiv 1 \pmod 6 \\ x \equiv 0 \pmod 7 \end{cases} \tag{2.6}$$

We will return to Equation 2.6 and the Hindu puzzle momentarily, but we first consider the problem of solving Equation 2.4. First of all, it is clear that in order for a simultaneous solution to exist, each individual congruence must have a solution, and from our development for single linear congruences, this means that we must have $d_i \mid c_i \quad (1 \le i \le k)$, where $d_i = \gcd(a_i, m_i)$. With these conditions being satisfied, in light of Algorithm 2.3, Equation 2.4 can be reduced to the simpler system:

$$\begin{cases} x \equiv b_1 \pmod{n_1} \\ x \equiv b_2 \pmod{n_2} \\ \quad \vdots \\ x \equiv b_k \pmod{n_k} \end{cases} \tag{2.7}$$

where $n_i = m_i/d_i$ and $b_i = (a_i/d_i)^{-1}(c_i/d_i) \pmod{n_i}$. The following theorem shows that Equation 2.7 always has a solution in cases where the moduli are *pairwise relatively prime*—that is, $\gcd(n_i, n_j) = 1$ whenever $i \ne j \quad (1 \le i, j \le k)$—and it includes a uniqueness statement. This theorem has been found to date back to a Chinese mathematics book that was published in 1247 a.d. by the Chinese mathematician Qin Jiushao

* An equivalent system of equations is one that has the same solution set as the original system.

(1202–1261),* and has come to be known as the *Chinese remainder theorem*. We will give a constructive (algorithmic) proof of the existence of the solution, and thus provide a practical method of solving the Equation 2.7 and hence also Equation 2.4.

Theorem 2.13: The Chinese Remainder Theorem

Suppose that $n_1, n_2, \cdots, n_k > 1$ are pairwise relatively prime integers. Then for any integers $b_1, b_2, \cdots, b_k$, the system of congruences:

$$\begin{cases} x \equiv b_1 \pmod{n_1} \\ x \equiv b_2 \pmod{n_2} \\ \vdots \\ x \equiv b_k \pmod{n_k} \end{cases} \tag{2.7}$$

has a simultaneous integer solution x that is unique modulo $N = n_1 n_2 \cdots n_k$.

As the following proof contains an algorithm, we will defer giving an example until after proving the theorem.

Proof: Part (a): *Existence*: (*Constructive Proof*) For each index i $(1 \le i \le k)$, since $\gcd(N / n_i, n_i) = 1$, there is a (unique) solution e_i of the congruence $e_i(N / n_i) \equiv 1 \pmod{n_i}$. We claim that

$$x = \sum_{i=1}^{k} b_i e_i (N / n_i) \tag{2.8}$$

is a simultaneous solution of Equation 2.7. Indeed, for each index j, we have $(\text{mod } n_j)$ $N / n_i \equiv 0$, unless $j = i$, and this forces all terms other than the jth term in the sum of Equation 2.8 to be $0 \pmod{n_j}$. Thus $x \equiv b_j e_j (N / n_j) \equiv b_j \cdot 1 \equiv b_j \pmod{n_j}$, as desired.

Part (b): *Uniqueness*: Suppose that x' is another simultaneous solution of Equation 2.7. It follows that for each index i, $x \equiv b_i \equiv x' \pmod{n_i}$, so that $n_i \mid (x - x')$. Since the n_i's are pairwise relatively prime, it follows (from the fundamental theorem of arithmetic) that their product N also divides $x - x'$; that is, $x \equiv x' \pmod{N}$. □

---

* Qin Jiushao (also transliterated as Ch'in Chiu-Shao) was a tour-de-force among ancient mathematicians; his principal scientific contributions were published in his 1247 book *Shushu Jiuzhang* (*Mathematical Treatise in Nine Sections*). The first chapter of his book contained the development and proof of (what is now called) the Chinese remainder theorem. The book also included analyses of higher-order equations that modeled certain interesting applied problems such as the following (from Chapter 2 of his book): Determine the height of rainfall on level ground, given that it reached a height h in a cylindrical vessel with circular top and bottom having respective radii $a > b$. Aside from his mathematics, Qin had quite an interesting military and government career. In his youth, he fought the armies of Genghis Khan. He was notorious for his corruption and manipulations of his government posts, from which he amassed a tremendous amount of wealth. His book was actually written during a hiatus from work when he returned to his hometown to mourn the death of his mother.

Example 2.10

Solve the following system of congruences:

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 6 \pmod{14} \end{cases}$$

Solution: Since the moduli are pairwise relatively prime, Equation 2.8 (in the proof of the Chinese remainder theorem) provides us with a scheme for obtaining a simultaneous solution. We first set $N = 3 \cdot 5 \cdot 14 = 210$. With $b_1, b_2, b_3 = 2,3,6$ and $n_1, n_2, n_3 = 3,5,14$, in order to use Equation 2.8, we must first determine e_1, e_2, e_3, by their defining equations: $e_i(N / n_i) \equiv 1 \pmod{n_i}$.

For e_1: $e_1 \cdot 70 \equiv 1 \pmod 3 \Leftrightarrow e_1 \cdot 1 \equiv 1 \pmod 3 \Leftrightarrow e_1 \equiv 1 \pmod 3$.

For e_2: $e_2 \cdot 42 \equiv 1 \pmod 5 \Leftrightarrow e_2 \cdot 2 \equiv 1 \pmod 5 \Leftrightarrow e_2 \equiv 3 \pmod 5$ [since $2^{-1} = 3 \pmod 5$].

