8.4 Modular Arithmetic with Applications to Cryptography

The "real" mathematics of the "real" mathematicians, the mathematics of Fermat and Euler and Gauss and Abel and Riemann, is almost wholly "useless." . . . It is not possible to justify the life of any genuine professional mathematician on the ground of the "utility" of his work. — G. H. Hardy, *A Mathematician's Apology*, 1941

Cryptography is the study of methods for sending secret messages. It involves **encryption,** in which a message, called **plaintext,** is converted into a form, called **ciphertext,** that may be sent over channels possibly open to view by outside parties. The receiver of the ciphertext uses **decryption** to convert the ciphertext back into plaintext.

In the past the primary use of cryptography was for government and military intelligence, and this use continues to be important. In fact, the National Security Agency, whose main business is cryptography, is the largest employer of mathematicians in the United States. With the rise of electronic communication systems, however, especially the Internet, an extremely important current use of cryptography is to make it possible to send private information, such as credit card numbers, banking data, medical records, and so forth, over electronic channels.

Many systems for sending secret messages require both the sender and the receiver to know both the encryption and the decryption procedures. For instance, an encryption system once used by Julius Caesar, and now called the **Caesar cipher**, encrypts messages by changing each letter of the alphabet to the one three places farther along, with X wrapping around to A, Y to B, and Z to C. In other words, say each letter of the alphabet is coded by its position relative to the others—so that A = 01, B = 02, . . . , Z = 26. If the numerical version of the plaintext for a letter is denoted M and the numeric version of the ciphertext is denoted C, then

$$C = (M + 3) \bmod 26.$$

The receiver of such a message can easily decrypt it by using the formula

$$M = (C - 3) \bmod 26.$$

For reference, here are the letters of the alphabet, together with their numeric equivalents:

A	B	C	D	E	F	G	H	I	J	K	L	M
01	02	03	04	05	06	07	08	09	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Example 8.4.1 Encrypting and Decrypting with the Caesar Cipher

a. Use the Caesar cipher to encrypt the message HOW ARE YOU.

b. Use the Caesar cipher to decrypt the message L DP ILQH.

Solution

a. First translate the letters of HOW ARE YOU into their numeric equivalents:

08 15 23 01 18 05 25 15 21.

Next encrypt the message by adding 3 to each number. The result is

11 18 26 04 21 08 02 18 24.

Finally, substitute the letters that correspond to these numbers. The encrypted message becomes

KRZ DUH BRX.

b. First translate the letters of L DP ILQH into their numeric equivalents:

12 04 16 09 12 17 08.

Next decrypt the message by subtracting 3 from each number:

09 01 13 06 09 14 05.

Then translate back into letters to obtain the original message: I AM FINE. ■

One problem with the Caesar cipher is that given a sufficient amount of ciphertext a person with knowledge of letter frequencies in the language can easily figure out the cipher. Partly for this reason, even Caesar himself did not make extensive use of it. Another problem with a system like the Caesar cipher is that knowledge of how to encrypt a message automatically gives knowledge of how to decrypt it. When a potential recipient of messages passes the encryption information to a potential sender of messages, the channel over which the information is passed may itself be insecure. Thus the information may leak out, enabling an outside party to decrypt messages intended to be kept secret.

With public-key cryptography, a potential recipient of encrypted messages openly distributes a public key containing the encryption information. However, knowledge of the public key provides virtually no clue about how messages are decrypted. Only the recipient has that knowledge. Regardless of how many people learn the encryption information, only the recipient should be able to decrypt messages that are sent.

The first public-key cryptography system was developed in 1976–1977 by three young mathematician/computer scientists working at M.I.T.: Ronald Rivest, Adi Shamir, and

Courtesy of Leonard Adleman

From left to right: Ronald Rivest (born 1948), Adi Shamir (born 1952), and Leonard Adleman (born 1945)

Leonard Adleman. In their honor it is called the RSA cipher. In order for you to learn how it works, you need to know some additional properties of congruence modulo n.

Properties of Congruence Modulo n

The first theorem in this section brings together a variety of equivalent ways of expressing the same basic arithmetic fact. Sometimes one way is most convenient; sometimes another way is best. You need to be comfortable moving from one to another, depending on the nature of the problem you are trying to solve.

Theorem 8.4.1 Modular Equivalences

Let a, b, and n be any integers and suppose $n > 1$. The following statements are all equivalent:

1. $n \mid (a - b)$
2. $a \equiv b \pmod{n}$
3. $a = b + kn$ for some integer k
4. a and b have the same (nonnegative) remainder when divided by n
5. $a \bmod n = b \bmod n$

Proof:

We will show that (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4) $\Rightarrow$ (5) $\Rightarrow$ (1). It will follow by the transitivity of if-then that all five statements are equivalent.

So let a, b, and n be any integers with $n > 1$.

***Proof that* (1) $\Rightarrow$ (2):** Suppose that $n \mid (a - b)$. By definition of congruence modulo n, we can immediately conclude that $a \equiv b \pmod{n}$.

***Proof that* (2) $\Rightarrow$ (3):** Suppose that $a \equiv b \pmod{n}$. By definition of congruence modulo n, $n \mid (a - b)$. Thus, by definition of divisibility, $a - b = kn$, for some integer k. Adding b to both sides gives that $a = b + kn$.

***Proof that* (3) $\Rightarrow$ (4):** Suppose that $a = b + kn$, for some integer k. Use the quotient-remainder theorem to divide a by n to obtain

$$a = qn + r \quad \text{where } q \text{ and } r \text{ are integers and } 0 \leq r < n.$$

Substituting $b + kn$ for a in this equation gives that

$$b + kn = qn + r$$

and subtracting kn from both sides and factoring out n yields

$$b = (q - k)n + r.$$

But since $0 \leq r < n$, the uniqueness property of the quotient-remainder theorem guarantees that r is also the remainder obtained when b is divided by n. Thus a and b have the same remainder when divided by n.

***Proof that* (4) $\Rightarrow$ (5):** Suppose that a and b have the same remainder when divided by n. It follows immediately from the definition of the *mod* function that $a \bmod n = b \bmod n$.

***Proof that* (5) ⇒ (1):** Suppose that $a \bmod n = b \bmod n$. By definition of the *mod* function, a and b have the same remainder when divided by n. Thus, by the quotient-remainder theorem, we can write

$a = q_1 n + r$ and $b = q_2 n + r$ where q_1, q_2, and r are integers and $0 \le r < n$.

It follows that

$$a - b = (q_1 n + r) - (q_2 n + r) = (q_1 - q_2)n.$$

Therefore, since $q_1 - q_2$ is an integer, $n \mid (a - b)$.

Another consequence of the quotient-remainder theorem is this: When an integer a is divided by a positive integer n, a unique quotient q and remainder r are obtained with the property that $a = nq + r$ and $0 \le r < n$. Because there are exactly n integers that satisfy the inequality $0 \le r < n$ (the numbers from 0 through $n - 1$), there are exactly n possible remainders that can occur. These are called the *least nonnegative residues modulo n* or simply the *residues modulo n*.

• Definition

Given integers a and n with $n > 1$, **the residue of *a* modulo *n*** is $a \bmod n$, the nonnegative remainder obtained when a is divided by n. The numbers $0, 1, 2, \ldots, n - 1$ are called a **complete set of residues modulo *n***. To **reduce a number modulo *n*** means to set it equal to its residue modulo n. If a modulus $n > 1$ is fixed throughout a discussion and an integer a is given, the words "modulo n" are often dropped and we simply speak of **the residue of *a***.

