



Cryptography (CS-501)

Mathematics of Cryptography Modular Arithmetic, Congruence, and Matrices

*Dr Samayveer Singh
Assistant Professor*

*Department of Computer Science & Engineering
National Institute Technology Jalandhar, Punjab, India
samays@nitj.ac.in*

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.

- 1.1 Set of Integers**
- 1.2 Binary Operations**
- 1.3 Integer Division**
- 1.4 Divisibility**
- 1.5 Linear Diophantine Equations**

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 1).

$$Z = \{ \dots, -2, -1, 0, 1, 2, \dots \}$$

Figure 1 *The set of integers*

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.

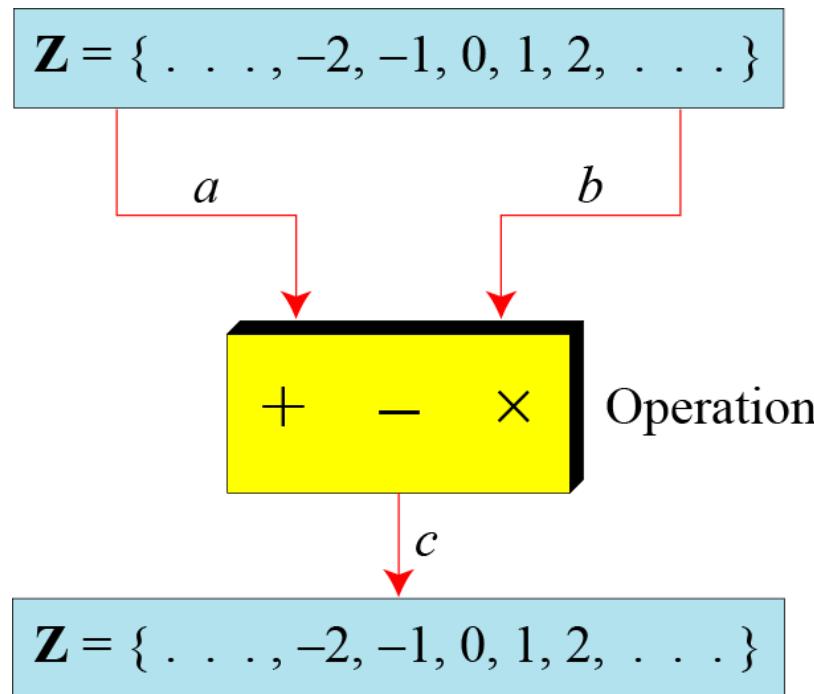


Figure 2 *Three binary operations for the set of integers*

1.2 Continued

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

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

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

1.3 Continued

Example 2

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

$$\begin{array}{r} 23 \xleftarrow{\text{q}} \\[-1ex] \boxed{255 \xleftarrow{\text{a}}} \\[-1ex] 22 \\ \hline 35 \\ 33 \\ \hline 2 \xleftarrow{\text{r}} \end{array}$$

Figure 3 Example 2, finding the quotient and the remainder

1.3 Continued

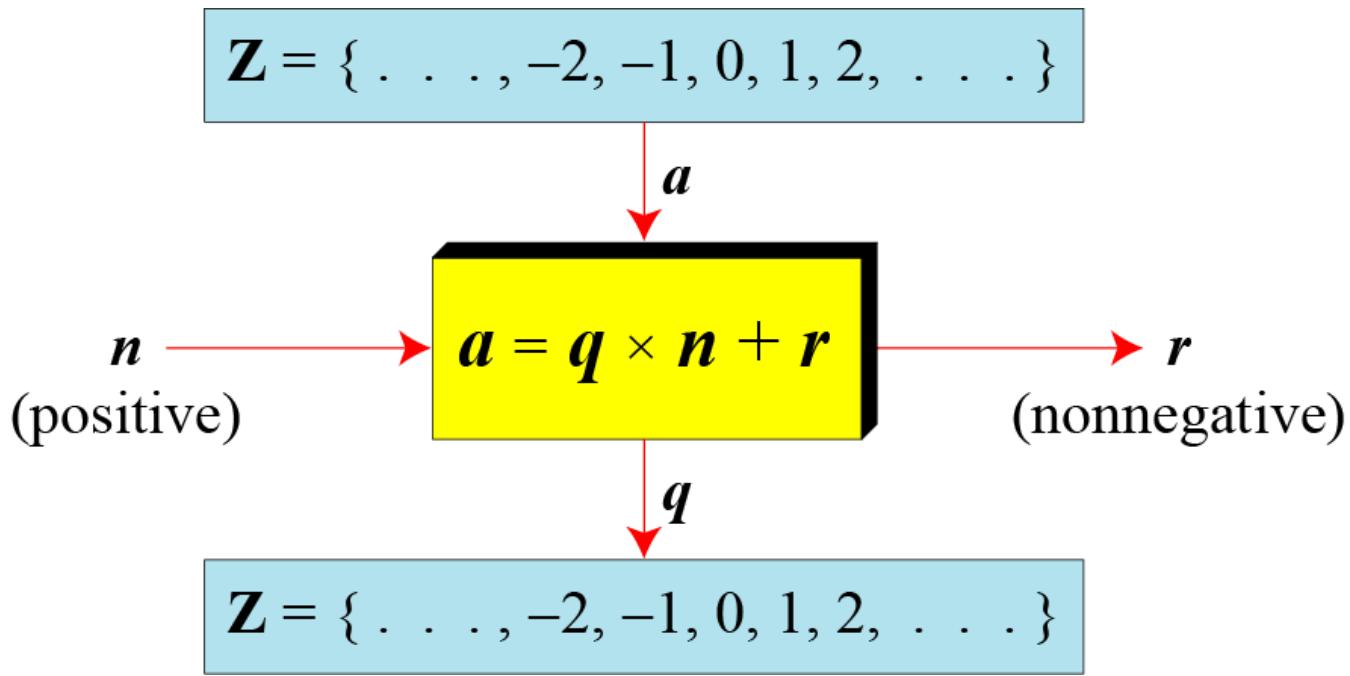


Figure 4 Division algorithm for integers

1.3 Continued

Example 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.

