CHAPTER 2

Mathematics of Cryptography

Part I: Modular Arithmetic, Congruence, and Matrices

Objectives

This chapter is intended to prepare the reader for the next few chapters in cryptography. The chapter has several objectives:

- ❏ To review integer arithmetic, concentrating on divisibility and finding the greatest common divisor using the Euclidean algorithm
- ❏ To understand how the extended Euclidean algorithm can be used to solve linear Diophantine equations, to solve linear congruent equations, and to find the multiplicative inverses
- ❏ To emphasize the importance of modular arithmetic and the modulo operator, because they are extensively used in cryptography
- ❏ To emphasize and review matrices and operations on residue matrices that are extensively used in cryptography
- ❏ To solve a set of congruent equations using residue matrices

Cryptography is based on some specific areas of mathematics, including number theory, linear algebra, and algebraic structures. In this chapter, we discuss only the topics in the above areas that are needed to understand the contents of the next few chapters. Readers who are familiar with these topics can skip this chapter entirely or partially. Similar chapters are provided throughout the book when needed. Proofs of theorems and algorithms have been omitted, and only their applications are shown. The interested reader can find proofs of the theorems and algorithms in Appendix P.

Proofs of theorems and algorithms discussed in this chapter can be found in Appendix P.

2.1 INTEGER ARITHMETIC

In **integer arithmetic,** we use a set and a few operations. You are familiar with this set and the corresponding operations, but they are reviewed here to create a background for modular arithmetic.

Set of Integers

The **set of integers,** denoted by **Z,** contains all integral numbers (with no fraction) from negative infinity to positive infinity (Figure 2.1).

Figure 2.1 *The set of integers*

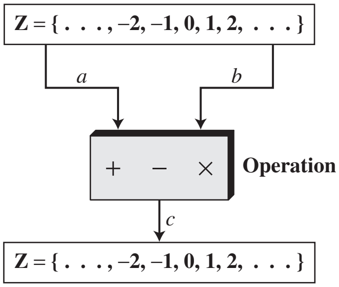
$$\mathbf{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

Binary Operations

In cryptography, we are interested in three binary operations applied to the set of integers. A **binary operation** takes two inputs and creates one output. Three common binary operations defined for integers are *addition, subtraction,* and *multiplication*. Each of these operations takes two inputs (a and b) and creates one output (c) as shown in Figure 2.2. The two inputs come from the set of integers; the output goes into the set of integers.

Note that *division* does not fit in this category because, as we will see shortly, it produces two outputs instead of one.

Figure 2.2 *Three binary operations for the set of integers*


Z = { . . . , –2, –1, 0, 1, 2, . . . }
a
b
+ – ×
Operation
c
Z = { . . . , –2, –1, 0, 1, 2, . . . }

Example 2.1

The following shows the results of the three binary operations on two integers. Because each input can be either positive or negative, we can have four cases for each operation.

Add:	$5 + 9 = 14$	$(-5) + 9 = 4$	$5 + (-9) = -4$	$(-5) + (-9) = -14$
Subtract:	$5 - 9 = -4$	$(-5) - 9 = -14$	$5 - (-9) = 14$	$(-5) - (-9) = +4$
Multiply:	$5 \times 9 = 45$	$(-5) \times 9 = -45$	$5 \times (-9) = -45$	$(-5) \times (-9) = 45$

Integer Division

In integer arithmetic, if we divide a by n, we can get q and r. The relationship between these four integers can be shown as

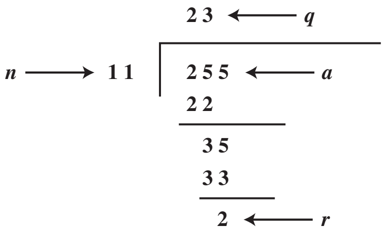
$$a = q \times n + r$$

In this relation, a is called the *dividend; q*, the *quotient; n*, the *divisor;* and r, the *remainder*. Note that this is not an operation, because the result of dividing a by n is two integers, q and r. We can call it *division relation*.

Example 2.2

Assume that $a = 255$ and $n = 11$. We can find $q = 23$ and $r = 2$ using the division algorithm we have learned in arithmetic as shown in Figure 2.3.

Figure 2.3 *Example 2.2, finding the quotient and the remainder*

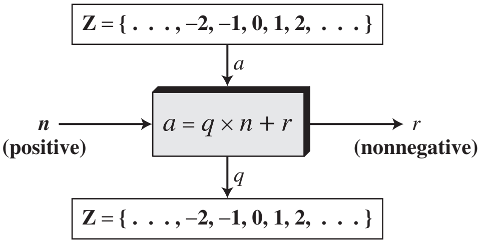


Most computer languages can find the quotient and the remainder using language-specific operators. For example, in the C language, the operator / can find the quotient and the operator % can find the remainder.

Two Restrictions

When we use the above division relationship in cryptography, we impose two restrictions. First, we require that the divisor be a positive integer ($n > 0$). Second, we require that the remainder be a nonnegative integer ($r \geq 0$). Figure 2.4 shows this relationship with the two above-mentioned restrictions.

Figure 2.4 *Division algorithm for integers*


Z = { . . . , –2, –1, 0, 1, 2, . . . }
a
n
(positive)
a = q × n + r
r
(nonnegative)
q
Z = { . . . , –2, –1, 0, 1, 2, . . . }

Example 2.3

When we use a computer or a calculator, r and q are negative when a is negative. How can we apply the restriction that r needs to be positive? The solution is simple, we decrement the value of q by 1 and we add the value of n to r to make it positive.

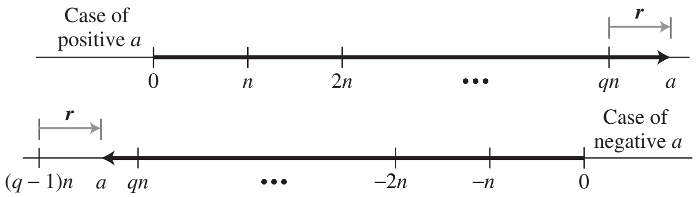
$$-255 = (-\mathbf{23} \times 11) + (-\mathbf{2}) \qquad \leftrightarrow \qquad -255 = (-\mathbf{24} \times 11) + \mathbf{9}$$

We have decremented −23 to become −24 and added 11 to −2 to make it 9. The above relation is still valid.

The Graph of the Relation

We can show the above relation with the two restrictions on n and r using two graphs in Figure 2.5. The first one shows the case when a is positive; the second when a is negative.

Figure 2.5 *Graph of division algorithm*



Starting from zero, the graph shows how we can reach the point representing the integer a on the line. In case of a positive a, we need to move $q \times n$ units to the right and then move extra r units in the same direction. In case of a negative a, we need to move $(q-1) \times n$ units to the left (q is negative in this case) and then move r units in the opposite direction. In both cases the value of r is positive.

Divisibility

Let us briefly discuss **divisibility,** a topic we often encounter in cryptography. If a is not zero and we let $r = 0$ in the division relation, we get

$$\boldsymbol{a = q \times n}$$

We then say that n divides a (or n is a divisor of a). We can also say that a is divisible by n. When we are not interested in the value of q, we can write the above relationship as $\boldsymbol{a|n}$. If the remainder is not zero, then n does not divide a and we can write the relationship as $\boldsymbol{a \nmid n}$.

Example 2.4

a. The integer 4 divides the integer 32 because $\mathbf{32} = 8 \times \mathbf{4}$. We show this as $4|32$.
b. The number 8 does not divide the number 42 because $\mathbf{42} = 5 \times \mathbf{8} + 2$. There is a remainder, the number 2, in the equation. We show this as $8 \nmid 42$.

Example 2.5

a. We have $13|78$, $7|98$, $-6|24$, $4|44$, and $11|(-33)$.

b. We have $13 \nmid 27$, $7 \nmid 50$, $-6 \nmid 23$, $4 \nmid 41$, and $11 \nmid (-32)$.

Properties

Following are several properties of divisibility. The interested reader can check Appendix P for proofs.

Property 1: if $a|1$, then $a = \pm 1$.
Property 2: if $a|b$ and $b|a$, then $a = \pm b$.
Property 3: if $a|b$ and $b|c$, then $a|c$.
Property 4: if $a|b$ and $a|c$, then $a|(m \times b + n \times c)$, where m and n are arbitrary integers.

Example 2.6

a. Since $3|15$ and $15|45$, according to the third property, $3|45$.

b. Since $3|15$ and $3|9$, according to the fourth property, $3|(15 \times 2 + 9 \times 4)$, which means $3|66$.

All Divisors

A positive integer can have more than one divisor. For example, the integer 32 has six divisors: 1, 2, 4, 8, 16, and 32. We can mention two interesting facts about divisors of positive integers:

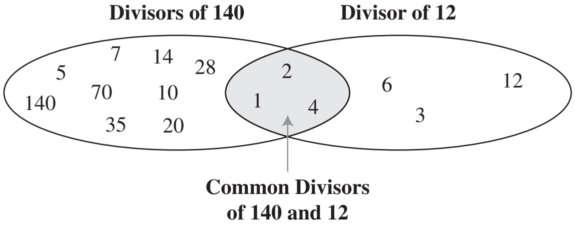
Fact 1: The integer 1 has only one divisor, itself.

Fact 2: Any positive integer has at least two divisors, 1 and itself (but it can have more).

Greatest Common Divisor

One integer often needed in cryptography is the **greatest common divisor** of two positive integers. Two positive integers may have many common divisors, but only one greatest common divisor. For example, the common divisors of 12 and 140 are 1, 2, and 4. However, the greatest common divisor is 4. See Figure 2.6.

Figure 2.6 *Common divisors of two integers*



The greatest common divisor of two positive integers is the largest integer that can divide both integers.