The following theorem generalizes several examples from Section 8.3.

Theorem 8.4.2 Congruence Modulo *n* Is an Equivalence Relation

If n is any integer with $n > 1$, congruence modulo n is an equivalence relation on the set of all integers. The distinct equivalence classes of the relation are the sets $[0], [1], [2], \ldots, [n - 1]$, where for each $a = 0, 1, 2, \ldots, n - 1$,

$$[a] = \{m \in Z \mid m \equiv a \pmod{n}\},$$

or, equivalently,

$$[a] = \{m \in Z \mid m = a + kn \text{ for some integer } k\}.$$

Proof:

Suppose n is any integer with $n > 1$. We must show that congruence modulo n is reflexive, symmetric, and transitive.

***Proof of reflexivity*:** Suppose a is any integer. To show that $a \equiv a \pmod{n}$, we must show that $n \mid (a - a)$. But $a - a = 0$, and $n \mid 0$ because $0 = n \cdot 0$. Therefore $a \equiv a \pmod{n}$.

continued on page 482

***Proof of symmetry*:** Suppose a and b are any integers such that $a \equiv b \pmod{n}$. We must show that $b \equiv a \pmod{n}$. But since $a \equiv b \pmod{n}$, then $n \mid (a - b)$. Thus, by definition of divisibility, $a - b = nk$, for some integer k. Multiply both sides of this equation by -1 to obtain

$$-(a - b) = -nk,$$

or, equivalently,

$$b - a = n(-k).$$

Thus, by definition of divisibility $n \mid (b - a)$, and so, by definition of congruence modulo n, $b \equiv a \pmod{n}$.

***Proof of transitivity*:** This is left as exercise 5 at the end of the section.

***Proof that the distinct equivalence classes are* [0], [1], [2], . . . , [$n - 1$]:** This is left as exercise 6 at the end of the section.

Observe that there is a one-to-one correspondence between the distinct equivalence classes for congruence modulo n and the elements of a complete set of residues modulo n.

Modular Arithmetic

A fundamental fact about congruence modulo n is that if you first perform an addition, subtraction, or multiplication on integers and then reduce the result modulo n, you will obtain the same answer as if you had first reduced each of the numbers modulo n, performed the operation, and then reduced the result modulo n. For instance, instead of computing

$$(5 \cdot 8) = 40 \equiv 1 \pmod{3}$$

you will obtain the same answer if you compute

$$(5 \textit{ mod } 3)(8 \textit{ mod } 3) = 2 \cdot 2 = 4 \equiv 1 \pmod{3}.$$

The fact that this process works is a result of the following theorem.

Theorem 8.4.3 Modular Arithmetic

Let a, b, c, d, and n be integers with $n > 1$, and suppose

$$a \equiv c \pmod{n} \text{ and } b \equiv d \pmod{n}.$$

Then

1. $(a + b) \equiv (c + d) \pmod{n}$[-2pt]
2. $(a - b) \equiv (c - d) \pmod{n}$[-2pt]
3. $ab \equiv cd \pmod{n}$
4. $a^m \equiv c^m \pmod{n}$ for all integers m.

Proof:

Because we will make greatest use of part 3 of this theorem, we prove it here and leave the proofs of the remaining parts of the theorem to exercises 9–11 at the end of the section.

***Proof of Part 3*:** Suppose a, b, c, d, and n are integers with $n > 1$, and suppose $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. By Theorem 8.4.1, there exist integers s and t such that

$$a = c + sn \quad \text{and} \quad b = d + tn.$$

Then

$$\begin{aligned} ab &= (c + sn)(d + tn) && \text{by substitution} \\ &= cd + ctn + snd + sntn \\ &= cd + n(ct + sd + stn) && \text{by algebra.} \end{aligned}$$

Let $k = ct + sd + stn$. Then k is an integer and $ab = cd + nk$. Thus by Theorem 8.4.1, $ab \equiv cd \pmod{n}$.

Example 8.4.2 Getting Started with Modular Arithmetic

The most practical use of modular arithmetic is to reduce computations involving large integers to computations involving smaller ones. For instance, note that $55 \equiv 3 \pmod{4}$ because $55 - 3 = 52$, which is divisible by 4, and $26 \equiv 2 \pmod{4}$ because $26 - 2 = 24$, which is also divisible by 4. Verify the following statements.

a. $55 + 26 \equiv (3 + 2) \pmod{4}$ b. $55 - 26 \equiv (3 - 2) \pmod{4}$

c. $55 \cdot 26 \equiv (3 \cdot 2) \pmod{4}$ d. $55^2 \equiv 3^2 \pmod{4}$

Solution

a. Compute $55 + 26 = 81$ and $3 + 2 = 5$. By definition of congruence modulo n, to show that $81 \equiv 5 \pmod{4}$, you need to show that $4 \mid (81 - 5)$. But this is true because $81 - 5 = 76$, and $4 \mid 76$ since $76 = 4 \cdot 19$.

b. Compute $55 - 26 = 29$ and $3 - 2 = 1$. By definition of congruence modulo n, to show that $29 \equiv 1 \pmod{4}$, you need to show that $4 \mid (29 - 1)$. But this is true because $29 - 1 = 28$, and $4 \mid 28$ since $28 = 4 \cdot 7$.

c. Compute $55 \cdot 26 = 1430$ and $3 \cdot 2 = 6$. By definition of congruence modulo n, to show that $1430 \equiv 6 \pmod{4}$, you need to show that $4 \mid (1430 - 6)$. But this is true because $1430 - 6 = 1424$, and $4 \mid 1424$ since $1424 = 4 \cdot 356$.

d. Compute $55^2 = 3025$ and $3^2 = 9$. By definition of congruence modulo n, to show that $3025 \equiv 9 \pmod{4}$, you need to show that $4 \mid (3025 - 9)$. But this is true because $3025 - 9 = 3016$, and $4 \mid 3016$ since $3016 = 4 \cdot 754$. ■

In order to facilitate the computations performed in this section, it is convenient to express part 3 of Theorem 8.4.3 in a slightly differently form.

Corollary 8.4.4

Let a, b, and n be integers with $n > 1$. Then

$$ab \equiv [(a \bmod n)(b \bmod n)] \pmod{n},$$

or, equivalently,

$$ab \bmod n = [(a \bmod n)(b \bmod n)] \bmod n.$$

In particular, if m is a positive integer, then

$$a^m \equiv [(a \bmod n)^m] \pmod{n}.$$

Example 8.4.3 Computing a Product Modulo *n*

As in Example 8.4.2, note that $55 \equiv 3 \pmod 4$ and $26 \equiv 2 \pmod 4$. Because both 3 and 2 are less than 4, each of these numbers is a least nonnegative residue modulo 4. Therefore, $55 \bmod 4 = 3$ and $26 \bmod 4 = 2$. Use the notation of Corollary 8.4.4 to find the residue of $55 \cdot 26$ modulo 4.

Solution Recall that to use a calculator to compute remainders, you can use the formula $n \bmod d = n - d \cdot \lfloor n/d \rfloor$. If you are using a hand calculator with an "integer part" feature and both n and d are positive, then $\lfloor n/d \rfloor$ is the integer part of the division of n by d. When you divide a positive integer n by a positive integer d with a more basic calculator, you can see $\lfloor n/d \rfloor$ on the calculator display by simply ignoring the digits that follow the decimal point.

