

**MATHEMATICS OF CRYPTOGRAPHY
PART I
MODULAR ARITHMETIC AND
CONGRUENCE**

1

**Book : Cryptography and Network
security by Behrouz A. Forouzan**

2

Integer Arithmetic

- In integer arithmetic, we use a set and a few operations.
- Reviewed here to create a background for modular arithmetic.

3

Set of Integers

- The set of integers, denoted by \mathbf{Z} , contains all integral numbers (with no fraction) from negative infinity to positive infinity

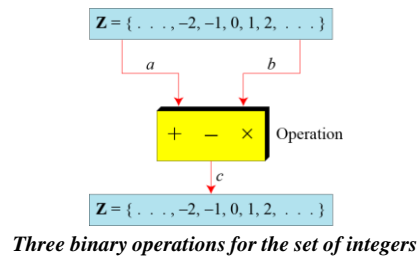
$$\mathbf{Z} = \{ \dots, -2, -1, 0, 1, 2, \dots \}$$

The set of integers

4

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.



5

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

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

6

Integer Division(cont.)

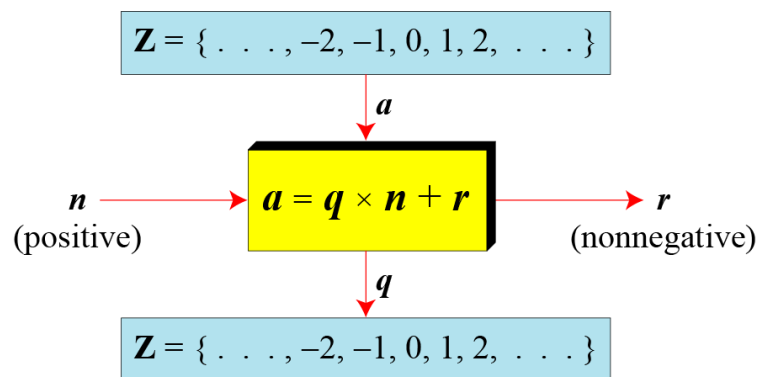
- Assume that $a = 255$ and $n = 11$. We can find $q = 23$ and $r = 2$ using the division algorithm.

$$\begin{array}{r}
 23 \leftarrow q \\
 \begin{array}{r}
 n \rightarrow 11 \quad \overline{) 255} \\
 \underline{22} \\
 35 \\
 \underline{33} \\
 2 \leftarrow r
 \end{array}
 \end{array}$$

Finding the quotient and the remainder

7

Integer Division(cont.)



Division algorithm for integers

8

Integer Division(cont.)

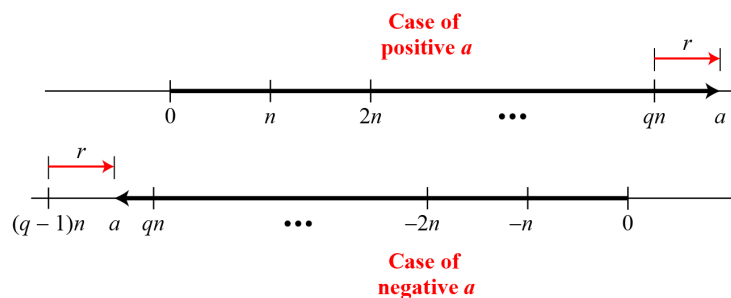
- When we use a computer or a calculator, r and q are negative when a is negative.
- How can we apply the restriction that r needs to be positive?
- The solution is simple, we decrement the value of q by 1 and we add the value of n to r to make it positive.

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

9

Integer Division(cont.)

- Graph of division algorithm



10

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

11

Divisibility(cont.)

- Properties

Property 1: if $a \mid 1$, then $a = \pm 1$.

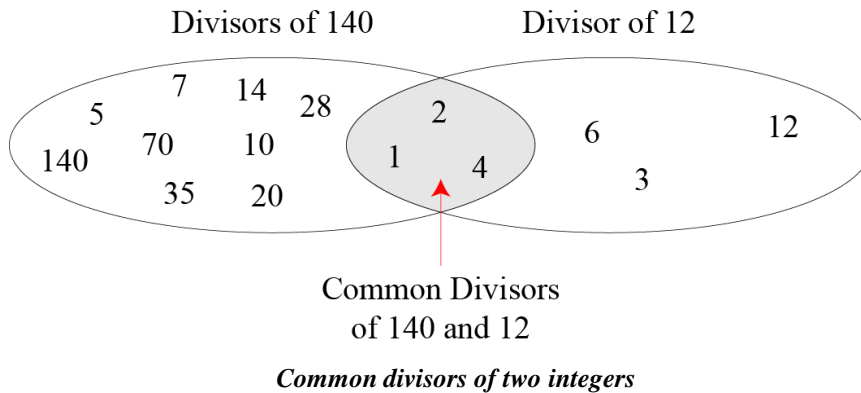
Property 2: if $a \mid b$ and $b \mid a$, then $a = \pm b$.