Euclidean Algorithm

Finding the greatest common divisor (gcd) of two positive integers by listing all common divisors is not practical when the two integers are large. Fortunately, more than 2000 years ago a mathematician named Euclid developed an algorithm that can find the greatest common divisor of two positive integers. The **Euclidean algorithm** is based on the following two facts (see Appendix P for the proof):

Fact 1: gcd $(a, 0) = a$

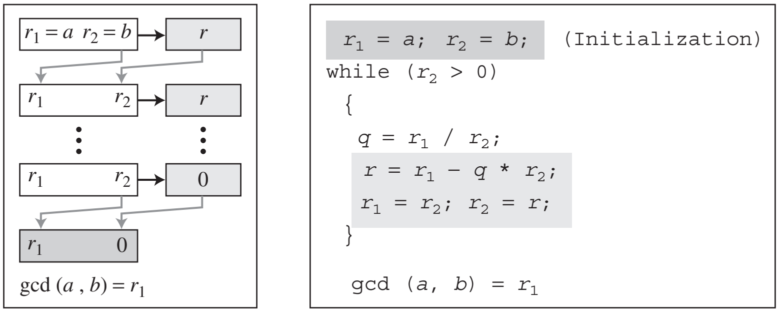
Fact 2: gcd $(a, b) =$ gcd (b, r), where r is the remainder of dividing a by b

The first fact tells us that if the second integer is 0, the greatest common divisor is the first one. The second fact allows us to change the value of a, b until b becomes 0. For example, to calculate the gcd (36, 10), we can use the second fact several times and the first fact once, as shown below.

gcd (36, 10) = gcd (10, 6) = gcd (6, 4) = gcd (4, 2) = gcd (2, 0) = 2

In other words, gcd (36, 10) = 2, gcd (10, 6) = 2, and so on. This means that instead of calculating gcd (36, 10), we can find gcd (2, 0). Figure 2.7 shows how we use the above two facts to calculate gcd (a, b).

Figure 2.7 *Euclidean algorithm*



```
r₁ = a;  r₂ = b;    (Initialization)
while (r₂ > 0)
 {
   q = r₁ / r₂;
    r = r₁ − q * r₂;
    r₁ = r₂;  r₂ = r;
 }

  gcd (a, b) = r₁
```

a. Process b. Algorithm

We use two variables, r_1 and r_2, to hold the changing values during the process of reduction. They are initialized to a and b. In each step, we calculate the remainder of r_1 divided by r_2 and store the result in the variable r. We then replace r_1 by r_2 and r_2 by r. The steps are continued until r_2 becomes 0. At this moment, we stop. The gcd (a, b) is r_1.

When gcd (a, b) = 1, we say that a and b are relatively prime.

Find the greatest common divisor of 2740 and 1760.

Solution

We apply the above procedure using a table. We initialize r_1 to 2740 and r_2 to 1760. We have also shown the value of q in each step. We have gcd (2740, 1760) = 20.

q	r_1	r_2	r
1	2740	1760	980
1	1760	980	780
1	980	780	200
3	780	200	180
1	200	180	20
9	180	20	0
	20	0	

Example 2.7

Find the greatest common divisor of 25 and 60.

Solution

We chose this particular example to show that it does not matter if the first number is smaller than the second number. We immediately get our correct ordering. We have gcd (25, 65) = 5.

q	r_1	r_2	r
0	25	60	25
2	60	25	10
2	25	10	5
2	10	5	0
	5	0	

The Extended Euclidean Algorithm

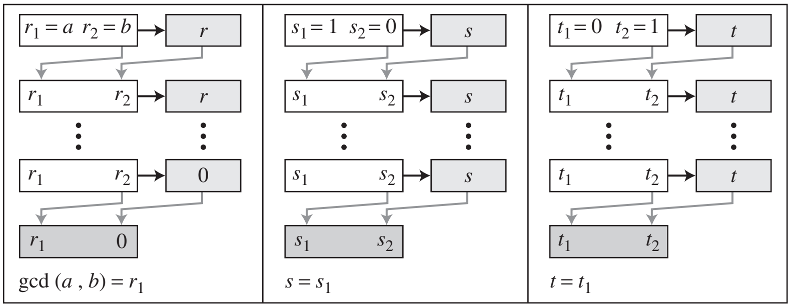
Given two integers a and b, we often need to find other two integers, s and t, such that

$$s \times a + t \times b = \text{gcd}\ (a, b)$$

The **extended Euclidean algorithm** can calculate the gcd (a, b) and at the same time calculate the value of s and t. The algorithm and the process is shown in Figure 2.8.

As shown in Figure 2.8, the extended Euclidean algorithm uses the same number of steps as the Euclidean algorithm. However, in each step, we use three sets of calculations and exchanges instead of one. The algorithm uses three sets of variables, r's, s's, and t's.

Figure 2.8 *Extended Euclidean algorithm*



a. Process

```
$r_1 = a;$   $r_2 = b;$
$s_1 = 1;$   $s_2 = 0;$     (Initialization)
$t_1 = 0;$   $t_2 = 1;$
while ($r_2 > 0$)
 {
  $q = r_1 / r_2;$
    $r = r_1 - q * r_2;$
    $r_1 = r_2;$   $r_2 = r;$        (Updating $r$'s)
    $s = s_1 - q * s_2;$
    $s_1 = s_2;$   $s_2 = s;$        (Updating $s$'s)
    $t = t_1 - q * t_2;$
    $t_1 = t_2;$   $t_2 = t;$        (Updating $t$'s)
 }
  gcd ($a$ , $b$) = $r_1$   $s = s_1$   $t = t_1$
```

b. Algorithm

In each step, r_1, r_2, and r have the same values in the Euclidean algorithm. The variables r_1 and r_2 are initialized to the values of a and b, respectively. The variables s_1 and s_2 are initialized to 1 and 0, respectively. The variables t_1 and t_2 are initialized to 0 and 1, respectively. The calculations of r, s, and t are similar, with one warning. Although r is the remainder of dividing r_1 by r_2, there is no such relationship between the other two sets. There is only one quotient, q, which is calculated as $r_1|r_2$ and used for the other two calculations.

Example 2.8

Given $a = 161$ and $b = 28$, find gcd (a, b) and the values of s and t.

Solution

$$r = r_1 - q \times r_2 \qquad s = s_1 - q \times s_2 \qquad t = t_1 - q \times t_2$$

We use a table to follow the algorithm.

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
5	161	28	21	1	0	1	0	1	−5
1	28	21	7	0	1	−1	1	−5	6
3	21	7	0	1	−1	4	−5	6	−23
	7	0		**−1**	4		**6**	−23	

We get gcd (161, 28) = 7, $s = -1$ and $t = 6$. The answers can be tested because we have

$$(-1) \times 161 + 6 \times 28 = 7$$

Example 2.9

Given $a = 17$ and $b = 0$, find gcd (a, b) and the values of s and t.

Solution

We use a table to follow the algorithm.

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
	17	0		**1**	**0**		**0**	**1**	

Note that we need no calculation for q, r, and s. The first value of r_2 meets our termination condition. We get gcd (17, 0) = 17, $s = 1$, and $t = 0$. This indicates why we should initialize s_1 to 1 and t_1 to 0. The answers can be tested as shown below:

$$(1 \times 17) + (0 \times 0) = 17$$

Example 2.10

Given $a = 0$ and $b = 45$, find gcd (a, b) and the values of s and t.

Solution

We use a table to follow the algorithm.

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
0	0	45	0	1	0	1	0	1	0
	45	0		0	1		**1**	0	

We get gcd (0, 45) = 45, $s = 0$, and $t = 1$. This indicates why we should initialize s_2 to 0 and t_2 to 1. The answer can be tested as shown below:

$$(0 \times 0) + (1 \times 45) = 45$$

Linear Diophantine Equations

Although we will see a very important application of the extended Euclidean algorithm in the next section, one immediate application is to find the solutions to the **linear Diophantine equations** of two variables, an equation of type $ax + by = c$. We need to find integer values for x and y that satisfy the equation. This type of equation has either no solution or an infinite number of solutions. Let $d = \gcd(a, b)$. If $d \nmid c$, then the equation has no solution. If $d | c$, then we have an infinite number of solutions. One of them is called the particular; the rest, general.

A linear Diophantine equation of two variables is $ax + by = c$.

Particular Solution

If d|c, a particular solution to the above equation can be found using the following steps:

1. Reduce the equation to $a_1x + b_1y = c_1$ by dividing both sides of the equation by d. This is possible because d divides a, b, and c by the assumption.
2. Solve for s and t in the relation $a_1s + b_1t = 1$ using the extended Euclidean algorithm.
3. The particular solution can be found:

Particular solution: $x_0 = (c/d)s$ ***and*** $y_0 = (c/d)t$

General Solutions

After finding the particular solution, the general solutions can be found:

General solutions: $x = x_0 + k\,(b/d)$ ***and*** $y = y_0 - k\,(a/d)$ **where** $k = 0, 1, 2, \ldots$

Example 2.11

Find the particular and general solutions to the equation $21x + 14y = 35$.

Solution

We have $d = \gcd(21, 7) = 7$. Since $7|35$, the equation has an infinite number of solutions. We can divide both sides by 7 to find the equation $3x + 2y = 5$. Using the extended Euclidean algorithm, we find s and t such as $3s + 2t = 1$. We have $s = 1$ and $t = -1$. The solutions are

Particular: $x_0 = 5 \times 1 = 5$ and $y_0 = 5 \times (-1) = -5$ since $35/7 = 5$
General: $x = 5 + k \times 2$ and $y = -5 - k \times 3$ where $k = 0, 1, 2, \ldots$

Therefore, the solutions are (5, −5), (7, −8), (9, −11), . . . We can easily test that each of these solutions satisfies the original equation.

Example 2.12

A very interesting application in real life is when we want to find different combinations of objects having different values. For example, imagine we want to cash a \$100 check and get some \$20 and some \$5 bills. We have many choices, which we can find by solving the corresponding Diophantine equation $20x + 5y = 100$. Since $d = \gcd(20, 5) = 5$ and $5|100$, the equation has an infinite number of solutions, but only a few of them are acceptable in this case (only answers in which both x and y are nonnegative integers). We divide both sides by 5 to get $4x + y = 20$. We then solve the equation $4s + t = 1$. We can find $s = 0$ and $t = 1$ using the extended Euclidean algorithm. The particular solutions are $x_0 = 0 \times 20 = 0$ and $y_0 = 1 \times 20 = 20$. The general solutions with x and y nonnegative are (0, 20), (1, 16), (2, 12), (3, 8), (4, 4), (5, 0). The rest of the solutions are not acceptable because y becomes negative. The teller at the bank needs to ask which of the above combinations we want. The first has no \$20 bills; the last has no \$5 bills.