By Corollary 8.4.4,

$$\begin{aligned}
(55 \cdot 26) \bmod 4 &= \{(55 \bmod 4)(26 \bmod 4)\} \bmod 4 \\
&\equiv (3 \cdot 2) \bmod 4 && \text{because } 55 \bmod 4 = 3 \text{ and } 26 \bmod 4 = 2 \\
&\equiv 6 \bmod 4 \\
&\equiv 2 && \text{because } 4 \mid (6 - 2) \text{ and } 2 < 4.
\end{aligned}$$

■

When modular arithmetic is performed with very large numbers, as is the case for RSA crytography, computations are facilitated by using two properties of exponents. The first is

$$\boxed{x^{2a} = (x^a)^2 \quad \text{for all real numbers } x \text{ and } a \text{ with } x \geq 0.} \qquad 8.4.1$$

Thus, for instance, if x is any positive real number, then

$$\begin{aligned}
x^4 \bmod n &= (x^2)^2 \bmod n && \text{because } (x^2)^2 = x^4 \\
&= (x^2 \bmod n)^2 \bmod n && \text{by Corollary 8.4.4.}
\end{aligned}$$

Hence you can reduce x^4 modulo n by reducing x^2 modulo n and then reducing the square of the result modulo n. Because all the residues are less than n, this process limits the size of the computations to numbers that are less than n^2, which makes them easier to work with, both for humans (when the numbers are relatively small) and for computers (when the numbers are very large).

A second useful property of exponents is

$$\boxed{x^{a+b} = x^a x^b \quad \text{for all real numbers } x, a, \text{ and } b \text{ with } x \geq 0.} \qquad 8.4.2$$

For instance, because $7 = 4 + 2 + 1$,

$$x^7 = x^4 x^2 x^1$$

Thus, by Corollary 8.4.4,

$$x^7 \bmod n = \{(x^4 \bmod n)(x^2 \bmod n)(x^1 \bmod n)\} \bmod n.$$

We first show an example that illustrates the application of formula (8.4.1) and then an example that uses both (8.4.1) and (8.4.2).

Example 8.4.4 Computing $a^k \bmod n$ When k Is a Power of 2

Find $144^4 \bmod 713$.

Solution Use property (8.4.1) to write $144^4 = (144^2)^2$. Then

$$\begin{aligned}
144^4 \bmod 713 &= (144^2)^2 \bmod 713 \\
&= (144^2 \bmod 713)^2 \bmod 713 \\
&= (20736 \bmod 713)^2 \bmod 713 && \text{because } 144^2 = 20736 \\
&= 59^2 \bmod 713 && \text{because } 20736 \bmod 713 = 59 \\
&= 3481 \bmod 713 && \text{because } 59^2 = 3481 \\
&= 629 && \text{because } 3481 \bmod 713 = 629. \quad \blacksquare
\end{aligned}$$

Example 8.4.5 Computing $a^k \bmod n$ When k Is Not a Power of 2

Find $12^{43} \bmod 713$.

Solution First write the exponent as a sum of powers of 2:

$$43 = 2^5 + 2^3 + 2 + 1 = 32 + 8 + 2 + 1.$$

Next compute 12^{2^k} for $k = 1, 2, 3, 4, 5$.

$$\begin{aligned}
12 \bmod 713 &= 12 \\
12^2 \bmod 713 &= 144 \\
12^4 \bmod 713 &= 144^2 \bmod 713 = 59 && \text{by Example 8.4.4} \\
12^8 \bmod 713 &= 59^2 \bmod 713 = 629 && \text{by Example 8.4.4} \\
12^{16} \bmod 713 &= 629^2 \bmod 713 = 639 && \text{by the method of Example 8.4.4} \\
12^{32} \bmod 713 &= 639^2 \bmod 713 = 485 && \text{by the method of Example 8.4.4}
\end{aligned}$$

By property (8.4.2),

$$12^{43} = 12^{32+8+2+1} = 12^{32} \cdot 12^8 \cdot 12^2 \cdot 12^1.$$

Thus, by Corollary 8.4.4,

$$12^{43} \bmod 713 = \{(12^{32} \bmod 713) \cdot (12^8 \bmod 713) \cdot (12^2 \bmod 713) \cdot (12 \bmod 713)\} \bmod 713.$$

By substitution,

$$\begin{aligned}
12^{43} \bmod 713 &= (485 \cdot 629 \cdot 144 \cdot 12) \bmod 713 \\
&= 527152320 \bmod 713 \\
&= 48. \quad \blacksquare
\end{aligned}$$

It is important to understand how to do the computations in Example 8.4.5 by hand using only a simple electronic calculator, but if you are computing a lot of residues, especially ones involving large numbers, you may want to write a short computer or calculator program to do the computations for you.

Extending the Euclidean Algorithm

An extended version of the Euclidean algorithm can be used to find a concrete expression for the greatest common divisor of integers a and b.

• Definition

An integer d is said to be a **linear combination of integers** a and b if, and only if, there exist integers s and t such that $as + bt = d$.

Theorem 8.4.5 Writing a Greatest Common Divisor as a Linear Combination

For all integers a and b, not both zero, if $d = \gcd(a, b)$, then there exist integers s and t such that $as + bt = d$.

Proof:

Given integers a and b, not both zero, and given $d = \gcd(a, b)$, let

$$S = \{x \mid x \text{ is a positive integer and } x = as + bt \text{ for some integers } s \text{ and } t\}.$$

Note that S is a nonempty set because (1) if $a > 0$ then $1 \cdot a + 0 \cdot b \in S$, (2) if $a < 0$ then $(-1) \cdot a + 0 \cdot b \in S$, and (3) if $a = 0$, then by assumption $b \neq 0$, and hence $0 \cdot a + 1 \cdot b \in S$ or $0 \cdot a + (-1) \cdot b \in S$. Thus, because S is a nonempty subset of positive integers, by the well-ordering principle for the integers there is a least element c in S. By definition of S,

$$c = as + bt \quad \text{for some integers } s \text{ and } t. \tag{8.4.3}$$

We will show that (1) $c \geq d$, and (2) $c \leq d$, and we will therefore be able to conclude that $c = d = \gcd(a, b)$.

(1) *Proof that $c \geq d$:*
[In this part of the proof, we show that d is a divisor of c and thus that $d \leq c$.] Because $d = \gcd(a, b)$, by definition of greatest common divisor, $d \mid a$ and $d \mid b$. Hence $a = dx$ and $b = dy$ for some integers x and y. Then

$$\begin{aligned} c &= as + bt && \text{by (8.4.3)} \\ &= (dx)s + (dy)t && \text{by substitution} \\ &= d(xs + yt) && \text{by factoring out the } d. \end{aligned}$$

But $xs + yt$ is an integer because it is a sum of products of integers. Thus, by definition of divisibility, $d \mid c$. Both c and d are positive, and hence, by Theorem 4.3.1, $c \geq d$.

(2) *Proof that $c \leq d$:*
[In this part of the proof, we show that c is a divisor of both a and b and therefore that c is less than or equal to the greatest common divisor of a and b, which is d.] Apply the quotient-remainder theorem to the division of a by c to obtain

$$a = cq + r \quad \text{for some integers } q \text{ and } r \text{ with } 0 \leq r < c. \tag{8.4.4}$$

Thus for some integers q and r with $0 \leq r < c$,

$$r = a - cq$$

Now $c = as + bt$. Therefore, for some integers q and r with $0 \leq r < c$,

$$\begin{aligned} r &= a - (as + bt)q && \text{by substitution} \\ &= a(1 - sq) - btq. \end{aligned}$$

Thus r is a linear combination of a and b. If $r > 0$, then r would be in S, and so r would be a smaller element of S than c, which would contradict the fact that c is the least element of S. Hence $r = 0$. By substitution into (8.4.4),

$$a = cq$$

and therefore $c \mid a$.

