Course: Cryptography and Network Security
Code: CS-34310
Branch: M.C.A - 4th Semester

Lecture – 4: Introduction to Cryptography Mathematics – Part-2

Faculty & Coordinator : Dr. J Sathish Kumar (JSK)

Department of Computer Science and Engineering

Motilal Nehru National Institute of Technology Allahabad,
Prayagraj-211004

Inverses

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

Additive Inverses

- In 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.

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).

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.

Multiplicative Inverses

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

Multiplicative Inverses

- 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).

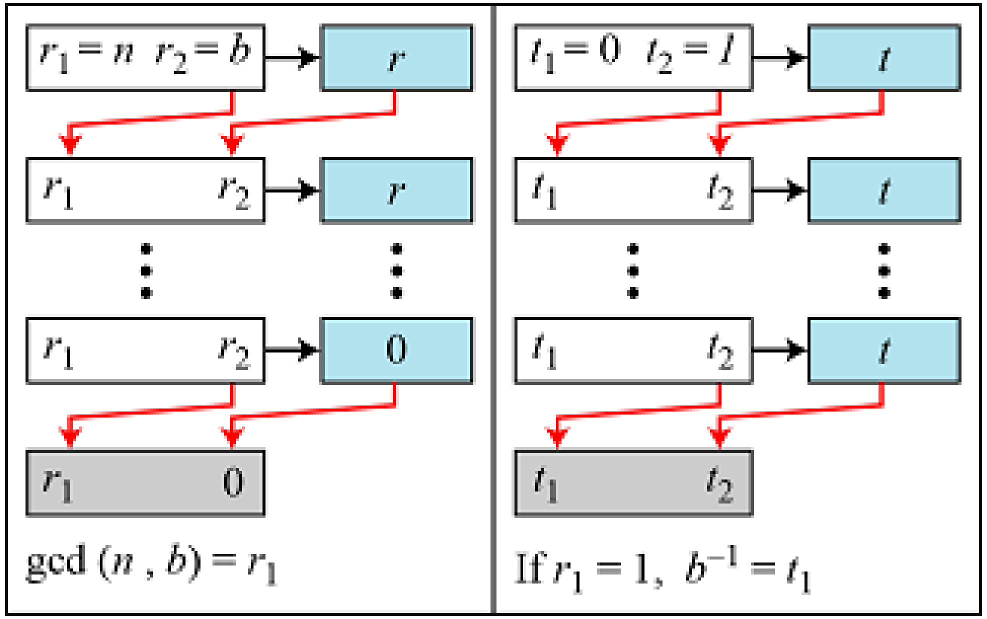
Multiplicative Inverses

- 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.
- If the multiplicative inverse of b exists, gcd (n, b) must be 1.

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

$$(s \times n + b \times t) \bmod n = 1 \bmod n$$
$$[(s \times n) \bmod n] + [(b \times t) \bmod n] = 1 \bmod n$$
$$0 + [(b \times t) \bmod n] = 1$$
$$(b \times t) \bmod n = 1 \quad \rightarrow \text{This means } t \text{ is the multiplicative inverse of } b \text{ in } Z_n$$

Multiplicative Inverses



a. Process

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

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

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

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

b. Algorithm

Using extended Euclidean algorithm to find multiplicative inverse

Multiplicative Inverses

- 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.

Multiplicative Inverses

- 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.

Multiplicative Inverses

- 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.

Addition and Multiplication Tables

- 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 $\mathbf{Z}_{10}$

Different Sets

- Some Z_n and Z_n* sets

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

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

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

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

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

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

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: Z_p and Z_p*.
- The modulus in these two sets is a primenumber.

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