Property 3: if $a \mid b$ and $b \mid c$, then $a \mid c$.

Property 4: if $a \mid b$ and $a \mid c$, then
 $a \mid (m \times b + n \times c)$, where m
 and n are arbitrary integers

12

Divisibility(cont.)



13

Divisibility(cont.)

Greatest Common Divisor

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

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

14

Divisibility(cont.)

- For example, to calculate the $\gcd(36,10)$, we use following steps:

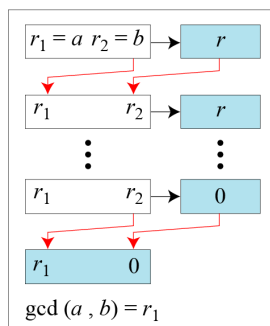
$\gcd(36, 10) = \gcd(10, 6)$by fact 2
 $\gcd(10, 6) = \gcd(6, 4)$by fact 2
 $\gcd(6, 4) = \gcd(4, 2)$by fact 2
 $\gcd(4, 2) = \gcd(2, 0)$by fact 2
 $\gcd(2, 0) = 2$by fact 1

Hence, Answer = 2

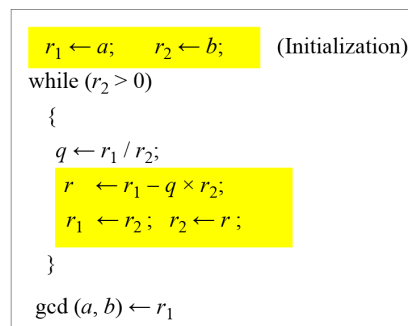
15

Divisibility(cont.)

Euclidean Algorithm



a. Process



b. Algorithm

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

16

Divisibility(cont.)

Find the greatest common divisor of 2740 and 1760.

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	

Answer: $\gcd(2740, 1760) = 20$.

17

Divisibility(cont.)

Find the greatest common divisor of 25 and 60.

18

Divisibility(cont.)

Extended Euclidean Algorithm

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

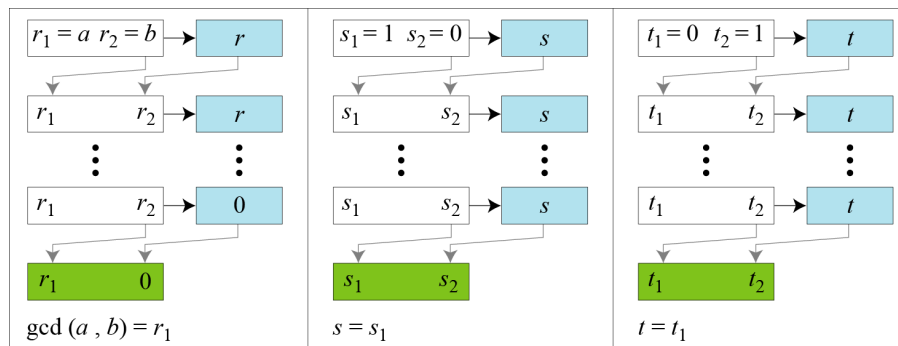
$$s \times a + t \times b = \gcd(a, b)$$

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

19

Divisibility(cont.)

Extended Euclidean algorithm, part a



a. Process

20

Divisibility(cont.)

Extended Euclidean algorithm, part b

```

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

```

b. Algorithm

21

Divisibility(cont.)

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

Solution

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 $t = 6$.

22

Divisibility(cont.)

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

Solution

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

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

23

Divisibility(cont.)

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

Solution

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 $t = 1$.

24

Divisibility(cont.)

Exercise:

Given $a = 84$ and $b = 320$, find $\gcd(a, b)$ and the values of s and t .

25

Divisibility(cont.)

Exercise:

Given $a = 84$ and $b = 320$, find $\gcd(a, b)$ and the values of s and t .

Solution:

$\gcd(84, 320) = 4$, $s = -19$, $t = 5$

26

Modular Arithmetic

27

Preliminary

- 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.

28

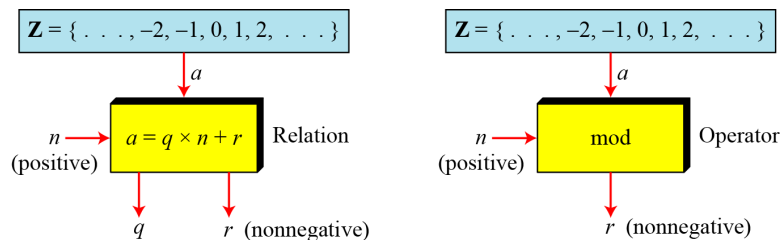
Preliminary(cont.)