For e_3: $e_3 \cdot 15 \equiv 1 \pmod{14} \Leftrightarrow e_3 \cdot 1 \equiv 1 \pmod{14} \Leftrightarrow e_3 \equiv 1 \pmod{14}$.

Now we have all that we need to apply Equation 2.8 to get a desired solution:

$$x = \sum_{i=1}^{3} b_i e_i (N/n_i) = 2 \cdot 1 \cdot (70) + 3 \cdot 3 \cdot (42) + 6 \cdot 1 \cdot (15)$$

$$= 608 \equiv 188 \pmod{210}$$

Thus 188 is the smallest positive integer solution of the original system.

Exercise for the Reader 2.13

Determine the general solution of the following system of congruences:

$$\begin{cases} x \equiv 0 \pmod 2 \\ x \equiv 2 \pmod 5 \\ 3x \equiv 4 \pmod 7 \end{cases}$$

Although we cannot apply the Chinese remainder theorem to the Equation 2.6 of the Hindu problem, part (b) of the following proposition, which generalizes Proposition 2.12, will allow us to convert Equation 2.6 into a form to which the theorem is applicable.

Proposition 2.14

(a) Any set of divisibility relations of the form $m_1 \mid b$, $m_2 \mid b, \cdots, m_k \mid b$ is equivalent to the single divisibility relation $\text{lcm}(m_1, m_2, \cdots, m_k) \mid b$.

(b) Any system of congruences of the form

$$\begin{cases} ax \equiv c \pmod{m_1} \\ ax \equiv c \pmod{m_2} \\ \quad\vdots \\ ax \equiv c \pmod{m_k} \end{cases}$$

(that is, the same congruence under different moduli) is equivalent to the single congruence:

$$ax \equiv c \pmod{\operatorname{lcm}(m_1, m_2, \cdots, m_k)}$$

Note: Unlike in the Chinese remainder theorem, the moduli need not be pairwise relatively prime in this result.

The proof is similar to that of Proposition 2.12 and is left to the following exercise for the reader.

Exercises for the Reader

Exercise 2.14

Prove Proposition 2.14.

Exercise 2.15

What is the answer to the ancient Hindu problem of Example 2.9?

Chapter 2 Exercises

1. Determine whether each of the statements below is true or false.
   (a) $9 \mid 128$
   (b) $3 \mid 111$
   (c) $13 \mid 5271$
   (d) $-1 \mid a$ for any $a \in \mathbb{Z}$
   (e) $a \mid ab$ for any $a, b \in \mathbb{Z}$
   (f) $0 \mid 12$

2. Determine whether each of the statements below is true or false.
   (a) $7 \mid -49$
   (b) $2 \mid 111$
   (c) $17 \mid 5271$
   (d) $1 \mid a$ for any $a \in \mathbb{Z}$
   (e) $a \mid a$ for any $a \in \mathbb{Z}$
   (f) $12 \mid 0$

3. If a and b are integers such that $a \mid b$, and $b \mid a$, show that $a = \pm b$.

4. If a, b, and c are positive integers such that $a \mid b$, show that $ac \mid bc$.

5. Which of the following integers is prime?
   (a) 67
   (b) 91
   (c) 893
   (d) 8671
   (e) 6581
   (f) 148,877

6. Which of the following integers is prime?
   (a) 83
   (b) 97
   (c) 893
   (d) 1229
   (e) 46,189
   (f) 12,499

7. Find the prime factorization of each of the following positive integers, as guaranteed by the fundamental theorem of arithmetic:
   (a) 24
   (b) 88
   (c) 675
   (d) 6400
   (e) 74,529
   (f) 183,495,637

8. Find the prime factorization of each of the following positive integers, as guaranteed by the fundamental theorem of arithmetic:
   (a) 52
   (b) 96
   (c) 512
   (d) 4725
   (e) 130,321
   (f) 7,817,095

9. Find the quotient and remainder when the division algorithm is applied to each of the following integer divisions:
   (a) $67 \div 2$
   (b) $108 \div 5$
   (c) $-77 \div 2$
   (d) $882 \div 13$
   (e) $1228 \div 25$
   (f) $-1582 \div 36$

10. Find the quotient and remainder when the division algorithm is applied to each of the following integer divisions.
    (a) $67 \div 3$
    (b) $180 \div 5$
    (c) $-90 \div 13$
    (d) $-564 \div 14$
    (e) $1268 \div 42$
    (f) $-8888 \div 25$

11. Using prime factorizations, compute the indicated greatest common divisors or least common multiples.
    (a) gcd(12, 36)
    (b) lcm(20, 25)
    (c) gcd(100, 56)
    (d) gcd(560, 1400)
    (e) lcm(120, 50)
    (f) gcd(121275, 5788125)

12. Using prime factorizations, compute the indicated greatest common divisors or least common multiples.
    (a) gcd(15, 40)
    (b) lcm(15, 40)
    (c) gcd(136, 86)
    (d) gcd(1925, 1568)
    (e) lcm(150, 350)
    (f) gcd(256500, 109395)

13. Use the Euclidean algorithm to compute each of the quantities in Chapter Exercise 11. For those that are lcm's, use the formula of Exercise for the Reader 2.2(c).

14. Use the Euclidean algorithm to compute each of the quantities in Chapter Exercise 12. For those that are lcm's, use the formula of Exercise for the Reader 2.2(c).