An almost identical argument establishes that $c \mid b$ and is left as exercise 30 at the end of the section.

Because $c \mid a$ and $c \mid b$, c is a common divisor of a and b. Hence it is less than or equal to the greatest common divisor of a and b. In other words, $c \leq d$.

From (1) and (2), we conclude that $c = d$. It follows that d, the greatest common divisor of a and b, is equal to $as + bt$.

The following example shows a practical method for expressing the greatest common divisor of two integers as a linear combination of the two.

Example 8.4.6 Expressing a Greatest Common Divisor as a Linear Combination

In Example 4.8.6 we showed how to use the Euclidean algorithm to find that the greatest common divisor of 330 and 156 is 6. Use the results of those calculations to express gcd(330, 156) as a linear combination of 330 and 156.

Solution The first four steps of the solution restate and extend results from Example 4.8.6, which were obtained by successive applications of the quotient-remainder theorem. The fifth step shows how to find the coefficients of the linear combination by substituting back through the results of the previous steps.

Step 1: $330 = 156 \cdot 2 + 18$, which implies that $18 = 330 - 156 \cdot 2$.

Step 2: $156 = 18 \cdot 8 + 12$, which implies that $12 = 156 - 18 \cdot 8$.

Step 3: $18 = 12 \cdot 1 + 6$, which implies that $6 = 18 - 12 \cdot 1$.

Step 4: $12 = 6 \cdot 2 + 0$, which implies that $\gcd(330, 156) = 6$.

Step 5: By substituting back through steps 3 to 1:

$$\begin{aligned}
6 &= 18 - 12 \cdot 1 && \text{from step 3} \\
&= 18 - (156 - 8 \cdot 18) \cdot 1 && \text{by substitution from step 2} \\
&= 9 \cdot 18 + (-1) \cdot 156 && \text{by algebra} \\
&= 9 \cdot (330 - 156 \cdot 2) + (-1) \cdot 156 && \text{by substitution from step 1} \\
&= 9 \cdot 330 + (-19) \cdot 156 && \text{by algebra.}
\end{aligned}$$

Thus $\gcd(330, 156) = 9 \cdot 330 + (-19) \cdot 156$. (It is always a good idea to check the result of a calculation like this to be sure you did not make a mistake. In this case, you find that $9 \cdot 330 + (-19) \cdot 156$ does indeed equal 6.) ■

The Euclidean algorithm given in Section 4.8 can be adapted so as to compute the coefficients of the linear combination of the gcd at the same time as it computes the gcd itself. This extended Euclidean algorithm is described in the exercises at the end of the section.

Finding an Inverse Modulo n

Suppose you want to solve the following congruence for x:

$$2x \equiv 3 \pmod 5$$

Note that $3 \cdot 2 = 6 \equiv 1 \pmod 5$. So you can think of 3 as a kind of inverse for 2 modulo 5 and multiply both sides of the congruence to be solved by 3 to obtain

$$6x = 3 \cdot 2x \equiv 3 \cdot 3 \pmod 5 \equiv 9 \pmod 5 \equiv 4 \pmod 5.$$

But $6 \equiv 1 \pmod 5$, and so by Theorem 8.4.3(3), $6x \equiv 1x \pmod 5 \equiv x \pmod 5$. Thus, by the symmetric and transitive properties of modular congruence,

$$x \equiv 4 \pmod 5,$$

and hence a solution is $x = 4$. (You can check that $2 \cdot 4 = 8 \equiv 3 \pmod 5$.)

Unfortunately, it is not always possible to find an "inverse" modulo an integer n. For instance, observe that

$$2 \cdot 1 \equiv 2 \pmod 4$$
$$2 \cdot 2 \equiv 0 \pmod 4$$
$$2 \cdot 3 \equiv 2 \pmod 4.$$

By Theorem 8.4.3, these calculations suffice for us to conclude that the number 2 does not have an inverse modulo 4.

Describing the circumstances in which inverses exist in modular arithmetic requires the concept of relative primeness.

• Definition

Integers a and b are **relatively prime** if, and only if, $\gcd(a, b) = 1$. Integers $a_1, a_2, a_3, \ldots, a_n$ are **pairwise relatively prime** if, and only if, $\gcd(a_i, a_j) = 1$ for all integers i and j with $1 \le i, j \le n$, and $i \ne j$.

Given the definition of relatively prime integers, the following corollary is an immediate consequence of Theorem 8.4.5.

Corollary 8.4.6

If a and b are relatively prime integers, then there exist integers s and t such that $as + bt = 1$.

Example 8.4.7 Expressing 1 as a Linear Combination of Relatively Prime Integers

Show that 660 and 43 are relatively prime, and find a linear combination of 660 and 43 that equals 1.

Solution

Step 1: Divide 660 by 43 to obtain $660 = 43 \cdot 15 + 15$, which implies that $15 = 660 - 43 \cdot 15$.

Step 2: Divide 43 by 15 to obtain $43 = 15 \cdot 2 + 13$, which implies that $13 = 43 - 15 \cdot 2$.

Step 3: Divide 15 by 13 to obtain $15 = 13 \cdot 1 + 2$, which implies that $2 = 15 - 13$.

Step 4: Divide 13 by 2 to obtain $13 = 2 \cdot 6 + 1$, which implies that $1 = 13 - 2 \cdot 6$.

Step 5: Divide 2 by 1 to obtain $2 = 1 \cdot 2 + 0$, which implies that $\gcd(660, 43) = 1$ and so 660 and 43 are relatively prime.

Step 6: To express 1 as a linear combination of 660 and 43, substitute back through steps 4 to 1:

$$\begin{aligned}
1 &= 13 - 2 \cdot 6 && \text{from step 4} \\
&= 13 - (15 - 13) \cdot 6 && \text{by substitution from step 3} \\
&= 7 \cdot 13 - 6 \cdot 15 && \text{by algebra} \\
&= 7 \cdot (43 - 15 \cdot 2) - 6 \cdot 15 && \text{by substitution from step 2} \\
&= 7 \cdot 43 - 20 \cdot 15 && \text{by algebra} \\
&= 7 \cdot 43 - 20 \cdot (660 - 43 \cdot 15) && \text{by substitution from step 1} \\
&= 307 \cdot 43 - 20 \cdot 660 && \text{by algebra.}
\end{aligned}$$

Thus $\gcd(660, 43) = 1 = 307 \cdot 43 - 20 \cdot 660$. (And a check by direct computation confirms that $307 \cdot 43 - 20 \cdot 660$ does indeed equal 1.) ■

A consequence of Corollary 8.4.6 is that under certain circumstances, it is possible to find an inverse for an integer modulo n.

Corollary 8.4.7 Existence of Inverses Modulo *n*

For all integers a and n, if $\gcd(a, n) = 1$, then there exists an integer s such that $as \equiv 1 \pmod{n}$. The integer s is called the **inverse of a modulo n.**

Proof:

Suppose a and n are integers and $\gcd(a, n) = 1$. By Corollary 8.4.6, there exist integers s and t such that

$$as + nt = 1.$$

Subtracting nt from both sides gives that

$$as = 1 - nt = 1 + (-t)n.$$

Thus, by definition of congruence modulo n,

$$as \equiv 1 \pmod{n}.$$

Example 8.4.8 Finding an Inverse Modulo *n*

a. Find an inverse for 43 modulo 660. That is, find an integer s such that $43s \equiv 1 \pmod{660}$.

b. Find a positive inverse for 3 modulo 40. That is, find a positive integer s such that $3s \equiv 1 \pmod{40}$.