- 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.

29

Modulo Operator

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



Division algorithm and modulo operator

30

Modulo Operator(cont.)

- Find the result of the following operations:
 - a. $27 \bmod 5$
 - b. $36 \bmod 12$
 - c. $-18 \bmod 14$
 - d. $-7 \bmod 10$

31

Modulo Operator(cont.)

- **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 , $r = 3$

32

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** .

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

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

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

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

Some Z_n sets

33

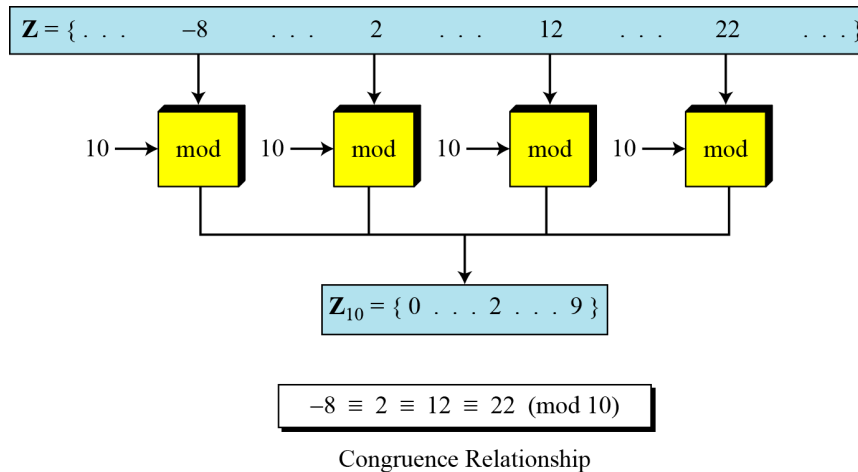
Congruence

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

$$\begin{array}{ll} 2 \equiv 12 \pmod{10} & 13 \equiv 23 \pmod{10} \\ 3 \equiv 8 \pmod{5} & 8 \equiv 13 \pmod{5} \end{array}$$

34

Congruence(cont.)



35

Congruence(cont.)

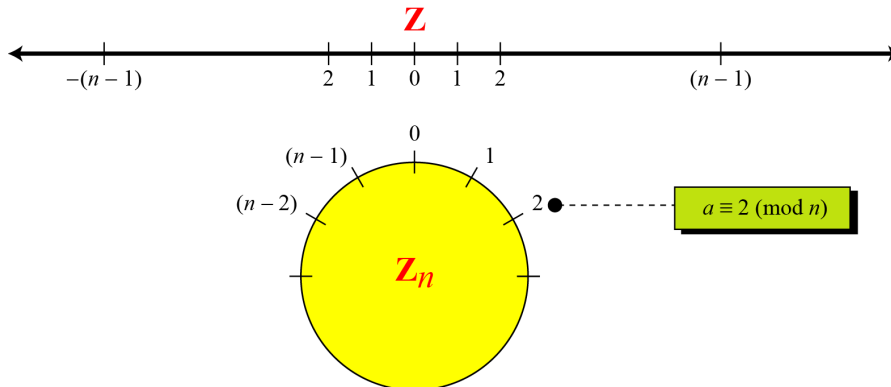
- Residue Classes
 - A residue class $[a]$ or $[a]_n$ is the set of integers congruent modulo n .
 - It is the set of all integers such that $x \equiv a \pmod{n}$
 - E.g. for $n=5$, we have five sets as shown below:

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

36

Congruence(cont.)

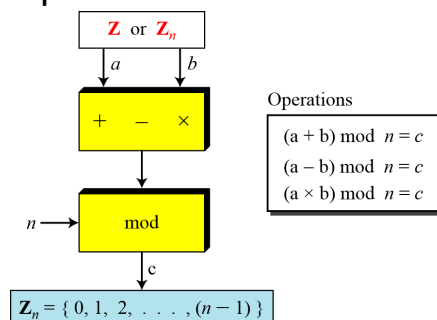
- Comparison of \mathbb{Z} and \mathbb{Z}_n using graphs



37

Operation in \mathbb{Z}_n

- The three binary operations that we discussed for the set \mathbb{Z} can also be defined for the set \mathbb{Z}_n . The result may need to be mapped to \mathbb{Z}_n using the mod operator.



38

Operation in Z_n (cont.)

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

39

Operation in Z_n (cont.)

- **Solution**

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

40

Operation in Z_n (cont.)

- 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} .

41

Operation in Z_n (cont.)