15. For each pair of integers a, b that are given, use the Euclidean algorithm (as explained in the proof of Theorem 2.6) to determine integers x and y, such that $\gcd(a, b) = ax + by$.
    (a) 12, 36
    (b) 100, 56
    (c) 560, 1400
    (d) 121275, 5788125

16. For each pair of integers a, b that are given, use the Euclidean algorithm (as explained in the proof of Theorem 2.6) to determine integers x and y, such that $\gcd(a, b) = ax + by$.
    (a) 15, 40
    (b) 136, 86
    (c) 1925, 1568
    (d) 256500, 109395

17. Determine whether each of the statements below is true or false.
    (a) $43 \equiv 1 \pmod 2$
    (b) $-43 \equiv 3 \pmod 4$
    (c) $488 \equiv 10 \pmod{12}$
    (d) $2205 \equiv 45 \pmod{360}$
    (e) $-443 \equiv 18 \pmod{22}$
    (f) $7^7 \equiv 5^8 \pmod{371}$

18. Determine whether each of the statements below is true or false.
    (a) $43 \equiv 2 \pmod 3$
    (b) $-43 \equiv 3 \pmod 6$
    (c) $2207 \equiv 11 \pmod{12}$
    (d) $11340 \equiv 90 \pmod{360}$
    (e) $-2444 \equiv -446 \pmod{666}$
    (f) $3^6 \equiv 5^2 \pmod{44}$

19. Perform the following operations in $\mathbb{Z}_{24}$:
    (a) $18 + 20$
    (b) $5 - 21$
    (c) $8 \cdot 8$
    (d) $2^8 - 3^8$
    (e) 21^{223}

    Suggestion: For part (e), compute some smaller powers first (mod 24) to build up to the final answer using laws of exponents.

20. Perform the following operations in $\mathbb{Z}_{53}$:
    (a) $39 + 47$
    (b) $25 - 36$
    (c) $18 \cdot 35$
    (d) $12^5 - 19^4$
    (e) 33^{100}

    Suggestion: For part (e), compute some smaller powers first (mod 53) to build up to the final answer using laws of exponents.

21. Create addition and multiplication tables for (a) $\mathbb{Z}_2$ and (b) $\mathbb{Z}_4$. (See Example 2.8.) By looking at the multiplication tables, determine all invertible elements.

22. Create addition and multiplication tables for (a) $\mathbb{Z}_3$ and (b) $\mathbb{Z}_9$. (See Example 2.8.) By looking at the multiplication tables, determine all invertible elements.

23. Find all invertible elements of $\mathbb{Z}_8$ and for each one find the inverse.

24. Find all invertible elements of $\mathbb{Z}_{10}$ and for each one find the inverse.

25. Find all invertible elements of $\mathbb{Z}_7$ and for each one find the inverse.

26. Find all invertible elements of $\mathbb{Z}_{11}$ and for each one find the inverse.

27. Solve each of the following congruences working in (mod 8):
    (a) $3x \equiv 5$
    (b) $7x + 2 \equiv 3$
    (c) $5x - 2 \equiv 2$

28. Solve each of the following congruences working in (mod 10):
    (a) $3x \equiv 5$
    (b) $7x + 2 \equiv 3$
    (c) $9x - 8 \equiv 7$

29. For each integer below, use the extended Euclidean algorithm (Algorithm 2.2) together with Proposition 2.11 to find the inverse in $\mathbb{Z}_{388}$, if the inverse exists.
    (a) 3
    (b) 55
    (c) 149
    (d) 97

30. For each integer below, use the extended Euclidean algorithm (Algorithm 2.2) together with Proposition 2.11 to find the inverse in $\mathbb{Z}_{299}$, if the inverse exists.
    (a) 2
    (b) 52
    (c) 80
    (d) 199

31. For each integer below, use the extended Euclidean algorithm (Algorithm 2.2) together with Proposition 2.11 to find the inverse in $\mathbb{Z}_{1353}$, if the inverse exists.
    (a) 2
    (b) 44
    (c) 886
    (d) 350

32. For each integer below, use the extended Euclidean algorithm (Algorithm 2.2) together with Proposition 2.11 to find the inverse in $\mathbb{Z}_{2555}$, if the inverse exists.
    (a) 2
    (b) 74
    (c) 98
    (d) 1972

33. Find all solutions for each of the following congruences:
    (a) $3x \equiv 59 \pmod{388}$
    (b) $149x \equiv 225 \pmod{388}$
    (c) $2x \equiv 1225 \pmod{1353}$
    (d) $886x \equiv 35 \pmod{1353}$

34. Find all solutions for each of the following congruences:
    (a) $2x \equiv 59 \pmod{299}$
    (b) $199x \equiv 99 \pmod{299}$
    (c) $2x \equiv 847 \pmod{2555}$
    (d) $1972x \equiv 363 \pmod{2555}$

35. Find all solutions for each of the following congruences:
    (a) $3x \equiv 6 \pmod{18}$
    (b) $15x \equiv 21 \pmod{51}$
    (c) $8x \equiv 12 \pmod{28}$
    (d) $8x \equiv 6 \pmod{28}$

36. Find all solutions for each of the following congruences:
    (a) $2x \equiv 6 \pmod{16}$
    (b) $6x \equiv 16 \pmod{27}$
    (c) $14x \equiv 21 \pmod{88}$
    (d) $25x \equiv 55 \pmod{95}$

37. Find all solutions for each of the following congruences:
    (a) $6x \equiv 28 \pmod{776}$
    (b) $15x \equiv 21 \pmod{1940}$
    (c) $596x \equiv 900 \pmod{1552}$
    (d) $3544x \equiv 900 \pmod{5412}$