Solution

a. By Example 8.4.7,

$$307 \cdot 43 - 20 \cdot 660 = 1.$$

Adding $20 \cdot 660$ to both sides gives that

$$307 \cdot 43 = 1 + 20 \cdot 660.$$

Thus, by definition of congruence modulo 660,

$$307 \cdot 43 \equiv 1 \pmod{660},$$

so 307 is an inverse for 43 modulo 660.

b. Use the technique of Example 8.4.7 to find a linear combination of 3 and 40 that equals 1.

Step 1: Divide 40 by 3 to obtain $40 = 3 \cdot 13 + 1$. This implies that $1 = 40 - 3 \cdot 13$.

Step 2: Divide 3 by 1 to obtain $3 = 3 \cdot 1 + 0$. This implies that $\gcd(3, 40) = 1$.

Step 3: Use the result of step 1 to write

$$3 \cdot (-13) = 1 + (-1)40.$$

This result implies that -13 is an inverse for 3 modulo 40. In symbols, $3 \cdot (-13) \equiv 1 \pmod{40}$. To find a positive inverse, compute $40 - 13$. The result is 27, and

$$27 \equiv -13 \pmod{40}$$

because $27 - (-13) = 40$. So, by Theorem 8.4.3(3),

$$3 \cdot 27 \equiv 3 \cdot (-13) \equiv 1 \pmod{40},$$

and thus by the transitive property of congruence modulo n, 27 is a positive integer that is an inverse for 3 modulo 40. ■

RSA Cryptography

At this point we have developed enough number theory to explain how to encrypt and decrypt messages using the RSA cipher. The effectiveness of the system is based on the fact that although modern computer algorithms make it quite easy to find two distinct large integers p and q—say on the order of several hundred digits each—that are virtually certain to be prime, even the fastest computers are not currently able to factor their product, an integer with approximately twice that many digits. In order to encrypt a message using the RSA cipher, a person needs to know the value of pq and of another integer e, both of which are made publicly available. But only a person who knows the individual values of p and q can decrypt an encrypted message.

We first give an example to show *how* the cipher works and then discuss some of the theory to explain *why* it works. The example is unrealistic in the sense that because p and q are so small, it would be easy to figure out what they are just by knowing their product. But working with small numbers conveys the idea of the system, while keeping the computations in a range that can be performed with a hand calculator.

Suppose Alice decides to set up an RSA cipher. She chooses two prime numbers, say $p = 5$ and $q = 11$, and computes $pq = 55$. She then chooses a positive integer e that is relatively prime to $(p - 1)(q - 1)$. In this case, $(p - 1)(q - 1) = 4 \cdot 10 = 40$, so she may take $e = 3$ because 3 is relatively prime to 40. (In practice, taking e to be small could compromise the secrecy of the cipher, so she would take a larger number than 3. However, the mathematics of the cipher works as well for 3 as for a larger number, and the smaller number makes for easier calculations.)

The two numbers $pq = 55$ and $e = 3$ are the **public key,** which she may distribute widely. Because the RSA cipher works only on numbers, Alice also informs people how she will interpret the numbers in the messages they send her. Let us suppose that she encodes letters of the alphabet the same way as was done for the Caesar cipher:

$$A = 1, B = 2, C = 3, \ldots, Z = 26.$$

Let us also assume that the messages Alice receives consist of blocks, each of which, for simplicity, is taken to be a single, numerically encoded letter of the alphabet.

Someone who wants to send Alice a message breaks the message into blocks, each consisting of a single letter, and finds the numeric equivalent for each block. The plaintext, M, in a block is converted into ciphertext, C, according to the following formula:

$$C = M^e \ mod \ pq. \tag{8.4.5}$$

Note that because both pq and e are public keys, anyone who is given the keys and knows modular arithmetic can encrypt a message to send to Alice.

Example 8.4.9 Encrypting a Message Using RSA Cryptography

Bob wants to send Alice the message HI. What is the ciphertext for his message?

Solution Bob will send his message in two blocks, one for the H and another for the I. Because H is the eighth letter in the alphabet, it is encoded as 08, or 8. The corresponding ciphertext is computed using formula (8.4.5) as follows:

$$\begin{aligned} C &= 8^3 \ mod \ 55 \\ &= 512 \ mod \ 55 \\ &= 17. \end{aligned}$$

Because I is the ninth letter in the alphabet, it is encoded as 09, or 9. The corresponding ciphertext is

$$\begin{aligned} C &= 9^3 \ mod \ 55 \\ &= 729 \ mod \ 55 \\ &= 14. \end{aligned}$$

Accordingly, Bob sends Alice the message: 17 14. ■

To decrypt the message, Alice needs to compute the decryption key, a number d that is a positive inverse to e modulo $(p - 1)(q - 1)$. She obtains the plaintext M from the ciphertext C by the formula

$$M = C^d \ mod \ pq. \tag{8.4.6}$$

Note that because $M + kpq \equiv M \pmod{pq}$, M must be taken to be less than pq, as in the above example, in order for the decryption to be guaranteed to produce the original message. But because p and q are normally taken to be so large, this requirement does not cause problems. Long messages are broken into blocks of symbols to meet the restriction and several symbols are included in each block to present decryption based on knowledge of letter frequencies.

Example 8.4.10 Decrypting a Message Using RSA Cryptography

Imagine that Alice has hired you to help her decrypt messages and has shared with you the values of p and q. Decrypt the following ciphertext for her: 17 14.

Solution Because $p = 5$ and $q = 11$, $(p-1)(q-1) = 40$, and so you first need to find the decryption key, which is a positive inverse for 3 modulo 40. Knowing that you would be needing this number, we computed it in Example 8.4.8(b) and found it to be 27. Thus you need to compute $M = 17^{27} mod\ 55$. To do so, note that $27 = 16 + 8 + 2 + 1 = 2^4 + 2^3 + 2 + 1$. Thus you will find the residues obtained when 17 is raised to successively higher powers of 2, up to $2^4 = 16$.

$$\begin{aligned}
17\ mod\ 55 &= 17\ mod\ 55 &&= 17\\
17^2\ mod\ 55 &= 17^2\ mod\ 55 &&= 14\\
17^4\ mod\ 55 &= (17^2)^2\ mod\ 55 &&= 14^2\ mod\ 55 &&= 31\\
17^8\ mod\ 55 &= (17^4)^2\ mod\ 55 &&= 31^2\ mod\ 55 &&= 26\\
17^{16}\ mod\ 55 &= (17^8)^2\ mod\ 55 &&= 26^2\ mod\ 55 &&= 16
\end{aligned}$$

Then you will use the fact that

$$17^{27} = 17^{16+8+2+1} = 17^{16} \cdot 17^8 \cdot 17^2 \cdot 17^1$$

to write

$$\begin{aligned}
17^{27}\ mod\ 55 &= (17^{16} \cdot 17^8 \cdot 17^2 \cdot 17)\ mod\ 55\\
&\equiv [(17^{16}\ mod\ 55)(17^8\ mod\ 55)(17^2\ mod\ 55)(17\ mod\ 55)]\ (\text{mod } 55)\\
&\qquad \text{by Corollary 8.4.4}\\
&\equiv (16 \cdot 26 \cdot 14 \cdot 17)\ (\text{mod } 55)\\
&\equiv 99008\ (\text{mod } 55)\\
&\equiv 8\ (\text{mod } 55).
\end{aligned}$$

Hence $17^{27}\ mod\ 55 = 8$, and thus the plaintext of the first part of Bob's message is 8, or 08. In the last step, you find the letter corresponding to 08, which is H. In exercises 14 and 15 at the end of this section, you are asked to show that when you decrypt 14, the result is 9, which corresponds to the letter I, so you can tell Alice that Bob's message is HI. ■

Euclid's Lemma

Another consequence of Theorem 8.4.5 is known as *Euclid's lemma*. It is the crucial fact behind the unique factorization theorem for the integers and is also of great importance in many other parts of number theory.

