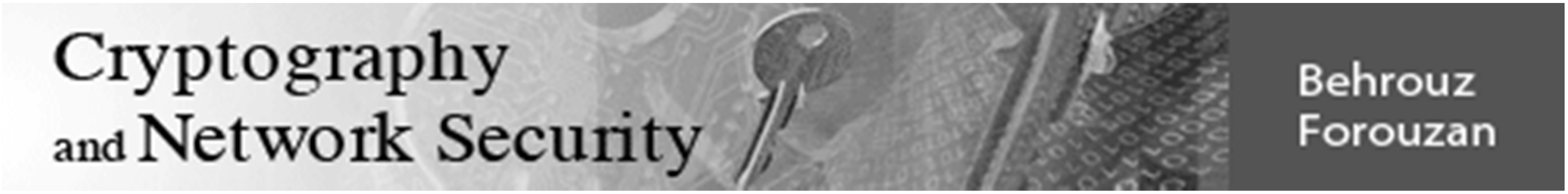


Chapter 2

Mathematics of Cryptography

Part I: Modular Arithmetic, Congruence, and Matrices

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

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.

Topics discussed in this section:

2.1.1 Set of Integers
2.1.2 Binary Operations
2.1.3 Integer Division
2.1.4 Divisibility
2.1.5 Linear Diophantine Equations

2.1.1 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).

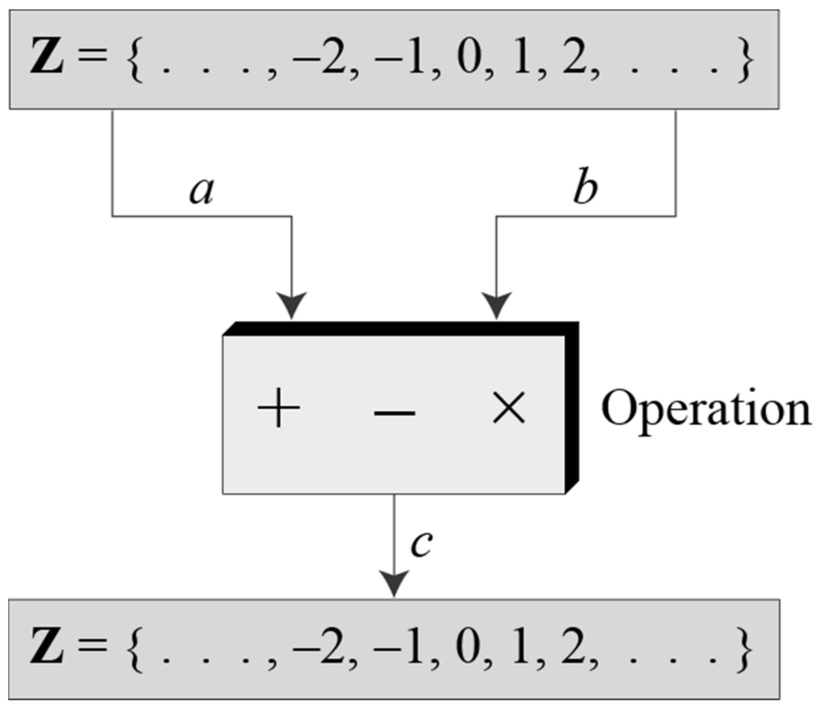
Figure 2.1 ***The set of integers***

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

2.1.2 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.

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



2.1.2 Continued

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:	$5 \times 9 = 45$	$(-5) \times 9 = -45$	$5 \times (-9) = -45$	$(-5) \times (-9) = 45$

2.1.3 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:

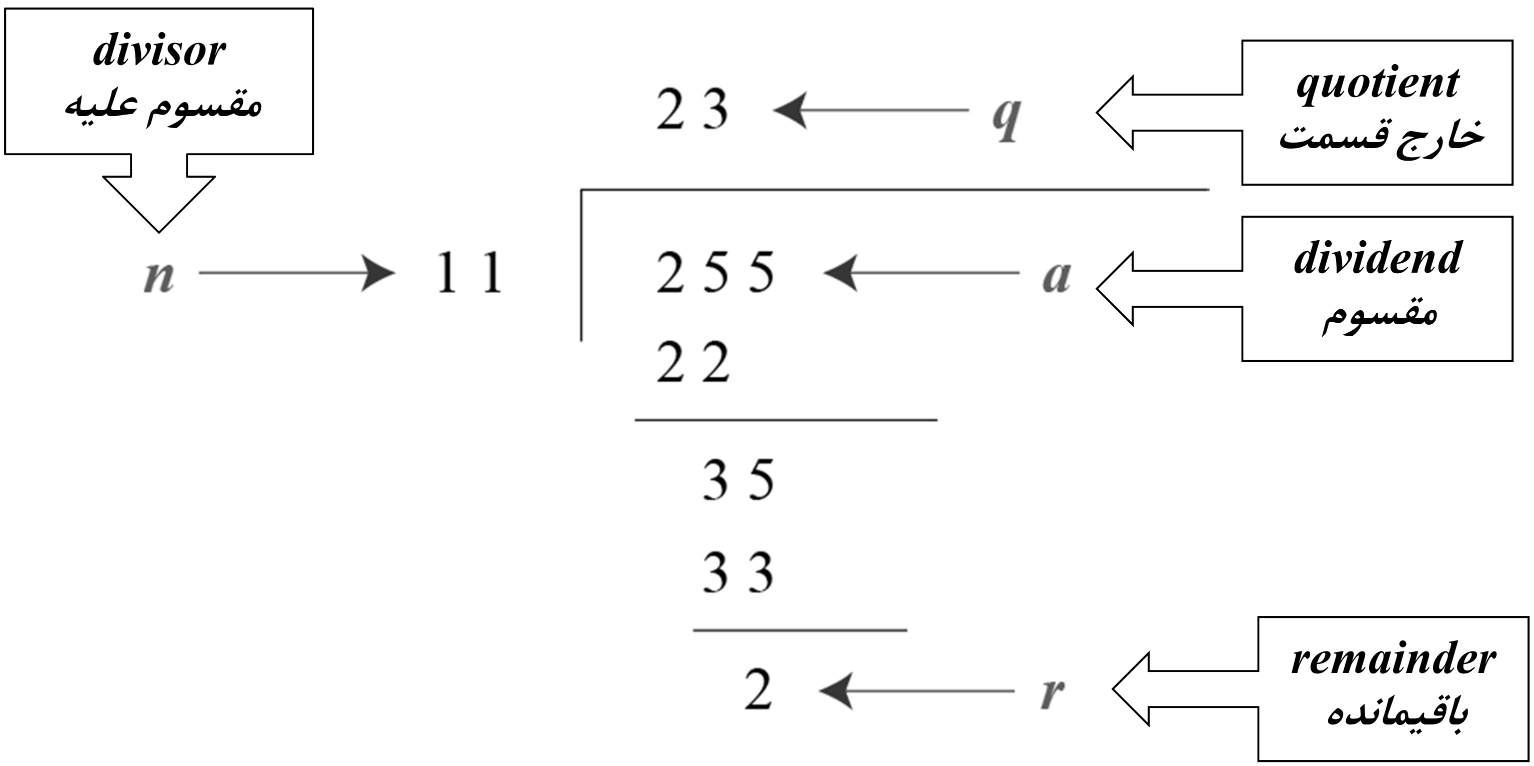
$$a = q \times n + r$$

2.1.3 Continued

Example 2.2

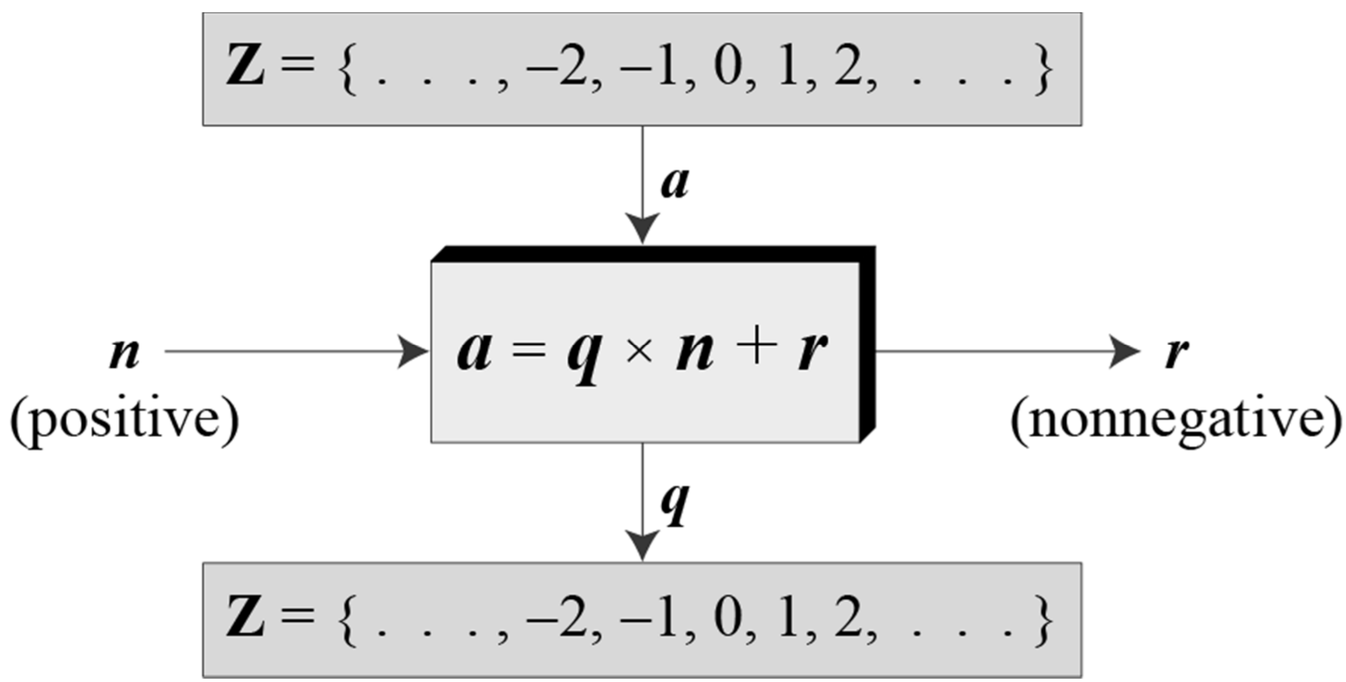
Assume that a = 255 and n = 11. We can find q = 23 and R = 2 using the division algorithm.

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



2.1.3 Continued

Figure 2.4 ***Division algorithm for integers***



2.1.3 Continued

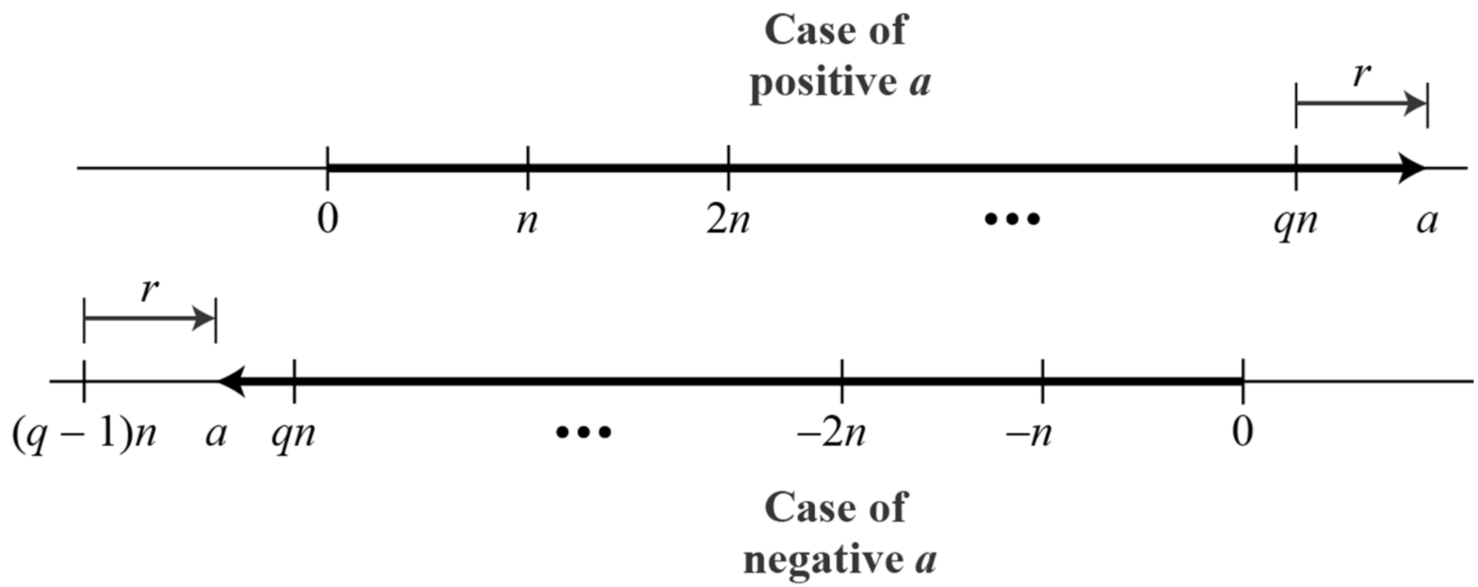
Example 2.3

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.

$$\underbrace{-255}_{a} = (\underbrace{\mathbf{-23}}_{q} \times \underbrace{11}_{n}) + (\underbrace{\mathbf{-2}}_{r}) \quad \leftrightarrow \quad -255 = (\underbrace{\mathbf{-24}}_{q-1} \times 11) + \underbrace{\mathbf{9}}_{n+r}$$

2.1.3 Continued

Figure 2.5 ***Graph of division alogorithm***



2.1.4 Divisbility (قابلیت تقسیم)

If a is not zero and we let r = 0 in the division relation, we get

$$a = q \times n$$

If the remainder is zero, $a \mid n$

If the remainder is not zero, $a \nmid n$

2.1.4 Continued

Example 2.4

a. The integer 4 divides the integer 32 because 32 = 8 × 4. We show this as

$$4 | 32$$

b. The number 8 does not divide the number 42 because 42 = 5 × 8 + 2. There is a remainder, the number 2, in the equation. We show this as

$$8 \nmid 42$$

2.1.4 Continued

Properties of divisibility

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

2.1.4 Continued

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 $11 \nmid (-32)$.