$$-255 = (-23 \times 11) + (-2) \quad \leftrightarrow \quad -255 = (-24 \times 11) + 9$$

1.3 Continued

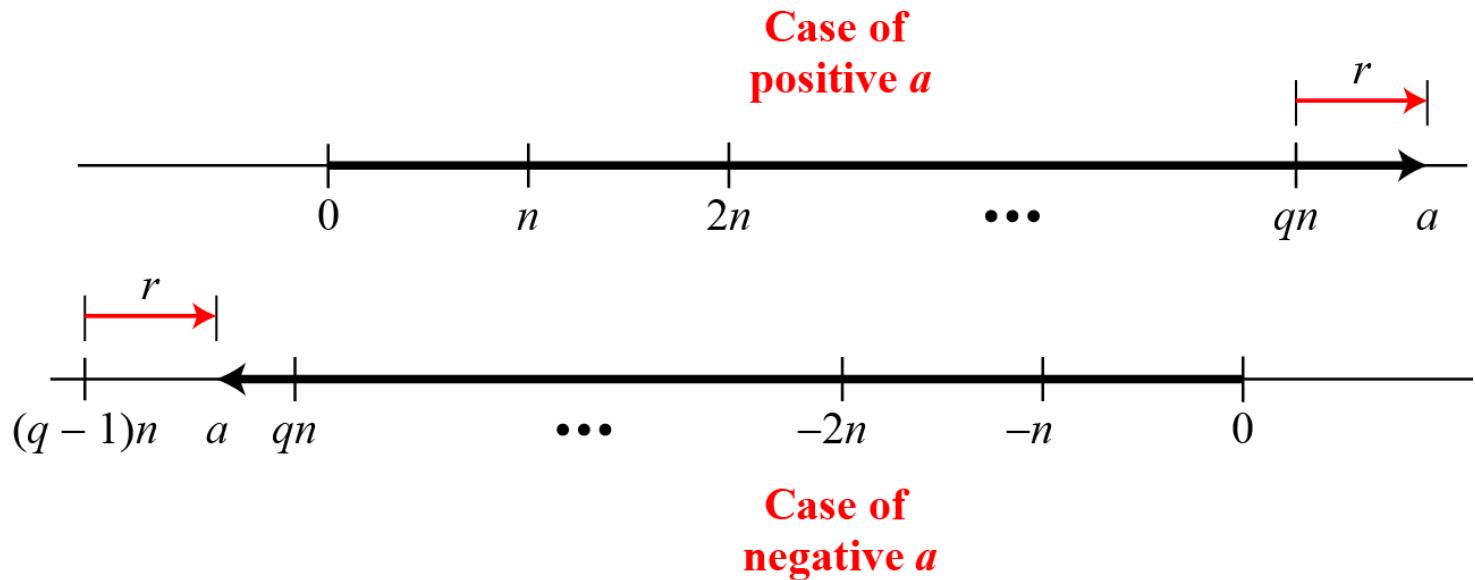


Figure 5 Graph of division algorithm

1.4 Divisibility

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, $a | n$

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

1.4 Continued

Example 4

- a. The integer 4 divides the integer 32 because $32 = 8 \times 4$. We show this as

$$4 | 32$$

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

$$8 \nmid 42$$

1.4 Continued

Properties

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

1.4 Continued

Example 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 $11\nmid (-32)$.

1.4 Continued

Example 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 $3|66$.

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).