Theorem 8.4.8 Euclid's Lemma

For all integers a, b, and c, if $\gcd(a, c) = 1$ and $a \mid bc$, then $a \mid b$.

Proof:

Suppose a, b and c are integers, $\gcd(a, c) = 1$, and $a \mid bc$. *[We must show that $a \mid b$.]* By Theorem 8.4.5, there exist integers s and t so that

$$as + ct = 1.$$

Multiply both sides of this equation by b to obtain

$$bas + bct = b. \tag{8.4.7}$$

Since $a \mid bc$, by definition of divisibility there exists an integer k such that

$$bc = ak. \tag{8.4.8}$$

Substituting (8.4.8) into (8.4.7), rewriting, and factoring out an a gives that

$$b = bas + (ak)t = a(bs + kt).$$

Let $r = bs + kt$. Then r is an integer (because b, s, k, and t are all integers), and $b = ar$. Thus $a \mid b$ by definition of divisibility.

The unique factorization theorem for the integers states that any integer greater than 1 has a unique representation as a product of prime numbers, except possibly for the order in which the numbers are written. The hint for exercise 13 of Section 3.4 outlined a proof of the existence part of the proof, and the uniqueness of the representation follows quickly from Euclid's lemma. In exercise 41 at the end of this section, we outline a proof for you to complete.

Another application of Euclid's lemma is a cancellation theorem for congruence modulo n. This theorem allows us—under certain circumstances—to divide out a common factor in a congruence relation.

Theorem 8.4.9 Cancellation Theorem for Modular Congruence

For all integers a, b, c, and n with $n > 1$, if $\gcd(c, n) = 1$ and $ac \equiv bc \pmod{n}$, then $a \equiv b \pmod{n}$.

Proof:

Suppose a, b, c, and n are any integers, $\gcd(c, n) = 1$, and $ac \equiv bc \pmod{n}$. [*We must show that* $a \equiv b \pmod{n}$.] By definition of congruence modulo n,

$$n \mid (ac - bc).$$

and so, since

$$ac - bc = (a - b)c,$$
$$n \mid (a - b)c.$$

Because $\gcd(c, n) = 1$, we may apply Euclid's lemma to obtain

$$n \mid (a - b),$$

and so, by definition of congruence modulo n,

$$a \equiv b \pmod{n}.$$

An alternative proof for Theorem 8.4.9 uses Corollary 8.4.7. Because $\gcd(c, n) = 1$, the corollary guarantees an inverse for c modulo n. In the proof of Theorem 8.4.9, let d denote an inverse for c. Apply Theorem 8.4.3(3) repeatedly, first to multiply both sides of $ac \equiv bc \pmod{n}$ by d to obtain $(ac)d \equiv (bd)d \pmod{n}$, and then to use the fact that $cd \equiv 1 \pmod{n}$ to simplify the congruence and conclude that $a \equiv b \pmod{n}$.

Fermat's Little Theorem

Fermat's little theorem was given that name to distinguish it from Fermat's last theorem, which we discussed in Section 4.1. It provides the theoretical underpinning for RSA cryptography.

Theorem 8.4.10 Fermat's Little Theorem

If p is any prime number and a is any integer such that $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

Proof:

Suppose p is any prime number and a is any integer such that $p \nmid a$. Note that $a \neq 0$ because otherwise p would divide a. Consider the set of integers

$$S = \{a, 2a, 3a, \ldots, (p-1)a\}.$$

We claim that no two elements of S are congruent modulo p. For suppose $sa \equiv ra \pmod{p}$ for some integers s and r with $1 \leq r < s \leq p-1$. Then, by definition of congruence modulo p,

$$p \mid (sa - ra), \quad \text{or, equivalently,} \quad p \mid (s-r)a.$$

Now $p \nmid a$ by hypothesis, and because p is prime, $\gcd(a, p) = 1$. Thus, by Euclid's lemma, $p \mid (s-r)$. But this is impossible because $0 < s - r < p$.

Consider the function F from S to the set $T = \{1, 2, 3, \ldots, (p-1)\}$ that sends each element of S to its residue modulo p. Then F is one-to-one because no two elements of S are congruent modulo p. In Section 9.4 we prove that if a function from one finite set to another is one-to-one, then it is also onto. Hence F is onto, and so the $p-1$ residues of the $p-1$ elements of S are exactly the numbers $1, 2, 3, \ldots, (p-1)$.

It follows by Theorem 8.4.3(3) that

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv [1 \cdot 2 \cdot 3 \cdots (p-1)] \pmod{p},$$

or equivalently,

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}.$$

But because p is prime, p and $(p-1)!$ are relatively prime. Thus, by the cancellation theorem for modular congruence (Theorem 8.4.9),

$$a^{p-1} \equiv 1 \pmod{p}.$$

Why Does the RSA Cipher Work?

For the RSA cryptography method, the formula

$$M = C^d \bmod pq$$

is supposed to produce the original plaintext message, M, when the encrypted message is C. How can we be sure that it always does so? Recall that we require that $M < pq$, and we know that $C = M^e \bmod pq$. So, by substitution,

$$C^d \bmod pq = (M^e \bmod pq)^d \bmod pq.$$

By Theorem 8.4.3(4),

$$(M^e \bmod pq)^d \equiv M^{ed} \pmod{pq}.$$

Thus $C^d \ mod \ pq \equiv M^{ed} (\text{mod } pq)$, and so it suffices to show that

$$M \equiv M^{ed} \ (\text{mod } pq).$$

Recall that d was chosen to be a positive inverse for e modulo $(p-1)(q-1)$, which exists because $\gcd(e, (p-1)(q-1)) = 1$. In other words,

$$ed \equiv 1 \ (\text{mod } (p-1)(q-1)),$$

or, equivalently,

$$ed = 1 + k(p-1)(q-1) \quad \text{for some positive integer } k.$$

Therefore,

$$M^{ed} = M^{1+k(p-1)(q-1)} = M(M^{p-1})^{k(q-1)} = M(M^{q-1})^{k(p-1)}$$

If $p \nmid M$, then by Fermat's little theorem, $M^{p-1} \equiv 1 \ (\text{mod } p)$, and so

$$M^{ed} = M(M^{p-1})^{k(q-1)} \equiv M(1)^{k(q-1)} \ (\text{mod } p) = M \ (\text{mod } p).$$

Similarly, if $q \nmid M$, then by Fermat's little theorem, $M^{q-1} \equiv 1 \ (\text{mod } q)$, and so

$$M^{ed} = M(M^{q-1})^{k(p-1)} \equiv M(1)^{k(p-1)} = M \ (\text{mod } q).$$

Thus, if M is relatively prime to pq,

$$M^{ed} \equiv M \ (\text{mod } p) \quad \text{and} \quad M^{ed} \equiv M \ (\text{mod } q).$$