2.1.4 Continued

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 $3|66$.

2.1.4 Continued

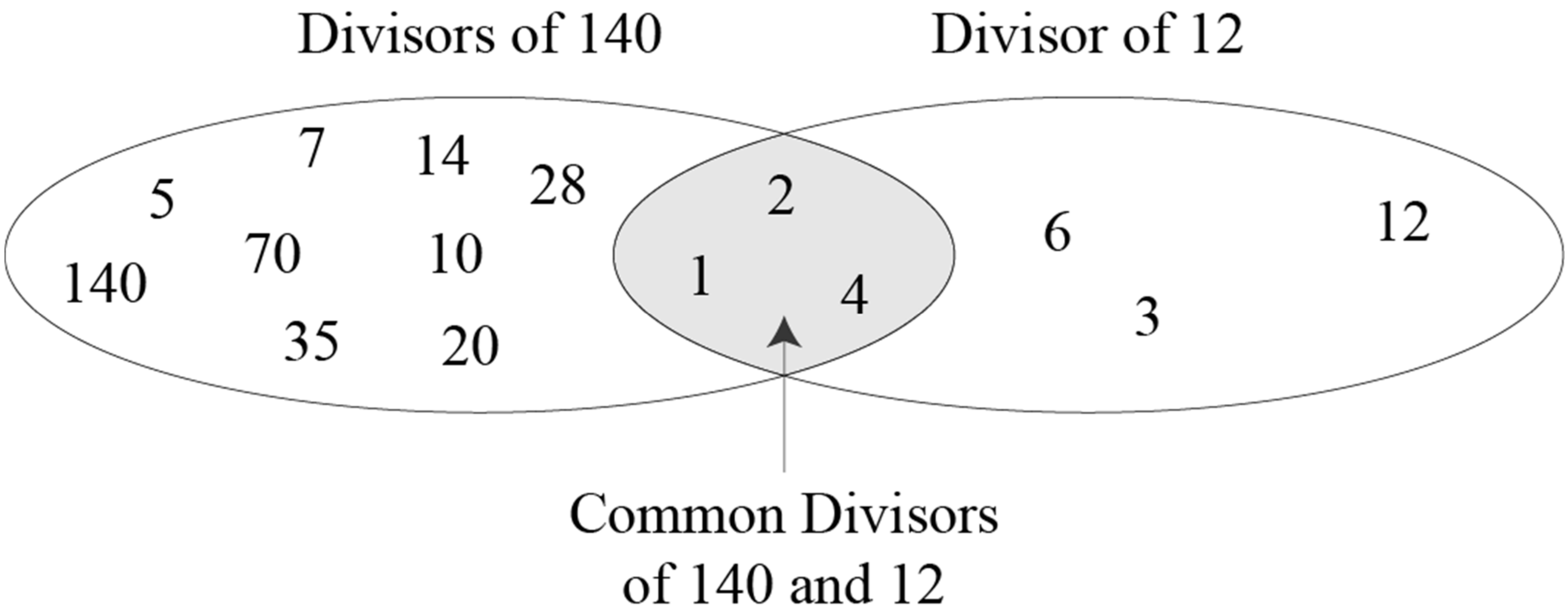
Note

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).

2.1.4 Continued

Figure 2.6 ***Common divisors of two integers***



2.1.4 Continued

Note **Greatest Common Divisor**

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

Note **Euclidean Algorithm**

Fact 1: gcd (a, 0) = a
Fact 2: gcd (a, b) = gcd (b, r), where r is the remainder of dividing a by b

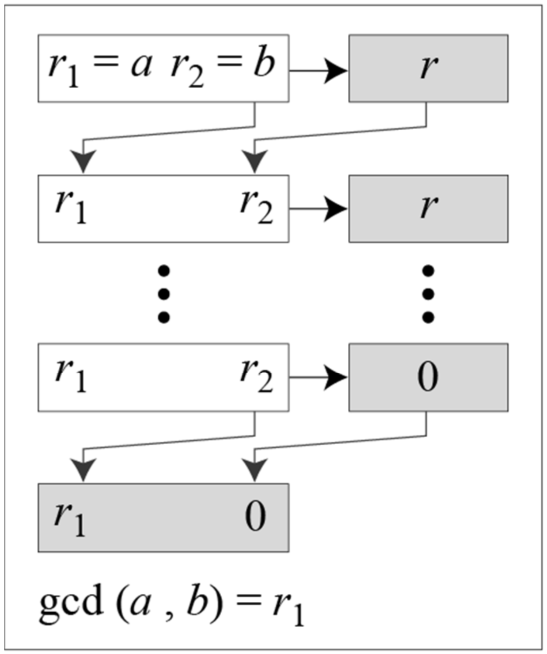
2.1.4 Continued

Euclidean Algorithm Fact 2 Example:

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

2.1.4 Continued

Figure 2.7 *Euclidean Algorithm*



a. Process

$r_1 \leftarrow a;$ $\quad r_2 \leftarrow b;$ (Initialization)

while ($r_2 > 0$)

{

$q \leftarrow r_1 / r_2;$

$r \leftarrow r_1 - q \times r_2;$

$r_1 \leftarrow r_2;$ $\quad r_2 \leftarrow r;$

}

gcd $(a, b) \leftarrow r_1$

b. Algorithm

2.1.4 Continued

Note

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

2.1.4 Continued

Example 2.7

Find the greatest common divisor of 2740 and 1760.

Solution

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	

2.1.4 Continued

Example 2.8

Find the greatest common divisor of 25 and 60.

