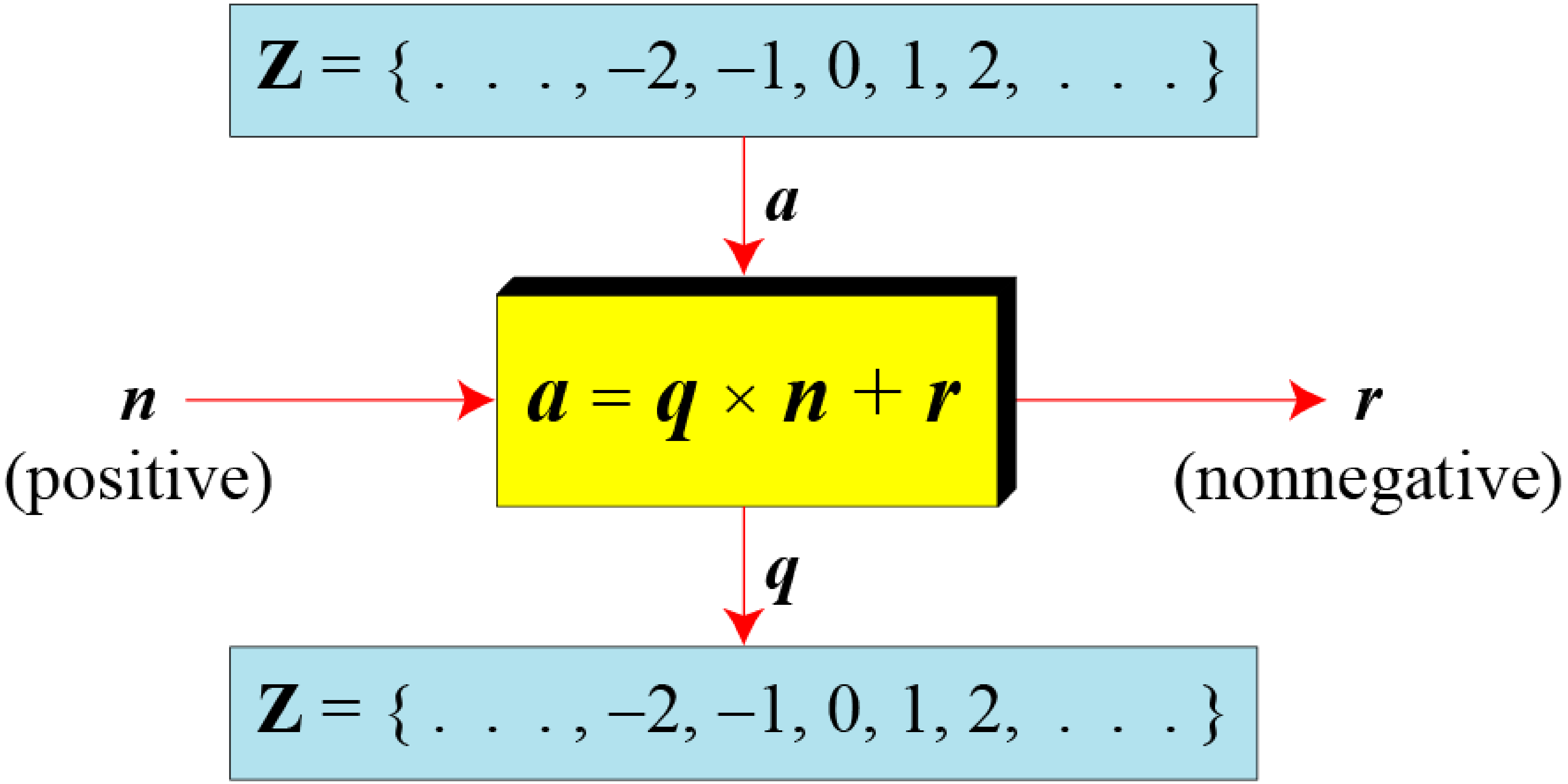
Mathematics of Cryptography-I

Objective

- **E**uclidean algorithm
- Extended Euclidean algorithm(EEA)
- Modular arithmetic
- Matrix and Residue matrix

Set of Integers and Integer Division

In integer arithmetic, if we divide ***a*** by ***n***, we can get ***q*** *a*nd ***r*** .



Answer the following Question

- When we use a computer or a calculator, *r* and *q* are negative when *a* is negative.
- How can we make *r* positive?

$$-255=(-23 \text{ x } 11) + (-2)$$

- 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.