38. Find all solutions for each of the following congruences:
    (a) $8x \equiv 16 \pmod{1196}$
    (b) $400x \equiv 125 \pmod{1495}$
    (c) $1393x \equiv 175 \pmod{2093}$
    (d) $17748x \equiv 6642 \pmod{22995}$

39. Find all solutions for each of the following systems of congruences:
    (a) $\begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 4 \pmod{7} \end{cases}$

    (b) $\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 1 \pmod{5} \\ x \equiv 3 \pmod{11} \end{cases}$

    (c) $\begin{cases} x \equiv 2 \pmod{6} \\ x \equiv 1 \pmod{5} \\ x \equiv 3 \pmod{7} \\ x \equiv 1 \pmod{13} \end{cases}$

40. Find all solutions for each of the following systems of congruences:
    (a) $\begin{cases} x \equiv 3 \pmod{4} \\ x \equiv 4 \pmod{5} \end{cases}$

    (b) $\begin{cases} x \equiv 0 \pmod{2} \\ x \equiv 1 \pmod{5} \\ x \equiv 6 \pmod{9} \end{cases}$

    (c) $\begin{cases} x \equiv 1 \pmod{4} \\ x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{9} \\ x \equiv 1 \pmod{11} \end{cases}$

41. A group of 15 pirates has just looted a stash of identical and very valuable gold coins. They plan to equally divide them the next morning. During the night, one pirate, who does not trust the others, gets up to divide the coins into 15 equal parts, finds there are 8 remaining, so takes these 8 with him. But he was unknowingly followed by another pirate who then kills him. This second pirate then divides the remaining coins by 14, finds there are 11 left, and stashes these 11 (plus the 8 he got from the first pirate) under the hull of the boat, but in the process falls overboard and drowns. The next morning the remaining 13 pirates divide the coins by 13 and find there are 5 left. What is the smallest number of coins that originally could have been present?

42. Suppose that a certain computer server has less than 1GB (1 billion bytes) of memory; any time it runs jobs, it allocates an equal number of bytes of memory to each job and leaves any remaining bytes unused. Suppose that when it runs 95 jobs, it has 86 unused bytes; when it runs 98 jobs, it has 13 unused bytes; when it runs 99 jobs, it has 46 unused bytes; and when it runs 101 jobs, all bytes get allocated. Determine the exact size of the computer's memory.

Note: Chapter Exercises 43 through 45 give some applications of congruences to coding theory. **Coding theory** is an area of applied mathematics involved with the efficient transportation of information that is prone to transmission errors (for example, either through incorrectly entering the data on the sender's end or through a noisy channel). The basic idea is to transmit some additional (redundant) information that can be used to detect and sometimes even correct errors. The exercises below deal with error-detecting codes in ISBN (International Standard Book Number) numbers and in credit card numbers. Error-correcting codes have built-in mechanisms that can actually correct errors. An example is with audio CDs, which can play fine with scratches on the playing surface, or even if one were to drill a 2.5 mm hole through the playing surface. Coding theory also makes use of other areas of mathematics such as linear algebra and abstract algebra. For a good general introduction, see, for example, [LiXi-04]. A more comprehensive treatment in error-correcting codes can be found in [Moo-05].

43. *Application of Congruences: ISBN Error-Detecting Codes.* Since the 1970s, to facilitate inventory control and the ordering/selling of books, almost all books published have an attached unique ISBN number. For over 30 years the same system had been in widespread use, but as of 2007, the 10-digit ISBNs were replaced by 13-digit ISBNs. This exercise will discuss 13-digit ISBNs, and the next one will look at the previously used 10-digit system. To distinguish, we refer to each system as ISBN-13 or ISBN-10. An ISBN-13 consists of five blocks of digits. For example, the ISBN-13 of the author's book, *Introduction to Numerical Ordinary and Partial Differential Equations Using MATLAB*, is 978-0-471-69738-1. The first block always consists of three digits. Most books presently in print use 978 in this field (for the U.S. ISBN Agency). The second group is a single digit encoding the country or language of the publisher (0 indicates English), the third group of digits may range from two to seven digits and indicates the publisher (471 indicates John Wiley & Sons), the fourth block of digits has length 8 less the number in the preceding field, and indicates the publisher's assigned number for the particular book. Thus, larger publishers will be assigned smaller publisher codes to allow for larger capacities in the book field (up to six digits, or 1 million books). The fifth and final group is a single **check digit** from 0 to 9. If the digits (in order) of an ISBN-13 number are $x_1x_2\cdots x_{13}$, then the check digit x_{13} is determined by the equation

$$x_{13} \equiv 10 - (x_1 + 3x_2 + x_3 + 3x_4 + \cdots + x_{11} + 3x_{12}) \pmod{10} \quad (2.9)$$

For example, the right-hand side of Equation 2.9 for the above-mentioned ISBN-13 number works out to be $10-(9+3\cdot7+8+3\cdot0+4+3\cdot7+1+3\cdot6+9+3\cdot7+3+3\cdot8)=-129\equiv 1 \pmod{10}$. This indeed coincides with the last check digit $x_{13}=1$. This check system (Equation 2.9) was designed to detect any single error of the following most common ones occurring in typing an ISBN number: mistyping one of the digits or switching two adjacent digits. This is important, since with a single error, the resulting incorrect ISBN could correspond to a totally different book and would otherwise go unnoticed.

(a) Each of the following is the first 12 digits of an ISBN-13 number. Find the 13th check digit for each: 978055215169, 978082482223, 978006123400.