Solution

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	

2.1.4 Continued

Extended Euclidean Algorithm

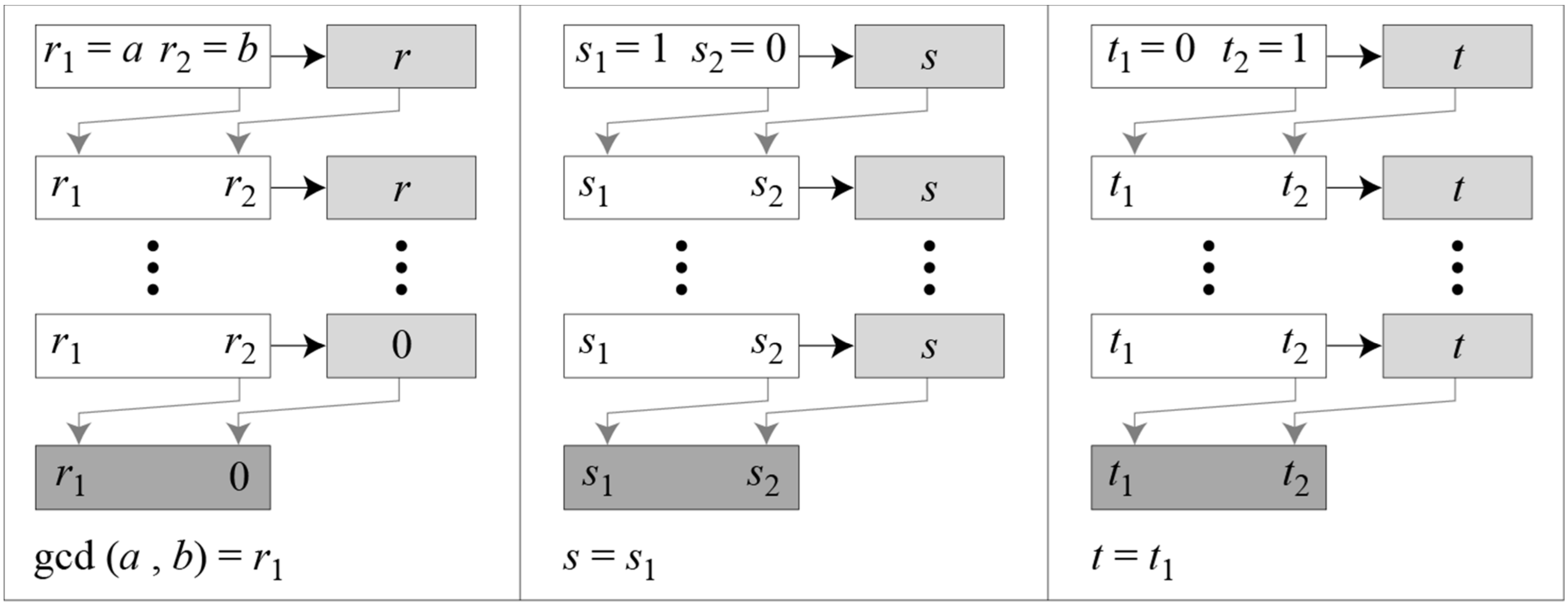
Given two integers *a* and *b*, we often need to find other two integers, *s* and *t*, such that

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

The extended Euclidean algorithm can calculate the gcd (*a*, *b*) and at the same time calculate the value of *s* and *t*.

2.1.4 Continued

Figure 2.8.a ***Extended Euclidean algorithm, part a***



a. Process

2.1.4 Continued

Figure 2.8.b *Extended Euclidean algorithm, part b*

$r_1 \leftarrow a;$ $r_2 \leftarrow b;$
$s_1 \leftarrow 1;$ $s_2 \leftarrow 0;$ (Initialization)
$t_1 \leftarrow 0;$ $t_2 \leftarrow 1;$

while ($r_2 > 0$)
{
  $q \leftarrow r_1 / r_2;$

  $r \leftarrow r_1 - q \times r_2;$
  $r_1 \leftarrow r_2;$ $r_2 \leftarrow r;$ (Updating r's)

  $s \leftarrow s_1 - q \times s_2;$
  $s_1 \leftarrow s_2;$ $s_2 \leftarrow s;$ (Updating s's)

  $t \leftarrow t_1 - q \times t_2;$
  $t_1 \leftarrow t_2;$ $t_2 \leftarrow$ t; (Updating t's)
}
gcd (a , b) $\leftarrow r_1;$ $s \leftarrow s_1;$ $t \leftarrow t_1$

b. Algorithm

2.1.4 Continued

Example 2.9

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

Solution

We get gcd (161, 28) = 7, *s* = −1 and *t* = 6.

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

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	

2.1.4 *Continued*

Example 2.10

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

Solution

We get gcd (17, 0) = 17, s = 1, and t = 0.

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

2.1.4 *Continued*

Example 2.11

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

Solution

We get gcd (0, 45) = 45, s = 0, and t = 1.

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	

2.1.4 Continued

Linear Diophantine Equation

یکی از کاربردهای الگوریتم اقلیدسی گسترش یافته پیدا کردن جــواب بــرای معادلــه‌ی خطــی دایوفانتاین است.

Note

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

Note

gcd (a,b)= d :
If $d \nmid c$, then the equation has no solution.
If d |c, then the equation has infinite number of solution.

2.1.4 Continued

Linear Diophantine Equation

Note

Particular solution:

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

Note

General solutions:

$x = x_0 + k\,(b/d)$ ***and*** $y = y_0 - k(a/d)$

where k is an integer

2.1.4 Continued

Example 2.12

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

Solution

۱- طرفین معادله را بر d تقسیم می‌کنیم. ((d = gcd(a,b))

d= gcd (21,14) = 7 then 3x+ 2y =5

۲- مقدار s و t را برای معادله‌ی $a_1s + b_1t = 1$ توسط الگوریتم اقلیدسی گسترش یافته به‌دست می‌آوریم: 3s+2t =1 مقدار s = 1 و t = -1 می‌شود. جواب خاص و عمومی معادله به شرح زیر است:

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 is an integer

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.

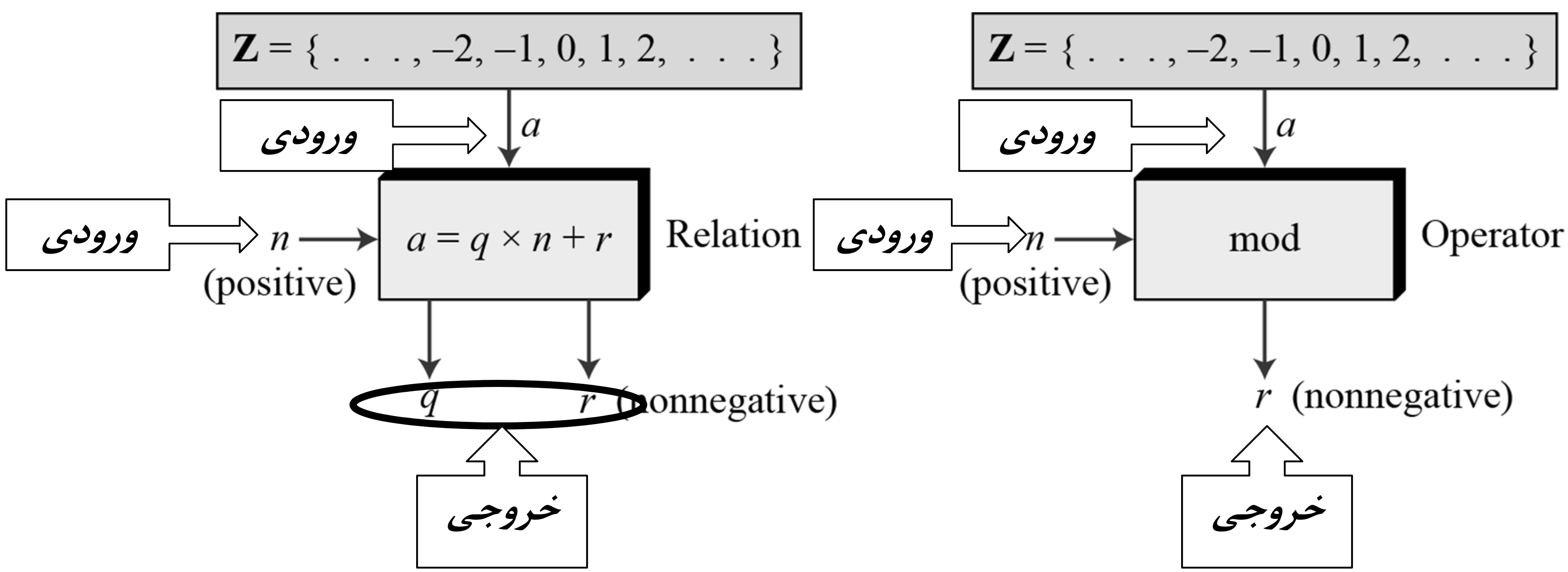
<u>Topics discussed in this section:</u>