1.4 Continued

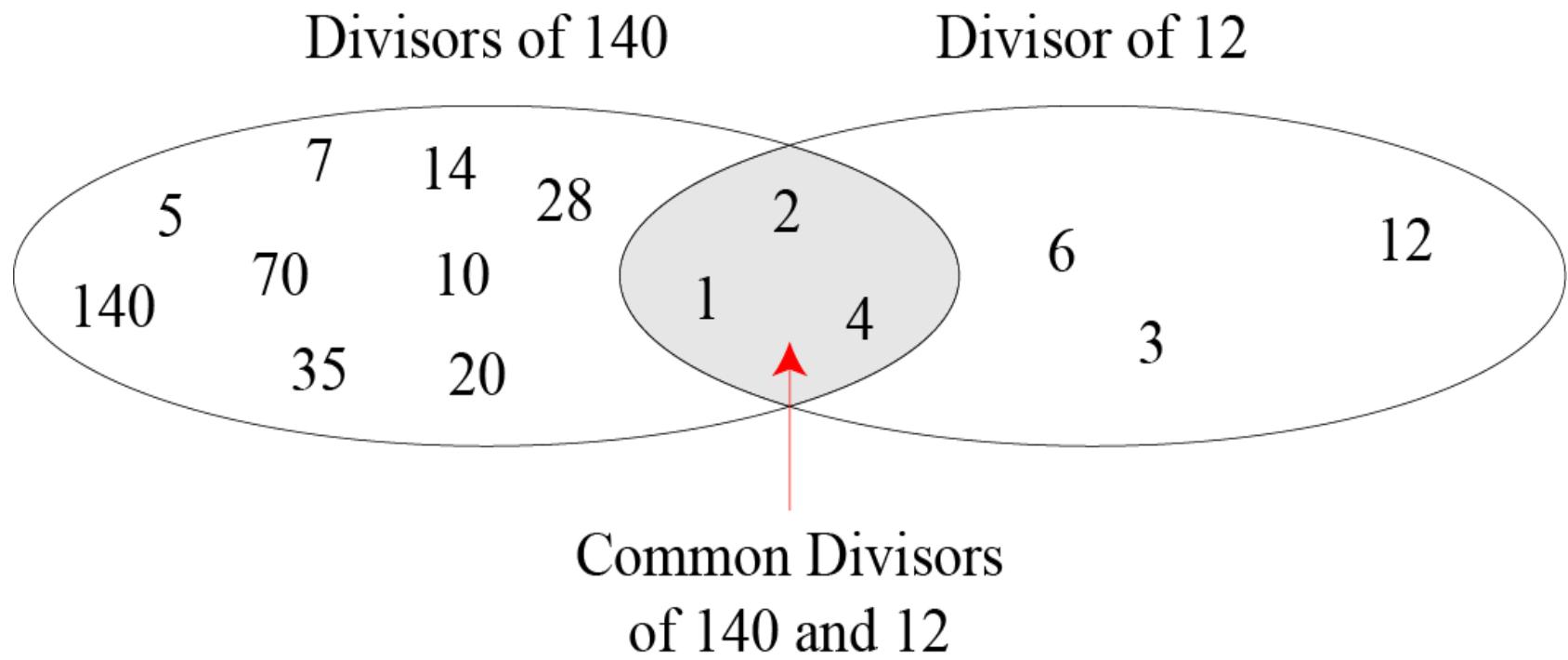


Figure 6 *Common divisors of two integers*

1.4 Continued

Note

Greatest Common Divisor

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

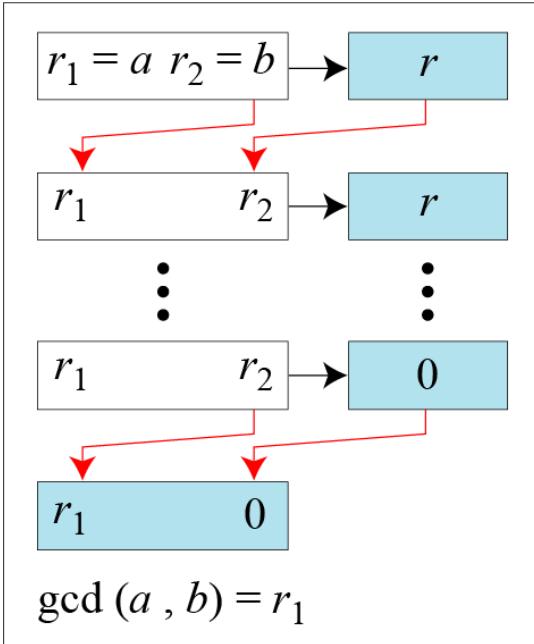
Note

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

1.4 Continued



a. Process

```
 $r_1 \leftarrow a; \quad r_2 \leftarrow b;$  (Initialization)  
while ( $r_2 > 0$ )  
{  
     $q \leftarrow r_1 / r_2;$   
     $r \leftarrow r_1 - q \times r_2;$   
     $r_1 \leftarrow r_2; \quad r_2 \leftarrow r;$   
}  
 $\text{gcd}(a, b) \leftarrow r_1$ 
```

b. Algorithm

Figure 7 *Euclidean Algorithm*

Note

When $\text{gcd}(a, b) = 1$, we say that a and b are relatively prime.

1.4 Continued

Note

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

1.4 Continued

Example 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	

1.4 Continued

Example 8

Find the greatest common divisor of 25 and 60.

Solution

We have $\gcd(25, 60) = 5$.

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

1.4 Continued

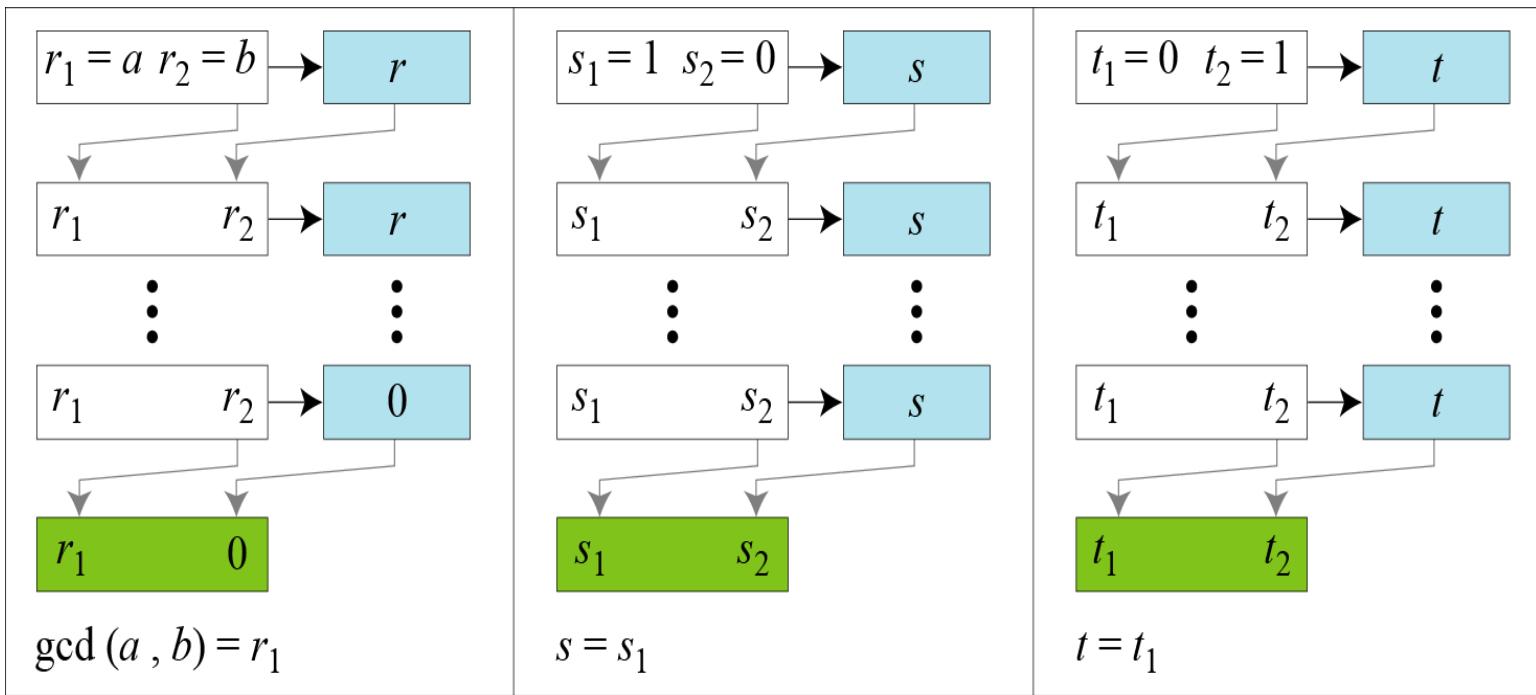
Extended Euclidean Algorithm

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 .