(b) Show that if a valid ISBN-13 number has exactly one mistyped digit, then Equation 2.9 will fail to hold; i.e., the error will be detected.

(c) Show that if a valid ISBN-13 number has two different adjacent digits that were typed in the wrong order, then Equation 2.9 may fail to detect this error.

(d) Give an example of an incorrectly typed ISBN-13 number, along with two corresponding valid ISBN-13 numbers that differ from the former in exactly one digit. This shows that although the ISBN-13 system can detect common errors, it cannot correct them.

Suggestions: For part (b): If $x_1x_2\cdots x_{13}$ was incorrectly typed as $y_1y_2\cdots y_{13}$, where each $y_i=x_i$, with a single exception $y_j\neq x_j$, assume that both ISBNs checked with Equation 2.9. Then, by subtracting the corresponding two equations, we would be left with either $y_j\equiv x_j$ or $3y_j\equiv 3x_j \pmod{10}$. But since 3 is invertible (mod 10), we could multiply both sides of the latter equation by the inverse to obtain $y_j\equiv x_j \pmod{10}$, which forces $y_j=x_j$—a contradiction! A similar argument works for part (c).

44. *Application of Congruences: ISBN Error-Detecting Codes.* The reader should first read Chapter Exercise 43 for some general background. From 1970 up to 2007, the ISBN-10 system was used for published books. Books published prior to 2007 needed to have their ISBN-10 numbers converted to ISBN-13. For example, the ISBN-10 number of the book *Introduction to Numerical Ordinary and Partial Differential Equations Using MATLAB* is 0-471-69738-9. The first three blocks correspond to the second through fourth blocks of the ISBN-13 numbers. The fourth and final block is a single **check digit** that is either a digit from 0 to 9, or the letter X (corresponding to 10). If the digits (in order) of an ISBN-10 number are $x_1x_2\cdots x_{10}$, then the check digit x_{10} is determined by the equation

$$x_{10}\equiv x_1+2x_2+3x_3+4x_4+\cdots+9x_9 \pmod{11} \qquad (2.10)$$

For example, the right-hand side of Equation 2.10 for the above-mentioned ISBN-10 number works out to be $0+2\cdot4+3\cdot7+4\cdot1+5\cdot6+6\cdot9+7\cdot7+8\cdot3+9\cdot8=262\equiv 9 \pmod{11}$. This indeed checks with the last check digit $x_{10}=9$. This check

system Equation 2.10 was designed to detect any single error of the following two: mistyping one of the digits or switching *any* two unequal digits. Thus, the ISBN-10 system can detect more general errors than the ISBN-13 system.

(a) Each of the following is the first 9 digits of an ISBN-10 number. Find the 10th check digit for each: 951020387, 082482223, 013014400.

(b) Show that if a valid ISBN-10 number has exactly one mistyped digit, then Equation 2.10 will fail to hold; i.e., the error will be detected.

(c) Show that if a valid ISBN-10 number has two different digits that were switched, then Equation 2.10 will fail to hold; i.e., the error will be detected.

(d) Give an example of an incorrectly typed ISBN-10 number along with two corresponding valid ISBN-10 numbers that differ from the former in exactly one digit. This shows that although the ISBN-10 system can detect common errors, it cannot correct them.

Suggestions: See the suggestions for Chapter Exercise 43 for ideas for parts (b) and (c).

Note: Comparing the error-detecting capabilities of ISBN-10 versus ISBN-13, although the latter system has a larger capacity, the former is better at detecting permutation errors [see part (c) of this and the preceding exercise].

45. *Application of Congruences: Credit Card Error-Detecting Codes.* Different credit cards use similar coding systems that include identifying information as well as a check digit. This is how Web sites can often immediately inform you if the number you keyed in is not a valid credit card number. In this exercise, we will explore the system that VISA cards use. VISA card numbers either contain 13 or 16 digits, and the first digit is always 4, indicating it is a VISA card (MasterCards always begin with 5). The second through the sixth digits identify the bank that issued the VISA card, and the seventh through the second-to-last digit give the account number. The final digit is the check digit. If the digits (in order) of a 16-digit VISA card number are $x_1x_2\cdots x_{16}$, then the check digit x_{16} is determined by the equation

$$x_{16} = -[2x_1 + x_2 + 2x_3 + x_4 + 2x_5 \cdots + x_{14} + 2x_{15}] - r \pmod{10} \tag{2.11}$$

where r is the number of terms in the bracketed expression that are greater than or equal to 10. For example, in the VISA card number 4784 5580 0246 1888, the bracket expression in Equation 2.11 is $[2\cdot4+7+2\cdot8+4+2\cdot5+5+2\cdot8+0+2\cdot0+2+2\cdot4+6\cdot+2\cdot1+8+2\cdot8] = [8 + 7 + 16 + 4 + 10 + 5 + 16 + 0 + 0 + 2 + 8 + 6 + 2 + 8 + 16]$ and has $r = 4$ two-digit terms and equals 108; thus, the right-hand side of Equation 2.11 equals $-108 - 4 \equiv 8 \pmod{10}$, which coincides (as it should) with the (last) check digit x_{16}.

(a) Which of the following are valid 16-digit VISA card numbers? For those that are not, explain why: 4238 1678 1139 5207, 5602 8333 5495 1777, 4671 8899 3663 1942.

(b) Show that if a valid VISA number has exactly one mistyped digit, then Equation 2.11 will fail to hold; i.e., the error will be detected.