2.2.1 Modular Operator
2.2.2 Set of Residues
2.2.3 Congruence
2.2.4 Operations in Z_n
2.2.5 Addition and Multiplication Tables
2.2.6 Different Sets

2.2.1 Modulo Operator (عملگر پیمانه ای)

***The modulo operator is shown as mod. The second input (n) is called the modulus* (پیمانه). *The output r is called the residue* (باقیمانده). (a mod n = r)**

Figure 2.9 ***Division algorithm and modulo operator***



2.1.4 Continued

Example 2.14

Find the result of the following operations:

a. 27 mod 5 **b. 36 mod 12**

c. −18 mod 14 **d. −7 mod 10**

Solution

a. Dividing 27 by 5 results in *r* = 2

b. Dividing 36 by 12 results in *r* = 0.

c. Dividing −18 by 14 results in *r* = −4. After adding the modulus *r* = 10

d. Dividing −7 by 10 results in r = −7. After adding the modulus to −7, r = 3.

2.2.2 Set of Residues

The modulo operation creates a set, which in modular arithmetic is referred to as the set of least residues modulo (پیمانه) n, or Z_n.

Figure 2.10 ***Some Z_n sets***

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

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

2.2.3 Congruence

In cryptography, we often used the concept of congruence instead of equality. To show that two integers are congruent (متجانس), we use the congruence (تجانس) operator (≡). For example, we write:

$$2 \equiv 12 \pmod{10} \qquad 13 \equiv 23 \pmod{10}$$
$$3 \equiv 8 \pmod{5} \qquad 8 \equiv 13 \pmod{5}$$

Congruence points

عملگر تجانس شبیه عملگر تساوی است اما تفاوت‌هایی هم دارد:

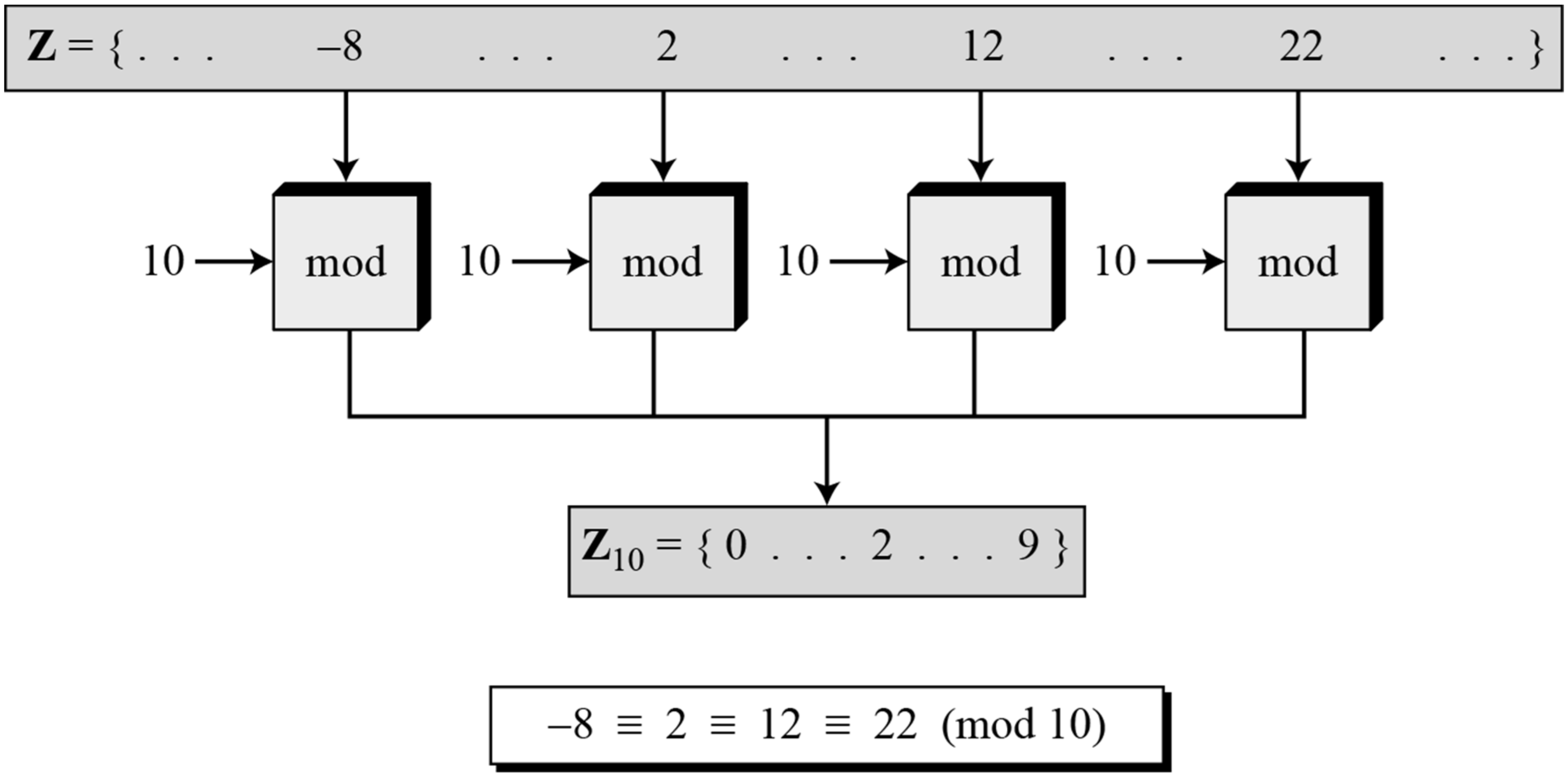
الف) اولاً عملگر تساوی اعضای مجموعه‌ی $\mathbf{Z}$ را به $\mathbf{Z}$ نگاشت می‌دهد. اما عملگر تجانس اعضای مجموعه‌ی $\mathbf{Z}$ را به $\mathbf{Z_n}$ نگاشت می‌دهد.

ثانیاً عملگر تساوی یک به یک (**one to one**) است اما عملگر تجانس تعداد زیادی به یک (**many to one**) است.

ب) عبارت (**mod n**) که ما در سمت راست عملگر تجانس استفاده می‌کنیم فقط برای مشخص کردن مجموعه مقصد ($\mathbf{Z_n}$) است. ما این عبارت را اضافه می‌کنیم تا نشان دهیم چه پیمانه‌ای در نگاشت استفاده می‌شود. نماد **mod** در این‌جا معنی متفاوتی با نماد **mod** در عملگز باینری دارد. به بیان دیگر نماد **mod** در **12 mod 10** *عملگر* است ولی عبارت (**mod 10**) در $2 \equiv 12 \pmod{10}$ به معنی این است که مجموعه‌ی مقصد $\mathbf{Z_{10}}$ است.