- **Solution**
- Add 17 to 27 in Z_{14} .
 - $(17+27) \bmod 14 = 2$
- Subtract 43 from 12 in Z_{13} .
 - $(12-43) \bmod 13 = 5$
- Multiply 123 by -10 in Z_{19} .
 - $(123 \times (-10)) \bmod 19 = 5$

42

Operation in \mathbb{Z}_n (cont.)

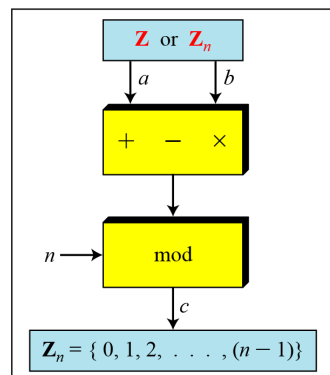
First Property: $(a + b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$

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

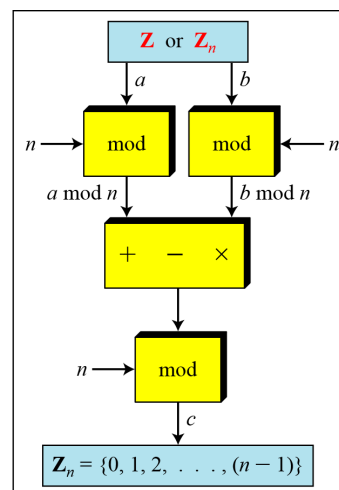
Third Property: $(a \times b) \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n$

43

Operation in \mathbb{Z}_n (cont.)



a. Original process



b. Applying properties

44

Operation in Z_n (cont.)

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

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

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

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

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

45

Operation in Z_n (cont.): Exercise

- 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 same as dividing 17 by 3.

Prove this claim using the properties of the mod operator.

46

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).

47

Additive Inverses

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

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

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

48

Additive Inverses

- Find all additive inverse pairs in Z_{10} .
- **Solution**
 - The six pairs of additive inverses are (0, 0), (1, 9), (2, 8), (3, 7), (4, 6), and (5, 5).

49

Multiplicative Inverses

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

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

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 .

50

Multiplicative Inverses(cont.)

- Find the multiplicative inverse of 8 in \mathbb{Z}_{10} .
 - 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.
- Find all multiplicative inverses in \mathbb{Z}_{10} .
 - 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.

51

Multiplicative Inverses(cont.)

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

52

Multiplicative Inverses(cont.)

- Find all multiplicative inverse pairs in Z_{11} .
 - **Solution**
 - We have seven pairs: (1, 1), (2, 6), (3, 4), (5, 9), (7, 8), (9, 9), and (10, 10).

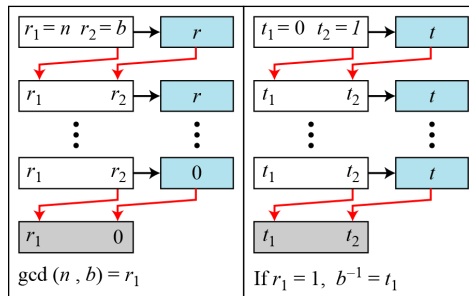
53

Multiplicative Inverses(cont.)

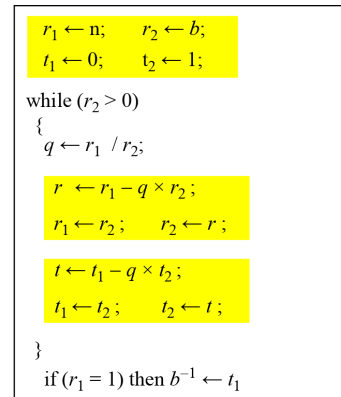
- The extended Euclidean algorithm finds the multiplicative inverses of b in Z_n when n and b are given and $\gcd(n, b) = 1$.
- The multiplicative inverse of b is the value of t after being mapped to Z_n .

54

Multiplicative Inverses(cont.)



a. Process



b. Algorithm

Using extended Euclidean algorithm to find multiplicative inverse

55

Multiplicative Inverses(cont.)

- Find the multiplicative inverse of 11 in \mathbb{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.

56

Multiplicative Inverses(cont.)

- Find the inverse of 12 in \mathbb{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.

57

Multiplicative Inverses(cont.)

- Find the multiplicative inverse of 23 in \mathbb{Z}_{100} .

58

Multiplicative Inverses(cont.)

- Find the multiplicative inverse of 23 in \mathbb{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.

59

Addition and Multiplication Tables

- Addition and multiplication table for \mathbb{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 \mathbb{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 \mathbb{Z}_{10}

60

Different Sets

- Some Z_n and Z_n^* sets

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

$$Z_6^* = \{1, 5\}$$

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

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

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

$$Z_{10}^* = \{1, 3, 7, 9\}$$

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

61

Two More Sets

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

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

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

62