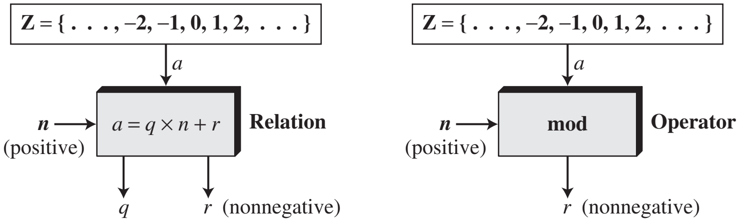
2.2 MODULAR ARITHMETIC

The division relationship ($a = q \times n + r$) discussed in the previous section has two inputs (a and n) and two outputs (q and r). In **modular arithmetic,** we are interested in only one of the outputs, the remainder r. We don't care about the quotient q. In other words, we want to know what is the value of r when we divide a by n. This implies that we can change the above relation into a binary operator with two inputs a and n and one output r.

Modulo Operator

The above-mentioned binary operator is called the **modulo operator** and is shown as *mod*. The second input (n) is called the **modulus.** The output r is called the **residue.** Figure 2.9 shows the division relation compared with the modulo operator.

Figure 2.9 *Division relation and modulo operator*



As Figure 2.9 shows, the modulo operator (**mod**) takes an integer (a) from the set **Z** and a positive modulus (n). The operator creates a nonnegative residue (r). We can say

$$a \bmod n = r$$

Example 2.13

Find the result of the following operations:

a. 27 mod 5
b. 36 mod 12
c. −18 mod 14
d. −7 mod 10

Solution

We are looking for the residue r. We can divide the a by n and find q and r. We can then disregard q and keep r.

a. Dividing 27 by 5 results in $r = 2$. This means that 27 mod 5 = 2.

b. Dividing 36 by 12 results in $r = 0$. This means that 36 mod 12 = 0.

c. Dividing −18 by 14 results in $r = -4$. However, we need to add the modulus (14) to make it nonnegative. We have $r = -4 + 14 = 10$. This means that −18 mod 14 = 10.

d. Dividing −7 by 10 results in $r = -7$. After adding the modulus to −7, we have $r = 3$. This means that −7 mod 10 = 3.

Set of Residues: $\mathbf{Z}_n$

The result of the modulo operation with modulus n is always an integer between 0 and $n - 1$. In other words, the result of a mod n is always a nonnegative integer less than n. We can say that the modulo operation creates a set, which in modular arithmetic is referred to as the **set of least residues modulo *n***, or $\mathbf{Z}_n$. However, we need to remember that although we have only one set of integers (**Z**), we have infinite instances of the set of residues ($\mathbf{Z}_n$), one for each value of n. Figure 2.10 shows the set $\mathbf{Z}_n$ and three instances, $\mathbf{Z}_2$, $\mathbf{Z}_6$, and $\mathbf{Z}_{11}$.

Figure 2.10 *Some $\mathbf{Z}_n$ sets*

$$\mathbf{Z}_n = \{\, 0, 1, 2, 3, \ldots, (n-1) \,\}$$

$$\mathbf{Z}_2 = \{\, 0, 1 \,\} \qquad \mathbf{Z}_6 = \{\, 0, 1, 2, 3, 4, 5 \,\} \qquad \mathbf{Z}_{11} = \{\, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 \,\}$$

Congruence

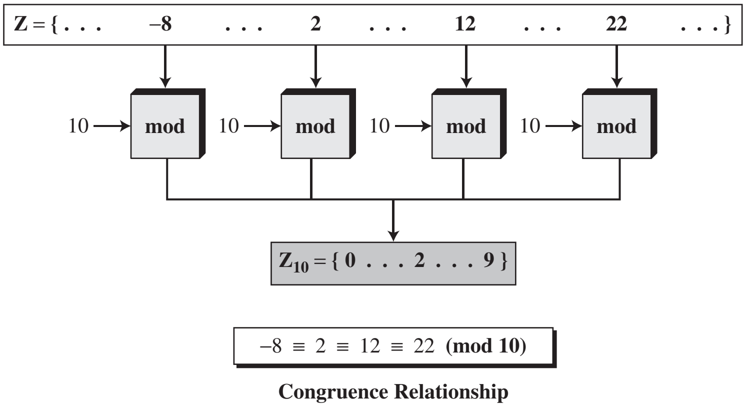
In cryptography, we often used the concept of **congruence** instead of equality. Mapping from **Z** to $\mathbf{Z}_n$ is not one-to-one. Infinite members of **Z** can map to one member of $\mathbf{Z}_n$. For example, the result of 2 mod 10 = 2, 12 mod 10 = 2, 22 mod 2 = 2, and so on. In modular arithmetic, integers like 2, 12, and 22 are called congruent mod 10. To show that two integers are congruent, we use the **congruence operator** (≡). We add the phrase (mod n) to the right side of the congruence to define the value of modulus that makes the relationship valid. For example, we write:

$2 \equiv 12 \pmod{10}$	$13 \equiv 23 \pmod{10}$	$34 \equiv 24 \pmod{10}$	$-8 \equiv 12 \pmod{10}$
$3 \equiv 8 \pmod{5}$	$8 \equiv 13 \pmod{5}$	$23 \equiv 33 \pmod{5}$	$-8 \equiv 2 \pmod{5}$

Figure 2.11 shows the idea of congruence. We need to explain several points.

a. The congruence operator looks like the equality operator, but there are differences. First, an equality operator maps a member of **Z** to itself; the congruence operator maps a member from **Z** to a member of $\mathbf{Z}_n$. Second, the equality operator is one-to-one; the congruence operator is many-to-one.

Figure 2.11 *Concept of congruence*


Z = { . . . −8 . . . 2 . . . 12 . . . 22 . . . }
10
mod
10
mod
10
mod
10
mod
Z10 = { 0 . . . 2 . . . 9 }
−8 ≡ 2 ≡ 12 ≡ 22 (mod 10)
Congruence Relationship

b. The phrase (mod n) that we insert at the right-hand side of the congruence operator is just an indication of the destination set ($\mathbf{Z}_n$). We need to add this phrase to show what modulus is used in the mapping. The symbol *mod* used here does not have the same meaning as the binary operator. In other words, the symbol *mod* in 12 mod 10 is an operator; the phrase (mod 10) in $2 \equiv 12 \pmod{10}$ means that the destination set is $\mathbf{Z}_{10}$.

Residue Classes

A **residue class** $[a]$ or $[a]_n$ is the set of integers congruent modulo n. In other words, it is the set of all integers such that $x = a \pmod{n}$. For example, if $n = 5$, we have five sets [0], [1], [2], [3], and [4] as shown below:

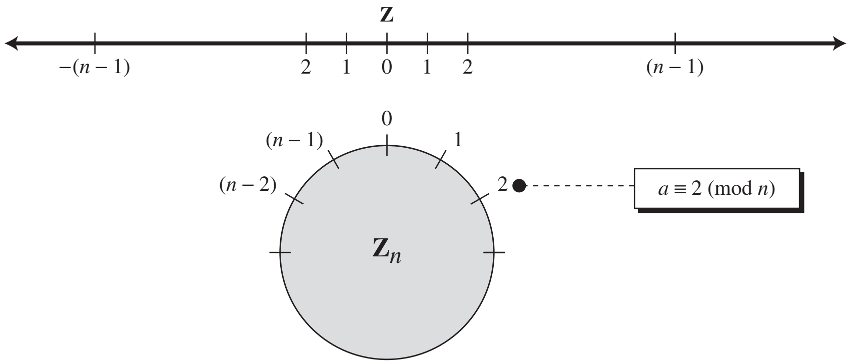
$[0] = \{\ldots, -15, \ -10, \ -5, 0, \ 5, 10, 15, \ldots\}$
$[1] = \{\ldots, -14, \ -9, \ -4, 1, \ 6, 11, 16, \ldots\}$
$[2] = \{\ldots, -13, \ -8, \ -3, 2, \ 7, 12, 17, \ldots\}$
$[3] = \{\ldots, -12, \ -7, \ -5, 3, \ 8, 13, 18, \ldots\}$
$[4] = \{\ldots, -11, \ -6, \ -1, 4, \ 9, 14, 19, \ldots\}$

The integers in the set [0] are all reduced to 0 when we apply the modulo 5 operation on them. The integers in the set [1] are all reduced to 1 when we apply the modulo 5 operation, and so on. In each set, there is one element called the least (nonnegative) residue. In the set [0], this element is 0; in the set [1], this element is 1; and so on. The set of all of these least residues is what we have shown as $\mathbf{Z}_5 = \{0, 1, 2, 3, 4\}$. In other words, the set $\mathbf{Z}_n$ is the set of all **least residue** modulo n.

Circular Notation

The concept of congruence can be better understood with the use of a circle. Just as we use a line to show the distribution of integers in $\mathbf{Z}$, we can use a circle to show the

Figure 2.12 *Comparison of* $\mathbf{Z}$ *and* $\mathbf{Z}_n$ *using graphs*



distribution of integers in $\mathbf{Z}_n$. Figure 2.12 shows the comparison between the two. Integers 0 to $n - 1$ are spaced evenly around a circle. All congruent integers modulo n occupy the same point on the circle. Positive and negative integers from $\mathbf{Z}$ are mapped to the circle in such a way that there is a symmetry between them.