2.2.3 Continued

Figure 2.11 *Concept of congruence*



Congruence Relationship

2.2.3 Continued

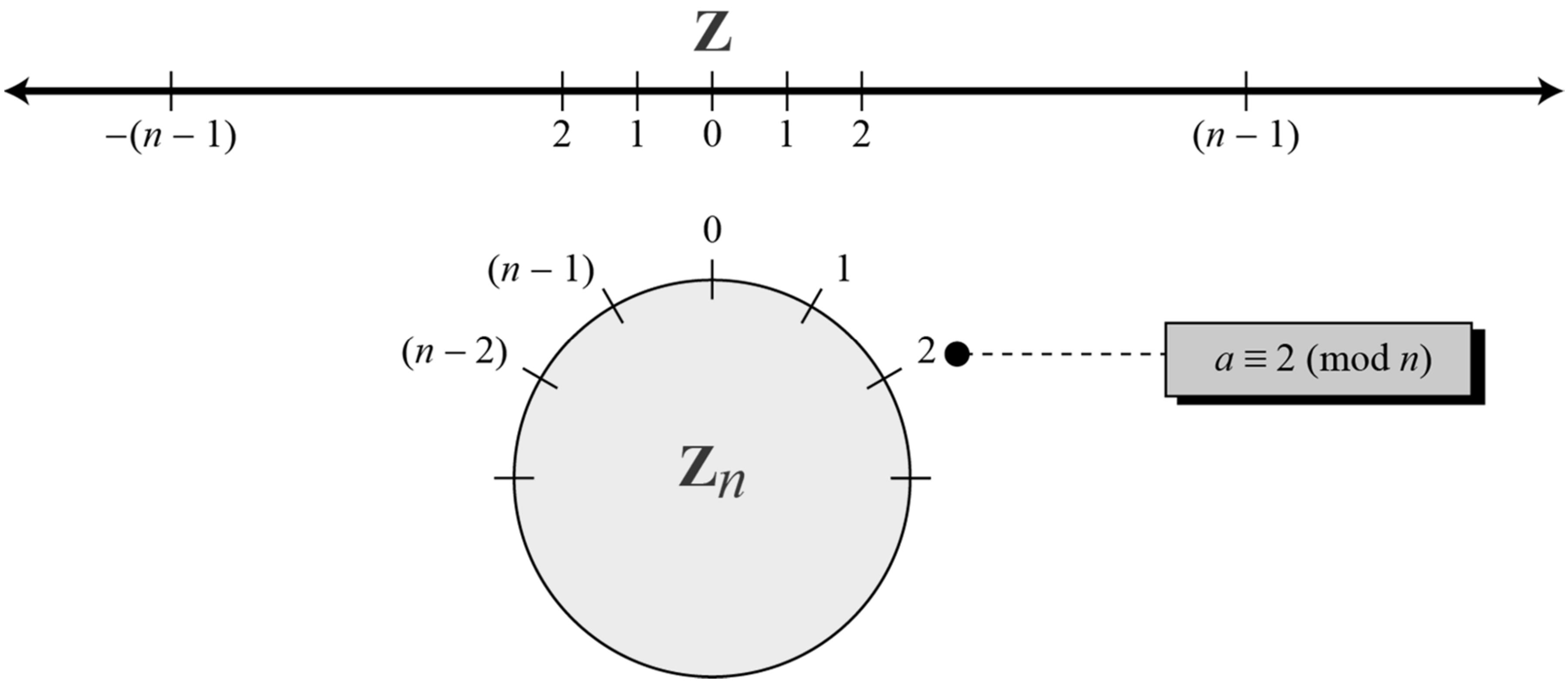
Residue Classes

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

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

2.2.3 Continued

Figure 2.12 ***Comparison of Z and Z_n using graphs***



2.2.3 Continued

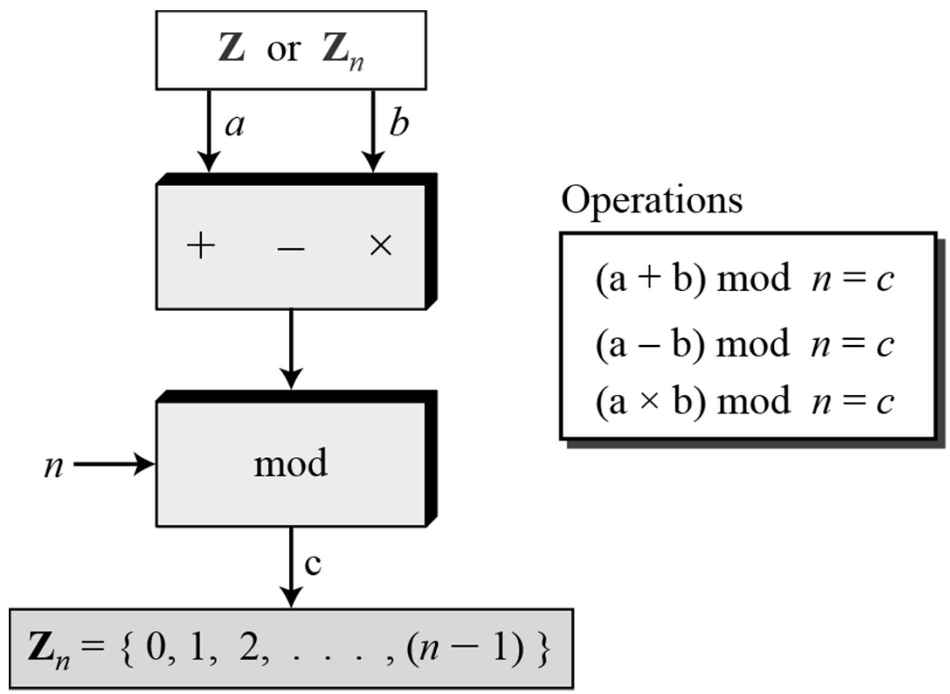
Example 2.15

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.

2.2.4 Operation in Z_n

The three binary operations that we discussed for the set Z can also be defined for the set Z_n. The result may need to be mapped to Z_n using the mod operator.

Figure 2.13 *Binary operations in Z_n*



Example 2.16

Perform the following operations (the inputs come from Zn):
a. Add 7 to 14 in Z_{15}.
b. Subtract 11 from 7 in Z_{13}.
c. Multiply 11 by 7 in Z_{20}.

Solution

$$(14 + 7) \bmod 15 \rightarrow (21) \bmod 15 = 6$$
$$(7 - 11) \bmod 13 \rightarrow (-4) \bmod 13 = 9$$
$$(7 \times 11) \bmod 20 \rightarrow (77) \bmod 20 = 17$$

2.2.4 *Continued*

Example 2.17

Perform the following operations (the inputs come from either Z or Z_n):
a. Add 17 to 27 in Z_{14}.
b. Subtract 43 from 12 in Z_{13}.
c. Multiply 123 by −10 in Z_{19}.