If M is not relatively prime to pq, then either $p \mid M$ or $q \mid M$. Without loss of generality, assume $p \mid M$. It follows that $M^{ed} \equiv 0 \equiv M \ (mod \ p)$. Moreover, because $M < pq$, $q \mid M$, and thus, as above, $M^{ed} \equiv M \ (mod \ q)$. Therefore, in this case also,

$$M^{ed} \equiv M \ (mod \ p) \quad \text{and} \quad M^{ed} \equiv M \ (mod \ q).$$

By Theorem 8.4.1,

$$p \mid (M^{ed} - M) \quad \text{and} \quad q \mid (M^{ed} - M),$$

and, by definition of divisibility,

$$M^{ed} - M = pt \text{ for some integer } t.$$

By substitution, $$q \mid pt,$$

and since q and p are distinct prime numbers, Euclid's lemma applies to give

$$q \mid t.$$

Thus $$t = qu \text{ for some integer } u$$

by definition of divisibility. By substitution,

$$M - M^{ed} = pt = p(qu) = (pq)u,$$

where u is an integer, and so,

$$pq \mid (M - M^{ed})$$

by definition of divisibility. Thus

$$M - M^{ed} \equiv 0 \ (\text{mod } pq)$$

by definition of congruence, or, equivalently,

$$M \equiv M^{ed} (\text{mod } pq).$$

Because $M < pq$, this last congruence implies that

$$M = M^{ed} \ mod \ pq,$$

and thus the RSA cipher gives the correct result.

Additional Remarks on Number Theory and Cryptography

The famous British mathematician G. H. Hardy (1877–1947) was fond of comparing the beauty of pure mathematics, especially number theory, to the beauty of art. Indeed, the theorems in this section have many beautiful and striking consequences beyond those we have had the space to describe, and the subject of number theory extends far beyond these theorems. Hardy also enjoyed describing pure mathematics as useless. Hence it is ironic that there are now whole books devoted to applications of number theory to computer science, RSA cryptography being just one such application. Furthermore, as the need for public-key cryptography has developed, techniques from other areas of mathematics, such as abstract algebra and algebraic geometry, have been used to develop additional cryptosystems.

Test Yourself

1. When letters of the alphabet are encrypted using the Caesar cipher, the encrypted version of a letter is _____.
2. If a, b, and n are integers with $n > 1$, all of the following are different ways to express the fact that $n \mid (a - b)$: _____, _____, _____, _____.
3. If a, b, c, d, m, and n are integers with $n > 1$ and if $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$, then $a + b \equiv$ _____, $a - b \equiv$ _____, $ab \equiv$ _____, and $a^m \equiv$ _____.
4. If a, n, and k are positive integers with $n > 1$, an efficient way to compute $a^k \pmod{n}$ is to write k as a _____ and use the facts about computing products and powers modulo n.
5. To express a greatest common divisor of two integers as a linear combination of the integers, use the extended _____ algorithm.
6. To find an inverse for a positive integer a modulo an integer n with $n > 1$, you express the number 1 as _____.
7. To encrypt a message M using RSA cryptography with public key pq and e, you use the formula _____, and to decrypt a message C, you use the formula _____, where _____.
8. Euclid's lemma says that for all integers a, b, and c if $\gcd(a, c) = 1$ and $a \mid bc$, then _____.
9. Format's little theorem says that if p is any prime number and a is any integer such that $p \mid a$ then _____.
10. The crux of the proof that the RSA cipher works is that if (1) p and q are distinct large prime numbers, (2) $M < pq$, (3) M is relatively prime to pq, (4) e is relatively prime to $(p - 1)(q - 1)$, and (5) d is a positive inverse for e modulo $(p - 1)(q - 1)$, then $M =$ _____.

Exercise Set 8.4

1. a. Use the Caesar cipher to encrypt the message WHERE SHALL WE MEET.
   b. Use the Caesar cipher to decrypt the message LQ WKH FDIHWHULD.

2. a. Use the Caesar cipher to encrypt the message AN APPLE A DAY.
   b. Use the Caesar cipher to decrypt the message NHHSV WKH GRFWRU DZDB.

3. Let $a = 25$, $b = 19$, and $n = 3$.
   a. Verify that $3 \mid (25 - 19)$.
   b. Explain why $25 \equiv 19 \pmod{3}$.
   c. What value of k has the property that $25 = 19 + 3k$?

d. What is the (nonnegative) remainder obtained when 25 is divided by 3? When 19 is divided by 3?
e. Explain why $25 \textit{ mod } 3 = 19 \textit{ mod } 3$.

4. Let $a = 67$, $b = 32$, and $n = 7$.
a. Verify that $7 \mid (68 - 33)$.
b. Explain why $68 \equiv 33 \pmod 7$.
c. What value of k has the property that $68 = 33 + 7k$?
d. What is the (nonnegative) remainder obtained when 68 is divided by 7? When 33 is divided by 7?
e. Explain why $68 \textit{ mod } 7 = 33 \textit{ mod } 7$.

5. Prove the transitivity of modular congruence. That is, prove that for all integers a, b, c, and n with $n > 1$, if $a \equiv b \pmod n$ and $b \equiv c \pmod n$ then $a \equiv c \pmod n$.

***H* 6.** Prove that the distinct equivalence classes of the relation of congruence modulo n are the sets $[0], [1], [2], \ldots, [n-1]$, where for each $a = 0, 1, 2, \ldots, n-1$,

$$[a] = \{m \in Z \mid m \equiv a \pmod n\}.$$

7. Verify the following statements.
a. $128 \equiv 2 \pmod 7$ and $61 \equiv 5 \pmod 7$
b. $(128 + 61) \equiv (2 + 5) \pmod 7$
c. $(128 - 61) \equiv (2 - 5) \pmod 7$
d. $(128 \cdot 61) \equiv (2 \cdot 5) \pmod 7$
e. $128^2 \equiv 2^2 \pmod 7$

8. Verify the following statements.
a. $45 \equiv 3 \pmod 6$ and $104 \equiv 2 \pmod 6$
b. $(45 + 104) \equiv (3 + 2) \pmod 6$
c. $(45 - 104) \equiv (3 - 2) \pmod 6$
d. $(45 \cdot 104) \equiv (3 \cdot 2) \pmod 6$
e. $45^2 \equiv 3^2 \pmod 6$

In 9–11, prove each of the given statements, assuming that a, b, c, d, and n are integers with $n > 1$ and that $a \equiv c \pmod n$ and $b \equiv d \pmod n$.

9. **a.** $(a + b) \equiv (c + d) \pmod n$
b. $(a - b) \equiv (c - d) \pmod n$

10. $a^2 \equiv c^2 \pmod n$

11. $a^m \equiv c^m \pmod n$ for all integers $m \geq 1$ (Use mathematical induction on m.)

12. **a.** Prove that for all integers $n \geq 0$, $10^n \equiv 1 \pmod 9$.
b. Use part (a) to prove that a positive integer is divisible by 9 if, and only if, the sum of its digits is divisible by 9.

13. a. Prove that for all integers $n \geq 1$, $10^n \equiv (-1)^n \pmod{11}$.
b. Use part (a) to prove that a positive integer is divisible by 11 if, and only if, the alternating sum of its digits is divisible by 11. (For instance, the alternating sum of the digits of 82,379 is $8 - 2 + 3 - 7 + 9 = 11$ and $82{,}379 = 11 \cdot 7489$.)