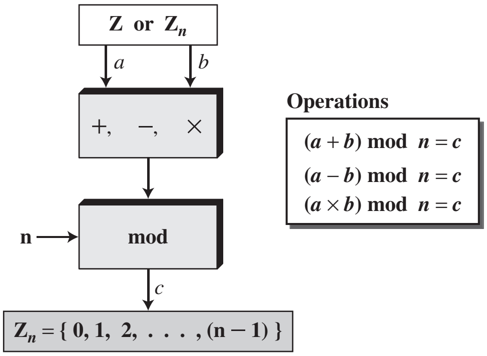
Example 2.14

We use modular arithmetic in our daily life; for example, we use a clock to measure time. Our clock system uses modulo 12 arithmetic. However, instead of a 0 we use the number 12. So our clock system starts with 0 (or 12) and goes until 11. Because our days last 24 hours, we navigate around the circle two times and denote the first revolution as A.M. and the second as P.M.

Operations in $\mathbf{Z}_n$

The three binary operations (*addition, subtraction,* and *multiplication*) that we discussed for the set $\mathbf{Z}$ can also be defined for the set $\mathbf{Z}_n$. The result may need to be mapped to $\mathbf{Z}_n$ using the mod operator as shown in Figure 2.13.

Figure 2.13 *Binary operations in* $\mathbf{Z}_n$



Actually, two sets of operators are used here. The first set is one of the binary operators (+, −, ×); the second is the mod operator. We need to use parentheses to emphasize the order of operations. As Figure 2.13 shows, the inputs (*a* and *b*) can be members of $\mathbf{Z}_n$ or $\mathbf{Z}$.

Example 2.15

Perform the following operations (the inputs come from $\mathbf{Z}_n$):

a. Add 7 to 14 in $\mathbf{Z}_{15}$.

b. Subtract 11 from 7 in $\mathbf{Z}_{13}$.

c. Multiply 11 by 7 in $\mathbf{Z}_{20}$.

Solution

The following shows the two steps involved in each case:

$$\begin{aligned}
&(14 + 7) \bmod 15 &&\rightarrow && (21) \bmod 15 = 6\\
&(7 - 11) \bmod 13 &&\rightarrow && (-4) \bmod 13 = 9\\
&(7 \times 11) \bmod 20 &&\rightarrow && (77) \bmod 20 = 17
\end{aligned}$$

Example 2.16

Perform the following operations (the inputs come from either $\mathbf{Z}$ or $\mathbf{Z}_n$):

a. Add 17 to 27 in $\mathbf{Z}_{14}$.

b. Subtract 34 from 12 in $\mathbf{Z}_{13}$.

c. Multiply 123 by −10 in $\mathbf{Z}_{19}$.

Solution

The following shows the two steps involved in each case:

$$\begin{aligned}
&(17 + 27) \bmod 14 &&\rightarrow && (44) \bmod 14 = 2\\
&(12 - 43) \bmod 13 &&\rightarrow && (-31) \bmod 13 = 8\\
&(123 \times (-10)) \bmod 19 &&\rightarrow && (-1230) \bmod 19 = 5
\end{aligned}$$

Properties

We mentioned that the two inputs to the three binary operations in the modular arithmetic can come from $\mathbf{Z}$ or $\mathbf{Z}_n$. The following properties allow us to first map the two inputs to $\mathbf{Z}_n$ (if they are coming from $\mathbf{Z}$) before applying the three binary operations (+, −, ×). Interested readers can find proofs for these properties in Appendix P.

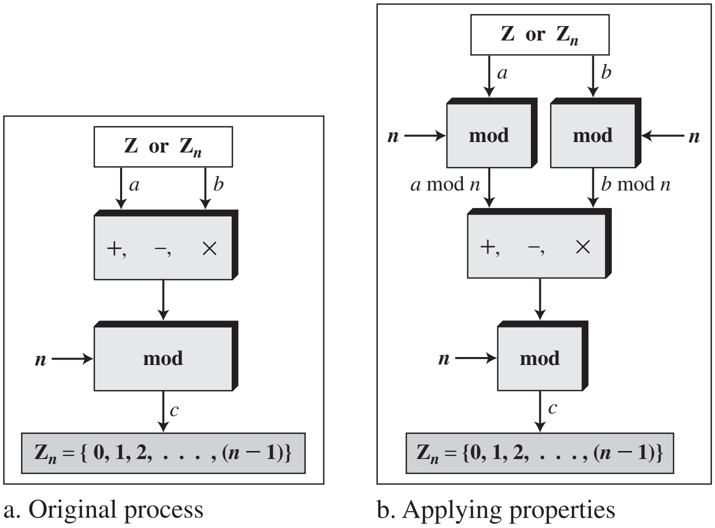
First Property: $(a + b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$

Second Property: $(a - b) \bmod n = [(a \bmod n) - (b \bmod n)] \bmod n$

Third Property: $(a \times b) \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n$

Figure 2.14 shows the process before and after applying the above properties. Although the figure shows that the process is longer if we apply the above properties, we should remember that in cryptography we are dealing with very large integers. For example, if we multiply a very large integer by another very large integer, we

Figure 2.14 *Properties of mod operator*



may have an integer that is too large to be stored in the computer. Applying the above properties make the first two operands smaller before the multiplication operation is applied. In other words, the properties us with smaller numbers. This fact will manifest itself more clearly in discussion of the exponential operation in later chapters.

Example 2.17

The following shows the application of the above properties:

1. (1,723,345 + 2,124,945) mod 11 = (8 + 9) mod 11 = 6
2. (1,723,345 – 2,124,945) mod 16 = (8 – 9) mod 11 = 10
3. (1,723,345 × 2,124,945) mod 16 = (8 × 9) mod 11 = 6

Example 2.18

In arithmetic, we often need to find the remainder of powers of 10 when divided by an integer. For example, we need to find 10 mod 3, 10^2 mod 3, 10^3 mod 3, and so on. We also need to find 10 mod 7, 10^2 mod 7, 10^3 mod 7, and so. The third property of the mod operator mentioned above makes life much easier.

$10^n \bmod x = (10 \bmod x)^n$ Applying the third property n times.

We have

$10 \bmod 3 = 1 \rightarrow 10^n \bmod 3 = (10 \bmod 3)^n = 1$
$10 \bmod 9 = 1 \rightarrow 10^n \bmod 9 = (10 \bmod 9)^n = 1$
$10 \bmod 7 = 3 \rightarrow 10^n \bmod 7 = (10 \bmod 7)^n = 3^n \bmod 7$

Example 2.19

We have been told in arithmetic that the remainder of an integer divided by 3 is the same as the remainder of the sum of its decimal digits. In other words, the remainder of dividing 6371 by 3 is the same as dividing 17 by 3 because 6 + 3 + 7 + 1 = 17. We can prove this claim using the properties of the mod operator. We write an integer as the sum of its digits multiplied by the powers of 10.

$$a = a_n \times 10^n + \cdots + a_1 \times 10^1 + a_0 \times 10^0$$

For example: $6371 = 6 \times 10^3 + 3 \times 10^2 + 7 \times 10^1 + 1 \times 10^0$

Now we can apply the mod operator to both sides of the equality and use the result of the previous example that 10^n mod 3 is 1.

$$\begin{aligned} a \bmod 3 &= (a_n \times 10^n + \cdots + a_1 \times 10^1 + a_0 \times 10^0) \bmod 3 \\ &= (a_n \times 10^n) \bmod 3 + \cdots + (a_1 \times 10^1) \bmod 3 + (a_0 \times 10^0) \bmod 3 \\ &= (a_n \bmod 3) \times (10^n \bmod 3) + \cdots + (a_1 \bmod 3) \times (10^1 \bmod 3) + \\ &\quad (a_0 \bmod 3) \times (10^0 \bmod 3) \\ &= a_n \bmod 3 + \cdots + a_1 \bmod 3 + a_0 \bmod 3 \\ &= (a_n + \cdots + a_1 + a_0) \bmod 3 \end{aligned}$$

Inverses

When we are working in modular arithmetic, we often need to find the inverse of a number relative to an operation. We are normally looking for an **additive inverse** (relative to an addition operation) or a **multiplicative inverse** (relative to a multiplication operation).

Additive Inverse

In $\mathbf{Z}_n$, two numbers a and b are additive inverses of each other if

$$a + b \equiv 0 \pmod{n}$$

In $\mathbf{Z}_n$, the additive inverse of a can be calculated as $b = n - a$. For example, the additive inverse of 4 in $\mathbf{Z}_{10}$ is $10 - 4 = 6$.

In modular arithmetic, each integer has an additive inverse.

The sum of an integer and its additive inverse is congruent to 0 modulo *n*.

Note that in modular arithmetic, each number has an additive inverse and the inverse is unique; each number has one and only one additive inverse. However, the inverse of the number may be the number itself.

Example 2.20

Find all additive inverse pairs in $\mathbf{Z}_{10}$.

Solution

The six pairs of additive inverses are (0, 0), (1, 9), (2, 8), (3, 7), (4, 6), and (5, 5). In this list, 0 is the additive inverse of itself; so is 5. Note that the additive inverses are reciprocal; if 4 is the additive inverse of 6, then 6 is also the additive inverse of 4.

Multiplicative Inverse

In $\mathbf{Z}_n$, two numbers a and b are the multiplicative inverse of each other if

$$a \times b \equiv 1 \pmod{n}$$

For example, if the modulus is 10, then the multiplicative inverse of 3 is 7. In other words, we have $(3 \times 7) \bmod 10 = 1$.

In modular arithmetic, an integer may or may not have a multiplicative inverse. When it does, the product of the integer and its multiplicative inverse is congruent to 1 modulo *n*.

It can be proved that a has a multiplicative inverse in $\mathbf{Z}_n$ if and only if $\gcd(n, a) = 1$. In this case, a and n are said to be **relatively prime.**

Example 2.21

Find the multiplicative inverse of 8 in $\mathbf{Z}_{10}$.

Solution

There is no multiplicative inverse because $\gcd(10, 8) = 2 \neq 1$. In other words, we cannot find any number between 0 and 9 such that when multiplied by 8, the result is congruent to 1.

Example 2.22

Find all multiplicative inverses in $\mathbf{Z}_{10}$.

Solution

There are only three pairs: (1, 1), (3, 7) and (9, 9). The numbers 0, 2, 4, 5, 6, and 8 do not have a multiplicative inverse. We can see that

$$(1 \times 1) \bmod 10 = 1 \qquad (3 \times 7) \bmod 10 = 1 \qquad (9 \times 9) \bmod 10 = 1$$

Example 2.23

Find all multiplicative inverse pairs in $\mathbf{Z}_{11}$.