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

Divisbility

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, $n \nmid a$

Example: Divisibility

a. The integer 5 divides the integer 30 because $30 = 6 \times 5$. So, we can write $5 \mid 30$

b. The number $8 \nmid 42$ because $42 = 5 \times 8 + 2$ has a remainder of 2.

Greatest Common Divisor(GCD)

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

Euclidean Algorithm

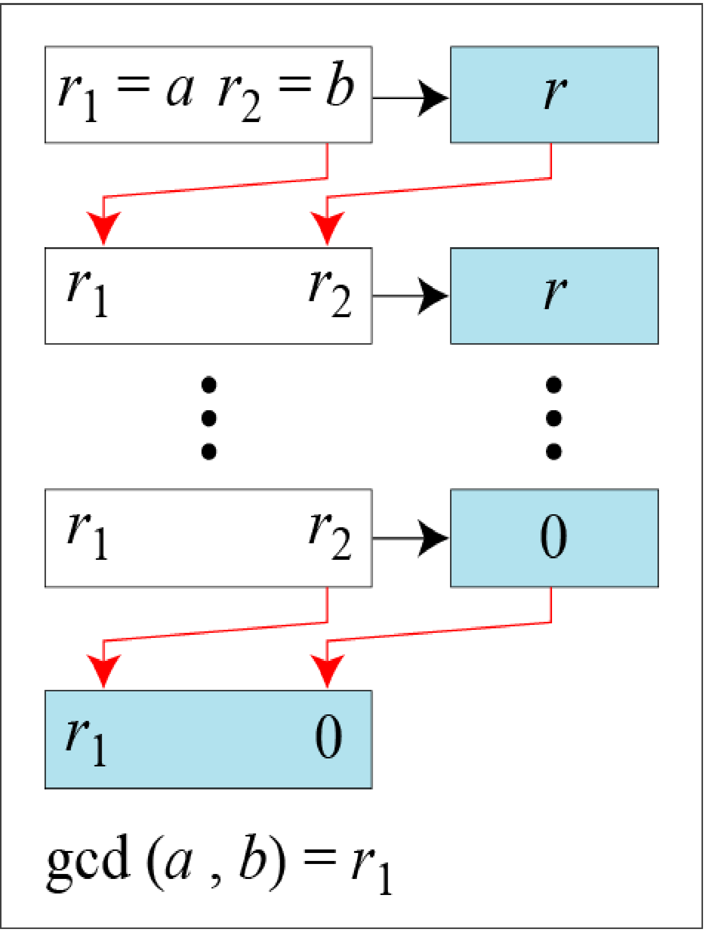
***Fact 1:** gcd (a, 0) = a*

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

Example: a=60, b=25

Gcd(60,25)=gcd(25,10)=gcd(10,5)=gcd(5,0)=Fact 1=5

Finding GCD(a,b) by using Euclidean Algo.



a. Process

Relatively prime or Coprime

Note

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

Examples:

gcd(13,5)=1 => 13 and 5 are relatively prime

gcd(12,5)=1 => 12 and 5 are relatively prime

gcd(10,2)=2

gcd(9,3)=3

gcd(9,5)=1 => 9 and 5 are relatively prime

Finding GCD by using Euclidean Algo.