(c) Show that if a valid VISA number has two different adjacent digits that were typed in the wrong order, then Equation 2.11 will fail to hold; i.e., the error will be detected. Can an error still be detected if the digits are not adjacent?

(d) Give an example of an incorrectly typed VISA card number along with two corresponding valid VISA card numbers that differ from the former in exactly one digit. This shows that although the VISA card system can detect common errors, it cannot correct them.

(e) Suppose that a 16-digit VISA card number was correctly sent in but one of the digits printed out illegibly. Is it always possible to recover the missing digit? Explain your answer.

Suggestions: See the suggestions for Chapter Exercise 43 for ideas for parts (b) and (c).

46. *Application of Congruences: Round Robin Tournaments.* In sports competitions involving matches among sets of teams (or individuals), a *round robin tournament* is a tournament in which each team plays every other team exactly once in a series of *rounds* (each team can play in at most one match per round). Congruences can be used to set up a round robin tournament among N teams that will go through exactly N rounds. Here is the algorithm:

(a) Label the teams as $1, 2, \cdots, N$.

(b) In the rth round ($1 \le r \le N$), match team i with team j ($1 \le i, j \le N, i \ne j$) if, and only if, $i + j \equiv r \pmod{N}$.

(i) Use this algorithm to set up a round robin tournament for a competition involving $N = 4$ teams.

(ii) Repeat the instructions of part (a) when $N = 6$.

(iii) Prove that this algorithm will always produce a round robin tournament.

(iv) Note (quite obviously) that with $N = 2$ teams, only one round is needed in a round robin tournament, but show that with $N = 3$ teams, any round robin tournament would need (at least) three rounds.

Suggestions for part (iii): To show that two (different) teams i and j play each other exactly once (in the N rounds), apply the division algorithm to the division of $i + j$ by N. The remainder will be the unique round in which i and j are matched (except if $r = 0$, this should mean the Nth round). Use this division to show also that i cannot play any other team in this same round (and similarly for j).

47. For each of the following divisibility statements, either prove it or give a counterexample. Assume throughout that all variables represent integers.

(a) If $a \mid b$ and $a \mid (b+1)$, then $a = \pm 1$.

(b) If n is even, then $4 \mid n^2$.

(c) If a and b are both even or both odd, then $a^2 - b^2$ is even.

48. For each of the following divisibility statements, either prove it or give a counterexample. Assume throughout that all variables represent integers.
    (a) If $a \mid b$ and $c \mid d$, then $ac \mid bd$.
    (b) If $a \mid b$ and $a \mid c$, then $a \mid \gcd(b, c)$.
    (c) If n is an integer, then $3 \mid n^3 - n$.

49. For each of the following statements, either prove it or give a counterexample. Assume throughout that all variables represent integers, unless otherwise specified.
    (a) $4 \mid [a(a+1)(a+2)]$
    (b) $4 \mid (a^4 - a^2)$
    (c) If $n > 1$ is an odd integer, then $4^n - 3$ is prime.

50. For each of the following statements, either prove it or give a counterexample. Assume throughout that all variables represent integers, unless otherwise specified.
    (a) If ab is a multiple of 4, then either a is a multiple of 4 or b is a multiple of 4.
    (b) If a is odd, then $4 \mid (a^2 - 1)$.
    (c) If a is odd, then $8 \mid (a^2 - 1)$.

51. (a) Prove the following identity: $\gcd(ab, ac) = a \gcd(b, c)$, whenever a, b, and c are positive integers.
    (b) Prove that if b and c are positive integers with $d = \gcd(b, c)$, then $\frac{b/d}{c/d}$ will be the lowest-terms representation of the fraction b/c.
    (c) Explain how the Euclidean algorithm can be used to create an algorithm for obtaining the lowest-terms representation of any fraction $\frac{b}{c}$ of positive integers. Apply your algorithm to obtain the lowest-terms representation of the fraction $\frac{1474}{39{,}463}$.

52. Prove the following variation of Euclid's lemma:
    If $a \mid bc$, and $\gcd(a, b) = 1$, then $a \mid c$.

    Suggestion: Use Theorem 2.6.

53. Prove that if $n \in \mathbb{Z}_+$ and $2^n - 1$ is prime, then n must be prime.

    Suggestion: Use the following (easily verified) algebraic factorization identity: $x^{ab} - 1 = (x^a - 1)(x^{a(b-1)} + x^{a(b-2)} + \cdots + x^a + 1)$.

Historical Note: The converse of Chapter Exercise 53 is false; for example, $2^{11} - 1 = 2047 = 23 \cdot 89$. Prime numbers of the form $2^n - 1$ are called *Mersenne primes*, after Marin Mersenne (1588–1648, French priest and scholar). Mersenne boldly stated (without proof) in the preface of his book *Cogitata Physica-Mathematica* (1644) that $2^n - 1$ is prime for whenever $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127$, and 257, and composite for all other values of n. The last of these numbers has 77 digits, so the claim would

have been very difficult to verify at the time, when all calculations had to be done by hand. Mersenne's conjecture initiated much activity in the area, and it was not until over a century later, in 1783, that someone discovered that Mersenne had missed one: $2^{61}-1$ was proved to be a Mersenne prime. Taking advantage of their unique form, specialized and very efficient algorithms have been developed to check whether 2^n-1 is prime, and because of these algorithms, the largest known primes are Mersenne primes. Since the mid-1990s there has been an open project—*The Great Internet Mersenne Prime Search* (GIMPS—http://www.mersenne.org/)—that has scientists across the world attempting to break new records. GIMPS offers $3,000 for each new Mersenne prime that is discovered, and their website provides free specialized software programs that can help. In 2009, the first (Mersenne) prime that broke the 10-million digit benchmark was discovered on a UCLA computer setup (using GIMPS software) by Edson Smith. This prime, $2^{37,156,667}-1$, has 12,978,189 digits, and garnered a long-standing $100,000 prize, offered by an anonymous donor for being the first to find a prime number with at least 10 million digits. The discovery of the 37th known Mersenne prime was made by Roland Clarkson, who worked independently, and at the time was a 19-year-old student at California State University–Dominguez Hills. There are still many theoretical questions that remain unanswered regarding Mersenne primes. For example, it is not yet known whether there are infinitely many Mersenne primes.