1.4 Continued



a. Process

Figure 8.a *Extended Euclidean algorithm, part a*

1.4 Continued

```
r1 ← a;      r2 ← b;  
s1 ← 1;      s2 ← 0;  
t1 ← 0;      t2 ← 1;          (Initialization)  
  
while (r2 > 0)  
{  
    q ← r1 / r2;  
  
    r ← r1 - q × r2;  
    r1 ← r2; r2 ← r;          (Updating r's)  
  
    s ← s1 - q × s2;  
    s1 ← s2; s2 ← s;          (Updating s's)  
  
    t ← t1 - q × t2;  
    t1 ← t2; t2 ← t;          (Updating t's)  
}  
  
gcd (a , b) ← r1; s ← s1; t ← t1
```

b. Algorithm

Figure 8.b *Extended Euclidean algorithm, part b*

1.4 Continued

Example 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 $t = 6$.

q	r_I	r_2	r	s_I	s_2	s	t_I	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	

1.4 Continued

Example 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	

1.4 Continued

Example 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	

1.4 Continued

Linear Diophantine Equation

Note

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

1.4 Continued

Linear Diophantine Equation

Note

Particular solution:

$$x_0 = (c/d)s \text{ and } y_0 = (c/d)t$$

Note

General solutions:

$$x = x_0 + k(b/d) \text{ and } y = y_0 - k(a/d)$$

where k is an integer

1.4 Continued

Example 12

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

Solution

Particular: $x_0 = 5 \times 1 = 5$ and $y_0 = 5 \times (-1) = -5$

General: $x = 5 + k \times 2$ and $y = -5 - k \times 3$

1.4 Continued

Example 13

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 $5 \mid 100$, the equation has an infinite number of solutions, but only a few of them are acceptable in this case. The general solutions with x and y nonnegative are

$$(0, 20), (1, 16), (2, 12), (3, 8), (4, 4), (5, 0).$$

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.

- 2.1 Modular Operator**
- 2.2 Set of Residues**
- 2.3 Congruence**
- 2.4 Operations in Z_n**
- 2.5 Addition and Multiplication Tables**
- 2.6 Different Sets**

2.1 Modulo Operator

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

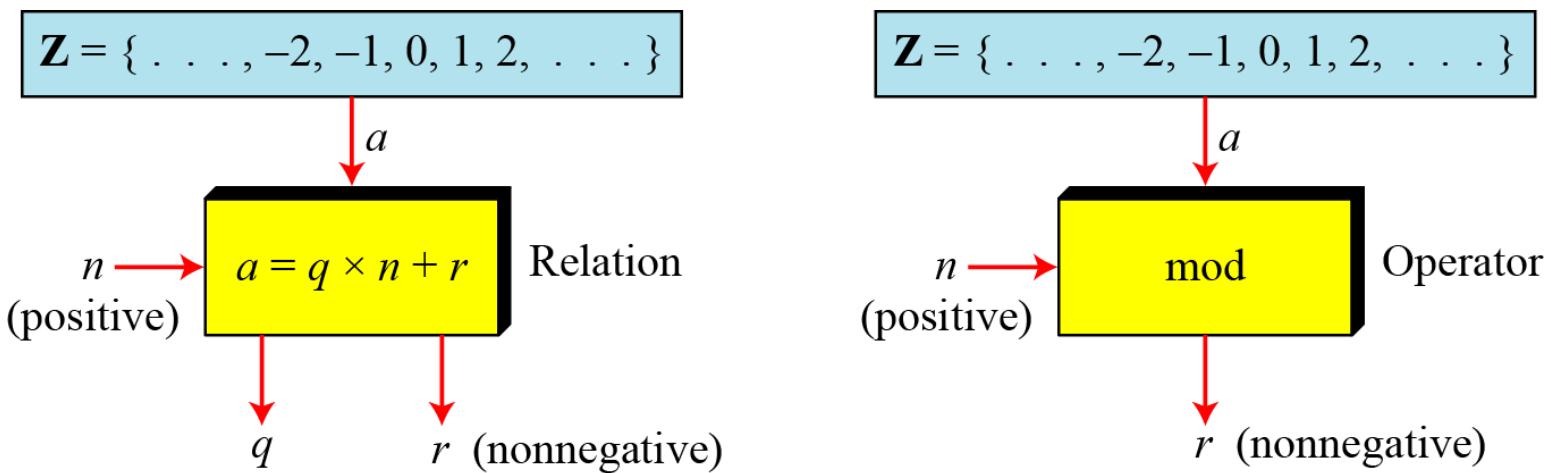


Figure 9 *Division algorithm and modulo operator*

1.4 Continued

Example 14

Find the result of the following operations:

- a. $27 \bmod 5$
- b. $36 \bmod 12$
- c. $-18 \bmod 14$
- d. $-7 \bmod 10$

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 Set of Residues

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

$$Z_n = \{ 0, 1, 2, 3, \dots, (n - 1) \}$$

$$Z_2 = \{ 0, 1 \}$$

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

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

Figure 10 Some Z_n sets

2.3 Congruence

To show that two integers are congruent, we use the congruence operator (\equiv). For example, we write:

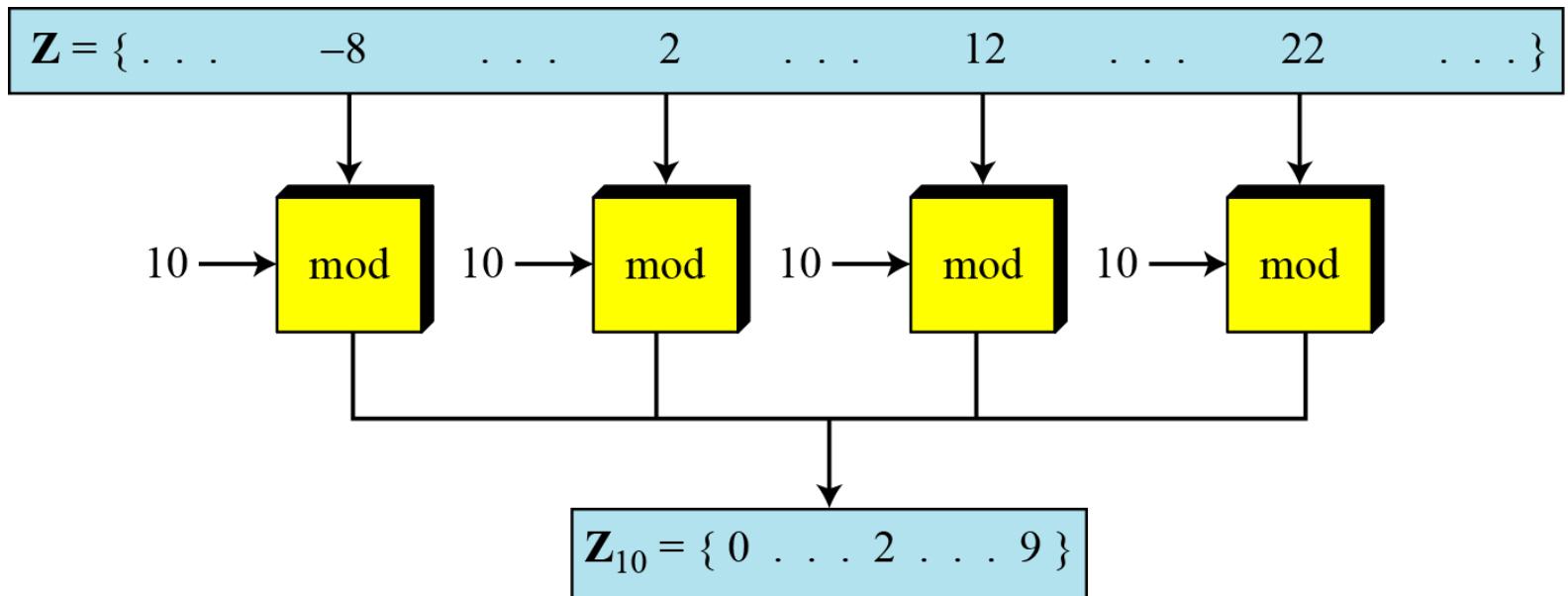
$$2 \equiv 12 \pmod{10}$$

$$3 \equiv 8 \pmod{5}$$

$$13 \equiv 23 \pmod{10}$$

$$8 \equiv 13 \pmod{5}$$

2.3 Continued



$$-8 \equiv 2 \equiv 12 \equiv 22 \pmod{10}$$

Congruence Relationship

Figure 11 *Concept of congruence*

2.3 Continued

Residue Classes

A residue class $[a]$ or $[a]_n$ is the set of integers congruent modulo n .