Example

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	

GCD

Do by yourself

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	

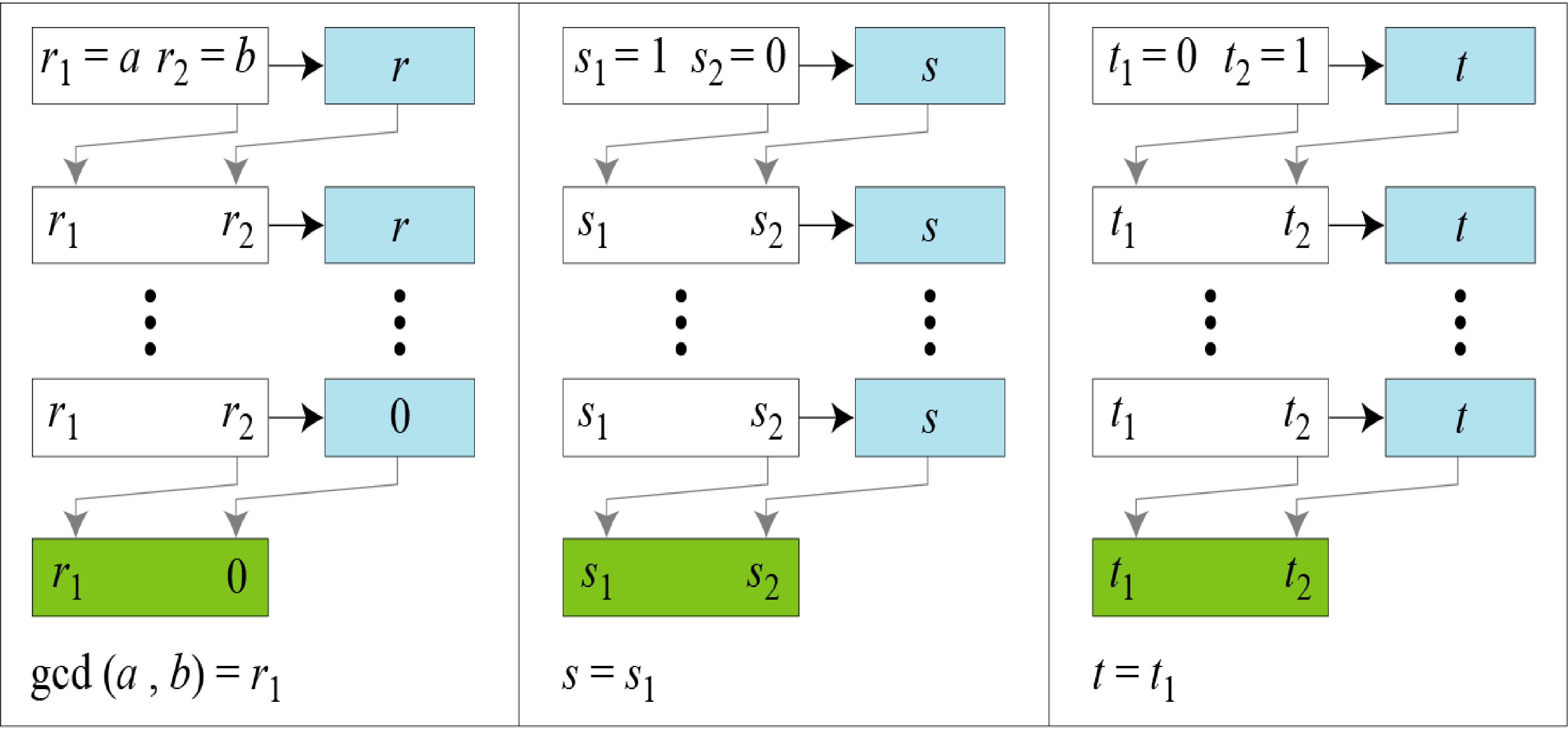
Extended Euclidean Algorithm (EEA)

Problem: Given two integers ***a*** and ***b***, find other two integers, ***s*** and ***t***, such that

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

- ***This equation is also called Bezout's identity or Bezout's Lemma.***
- ***s and t are called Bezout's coefficients for (a,b).***
- The **EEA** can be used to calculate the gcd (a, b) and values of s and t.

Process of Extended Euclidean Algorithm



Extended **E**uclidean **A**lgorithm**(EEA)**

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

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

Solving Problem by using EEA

Example

Given a = 161 and b = 28, find gcd (a, b) and the values of s and t of *Bezout's identity* **(s x a + t x b = *gcd(a,b)*).**

Solution

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

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	

Solving Problem by using EEA

Example

Given a = 17 and b = 0, find gcd (a, b) and the values of s and t of *Bezout's identity* ***(s* x *a* + *t* x *b* = *gcd(a,b)*****.** .

