

# Mathematical Background for Cryptography

Sankita Patel

Sardar Vallabhbhai National Institute of Technology

*[sjp@coed.svnit.ac.in](mailto:sjp@coed.svnit.ac.in)*

January 12, 2024

# Part I - Modular Arithmetic and Congruence

# Preliminary

- ▶ The division relationship  $a = q \times n + r$  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  $r$ .
- ▶ 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.

# Modulo Operator

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

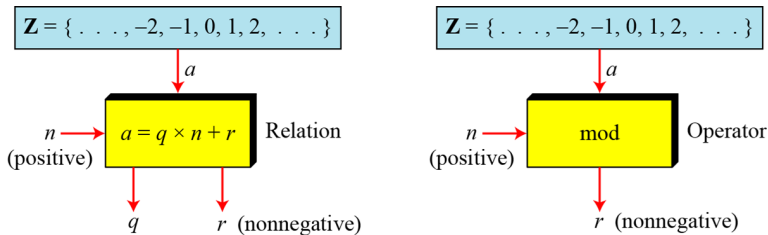


Figure: Division algorithm and modulo operator

## Modulo Operator(cont.)

Find the result of the following operations :

- ▶  $27 \bmod 5$

Dividing 27 by 5 results in  $r = 2$

- ▶  $36 \bmod 12$

Dividing 36 by 12 results in  $r = 0$

- ▶  $-18 \bmod 14$

Dividing -18 by 14 results in  $r = -4$ . After adding the modulus  $r = 10$

- ▶  $-7 \bmod 10$

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

# 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  $Z_n$ .

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

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

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

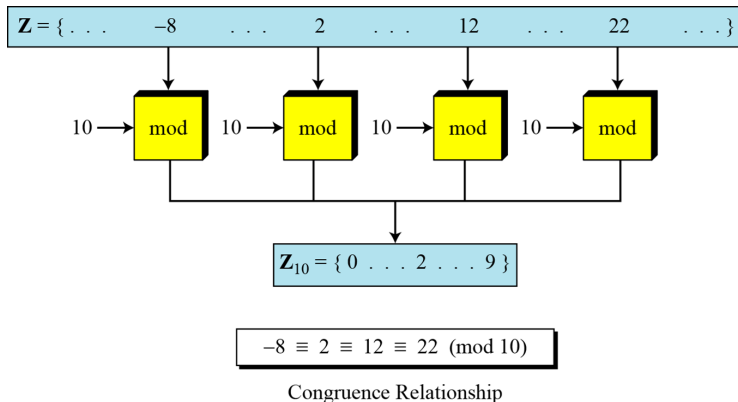
$$Z_{11} = \{ 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 \}$$

Figure: Some  $Z_n$  sets

# Congruence

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

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



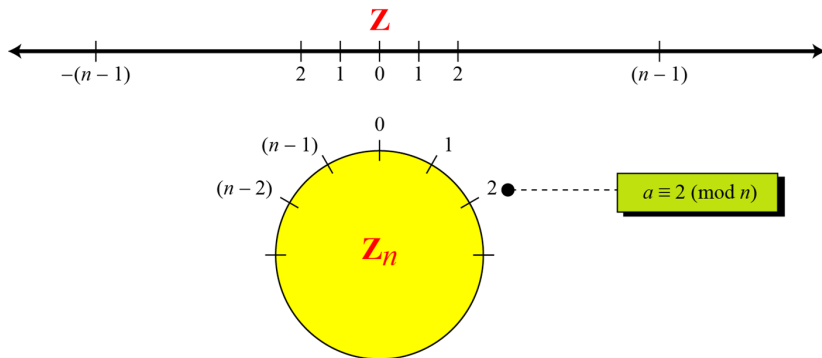
# Residue Classes

- ▶ 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:

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

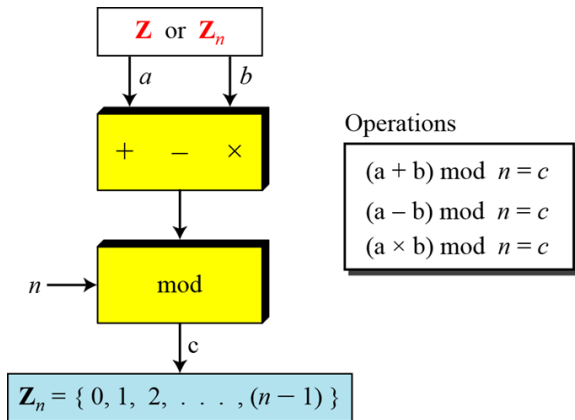


# Comparison of $\mathbb{Z}$ and $\mathbb{Z}_n$ using graphs



## 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.



# Operation in $\mathbb{Z}_n$

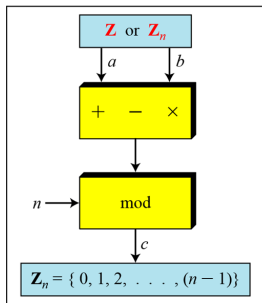
---

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

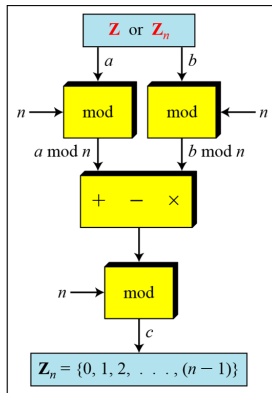
**Second Property:**  $(a - b) \bmod n = [(a \bmod n) - (b \bmod n)] \bmod n$

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

---



a. Original process



b. Applying properties

## Operation in $Z_n$

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

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

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

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

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

**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.

# 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).
- ▶ 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  $n$ .**

- ▶ 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(cont.)

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

**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.

- Find all multiplicative inverses in  $Z_{10}$ .

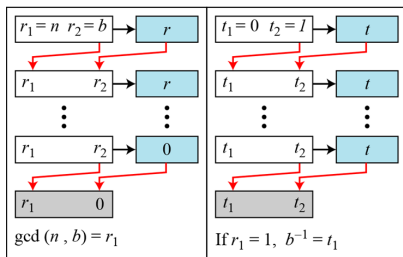
**Solution :** There are only three pairs: (1, 1), (3, 7) and (9, 9). The numbers 0, 2, 4, 5, 6, and 8 do not have a multiplicative inverse.

- Find all multiplicative inverses in  $Z_{11}$ .

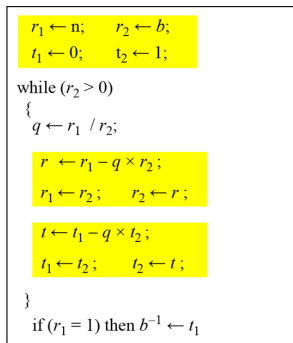
**Solution :** We have seven pairs: (1, 1), (2, 6), (3, 4), (5, 9), (7, 8), (9, 9), and (10, 10).

# Euclidean algorithm

- ▶ 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  $Z_n$ .



a. Process



b. Algorithm

Figure: Using extended Euclidean algorithm to find multiplicative inverse



## Euclidean algorithm (cont.)

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 or 19.

## Euclidean algorithm (cont.)

Find the multiplicative 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.

## Euclidean algorithm (cont.)

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

## Euclidean algorithm (cont.)

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

$q$	$r_1$	$r_2$	$r$	$t_1$	$t_2$	$t$
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.

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

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

Cryptography often uses two more sets:  $\mathbf{Z}_p$  and  $\mathbf{Z}_p^*$ . The modulus in these two sets is a prime number.

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

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

# References

1. Forouzan, Behrouz A. "Cryptography & Network Security. 2011."

Last updated by S J Patel on January 12, 2024