$$[0] = \{ \dots, -15, -10, -5, 0, 5, 10, 15, \dots \}$$

$$[1] = \{ \dots, -14, -9, -4, 1, 6, 11, 16, \dots \}$$

$$[2] = \{ \dots, -13, -8, -3, 2, 7, 12, 17, \dots \}$$

$$[3] = \{ \dots, -12, -7, -5, 3, 8, 13, 18, \dots \}$$

$$[4] = \{ \dots, -11, -6, -1, 4, 9, 14, 19, \dots \}$$

2.3 Continued

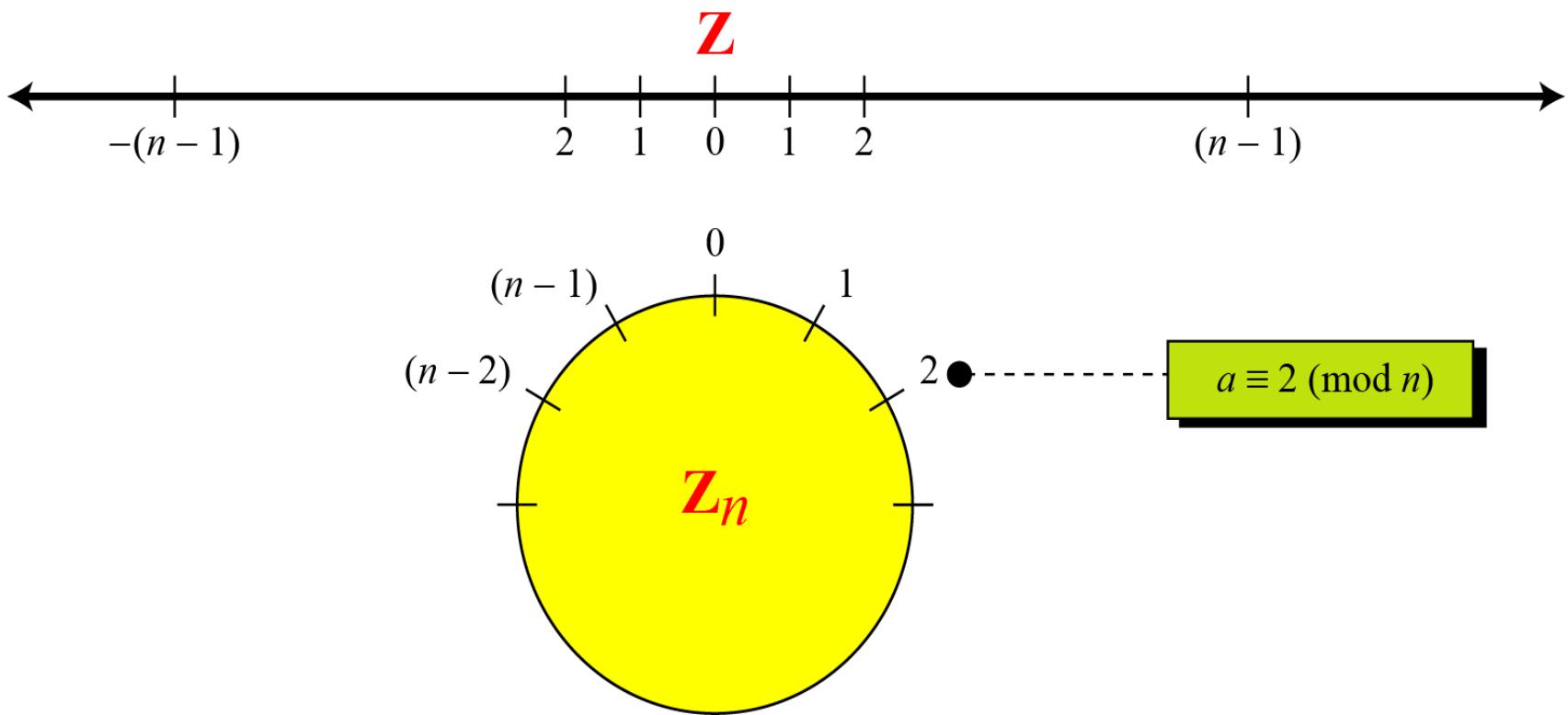


Figure 12 Comparison of \mathbb{Z} and \mathbb{Z}_n using graphs

2.3 Continued

Example 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.

2.4 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.

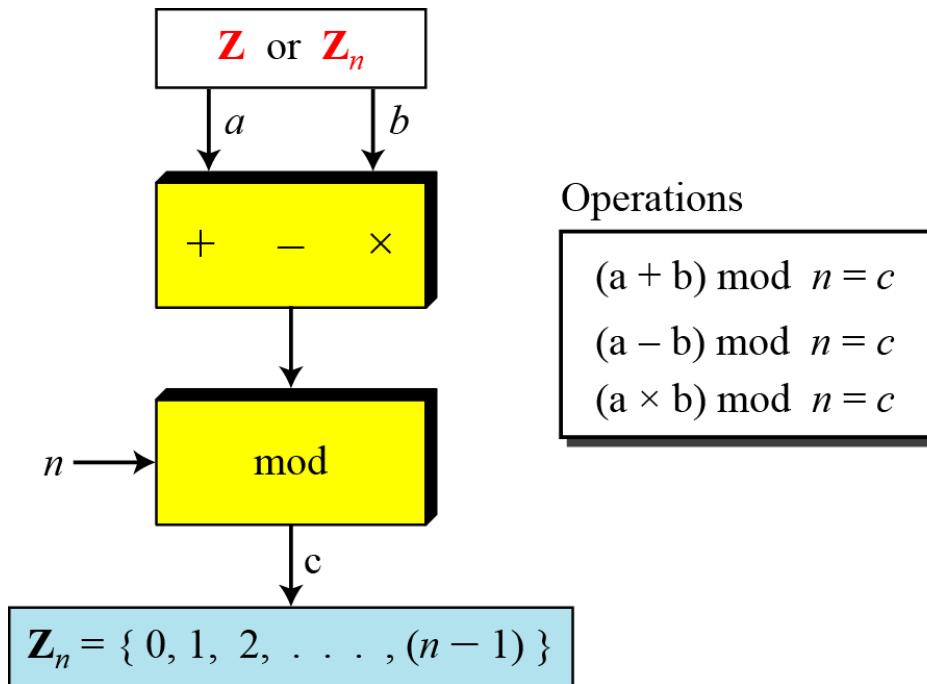


Figure 13 Binary operations in Z_n

2.4 Continued

Example 16

Perform the following operations (the inputs come from Z_n):

- Add 7 to 14 in Z_{15} .
- Subtract 11 from 7 in Z_{13} .
- Multiply 11 by 7 in Z_{20} .

Solution

$$(14 + 7) \text{ mod } 15 \rightarrow (21) \text{ mod } 15 = 6$$

$$(7 - 11) \text{ mod } 13 \rightarrow (-4) \text{ mod } 13 = 9$$

$$(7 \times 11) \text{ mod } 20 \rightarrow (77) \text{ mod } 20 = 17$$

2.4 Continued

Example 17

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

- Add 17 to 27 in \mathbb{Z}_{14} .
- Subtract 43 from 12 in \mathbb{Z}_{13} .
- Multiply 123 by -10 in \mathbb{Z}_{19} .