14. Use the technique of Example 8.4.4 to find $14^2 \textit{ mod } 55$, $14^4 \textit{ mod } 55$, $14^8 \textit{ mod } 55$, and $14^{16} \textit{ mod } 55$.

15. Use the result of exercise 14 and the technique of Example 8.4.5 to find $14^{27} \textit{ mod } 55$.

In 16–18, use the techniques of Example 8.4.4 and Example 8.4.5 to find the given numbers.

16. $675^{307} \textit{ mod } 713$ 17. $89^{307} \textit{ mod } 713$

18. $48^{307} \textit{ mod } 713$

In 19–24, use the RSA cipher from Examples 8.4.9 and 8.4.10. In 19–21, translate the message into its numeric equivalent and encrypt it. In 22–24, decrypt the ciphertext and translate the result into letters of the alphabet to discover the message.

19. HELLO 20. WELCOME 21. EXCELLENT

22. 13 20 20 09 23. 08 05 15 24. 51 14 49 15

***H* 25.** Use Theorem 5.2.3 to prove that if a and n are positive integers and $a^n - 1$ is prime, then $a = 2$ and n is prime.

In 26 and 27, use the extended Euclidean algorithm to find the greatest common divisor of the given numbers and express it as a linear combination of the two numbers.

26. 6664 and 765 27. 4158 and 1568

Exercises 28 and 29 refer to the following formal version of the extended Euclidean algorithm.

Algorithm 8.4.1 Extended Euclidean Algorithm

[Given integers A and B with $A > B > 0$, this algorithm computes gcd(A, B) *and finds integers s and t such that $sA + tB =$* gcd(A, B).*]*

Input: A, B *[integers with $A > B > 0$]*

Algorithm Body:

$a := A, b := B, s := 1, t := 0, u := 0, v := 1$,
[pre-condition: $a = sA + tB$ and $b = uA + vB$]

while $(b \neq 0)$

[loop invariant: $a = sA + tB$ and $b = uA + vB$, $gcd(a, b) = gcd(A, B)$]

$r := a \textit{ mod } b, q := a \textit{ div } b$

$a := b, b := r$

$newu := s - uq, newv := t - vq$

$s := u, t := v$

$u := newu, v := newv$

end while

gcd $:= a$

[post-condition: $gcd(A, B) = a = sA + tB$]

Output: gcd*[a positive integer]*, s, t *[integers]*

In 28 and 29, for the given values of A and B, make a table showing the value of s, t, and $sA + tB$ before the start of the **while** loop and after each iteration of the loop.

28. $A = 330, B = 156$ 29. $A = 284, B = 168$

30. Finish the proof of Theorem 8.4.5 by proving that if a, b and c are as in the proof, then $c \mid b$.

31. a. Find an inverse for 210 modulo 13.
b. Find a positive inverse for 210 modulo 13.
c. Find a positive solution for the congruence $210x \equiv 8 \pmod{13}$.

32. a. Find an inverse for 41 modulo 660.
b. Find the least positive solution for the following congruence: $41x \equiv 125 \pmod{660}$.

***H* 33.** Use Theorem 8.4.5 to prove that for all integers a, b, and c, if $\gcd(a, b) = 1$ and $a \mid c$ and $b \mid c$, then $ab \mid c$.

34. Give a counterexample to show that the converse of exercise 33 is false.

35. Corollary 8.4.7 guarantees the existence of an inverse modulo n for an integer a when a and n are relatively prime. Use Euclid's lemma to prove that the inverse is unique modulo n. In other words, show that any two integers whose product with a is congruent to 1 modulo n are congruent to each other modulo n.

In 36, 37, 39, and 40, use the RSA cipher with public key $n = 713 = 23 \cdot 31$ and $e = 43$. In 36 and 37, encode the messages into their numeric equivalents and encrypt them. In 39 and 40, decrypt the given ciphertext and find the original messages.

36. HELP

37. COME

38. Find the least positive inverse for 43 modulo 660.

39. 675 089 089 048

40. 028 018 675 129

***H* 41. a.** Use mathematical induction and Euclid's lemma to prove that for all positive integers s, if p and $q_1, q_2, \ldots, q_s$ are prime numbers and $p \mid q_1 q_2 \cdots q_s$, then $p = q_i$ for some i with $1 \le i \le s$.

b. The uniqueness part of the unique factorization theorem for the integers says that given any integer n, if

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

for some positive integers r and s and prime numbers $p_1 \le p_2 \le \cdots \le p_r$ and $q_1 \le q_2 \le \cdots \le q_s$, then $r = s$ and $p_i = q_i$ for all integers i with $1 \le i \le r$.

Use the result of part (a) to fill in the details of the following sketch of a proof: Suppose that n is an integer with two different prime factorizations: $n = p_1 p_2 \cdots p_t = q_1 q_2 \cdots q_u$. All the prime factors that appear on both sides can be cancelled (as many times as they appear on both sides) to arrive at the situation where $p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$, $p_1 \le p_2 \le \cdots \le p_r$, $q_1 \le q_2 \le \cdots \le q_s$, and $p_i \ne q_j$ for any integers i and j. Then use part (a) to deduce a contradiction, and so the prime factorization of n is unique except, possibly, for the order in which the prime factors are written.

42. According to Fermat's little theorem, if p is a prime number and a and p are relatively prime, then $a^{p-1} \equiv 1 \pmod{p}$. Verify that this theorem gives correct results for
a. $a = 15$ and $p = 7$ b. $a = 8$ and $p = 11$

43. Fermat's little theorem can be used to show that a number is not prime by finding a number a relatively prime to p with the property that $a^{p-1} \not\equiv 1 \pmod{p}$. However, it cannot be used to show that a number *is* prime. Find an example to illustrate this fact. That is, find integers a and p such that a and p are relatively prime and $a^{p-1} \equiv 1 \pmod{p}$ but p is not prime.

Answers for Test Yourself

1. three places in the alphabet to the right of the letter, with X wrapped around to A, Y to B, and Z to C 2. $a \equiv b \pmod{n}$; $a = b + kn$ for some integer k; a and b have the same nonnegative remainder when divided by n; $a \bmod n = b \bmod n$ 3. $(c + d) \pmod{n}$; $(c - d) \pmod{n}$; $(cd) \pmod{n}$; $c^m \pmod{n}$ 4. sum of powers of 2 5. version of the Euclidean 6. a linear combination of a and n 7. $C = M^c \bmod pq$; $M = C^d \bmod pq$; d is a positive inverse for e modulo $(p - 1)(q - 1)$ 8. $a \mid b$ 9. $a^{p-1} \equiv 1 \pmod{p}$ 10. $M^{ed} \bmod pq$

8.5 Partial Order Relations

There is no branch of mathematics, however abstract, which may not some day be applied to phenomena of the real world. — Nicolai Ivanovitch Lobachevsky, 1792–1856

In order to obtain a degree in computer science at a certain university, a student must take a specified set of required courses, some of which must be completed before others can be started. Given the prerequisite structure of the program, one might ask what is the least number of school terms needed to fulfill the degree requirements, or what is the maximum number of courses that can be taken in the same term, or whether there is a sequence in which a part-time student can take the courses one per term. Later in this section, we will show how representing the prerequisite structure of the program as a partial order relation makes it relatively easy to answer such questions.