Solution

We have seven pairs: (1, 1), (2, 6), (3, 4), (5, 9), (7, 8), (9, 9), and (10, 10). In moving from $\mathbf{Z}_{10}$ to $\mathbf{Z}_{11}$, the number of pairs doubles. The reason is that in $\mathbf{Z}_{11}$, $\gcd(11, a)$ is 1 (relatively prime) for all values of a except 0. It means all integers 1 to 10 have multiplicative inverses.

The integer a in $\mathbf{Z}_n$ has a multiplicative inverse if and only if $\gcd(n, a) \equiv 1 \pmod{n}$

The extended Euclidean algorithm we discussed earlier in the chapter can find the multiplicative inverse of b in $\mathbf{Z}_n$ when n and b are given and the inverse exists. To show this, let us replace the first integer a with n (the modulus). We can say that the algorithm can find s and t such $s \times n + b \times t = \gcd(n, b)$. However, if the multiplicative inverse of b exists, $\gcd(n, b)$ must be 1. So the relationship is

$$\boldsymbol{(s \times n) + (b \times t) = 1}$$

Now we apply the modulo operator to both sides. In other words, we map each side to $\mathbf{Z}_n$. We will have

$$\begin{aligned}
&(s \times n + b \times t) \bmod n = 1 \bmod n\\
&[(s \times n) \bmod n] + [(b \times t) \bmod n] = 1 \bmod n\\
&0 + [(b \times t) \bmod n] = 1\\
&(b \times t) \bmod n = 1 \qquad \rightarrow \text{This means } t \text{ is the multiplicative inverse of } b \text{ in } \mathrm{Z}_n
\end{aligned}$$

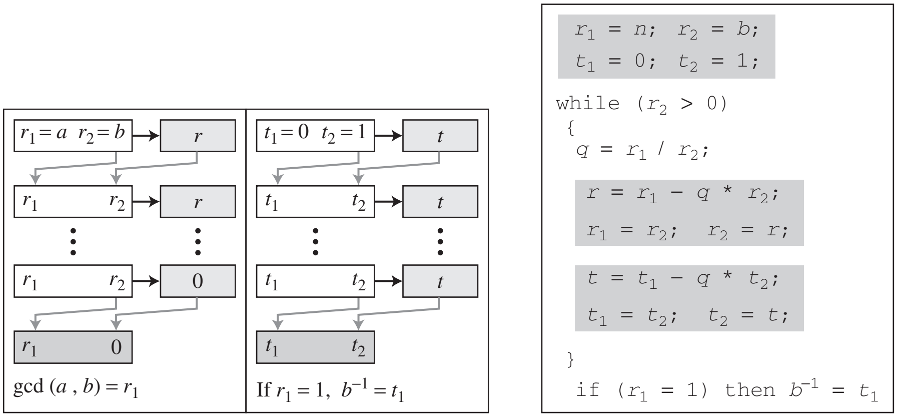
Note that $[(s \times n) \bmod n]$ in the third line is 0 because if we divide $(s \times n)$ by n, the quotient is s but the remainder is 0.

The extended Euclidean algorithm finds the multiplicative inverses of b in $\mathbf{Z}_n$ when n and b are given and $\gcd(n, b) = 1$.

The multiplicative inverse of b is the value of t after being mapped to $\mathbf{Z}_n$.

Figure 2.15 shows how we find the multiplicative inverse of a number using the extended Euclidean algorithm.

Figure 2.15 *Using the extended Euclidean algorithm to find the multiplicative inverse*



```
r1 = n;  r2 = b;
t1 = 0;  t2 = 1;

while (r2 > 0)
 {
  q = r1 / r2;

   r = r1 − q * r2;
   r1 = r2;  r2 = r;

   t = t1 − q * t2;
   t1 = t2;  t2 = t;
 }
  if (r1 = 1) then b^-1 = t1
```

a. Process

b. Algorithm

Example 2.24

Find the multiplicative inverse of 11 in $\mathbf{Z}_{26}$.

Solution

We use a table similar to the one we used before with $r_1 = 26$ and $r_2 = 11$. We are interested only in the value of *t*.

q	r_1	r_2	r	t_1	t_2	t
2	26	11	4	0	1	−2
2	11	4	3	1	−2	5
1	4	3	1	−2	5	−7
3	3	1	0	5	−7	26
	1	0		−7	26	

The gcd (26, 11) is 1, which means that the multiplicative inverse of 11 exists. The extended Euclidean algorithm gives $t_1 = -7$. The multiplicative inverse is (−7) mod 26 = 19. In other words, 11 and 19 are multiplicative inverse in $\mathbf{Z_{26}}$. We can see that (11 × 19) mod 26 = 209 mod 26 = 1.

Example 2.25

Find the multiplicative inverse of 23 in $\mathbf{Z_{100}}$.

Solution

We use a table similar to the one we used before with $r_1 = 100$ and $r_2 = 23$. We are interested only in the value of *t*.

q	r_1	r_2	r	t_1	t_2	t
4	100	23	8	0	1	−4
2	23	8	7	1	−4	19
1	8	7	1	−4	9	−13
7	7	1	0	9	−13	100
	1	0		−13	100	

The gcd (100, 23) is 1, which means the inverse of 23 exists. The extended Euclidean algorithm gives $t_1 = -13$. The inverse is (−13) mod 100 = 87. In other words, 13 and 87 are multiplicative inverses in $\mathbf{Z_{100}}$. We can see that (23 × 87) mod 100 = 2001 mod 100 = 1.

Example 2.26

Find the inverse of 12 in $\mathbf{Z_{26}}$.

Solution

We use a table similar to the one we used before, with $r_1 = 26$ and $r_2 = 12$.

q	r_1	r_2	r	t_1	t_2	t
2	26	12	2	0	1	−2
6	12	2	0	1	−2	13
	2	0		−2	13	

The gcd (26, 12) = 2 ≠ 1, which means there is no multiplicative inverse for 12 in $\mathbf{Z_{26}}$.

Addition and Multiplication Tables

Figure 2.16 shows two tables for addition and multiplication. In the addition table, each integer has an additive inverse. The inverse pairs can be found when the result of addition is zero. We have (0, 0), (1, 9), (2, 8), (3, 7), (4, 6), and (5, 5). In the multiplication table we have only three multiplicative pairs (1, 1), (3, 7) and (9, 9). The pairs can be found whenever the result of multiplication is 1. Both tables are symmetric with respect to the diagonal of elements that moves from the top left to the bottom right, revealing the commutative property for addition and multiplication ($a + b = b + a$ and $a \times b = b \times a$). The addition table also shows that each row or column is a permutation of another row or column. This is not true for the multiplication table.

Figure 2.16 *Addition and multiplication tables for* $\mathbf{Z}_{10}$

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

Addition Table in $\mathbf{Z}_{10}$

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	0	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

Multiplication Table in $\mathbf{Z}_{10}$

Different Sets for Addition and Multiplication

In cryptography we often work with inverses. If the sender uses an integer (as the encryption key), the receiver uses the inverse of that integer (as the decryption key). If the operation (encryption/decryption algorithm) is addition, $\mathbf{Z}_n$ can be used as the set of possible keys because each integer in this set has an additive inverse. On the other hand, if the operation (encryption/decryption algorithm) is multiplication, $\mathbf{Z}_n$ cannot be the set of possible keys because only some members of this set have a multiplicative inverse. We need another set. The new set, which is a subset of $\mathbf{Z}_n$ includes only integers in $\mathbf{Z}_n$ that have a unique multiplicative inverse. This set is called $\mathbf{Z}_{n}*$. Figure 2.17 shows some instances of two sets. Note that $\mathbf{Z}_{n}*$ can be made from multiplication tables, such as the one shown in Figure 2.16.

Each member of $\mathbf{Z}_n$ has an additive inverse, but only some members have a multiplicative inverse. Each member of $\mathbf{Z}_{n}*$ has a multiplicative inverse, but only some members have an additive inverse.

We need to use $\mathbf{Z}_n$ when additive inverses are needed; we need to use $\mathbf{Z}_n*$ when multiplicative inverses are needed.

Figure 2.17 *Some* $\mathbf{Z}_n$ *and* $\mathbf{Z}_{n^*}$ *sets*

$\mathbf{Z_6 = \{0, 1, 2, 3, 4, 5\}}$ $\mathbf{Z_6^* = \{1, 5\}}$

$\mathbf{Z_7 = \{0, 1, 2, 3, 4, 5, 6\}}$ $\mathbf{Z_7^* = \{1, 2, 3, 4, 5, 6\}}$

$\mathbf{Z_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}}$ $\mathbf{Z_{10}^* = \{1, 3, 7, 9\}}$

Two More Sets

Cryptography often uses two more sets: $\mathbf{Z}_p$ and $\mathbf{Z}_{p^*}$. The modulus in these two sets is a prime number. Prime numbers will be discussed in later chapters; suffice it to say that a prime number has only two divisors: integer 1 and itself.

The set $\mathbf{Z}_p$ is the same as $\mathbf{Z}_n$ except that n is a prime. $\mathbf{Z}_p$ contains all integers from 0 to $p - 1$. Each member in $\mathbf{Z}_p$ has an additive inverse; each member except 0 has a multiplicative inverse.

The set $\mathbf{Z}_{p^*}$ is the same as $\mathbf{Z}_{n^*}$ except that n is a prime. $\mathbf{Z}_{p^*}$ contains all integers from 1 to $p - 1$. Each member in $\mathbf{Z}_{p^*}$ has an additive and a multiplicative inverse. $\mathbf{Z}_{p^*}$ is a very good candidate when we need a set that supports both additive and multiplicative inverse.

The following shows these two sets when $p = 13$.

$Z_{13} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$
$Z_{13^*} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$

2.3 MATRICES

In cryptography we need to handle matrices. Although this topic belongs to a special branch of algebra called linear algebra, the following brief review of matrices is necessary preparation for the study of cryptography. Readers who are familiar with this topic can skip part or all of this section. The section begins with some definitions and then shows how to use matrices in modular arithmetic.