Solution

$$(14 + 7) \text{ mod } 15 \rightarrow (21) \text{ mod } 15 = 6$$

$$(7 - 11) \text{ mod } 13 \rightarrow (-4) \text{ mod } 13 = 9$$

$$(7 \times 11) \text{ mod } 20 \rightarrow (77) \text{ mod } 20 = 17$$

2.4 Continued

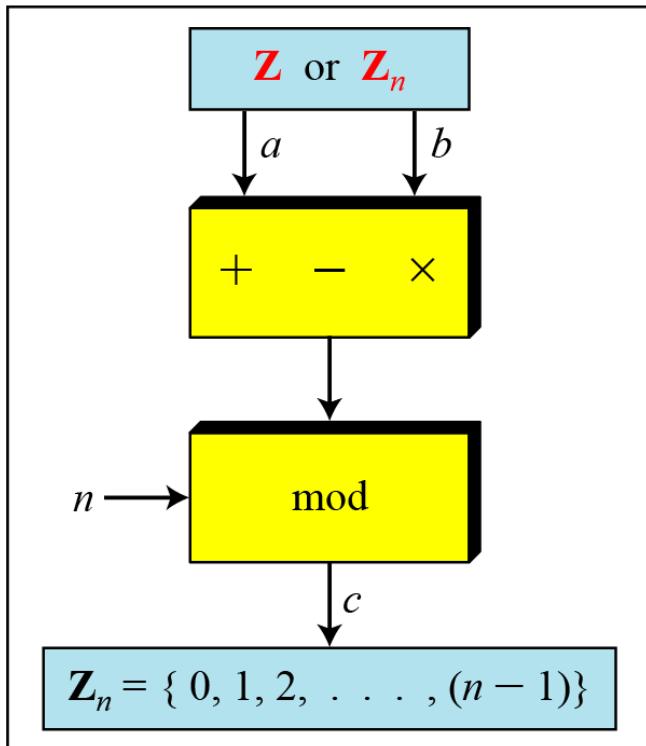
Properties

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

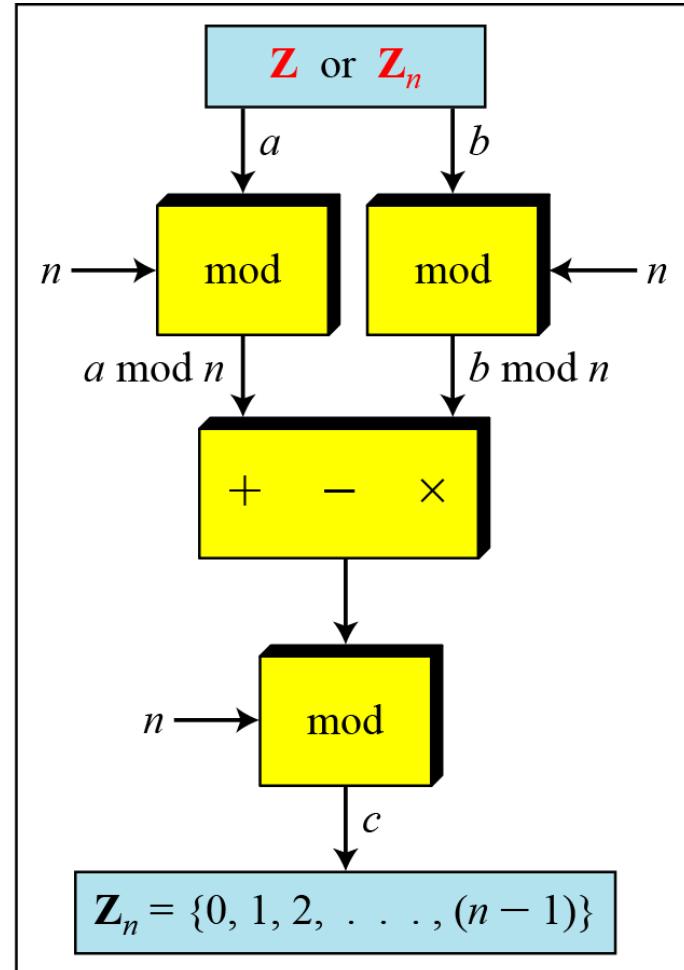
Second Property: $(a - b) \bmod n = [(a \bmod n) - (b \bmod n)] \bmod n$

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

2.4 Continued



a. Original process



b. Applying properties

Figure 14 Properties of mode operator

2.4 Continued

Example 18

The following shows the application of the above properties:

1. $(1,723,345 + 2,124,945) \text{ mod } 11 = (8 + 9) \text{ mod } 11 = 6$
2. $(1,723,345 - 2,124,945) \text{ mod } 16 = (8 - 9) \text{ mod } 11 = 10$
3. $(1,723,345 \times 2,124,945) \text{ mod } 16 = (8 \times 9) \text{ mod } 11 = 6$

2.4 Continued

Example 19

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

$$10^n \text{ mod } x = (10 \text{ mod } x)^n \quad \text{Applying the third property } n \text{ times.}$$

$$10 \text{ mod } 3 = 1 \rightarrow 10^n \text{ mod } 3 = (10 \text{ mod } 3)^n = 1$$

$$10 \text{ mod } 9 = 1 \rightarrow 10^n \text{ mod } 9 = (10 \text{ mod } 9)^n = 1$$

$$10 \text{ mod } 7 = 3 \rightarrow 10^n \text{ mod } 7 = (10 \text{ mod } 7)^n = 3^n \text{ mod } 7$$

2.4 Continued

Example 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.

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

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

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

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).

2.5 Continue

Additive Inverse

In \mathbf{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.

2.5 Continued

Example 21

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

Solution

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

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.

2.5 Continued

Example 22

Find the multiplicative inverse of 8 in \mathbb{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 23

Find all multiplicative inverses in \mathbb{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.

2.5 Continued

Example 24

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

Solution

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

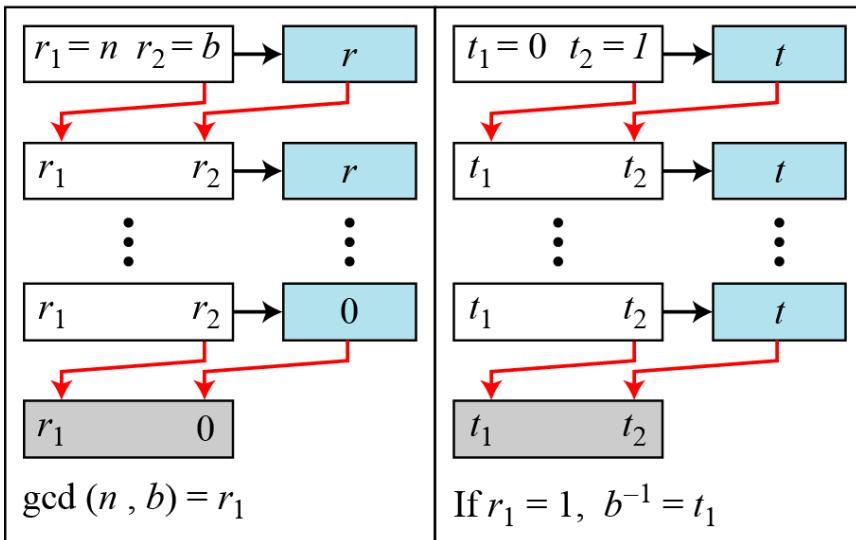
2.5 Continued

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 .