54. *Application of Congruences: Divisibility Criteria.*
   (a) Prove that for any positive integer n, $3 \mid n$ if, and only if, 3 divides the sum of the digits of n. Equivalently, if we write $n=\sum_{k=0}^{D} d_k \cdot 10^k$, where $0 \le d_k \le 9$ (the digits), $3 \mid n \Leftrightarrow n=\sum_{k=0}^{D} d_k$.
   (b) With the notation of part (a), prove that $4 \mid n \Leftrightarrow 4 \mid (d_0+10d_1)$.

   Suggestion: For part (a), show that $n \equiv \sum_{k=0}^{D} d_k \pmod 3$. For part (b), use the fact that $4 \mid 10^2$.

55. *Application of Congruences: Divisibility Criteria.*
   (a) Prove that for any positive integer $n=\sum_{k=0}^{D} d_k \cdot 10^k$, $11 \mid n$ if, and only if, $11 \mid (d_0+d_2+d_4+\cdots-d_1-d_3-d_5-\cdots)$. For example, $11 \mid 930391$ since $11 \mid (9+0+9-3-3-1)$.
   (b) With the notation of part (a), prove that $7 \mid n \Leftrightarrow 7 \mid (d_0+10d_1+100d_2-d_3-10d_4-100d_5+d_6+10d_7+100d_8-\cdots)$. For example, $7 \mid 4001006002$ since $7 \mid (4-1+6-2)=(4+10\cdot 0+100\cdot 0-1-10\cdot 0-100\cdot 0+6+10\cdot 0+100\cdot 0-2)$.

56. Prove that for any odd modulus $m > 2$, we have $\sum_{k=1}^{m-1} k \equiv 0 \pmod m$.

57. Prove that for any even modulus $m > 1$, we have $\sum_{k=1}^{m-1} k \equiv m/2 \pmod m$.

58. In the notation of our (constructive) proof of the Chinese remainder theorem (Theorem 2.13), prove that $\sum_{i=1}^{k-1} e_i(N/n_i) \equiv 1 \pmod N$.

59. Suppose that a is an integer and n and m are relatively prime integers, both greater than 1.
   (a) If $x \equiv a \pmod{m}$ and $x \equiv a \pmod{n}$, show that $x \equiv a \pmod{mn}$.
   (b) Does the result of part (a) remain valid without the assumption that m and n are relatively prime? Either prove that it does or provide a counterexample.

Note: An integer a is said to have a **square root modulo m** ($m > 1$ an integer) if the equation $x^2 \equiv a \pmod{m}$ has at least one solution. Any solution is called a **square root of a mod m**. Exercises 60–63 will explore some situations in which it can be determined if a certain number a has a square root modulo a certain m, and also the problem of determining how many square roots a has, once it is known to have at least one.

60. *Square Roots Modulo a Prime.* Let p be an odd prime (positive) integer.
   (a) Prove that the integers that have square roots mod p are precisely those in the set $\{0^2, 1^2, 2^2, \cdots, [(p-1)/2]^2\} \pmod{p}$.
   (b) Show that the elements listed in the set of part (a) are all different mod p.
   (c) Show that if $p > 2$, then each of the $(p-1)/2$ *nonzero* elements listed in the set of part (a) has exactly two (distinct) square roots mod p.
   (d) Find all the numbers in $\mathbb{Z}_{11}$ that have square roots, and for each one, find all of its square roots (mod 11).
   (e) Repeat the instructions of part (d) for $\mathbb{Z}_{13}$.
   (f) What happens to the results of parts (a), (b), (c) in case $p = 2$?

   Suggestions: For part (a), if $z > (p-1)/2$, show that $w = p - z$ is $\leq (p-1)/2$ and $z^2 \equiv w^2 \pmod{p}$. For part (b), suppose that $0 \leq w < z \leq (p-1)/2$ but that $w^2 \equiv z^2 \pmod{p}$. This means that $p \mid z^2 - w^2 = (z+w)(z-w)$. Use Euclid's lemma (Proposition 2.7) to obtain a contradiction. For part (c), if z is a square root, then so is $-z (\equiv p - z) \pmod{p}$.

61. *Square Roots Modulo a Product of Distinct Primes.* Let $p < q$ both be odd primes.
   (a) Show that the equation $x^2 \equiv a \pmod{pq}$ is equivalent to the system $\begin{cases} x^2 \equiv a \pmod{p} \\ x^2 \equiv a \pmod{q} \end{cases}$. Indicate a scheme for finding all square roots of an integer a mod pq.
   (b) Using Chapter Exercise 60 and the result of part (a), obtain a result for the existence of square roots modulo a product of distinct odd primes.
   (c) Find (i) all (if any) square roots of 9 mod 35, and then (ii) compute $\sqrt{51} \pmod{493}$.
   (d) How would the results found in parts (a) and (b) change in case $p = 2$?
   (e) Find the following square roots (if they exist): (i) $\sqrt{11} \pmod{26}$, and (ii) $\sqrt{68} \pmod{86}$.