Solution

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

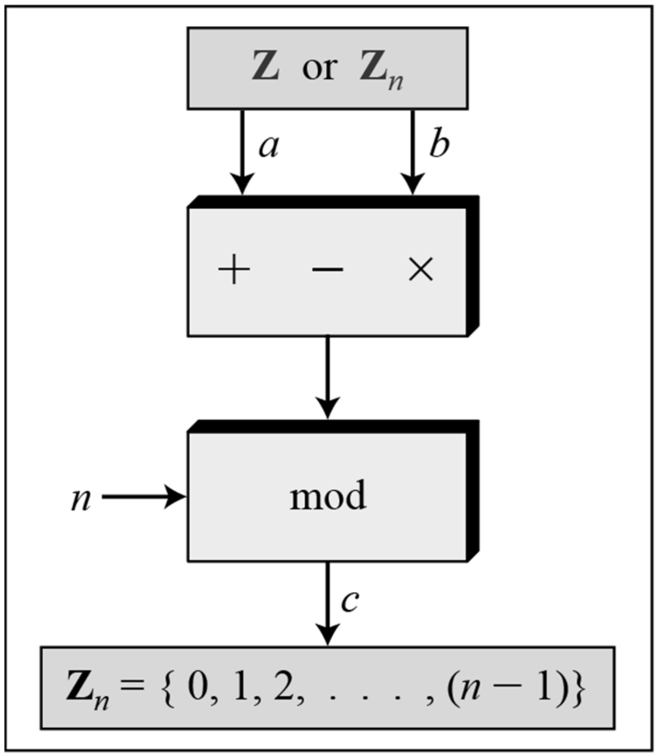
2.2.4 Continued

Properties

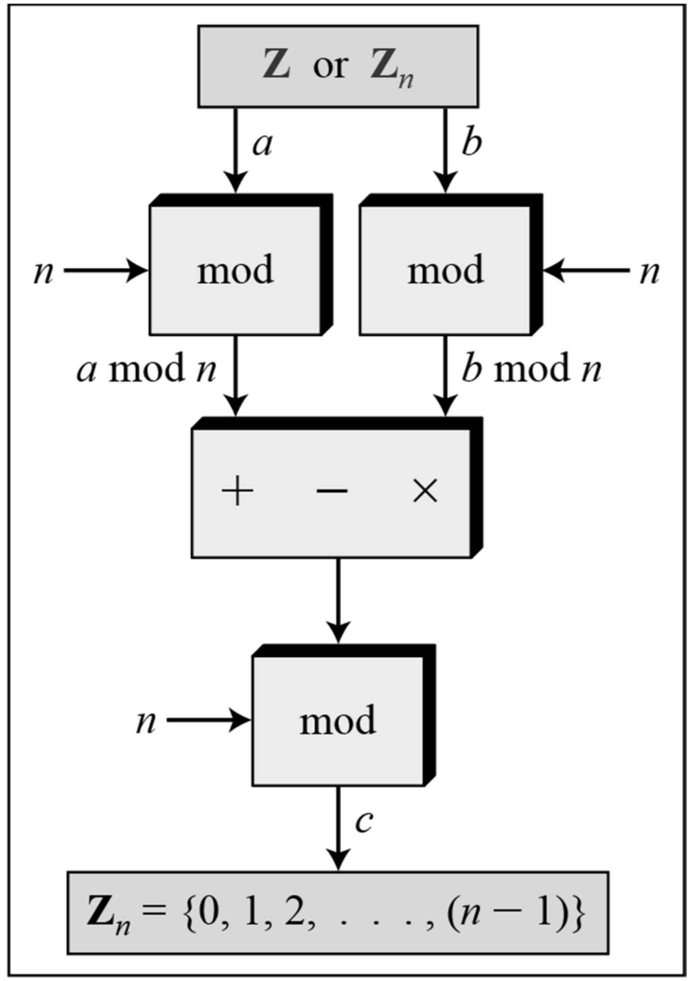
First Property:	$(a + b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$
Second Property:	$(a - b) \bmod n = [(a \bmod n) - (b \bmod n)] \bmod n$
Third Property:	$(a \times b) \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n$

2.2.4 Continued

Figure 2.14 ***Properties of mode operator***



a. Original process



b. Applying properties

2.2.4 Continued

Example 2.18

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

2.2.4 Continued

Example 2.19

In arithmetic, we often need to find the remainder of powers of 10 when divided by an integer.

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

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

2.2.4 Continued

Example 2.20

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

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

2.2.5 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).

2.2.5 Continue

Additive Inverse

In Z_n, two numbers *a* and *b* are additive inverses of each other if

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

Note

In modular arithmetic, each integer has an additive inverse. The sum of an integer and its additive inverse is congruent to 0 modulo n.

2.2.5 Continued

Example 2.21

Find all additive inverse pairs in Z10.

Solution

The six pairs of additive inverses are (0, 0), (1, 9), (2, 8), (3, 7), (4, 6), and (5, 5).

2.2.5 Continue

Multiplicative Inverse

In Z_n, two numbers *a* and *b* are the multiplicative inverse of each other if

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

Note

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.

2.2.5 Continue

Multiplicative Inverse

In Z_n, two numbers a and b are the multiplicative inverse of each other if

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

Note

a has a multiplicative inverse in Z_n, if and only if gcd (n, a) = 1.
In this case, a and n are said to be relatively prime.

Example 2.22

Find the multiplicative inverse of 8 in Z_{10}.

Solution

There is no multiplicative inverse because gcd (10, 8) = 2 ≠ 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 2.23

Find all multiplicative inverses in 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.

2.2.5 Continued

Example 2.24

Find all multiplicative inverse pairs in Z_{11}.

Solution

We have seven pairs: (1, 1), (2, 6), (3, 4), (5, 9), (7, 8), and (10, 10).

2.2.5 *Continued*

Multiplicative Inverse

The extended Euclidean algorithm we discussed earlier in the chapter can find the multiplicative inverse of b in 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

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

Now we apply the modulo operator to both sides. In other words, we map each side to Z_n. We will have

$(s \times n + b \times t) \bmod n = 1 \bmod n$

$[(s \times n) \bmod n] + [(b \times t) \bmod n] = 1 \bmod n$

$0 + [(b \times t) \bmod n] = 1$

$(b \times t) \bmod n = 1$ → This means t is the multiplicative inverse of b in Z_n

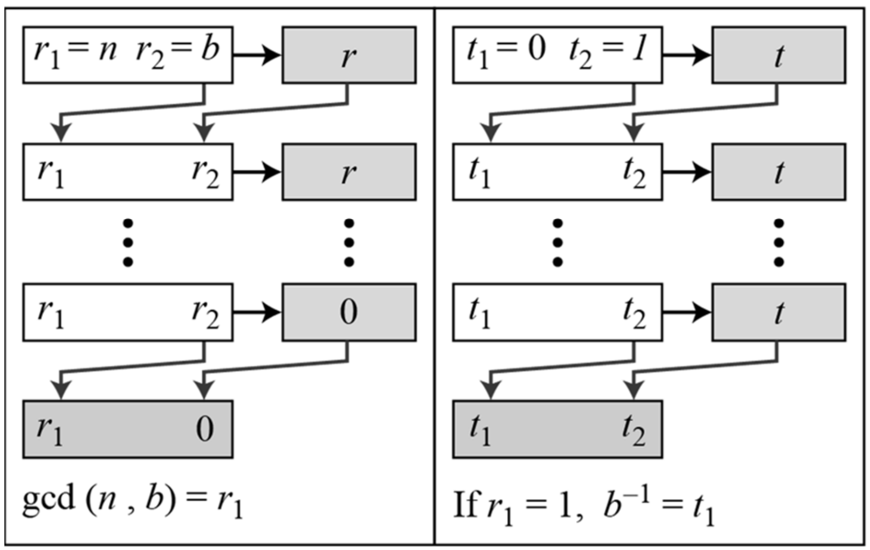
2.2.5 Continued

Note

The extended Euclidean algorithm finds the multiplicative inverses of b in 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 Z_n.