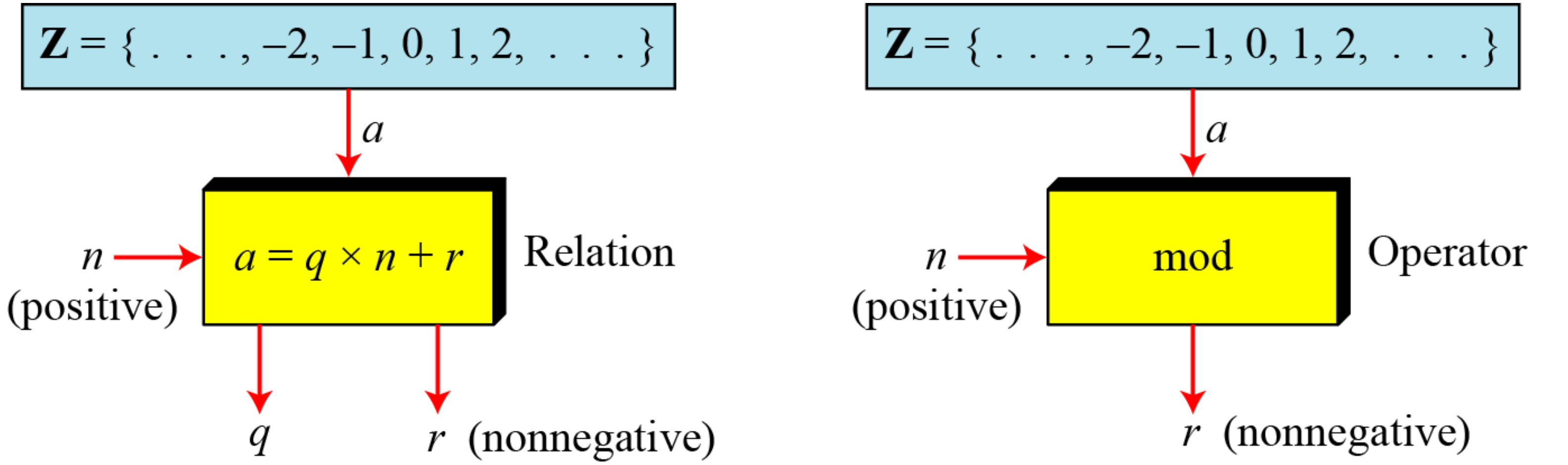
Solution

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	

MODULAR ARITHMETIC

- If a is an integer and n is a positive integer, we define r as the remainder (residue) such as $r = a \textbf{ mod } n$.
- So, we can write $a = q \times n + r$.
- The integer n is called the modulus.



Examples: Modulo operation

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.

Congruence

- This can be written with the help of a congruence operator (≡) i.e. ***a* ≡ *b* (mod *n*)**
- Two integers ***a*** and ***b*** are said to be congruent modulo ***n***, if **(*a* mod *n*)=(*b* mod *n*)**

Examples:

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

Can we say 12 ≡ 23 mod 8 ?

14 ≡ 36 mod 7 ?

Properties of Congruence

1. $a \equiv b \pmod{n}$ if $n \mid (a-b)$
2. $a \equiv b \pmod{n}$ implies $b \equiv a \pmod{n}$
3. $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ imply $a \equiv c \pmod{n}$

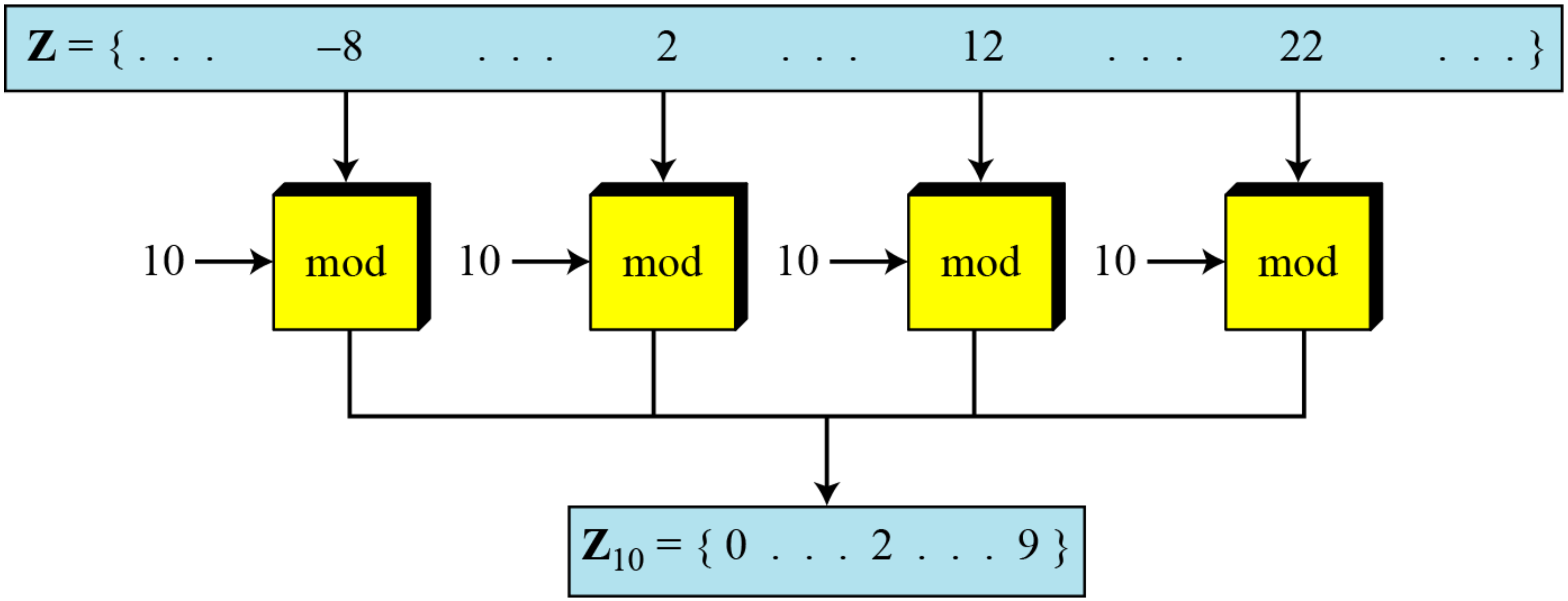
Examples:

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

Example (Property *3***):**

- $2 \equiv 12 \bmod 10$ and $12 \equiv 22 \bmod 10$,
  then $2 \equiv 22 \bmod 10$

Concept of congruence relationship



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

Congruence Relationship

The set Z_n

- The (mod n) operator maps all integers into the set of integers **{0, 1, 2, …, (n-1)}**
- This is also called the set of least residues modulo n, or Z_n
- **What are the elements of set** Z_2 ,Z_5 , Z_{10} ?

  $Z_2 = \{0,1\}$

  $Z_5 = \{0, 1, 2, 3, 4\}$

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

Example: Modulo operator

Can you give an example of modulo operator, used in our daily life ?

- We use a clock to measure time.
- Our clock system uses modulo 12 arithmetic.
- However, instead of a 0 we use the number 12.

Operations on set Z_n

- The three binary operations (+, – , ×) defined on set Z can also be applied to set Z_n.
- The operations are done as usual just like set Z, but, if the result exceeds the numbers defined in Z_n then it is converted to a number in Z_n using the mod operator.
- This is called modular arithmetic

Z_n: Examples

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

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

$$(14 + 7) \bmod 15 \quad \rightarrow \quad (21) \bmod 15 = 6$$

$$(7 - 11) \bmod 13 \quad \rightarrow \quad (-4) \bmod 13 = 9$$

$$(7 \times 11) \bmod 20 \quad \rightarrow \quad (77) \bmod 20 = 17$$

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

Examples: Operations in Z_n

- $(1{,}723{,}345 + 2{,}124{,}945) \bmod 11$
  $= (8 + 9) \bmod 11 = 6$
- $(1{,}723{,}345 - 2{,}124{,}945) \bmod 11$
  $= (8 - 9) \bmod 11 = 10$
- $(1{,}723{,}345 \times 2{,}124{,}945) \bmod 11$
  $= (8 \times 9) \bmod 11 = 6$

More Examples: Operations in Z_n

Compute the followings:

$10^{12} \bmod 3 = 1$

$10^{50} \bmod 7 = 3^{50} \bmod 7 = 2$

$5^4 \bmod 7 = 2$

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

$3^{2x25}=(3^2)^{25}=9^{25} \bmod 7= (9 \bmod 7)^{25} =2^{25} \bmod 7$

$2^{25}(\bmod 7)=2 \times 2^{24} \bmod 7=2 \times (2^{3x8}) \bmod 7$

$=2 \times (2^3 \bmod 7)^8= 2x1^8 \bmod 7=2 \times 1=2$

Square and Multiply Technique

Inverse of a number in Z_n

- In modular arithmetic, we often need to find the inverse of a number relative to an operation.
- It can be an **additive inverse** (relative to an addition operation(+)) or
- a **multiplicative inverse**(relative to a multiplication operation (×)).

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.*

Examples

1. Find the additive inverse of 4 in Z_7

Answer: 3

2. Find all additive inverse pairs in $\mathbf{Z_{10}}$**.**

Answer:

There are **six pairs** of additive inverses:

(0, 0), (1, 9), (2, 8), (3, 7), (4, 6), and (5, 5).

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 has, the product of the integer and its multiplicative inverse is congruent to 1 modulo n.

Examples

Example 1

Find the multiplicative inverse of 7 and 8 in $\mathbf{Z}_{10}$.

Multiplicative inverse of 7 is 3, but 8 has no multiplicative inverse.