Definitions

A **matrix** is a rectangular array of $l \times m$ elements, in which l is the number of rows and m is the number of columns. A matrix is normally denoted with a boldface uppercase letter such as **A**. The element a_{ij} is located in the ith row and jth column. Although the elements can be a set of numbers, we discuss only matrices with elements in **Z**. Figure 2.18 shows a matrix.

If a matrix has only one row ($l = 1$), it is called a **row matrix;** if it has only one column ($m = 1$), it is called a **column matrix.** In a **square matrix,** in which there is the

Figure 2.18 *A matrix of size $l \times m$*

$$\textbf{Matrix A:}\quad \begin{array}{cc} & m \text{ columns} \\ \rotatebox{90}{l rows} & \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & & \vdots \\ a_{l1} & a_{l2} & \cdots & a_{lm} \end{bmatrix} \end{array}$$

same number of rows and columns ($l = m$), the elements a_{11}, a_{22}, . . . , a_{mm} make the **main diagonal.** An additive identity matrix, denoted as **0**, is a matrix with all rows and columns set to 0's. An **identity matrix,** denoted as **I,** is a square matrix with 1s on the main diagonal and 0s elsewhere. Figure 2.19 shows some examples of matrices with elements from **Z**.

Figure 2.19 *Example of matrices*

$$\underset{\text{Row matrix}}{\begin{bmatrix} 2 & 1 & 5 & 11 \end{bmatrix}} \quad \underset{\substack{\text{Column}\\ \text{matrix}}}{\begin{bmatrix} 2 \\ 4 \\ 12 \end{bmatrix}} \quad \underset{\substack{\text{Square}\\ \text{matrix}}}{\begin{bmatrix} 23 & 14 & 56 \\ 12 & 21 & 18 \\ 10 & 8 & 31 \end{bmatrix}} \quad \underset{\mathbf{0}}{\begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}} \quad \underset{\mathbf{I}}{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}}$$

Operations and Relations

In linear algebra, one relation (equality) and four operations (addition, subtraction, multiplication, and scalar multiplication) are defined for matrices.

Equality

Two matrices are equal if they have the same number of rows and columns and the corresponding elements are equal. In other words, **A** = **B** if we have $a_{ij} = b_{ij}$ for all i's and j's.

Addition and Subtraction

Two matrices can be added if they have the same number of columns and rows. This addition is shown as **C** = **A** + **B**. In this case, the resulting matrix **C** has also the same number of rows and columns as **A** or **B**. Each element of **C** is the sum of the two corresponding elements of **A** and **B**: $c_{ij} = a_{ij} + b_{ij}$. Subtraction is the same except that each element of **B** is subtracted from the corresponding element of **A**: $d_{ij} = a_{ij} - b_{ij}$.

Example 2.27

Figure 2.20 shows an example of addition and subtraction.

Figure 2.20 *Addition and subtraction of matrices*

$$\underbrace{\begin{bmatrix}12 & 4 & 4\\ 11 & 12 & 30\end{bmatrix} = \begin{bmatrix}5 & 2 & 1\\ 3 & 2 & 10\end{bmatrix} + \begin{bmatrix}7 & 2 & 3\\ 8 & 10 & 20\end{bmatrix}}_{\mathbf{C} \,=\, \mathbf{A} \,+\, \mathbf{B}} \qquad \underbrace{\begin{bmatrix}-2 & 0 & -2\\ -5 & -8 & 10\end{bmatrix} = \begin{bmatrix}5 & 2 & 1\\ 3 & 2 & 10\end{bmatrix} - \begin{bmatrix}7 & 2 & 3\\ 8 & 10 & 20\end{bmatrix}}_{\mathbf{D} \,=\, \mathbf{A} \,-\, \mathbf{B}}$$

Multiplication

We can multiply two matrices of different sizes if the number of columns of the first matrix is the same as the number of rows of the second matrix. If **A** is an $l \times m$ matrix and **B** is an $m \times p$ matrix, the product of the two is a matrix **C** of size $l \times p$. If each element of matrix **A** is called a_{ij}, each element of matrix **B** is called b_{jk}, then each element of matrix **C**, c_{ik}, can be calculated as

$$c_{ik} = \sum a_{ij} \times b_{jk} = a_{i1} \times b_{1j} + a_{i2} \times b_{2j} + \cdots + a_{im} \times b_{mj}$$

Example 2.28

Figure 2.21 shows the product of a row matrix (1×3) by a column matrix (3×1). The result is a matrix of size 1×1.

Figure 2.21 *Multiplication of a row matrix by a column matrix*

$$\overset{\mathbf{C}}{\begin{bmatrix}53\end{bmatrix}} = \overset{\mathbf{A}}{\underset{\longrightarrow}{\begin{bmatrix}5 & 2 & 1\end{bmatrix}}} \times \overset{\mathbf{B}}{\begin{bmatrix}7\\ 8\\ 2\end{bmatrix}}\Big\downarrow \qquad \text{In which: } \boxed{53 = 5 \times 7 + 2 \times 8 + 1 \times 2}$$

Example 2.29

Figure 2.22 shows the product of a 2×3 matrix by a 3×4 matrix. The result is a 2×4 matrix.

Figure 2.22 *Multiplication of a 2 × 3 matrix by a 3 × 4 matrix*

$$\overset{\mathbf{C}}{\begin{bmatrix}52 & 18 & 14 & 9\\ 41 & 21 & 22 & 7\end{bmatrix}} = \overset{\mathbf{A}}{\begin{bmatrix}5 & 2 & 1\\ 3 & 2 & 4\end{bmatrix}} \times \overset{\mathbf{B}}{\begin{bmatrix}7 & 3 & 2 & 1\\ 8 & 0 & 0 & 2\\ 1 & 3 & 4 & 0\end{bmatrix}}$$

Scalar Multiplication

We can also multiply a matrix by a number (called a **scalar**). If **A** is an $l \times m$ matrix and x is a scalar, $\mathbf{C} = x\mathbf{A}$ is a matrix of size $l \times m$, in which $\mathrm{c}_{ij} = x \times \mathrm{a}_{ij}$.

Figure 2.23 *Scalar multiplication*

$$\overset{\mathbf{B}}{\begin{bmatrix} 15 & 6 & 3 \\ 9 & 6 & 12 \end{bmatrix}} = 3 \times \overset{\mathbf{A}}{\begin{bmatrix} 5 & 2 & 1 \\ 3 & 2 & 4 \end{bmatrix}}$$

Example 2.30

Figure 2.23 shows an example of scalar multiplication.

Determinant

The **determinant** of a square matrix **A** of size $m \times m$ denoted as det (**A**) is a scalar calculated recursively as shown below:

1. If $m = 1$, det $(\mathbf{A}) = a_{11}$
2. If $m > 1$, det $(\mathbf{A}) = \sum_{\mathrm{i=1...m}} (-1)^{\mathrm{i+j}} \times a_{\mathrm{ij}} \times \det(\mathbf{A}_{\mathrm{ij}})$

   Where $\mathbf{A}_{\mathrm{ij}}$ is a matrix obtained from **A** by deleting the *i*th row and *j*th column.

The determinant is defined only for a square matrix.

Example 2.31

Figure 2.24 shows how we can calculate the determinant of a 2×2 matrix based on the determinant of a 1×1 matrix using the above recursive definition. The example shows that when m is 1 or 2, it is very easy to find the determinant of a matrix.

Figure 2.24 *Calculating the determinant of a 2 × 2 matrix*

$$\det \begin{bmatrix} 5 & 2 \\ 3 & 4 \end{bmatrix} = (-1)^{1+1} \times 5 \times \det[\,4\,] + (-1)^{1+2} \times 2 \times \det[\,3\,] \longrightarrow 5 \times 4 - 2 \times 3 = 14$$

$$\text{or} \quad \boxed{\det \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = a_{11} \times a_{22} - a_{12} \times a_{21}}$$

Example 2.32

Figure 2.25 shows the calculation of the determinant of a 3×3 matrix.

Figure 2.25 *Calculating the determinant of a 3 × 3 matrix*

$$\det \begin{bmatrix} 5 & 2 & 1 \\ 3 & 0 & -4 \\ 2 & 1 & 6 \end{bmatrix} = (-1)^{1+1} \times 5 \times \det \begin{bmatrix} 0 & -4 \\ 1 & 6 \end{bmatrix} + (-1)^{1+2} \times 2 \times \det \begin{bmatrix} 3 & -4 \\ 2 & 6 \end{bmatrix} + (-1)^{1+3} \times 1 \times \det \begin{bmatrix} 3 & 0 \\ 2 & 1 \end{bmatrix}$$

$$= (+1) \times 5 \times (+4) \quad + \quad (-1) \times 2 \times (24) \quad + \quad (+1) \times 1 \times (3) = -25$$

We give some algorithms for finding the determinant of a square matrix in Appendix ****.

Inverses

Matrices have both additive and multiplicative inverses.

Additive Inverse

The additive inverse of matrix **A** is another matrix **B** such that **A** + **B** = **0**. In other words, we have $b_{ij} = - a_{ij}$ for all values of i and j. Normally the additive inverse of **A** is defined by −**A**.

Multiplicative Inverse

The multiplicative inverse is defined only for square matrices. The multiplicative inverse of a square matrix **A** is a square matrix **B** such that $\mathbf{A} \times \mathbf{B} = \mathbf{B} \times \mathbf{A} = \mathbf{I}$. Normally the multiplicative inverse of **A** is defined by $\mathbf{A}^{-1}$. The multiplicative inverse exists only if the (**A**) has a multiplicative inverse in the corresponding set. Since no integer has a multiplicative inverse in **Z**, there is no multiplicative inverse of a matrix in **Z**. However, matrices with real elements have matrices only if det (**A**) ≠ 0.

Multiplicative inverses are only defined for square matrices.

Residue Matrices

Cryptography uses residue matrices: matrices in all elements are in $\mathbf{Z}_n$. All operations on residue matrices are performed the same as for the integer matrices except that the operations are done in modular arithmetic. One interesting result is that a residue matrix has a multiplicative inverse if the determinant of the matrix has a multiplicative inverse in $\mathbf{Z}_n$. In other words, a residue matrix has a multiplicative inverse if gcd (det(**A**), n) = 1.