2.2.5 Continued

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



a. Process

$r_1 \leftarrow n$; $r_2 \leftarrow b$;
$t_1 \leftarrow 0$; $t_2 \leftarrow 1$;

while $(r_2 > 0)$
{
$q \leftarrow r_1 / r_2$;

$r \leftarrow r_1 - q \times r_2$;
$r_1 \leftarrow r_2$; $r_2 \leftarrow r$;

$t \leftarrow t_1 - q \times t_2$;
$t_1 \leftarrow t_2$; $t_2 \leftarrow t$;
}
if $(r_1 = 1)$ then $b^{-1} \leftarrow t_1$

b. Algorithm

2.2.5 Continued

Example 2.25

Find the multiplicative inverse of 11 in Z_{26}.

Solution

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; the inverse of 11 is –7 or 19.

2.2.5 *Continued*

Example 2.26

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

Solution

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; the inverse of 23 is –13 or 87.

Example 2.27

Find the inverse of 12 in Z_{26}.

Solution

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) is 2; the inverse does not exist.

2.2.6 Addition and Multiplication Tables

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

2.2.7 *Different Sets*

Figure 2.17 ***Some Z_n and $Z_n{}^*$ sets***

$\mathbf{Z}_6 = \{0, 1, 2, 3, 4, 5\}$	$\mathbf{Z}_6{}^* = \{1, 5\}$
$\mathbf{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$	$\mathbf{Z}_7{}^* = \{1, 2, 3, 4, 5, 6\}$
$\mathbf{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$	$\mathbf{Z}_{10}{}^* = \{1, 3, 7, 9\}$

Note

We need to use Z_n when additive inverses are needed; we need to use Z_n* when multiplicative inverses are needed.

2.2.8 Two More Sets

Cryptography often uses two more sets: Z_p and Z_p*. The **modulus** ***in these two sets is a*** **prime number.**

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

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.

Topics discussed in this section:

2.3.1 Definitions
2.3.2 Operations and Relations
2.3.3 Determinants
2.3.4 Residue Matrices

2.3.1 Definition

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

$$\text{Matrix } \mathbf{A}: \; l \text{ rows} \overbrace{\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & & \vdots \\ a_{l1} & a_{l2} & \cdots & a_{lm} \end{bmatrix}}^{m \text{ columns}}$$

The element a_{ij} is located in the ith row and jth column.

2.3.1 Continued

Figure 2.19 ***Examples of matrices***

$$\begin{bmatrix} 2 & 1 & 5 & 11 \end{bmatrix}$$

Row matrix

$$\begin{bmatrix} 2 \\ 4 \\ 12 \end{bmatrix}$$

Column matrix

$$\begin{bmatrix} 23 & 14 & 56 \\ 12 & 21 & 18 \\ 10 & 8 & 31 \end{bmatrix}$$

Square matrix

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}$$

0

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

I

2.3.2 Operations and Relations

Example 2.28

Figure 2.20 shows an example of addition and subtraction.

Figure 2.20 ***Addition and subtraction of matrices***

$$\begin{bmatrix} 12 & 4 & 4 \\ 11 & 12 & 30 \end{bmatrix} = \begin{bmatrix} 5 & 2 & 1 \\ 3 & 2 & 10 \end{bmatrix} + \begin{bmatrix} 7 & 2 & 3 \\ 8 & 10 & 20 \end{bmatrix}$$

$$\mathbf{C} = \mathbf{A} + \mathbf{B}$$

$$\begin{bmatrix} -2 & 0 & -2 \\ -5 & -8 & 10 \end{bmatrix} = \begin{bmatrix} 5 & 2 & 1 \\ 3 & 2 & 10 \end{bmatrix} - \begin{bmatrix} 7 & 2 & 3 \\ 8 & 10 & 20 \end{bmatrix}$$

$$\mathbf{D} = \mathbf{A} - \mathbf{B}$$

Example 2. 29

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*

$$\underset{\mathbf{C}}{\begin{bmatrix} 53 \end{bmatrix}} = \underset{\mathbf{A}}{\begin{bmatrix} 5 & 2 & 1 \end{bmatrix}} \times \underset{\mathbf{B}}{\begin{bmatrix} 7 \\ 8 \\ 2 \end{bmatrix}}$$

In which: $53 = 5 \times 7 + 2 \times 8 + 1 \times 2$

2.3.2 Continued

Example 2. 30

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***

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

2.3.2 Continued

Example 2. 31

Figure 2.23 shows an example of scalar multiplication.

Figure 2.23 ***Scalar multiplication*** **(ضرب عددی)**

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

2.3.3 Determinant

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

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

Where $\mathbf{A}_{ij}$ is a matrix obtained from **A** by deleting the ith row and jth column.

Note

The determinant is defined only for a square matrix.

2.3.3 Continued

Example 2. 32

Figure 2.24 shows how we can calculate the determinant of a 2 × 2 matrix based on the determinant of a 1 × 1 matrix.

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

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

or

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

2.3.3 Continued

Example 2. 33

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***

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

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

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

2.3.4 Inverses

Note

The additive inverse of matrix A is another matrix B such that A + B = 0.

Note

***Multiplicative inverses are only defined for* square matrices.**
The multiplicative inverse of a square matrix A is a square matrix B such that
A × B = B × A = I

2.3.5 Residue Matrices

Cryptography uses residue matrices: matrices where all elements are in Z_n. A residue matrix has a multiplicative inverse if gcd (det(A), n) = 1.

Example 2. 34

Figure 2.26 ***A residue matrix and its multiplicative inverse***

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

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

2-4 LINEAR CONGRUENCE

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

<u>Topics discussed in this section:</u>

2.4.1 Single-Variable Linear Equations
2.4.2 Set of Linear Equations

2.4.1 Single-Variable Linear Equations

Equations of the form $ax \equiv b \pmod{n}$ 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.

1. Reduce the equation by dividing both sides of the equation (including the modulus) by d.
2. Multiply both sides of the reduced equation by the multiplicative inverse of a to find the <u>particular solution</u> x_o.
3. The <u>general solutions</u> are $x = x_o + k\,(n/d)$ for $k = 0, 1, \ldots, (d - 1)$.

2.4.1 Continued

Example 2.35

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

Solution

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

Example 2.36

Solve the equation 14 $x \equiv 12 \pmod{18}$. ($7^{-1} = 4$)

Solution

$$14x \equiv 12 \pmod{18} \rightarrow \quad 7x \equiv 6 \pmod{9} \quad \rightarrow \quad x \equiv 6\ (7^{-1}) \pmod{9}$$

$$x_0 = (6 \times 7^{-1}) \bmod 9 = (6 \times 4) \pmod{9} = 6$$

$$x_1 = x_0 + 1 \times (18/2) = 15$$

2.4.1 Continued

Example 2.37

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: $3 \times 5 + 4 \equiv 6 \pmod{13}$.

2.4.2 Single-Variable 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.

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 2.38

Solve the set of following three equations:

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

Solution

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.