Note: gcd can help us to quickly find out whether a given number has multiplicative inverse or not.

gcd(10,7)=1=> 7 has multiplicative inverse in modulo 10

gcd (10, 8) = 2 $\neq$ 1 => 8 has no multiplicative inverse in modulo 10

Example 2

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

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.

Continued

Example 3

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

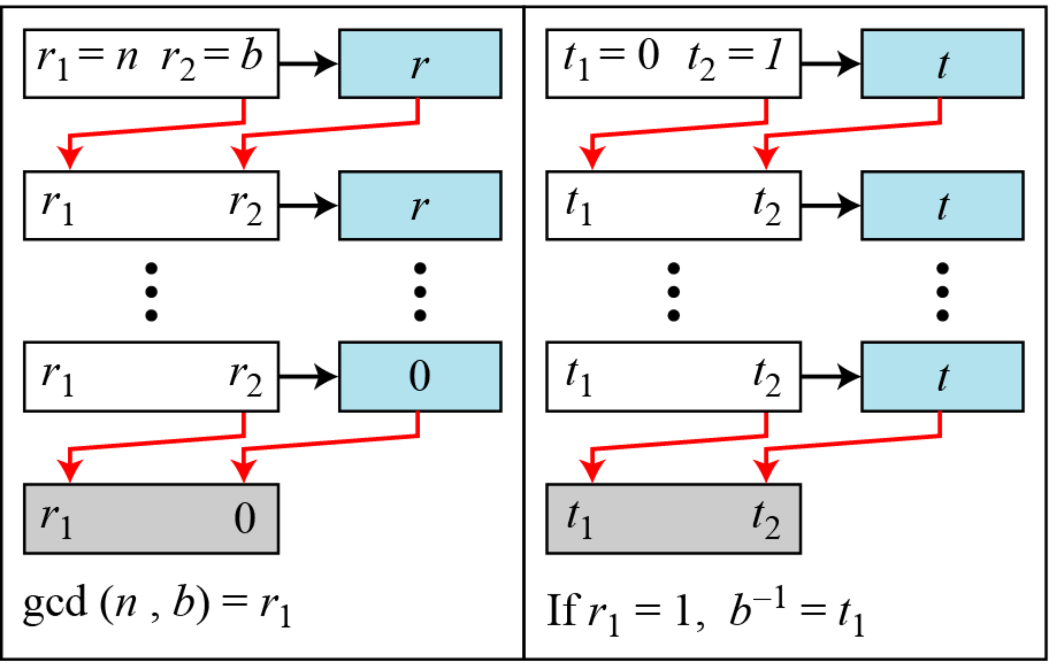
We have seven pairs:
(1, 1), (2, 6), (3, 4), (5, 9), (7, 8), (9, 9), and (10, 10).

How to find out Multiplicative Inverse of BIG Number?

Note

- The Extended Euclidean algorithm(EEA) 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.

Using Extended Euclidean algorithm to find Multiplicative inverse



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

Continued

Example

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

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(=19).

Continued

Example

Find the inverse of 12 in Z_{26}.

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.

Z_n and Z_n*

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

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

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

Note

- We need to use Zn when additive inverses are needed
- We need to use Zn* when multiplicative inverses are needed.

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.

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

What are the uses of Additive and Multiplicative inverses in Cryptography?

- When a sender uses a key for encryption, he may choose an integer from the set Zn or Zn* depending on the algorithms used.
- If he chooses from Zn, the receiver has to find the additive inverse of that integer for getting the key for decryption.
- Similar logic applies for multiplicative inverse in Zn*.

MATRICES

- Matrices are widely used in Cryptography.
- A matrix is a linear array of *l* x *m* elements.

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

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

Operations and Relations

Example

Addition and Subtraction

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

C = A + B

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

D = A − B

Continued

Example

Multiplication of a row matrix by a column matrix

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

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

Continued

Example

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

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

Continued

Example

Scalar multiplication

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

Inverse of a Square matrix

The inverse of a matrix A , denoted as A^{-1} should hold the following relation:

$$\mathbf{A\,A^{-1} = I},$$

where **I** is the identity matrix

Note

Multiplicative inverses are only defined for square matrices.

Inverse *(Continued)*

For $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$,

the inverse can be found by using the formula:

$$A^{-1} = \frac{1}{\det A}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Residue Matrix and Inverse

- 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

Find the inverse of a matrix $\begin{pmatrix} 7 & 3 \\ 1 & 2 \end{pmatrix} \bmod 26$

The inverse of the given matrix $\begin{pmatrix} 12 & 21 \\ 7 & 3 \end{pmatrix} \bmod 26$