Example 2.33

Figure 2.26 shows a residue matrix **A** in $\mathbf{Z}_{26}$ and its multiplicative inverse $\mathbf{A}^{-1}$. We have det(**A**) = 21 which has the multiplicative inverse 5 in $\mathbf{Z}_{26}$. Note that when we multiply the two matrices, the result is the multiplicative identity matrix in $\mathbf{Z}_{26}$.

Figure 2.26 *A residue matrix and its multiplicative inverse*

$$\mathbf{A} = \begin{bmatrix} 3 & 5 & 7 & 2 \\ 1 & 4 & 7 & 2 \\ 6 & 3 & 9 & 17 \\ 13 & 5 & 4 & 16 \end{bmatrix} \qquad \mathbf{A}^{-1} = \begin{bmatrix} 15 & 21 & 0 & 15 \\ 23 & 9 & 0 & 22 \\ 15 & 16 & 18 & 3 \\ 24 & 7 & 15 & 3 \end{bmatrix}$$

$$\det(\mathbf{A}) = 21 \qquad \det(\mathbf{A}^{-1}) = 5$$

Congruence

Two matrices are congruent modulo n, written as $\mathbf{A} \equiv \mathbf{B} \pmod{n}$, if they have the same number of rows and columns and all corresponding elements are congruent modulo n. In other words, $\mathbf{A} \equiv \mathbf{B} \pmod{n}$ if $a_{ij} \equiv b_{ij} \pmod{n}$ for all i's and j's.

2.4 LINEAR CONGRUENCE

Cryptography often involves solving an equation or a set of equations of one or more variables with coefficient in $\mathbf{Z}_n$. This section shows how to solve equations when the power of each variable is 1 (linear equation).

Single-Variable Linear Equations

Let us see how we can solve equations involving a single variable—that is, equations of the form $ax \equiv b \pmod{n}$. An equation of this type might have no solution or a limited number of solutions. Assume that the gcd $(a, n) = d$. If $d \nmid b$, there is no solution. If $d|b$, there are d solutions.

If $d|b$, we use the following strategy to find the solutions:

1. Reduce the equation by dividing both sides of the equation (including the modulus) by d.
2. Multiply both sides by the multiplicative inverse of $a|\text{gcd}(a, n)$ to find the particular solution x_0.
3. The general solutions are $x = x_0 + k\,(n|d)$ for $k = 0, 1, \ldots, (d - 1)$.

Example 2.34

Solve the equation $10x \equiv 2 \pmod{15}$.

Solution

First we find the gcd (10 and 15) = 5. Since 5 does not divide 2, we have no solution.

Example 2.35

Solve the equation $14x \equiv 12 \pmod{18}$.

Solution

Note that gcd (14 and 18) = 2. Since 2 divides 12, we have exactly two solutions, but first we reduce the equation.

$$14x \equiv 12 \pmod{18} \rightarrow \quad 7x \equiv 6 \pmod{9} \quad \rightarrow \; x \equiv 6\,(7^{-1}) \pmod{9}$$
$$x_0 = (6 \times 7^{-1}) \bmod 9 = (6 \times 4) \pmod{9} = 6$$
$$x_1 = x_0 + 1 \times (18/2) = 15$$

Both solutions, 6 and 15 satisfy the congruence relation, because (14 × 6) mod 18 = 12 and also (14 × 15) mod 18 = 12.

Example 2.36

Solve the equation $3x + 4 \equiv 6 \pmod{13}$.

Solution

First we change the equation to the form $ax \equiv b \pmod{n}$. We add -4 (the additive inverse of 4) to both sides, which give $3x \equiv 2 \pmod{13}$. Because gcd (3, 13) = 1, the equation has only one solution, which is $x_0 = (2 \times 3^{-1}) \bmod 13 = 18 \bmod 13 = 5$. We can see that the answer satisfies the original equation: $3 \times 5 + 4 \equiv 6 \pmod{13}$.

Set of Linear Equations

We can also solve a set of linear equations with the same modulus if the matrix formed from the coefficients of the variables is invertible. We make three matrices. The first is the square matrix made from the coefficients of variables. The second is a column matrix made from the variables. The third is a column matrix made from the values at the right-hand side of the congruence operator. We can interpret the set of equations as matrix multiplication. If both sides of congruence are multiplied by the multiplicative inverse of the first matrix, the result is the variable matrix at the right-hand side, which means the problem can be solved by a matrix multiplication as shown in Figure 2.27.

Figure 2.27 *Set of linear equations*

$$\begin{array}{ccccccccc}
a_{11}x_1 & + & a_{12}x_2 & + & \cdots & + & a_{1n}x_n & \equiv & b_1 \\
a_{21}x_1 & + & a_{22}x_2 & + & \cdots & + & a_{2n}x_n & \equiv & b_2 \\
\vdots & & \vdots & & & & \vdots & & \vdots \\
a_{n1}x_1 & + & a_{n2}x_2 & + & \cdots & + & a_{nn}x_n & \equiv & b_n
\end{array}$$

a. Equations

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \equiv \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}$$

b. Interpretation

$$\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \equiv \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}^{-1} \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}$$

c. Solution

Example 2.37

Solve the set of following three equations:

$$\begin{aligned}
3x + 5y + 7z &\equiv 3 \pmod{16} \\
x + 4y + 13z &\equiv 5 \pmod{16} \\
2x + 7y + 3z &\equiv 4 \pmod{16}
\end{aligned}$$

Solution

Here x, y, and z play the roles of x_1, x_2, and x_3. The matrix formed by the set of equations is invertible. We find the multiplicative inverse of the matrix and multiply it by the column matrix formed from 3, 5, and 4. The result is $x \equiv 15 \pmod{16}$, $y \equiv 4 \pmod{16}$, and $z \equiv 14 \pmod{16}$. We can check the answer by inserting these values into the equations.

2.5 RECOMMENDED READING

For more details about subjects discussed in this chapter, we recommend the following books and sites. The items enclosed in brackets refer to the reference list at the end of the book.

Books

Several books give an easy but thorough coverage of number theory including [Ken93], [Yan02], [Sch99], [Cou99], and [DS00]. Matrices are discussed in any book about linear algebra; [LEF04] and [LL01] are good texts to start with.

Websites

The following sites are related to topics discussed in this chapter.

❑ ******************* This is the book site in which you can find all programs for algorithms used in this chapter in two languages (C and Java).

❑ ********

2.6 KEY TERMS

additive inverse
binary operation
column matrix
congruence
congruence operator
determinant
divisibility
Euclidean algorithm
extended Euclidean algorithm
greatest common divisor
identity matrix
integer arithmetic
least residue
linear congruence
linear Diophantine equation
main diagonal
matrix
modular arithmetic
modulo operator (mod)
modulus
multiplicative inverse
relatively prime
residue
residue class
row matrix
scalar
set of integers, $\mathbf{Z}$
set of residues, $\mathbf{Z}_n$
square matrix

2.7 SUMMARY

- The set of integers, denoted by **Z**, contains all integral numbers from negative infinity to positive infinity. Three common binary operations defined for integers are addition, subtraction, and multiplication. Division does not fit in this category because it produces two outputs instead of one.
- In integer arithmetic, if we divide a by n, we can get q and r. The relationship between these four integers can be shown as $a = q \times n + r$. We say a|b if $a = q \times n$. We mentioned four properties of divisibility in this chapter.
- Two positive integers can have more than one common divisor. But we are normally interested in the greatest common divisor. The Euclidean algorithm gives an efficient and systematic way to calculation of the greatest common divisor of two integer.
- The extended Euclidean algorithm can calculate gcd (a, b) and at the same time calculate the value of s and t to satisfy the equation $as + bt = \gcd(a, b)$.
- A linear Diophantine equation of two variables is $ax + by = c$. It has a particular and general solution.
- In modular arithmetic, we are interested only in remainders; we want to know the value of r when we divide a by n. We use a new operator called modulo operator (mod) so that $a \bmod n = r$. Now n is called the modulus; r is called the residue.
- The result of the modulo operation with modulus n is always an integer between 0 and. We can say that the modulo operation creates a set, which in modular arithmetic is referred to as the set of least residues modulo n, or $\mathbf{Z}_n$.
- Mapping from **Z** to $\mathbf{Z}_n$ is not one-to-one. Infinite members of **Z** can map to one member of $\mathbf{Z}_n$. In modular arithmetic, all integers in **Z** that map to one integer in $\mathbf{Z}_n$ are called congruent modulo n. To show that two integers are congruent, we use the congruence operator (≡).
- A residue class [a] is the set of integers congruent modulo n. It is the set of all integers such that $x = a \pmod{n}$.
- The three binary operations (addition, subtraction, and multiplication) defined for the set **Z** can also be defined for the set $\mathbf{Z}_n$. The result may need to be mapped to $\mathbf{Z}_n$ using the mod operator.
- Several properties were defined for the modulo operation in this chapter.
- In $\mathbf{Z}_n$, two numbers a and b are additive inverses of each other if $a + b \equiv 0 \pmod{n}$. They are the multiplicative inverse of each other if $a \times b \equiv 1 \pmod{n}$. The integer a has a multiplicative inverse in $\mathbf{Z}_n$ if and only if $\gcd(n, a) = 1$ (a and n are relatively prime).
- The extended Euclidean algorithm finds the multiplicative inverses of b in $\mathbf{Z}_n$ when n and b are given and $\gcd(n, b) = 1$. The multiplicative inverse of b is the value of t after being mapped to $\mathbf{Z}_n$.
- A matrix is a rectangular array of $l \times m$ elements, in which l is the number of rows and m is the number of columns. We show a matrix with a boldface uppercase letter such as **A**. The element a_{ij} is located in the ith row and jth column.