   Suggestions: Make use of the Chinese remainder theorem.

62. *Square Roots Modulo a Prime-Efficient Algorithms.* Chapter Exercise 60 completely explained the existence and number of square roots that an integer can have modulo a prime; however, the resulting method for extracting square roots was not very much faster than a brute-force search. The following proposition gives a fast method for finding all square roots of any integer modulo a prime p in the case that $p \equiv 3 \pmod 4$.

Proposition 2.15

Assume that p is a prime number that is congruent to 3(mod 4), and let $x \not\equiv 0$ be any integer (mod p). Then either x or $-x$, but not both, will have two square roots (mod p), and these square roots are given by $\pm w$, where $w = x^{(p+1)/4} \pmod p$.

For a proof as well as another theorem covering the remaining case where $p \equiv 1 \pmod 4$, we refer to [Coh-93]. Here we look only at the practical applications of Proposition 2.14.* Use Proposition 2.14 to determine all square roots of the following:

(a) $\sqrt{7} \pmod{59}$
(b) $\sqrt{142} \pmod{607}$
(c) $\sqrt{10} \pmod{2143}$

63. *More Square Roots Modulo a Product of Distinct Primes.* Let $p \neq q$ both be prime (positive) integers. The technique for extracting square roots mod pq given in Chapter Exercise 61 can be speeded up if one of the two primes is congruent to 3(mod 4), since Proposition 2.14 of Chapter Exercise 62 can then be applied. Use these ideas to find all square roots of the following:

(a) $\sqrt{5} \pmod{413}$
(b) $\sqrt{32} \pmod{22459}$
(c) $\sqrt{34} \pmod{23573}$

64. *Wilson's Theorem.* Wilson's theorem states that if p is a prime, then $(p-1)! \equiv -1 \pmod p$.
   (a) Show that the converse of Wilson's theorem is true, i.e., show that if $n > 1$ is an integer that satisfies $(n-1)! \equiv -1 \pmod n$, then n must be prime.
   (b) Use Wilson's theorem to prove that $p \mid 2(p-3)! + 1$ for any odd prime number p.

65. Prove that if a is any integer and n is any nonnegative integer, then a and a^{4n+1} have the same last digit.

66. Suppose that $a > 1$ is an integer and that $k > \ell$ are positive integers.
   (a) Let r be the remainder of the division $k \div \ell$, i.e., $r = k - \text{floor}(k / \ell)$. Prove that the remainder of the division $(a^k - 1) \div (a^\ell - 1)$ is $a^r - 1$.
   (b) Prove that $\gcd(a^k - 1, a^\ell - 1) = a^{\gcd(k,\ell)} - 1$.

* More efficient implementations of Proposition 2.14 will be possible after we introduce an algorithm for fast modular exponentiation in Chapter 6. For now, when taking large powers in modular arithmetic, the reader should begin with small powers and work his or her way up, as suggested in Exercises 19 and 20.

Suggestion for part (b): Apply the Euclidean algorithm in conjunction with the result of part (a).

Chapter 2 Computer Implementations and Exercises

Note: If your computing platform is a floating point arithmetic system, it may allow you only up to 15 or so significant digits of accuracy. Symbolic systems allow for much greater precision, being able to handle 100s or 1000s of significant digits. Some platforms allow the user to choose if he or she wishes to work in floating point or symbolic arithmetic but will work in floating point arithmetic by default since operations are faster and usually sufficiently accurate for general purposes. If you have access only to a floating point system, you should keep these limitations in mind when you do computer calculations with large integers. The specific computations asked for below should be amenable to all floating point systems, which tend to be accurate to about 15 significant digits.

1. *Program for Check if a Positive Integer Is Prime.*
   (a) Write a program `y = PrimeCheck(n)` that inputs an integer $n > 1$, and outputs an integer y that is 1 if n is a prime number and 0 if it is not. The method used should be a brute-force check to see whether n has any positive integer factor k, checking all values of k (if necessary) up to floor($\sqrt{n}$).
   (b) Run your program with each of the following input values: $n = 30, 31, 487, 8893, 987654323, 131317171919$.
   (c) Assuming that your computing platform can perform 1 billion divisions per second [and assuming that the rest of the program in part (a) takes negligible time], what is the largest number of digits an inputted integer n could have so that the program could be guaranteed to execute in less than one minute?
   (d) Under the assumption of part (c), how long could it take for the program in part (a) to check whether a 100-digit integer is prime?
   Note: Of course, the program could execute very fast if a small prime factor is found quickly. A prime input would always take the most time since the full range of k values would need to be checked. There are some efficiency enhancements that we could incorporate into the above program: For example, after it is checked that 2 is not a factor, we need only check odd integers after 2. Such a fix could cut the runtimes essentially in half, but there are more efficient (and sophisticated) prime checking algorithms than such brute-force methods. For more on this interesting area, we refer the reader to [BaSh-96].

2. *Program for Prime Factorization of Positive Integers.*
   (a) Write a program `FactorList = PrimeFactors(n)` that inputs an integer $n > 1$, and outputs a vector `FactorList` that lists all of the prime factors, from smallest to largest, and with repetitions for multiple factors. For example, since the prime factorization of 24 is $2^3 \cdot 3$, the output of