2.5 Continued



a. Process

```

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

```

while ($r_2 > 0$)

{
 $q \leftarrow r_1 / r_2;$

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

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

$t \leftarrow t_1 - q \times t_2;$

$t_1 \leftarrow t_2; \quad t_2 \leftarrow t;$

}

if ($r_1 = 1$) then $b^{-1} \leftarrow t_1$

b. Algorithm

Figure 15 Using extended Euclidean algorithm to find multiplicative inverse

2.5 Continued

Example 25

Find the multiplicative inverse of 11 in \mathbf{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.

2.5 Continued

Example 26

Find the multiplicative inverse of 23 in \mathbf{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.

2.5 Continued

Example 27

Find the inverse of 12 in \mathbf{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.

2.6 Addition and Multiplication Tables

	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}

Figure 16 *Addition and multiplication table for \mathbf{Z}_{10}*

2.7 Different Sets

$$\mathbf{Z}_6 = \{0, 1, 2, 3, 4, 5\}$$

$$\mathbf{Z}_6^* = \{1, 5\}$$

$$\mathbf{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$$

$$\mathbf{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$$

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

$$\mathbf{Z}_{10}^* = \{1, 3, 7, 9\}$$

Figure 17 Some \mathbf{Z}_n and \mathbf{Z}_n^* sets

Note

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

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.*

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

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.

3.1 Definitions

3.2 Operations and Relations

3.3 Determinants

3.4 Residue Matrices

3.1 Definition

Matrix A:

m columns

l rows

$$\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \vdots & \vdots & & \vdots \\ \vdots & \vdots & & \vdots \\ a_{l1} & a_{l2} & \dots & a_{lm} \end{bmatrix}$$

Figure 18 A matrix of size $l \times m$

3.1 Continued

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

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

Figure 19 *Examples of matrices*

3.2 Operations and Relations

Example 28

Figure 20 shows an example of addition and subtraction.

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

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

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

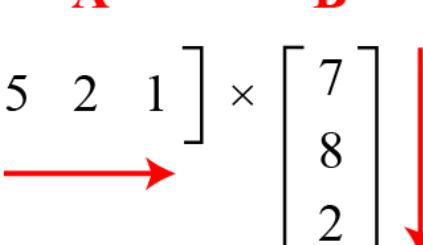
$$\mathbf{D} = \mathbf{A} - \mathbf{B}$$

Figure 20 *Addition and subtraction of matrices*

3.2 Continued

Example 29

Figure 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 .

$$\begin{matrix} \mathbf{C} & & \mathbf{A} & & \mathbf{B} \\ \left[\begin{matrix} 5 & 3 \end{matrix} \right] & = & \left[\begin{matrix} 5 & 2 & 1 \end{matrix} \right] & \times & \left[\begin{matrix} 7 \\ 8 \\ 2 \end{matrix} \right] \end{matrix}$$


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

Figure 21 *Multiplication of a row matrix by a column matrix*

3.2 Continued

Example 30

Figure 22 shows the product of a 2×3 matrix by a 3×4 matrix. The result is a 2×4 matrix.

$$\begin{matrix} & \text{C} & & & \text{B} \\ & \left[\begin{matrix} 52 & 18 & 14 & 9 \\ 41 & 21 & 22 & 7 \end{matrix} \right] & = & \left[\begin{matrix} 5 & 2 & 1 \\ 3 & 2 & 4 \end{matrix} \right] & \times & \left[\begin{matrix} 7 & 3 & 2 & 1 \\ 8 & 0 & 0 & 2 \\ 1 & 3 & 4 & 0 \end{matrix} \right] \end{matrix}$$

Figure 22 Multiplication of a 2×3 matrix by a 3×4 matrix

3.2 Continued

Example 31

Figure 23 shows an example of scalar multiplication.

$$\begin{matrix} \mathbf{B} \\ \left[\begin{matrix} 15 & 6 & 3 \\ 9 & 6 & 12 \end{matrix} \right] \end{matrix} = 3 \times \begin{matrix} \mathbf{A} \\ \left[\begin{matrix} 5 & 2 & 1 \\ 3 & 2 & 4 \end{matrix} \right] \end{matrix}$$

Figure 23 Scalar multiplication

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

Where A_{ij} is a matrix obtained from A by deleting the i th row and j th column.

Note

The determinant is defined only for a square matrix.

3.3 Continued

Example 32

Figure 24 shows how we can calculate the determinant of a 2×2 matrix based on the determinant of a 1×1 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

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

Figure 24 Calculating the determinant of a 2×2 matrix

3.3 Continued

Example 33

Figure 25 shows the calculation of the determinant of a 3×3 matrix.

$$\begin{aligned}\det \begin{bmatrix} 5 & 2 & 1 \\ 3 & 0 & -4 \\ 2 & 1 & 6 \end{bmatrix} &= (-1)^{1+1} \times 5 \times \det \begin{bmatrix} 0 & -4 \\ 1 & 6 \end{bmatrix} + (-1)^{1+2} \times 2 \times \det \begin{bmatrix} 3 & -4 \\ 2 & 6 \end{bmatrix} + (-1)^{1+3} \times 1 \times \det \begin{bmatrix} 3 & 0 \\ 2 & 1 \end{bmatrix} \\ &= (+1) \times 5 \times (+4) \quad + \quad (-1) \times 2 \times (24) \quad + \quad (+1) \times 1 \times (3) = -25\end{aligned}$$

Figure 25 Calculating the determinant of a 3×3 matrix

3.4 Inverses

Note

Multiplicative inverses are only defined for square matrices.

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 34

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

Figure 26 A residue matrix and its multiplicative inverse

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).

4.1 Single-Variable Linear Equations

4.2 Set of Linear Equations

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.

4.1 Continued

Example 35

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 36

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

Solution

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

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

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

4.1 Continued

Example 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 $x_0 = (2 \times 3^{-1}) \pmod{13} = 18 \pmod{13} = 5$. We can see that the answer satisfies the original equation: $3 \times 5 + 4 \equiv 6 \pmod{13}$.

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.

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

a. Equations

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

b. Interpretation

c. Solution

Figure 27 Set of linear equations

4.2 Continued

Example 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.