- Two matrices are equal if they have the same number of rows and columns and the corresponding elements are equal.
- Addition and subtraction are done only on matrices of equal sizes. We can multiply two matrices of different sizes if the number of columns of the first matrix is the same as the number of rows of the second matrix.
- In residue matrices, all elements are in $\mathbf{Z}_n$. All operations on residue matrices are done in modular arithmetic. A residue matrix has an inverse if the determinant of the matrix has an inverse.
- An equation of the form $ax \equiv b \pmod{n}$ may have no solution or a limited number of solutions. If $\gcd(a, n) \mid b$, there is a limited number of solutions.
- A set of linear equations with the same modulus can be solved if the matrix formed from the coefficients of variables has an inverse.

2.8 PRACTICE SET

Review Questions

1. Distinguish between $\mathbf{Z}$ and $\mathbf{Z}_n$. Which set can have negative integers? How can we map an integer in $\mathbf{Z}$ to an integer in $\mathbf{Z}_n$?
2. List four properties of divisibility discussed in this chapter. Give an integer with only one divisor. Give an integer with only two divisors. Give an integer with more than two divisors.
3. Define the greatest common divisor of two integers. Which algorithm can effectively find the greatest common divisor?
4. What is a linear Diophantine equation of two variables? How many solutions can such an equation have? How can the solution(s) be found?
5. What is the modulo operator, and what is its application? List all properties we mentioned in this chapter for the modulo operation.
6. Define congruence and compare with equality.
7. Define a residue class and a least residue.
8. What is the difference between the set $\mathbf{Z}_n$ and the set $\mathbf{Z}_{n*}$? In which set does each element have an additive inverse? In which set does each element have a multiplicative inverse? Which algorithm is used to find the multiplicative inverse of an integer in $\mathbf{Z}_n$?
9. Define a matrix. What is a row matrix? What is a column matrix? What is a square matrix? What type of matrix has a determinant? What type of matrix can have an inverse?
10. Define linear congruence. What algorithm can be used to solve an equation of type $ax \equiv b \pmod{n}$? How can we solve a set of linear equations?

Exercises

11. Which of the following relations are true and which are false?

$5 \mid 26 \quad 3 \mid 123 \quad 27 \nmid 127 \quad 15 \nmid 21 \quad 23 \mid 96 \quad 8 \mid 5$

12. Using the Euclidean algorithm, find the greatest common divisor of the following pairs of integers.
    a. 88 and 220
    b. 300 and 42
    c. 24 and 320
    d. 401 and 700
13. Solve the following.
    a. Given gcd (a, b) = 24, find gcd (a, b, 16).
    b. Given gcd (a, b, c) = 12, find gcd (a, b, c, 16)
    c. Find gcd (200, 180, and 450).
    d. Find gcd (200, 180, 450, 610).
14. Assume that *n* is a nonnegative integer.
    a. Find gcd ($2n + 1$, *n*).
    b. Using the result of part a, find gcd (201, 100), gcd (81, 40), and gcd (501, 250).
15. Assume that *n* is a nonnegative integer.
    a. Find gcd ($3n + 1$, $2n + 1$).
    b. Using the result of part a, find gcd (301, 201) and gcd (121, 81).
16. Using the extended Euclidean algorithm, find the greatest common divisor of the following pairs and the value of *s* and *t*.
    a. 4 and 7
    b. 291 and 42
    c. 84 and 320
    d. 400 and 60
17. Find the results of the following operations.
    a. 22 mod 7
    b. 140 mod 10
    c. −78 mod 13
    d. 0 mod 15
18. Perform the following operations using reduction first.
    a. (273 + 147) mod 10
    b. (4223 + 17323) mod 10
    c. (148 + 14432) mod 12
    d. (2467 + 461) mod 12
19. Perform the following operations using reduction first.
    a. (125 × 45) mod 10
    b. (424 × 32) mod 10
    c. (144 × 34) mod 12
    d. (221 × 23) mod 22

20. Use the properties of the mod operator to prove the following:

    a. The remainder of any integer when divided by 10 is the rightmost digit.

    b. The remainder of any integer when divided by 100 is the integer made of the two rightmost digits.

    c. The remainder of any integer when divided by 1000 is the integer made of the three rightmost digits.

21. We have been told in arithmetic that the remainder of an integer divided by 5 is the same as the remainder of division of the rightmost digit by 5. Use the properties of the mod operator to prove this claim.

22. We have been told in arithmetic that the remainder of an integer divided by 2 is the same as the remainder of division of the rightmost digit by 2. Use the properties of the mod operator to prove this claim.

23. We have been told in arithmetic that the remainder of an integer divided by 4 is the same as the remainder of division of the two rightmost digits by 4. Use the properties of the mod operator to prove this claim.

24. We have been told in arithmetic that the remainder of an integer divided by 8 is the same as the remainder of division of the rightmost three digits by 8. Use the properties of the mod operator to prove this claim.

25. We have been told in arithmetic that the remainder of an integer divided by 9 is the same as the remainder of division of the sum of its decimal digits by 9. In other words, the remainder of dividing 6371 by 9 is the same as dividing 17 by 9 because $6 + 3 + 7 + 1 = 17$. Use the properties of the mod operator to prove this claim.

26. The following shows the remainders of powers of 10 when divided by 7. We can prove that the pattern will be repeated for higher powers.

    $$\begin{array}{lll} 10^0 \bmod 7 = 1 & 10^1 \bmod 7 = 3 & 10^2 \bmod 7 = 2 \\ 10^3 \bmod 7 = -1 & 10^4 \bmod 7 = -3 & 10^5 \bmod 7 = -2 \end{array}$$

    Using the above information, find the remainder of an integer when divided by 7. Test your method with 631453672.

27. The following shows the remainders of powers of 10 when divided by 11. We can prove that the pattern will be repeated for higher powers.

    $$10^0 \bmod 11 = 1 \quad 10^1 \bmod 11 = -1 \quad 10^2 \bmod 11 = 1 \quad 10^3 \bmod 11 = -1$$

    Using the above information, find the remainder of an integer when divided by 11. Test your method with 631453672.

28. The following shows the remainders of powers of 10 when divided by 13. We can prove that the pattern will be repeated for higher powers.

    $$\begin{array}{lll} 10^0 \bmod 13 = 1 & 10^1 \bmod 13 = -3 & 10^2 \bmod 13 = -4 \\ 10^0 \bmod 13 = -1 & 10^1 \bmod 13 = 3 & 10^2 \bmod 13 = 4 \end{array}$$

    Using the above information, find the remainder of an integer when divided by 13. Test your method with 631453672.

29. Let us assign numeric values to the uppercase alphabet (A = 0, B = 1, . . . Z = 25). We can now do modular arithmetic on the system using modulo 26.
    a. What is (A + N) mod 26 in this system?
    b. What is (A + 6) mod 26 in this system?
    c. What is (Y − 5) mod 26 in this system?
    d. What is (C −10) mod 26 in this system?
30. List all additive inverse pairs in modulus 20.
31. List all multiplicative inverse pairs in modulus 20.
32. Find the multiplicative inverse of each of the following integers in $\mathbf{Z}_{180}$ using the extended Euclidean algorithm.
    a. 38
    b. 7
    c. 132
    d. 24
33. Find the particular and the general solutions to the following linear Diophantine equations.
    a. $25x + 10y = 15$
    b. $19x + 13y = 20$
    c. $14x + 21y = 77$
    d. $40x + 16y = 88$
34. Show that there are no solutions to the following linear Diophantine equations:
    a. $15x + 12y = 13$
    b. $18x + 30y = 20$
    c. $15x + 25y = 69$
    d. $40x + 30y = 98$
35. A post office sells only 39-cent and 15-cent stamps. Find the number of stamps a customer needs to buy to put $2.70 postage on a package. Find a few solutions.
36. Find all solutions to each of the following linear equations:
    a. $3x \equiv 4 \pmod{5}$
    b. $4x \equiv 4 \pmod{6}$
    c. $9x \equiv 12 \pmod{7}$
    d. $256x \equiv 442 \pmod{60}$
37. Find all solutions to each of the following linear equations:
    a. $3x + 5 \equiv 4 \pmod{5}$
    b. $4x + 6 \equiv 4 \pmod{6}$
    c. $9x + 4 \equiv 12 \pmod{7}$
    d. $232x + 42 \equiv 248 \pmod{50}$
38. Find $(\mathbf{A} \times \mathbf{B})$ mod 16 using the matrices in Figure 2.28.

Figure 2.28 *Matrices for Exercise 38*

$$\underset{\mathbf{A}}{\begin{bmatrix} 3 & 7 & 10 \end{bmatrix}} \times \underset{\mathbf{B}}{\begin{bmatrix} 2 \\ 4 \\ 12 \end{bmatrix}} \qquad \underset{\mathbf{A}}{\begin{bmatrix} 3 & 4 & 6 \\ 1 & 1 & 8 \\ 5 & 8 & 3 \end{bmatrix}} \times \underset{\mathbf{B}}{\begin{bmatrix} 2 & 0 & 1 \\ 1 & 1 & 0 \\ 5 & 2 & 4 \end{bmatrix}}$$

39. In Figure 2.29, find the determinant and the multiplicative inverse of each residue matrix over $\mathbf{Z}_{10}$.

Figure 2.29 *Matrices for Exercise 39*

$$\underset{\mathbf{A}}{\begin{bmatrix} 3 & 0 \\ 1 & 1 \end{bmatrix}} \qquad \underset{\mathbf{B}}{\begin{bmatrix} 4 & 2 \\ 1 & 1 \end{bmatrix}} \qquad \underset{\mathbf{C}}{\begin{bmatrix} 3 & 4 & 6 \\ 1 & 1 & 8 \\ 5 & 8 & 3 \end{bmatrix}}$$

40. Find all solutions to the following sets of linear equations:

a. $3x + 5y \equiv 4 \pmod{5}$
$2x + y \equiv 3 \pmod{5}$

b. $3x + 2y \equiv 5 \pmod{7}$
$4x + 6y \equiv 4 \pmod{7}$

c. $7x + 3y \equiv 3 \pmod{7}$
$4x + 2y \equiv 5 \pmod{7}$

d. $2x + 3y \equiv 5 \pmod{8}$
$x + 6y \equiv 3 \pmod{8}$