Introduction to Number Theory

Dr. E.SURESH BABU

Assistant Professor

Computer Science and Engineering Department

National Institute of Technology, Warangal

Warangal

Basic Concepts

Basic Concepts

- Before going into modular arithmetic, let's review some **basic concepts**

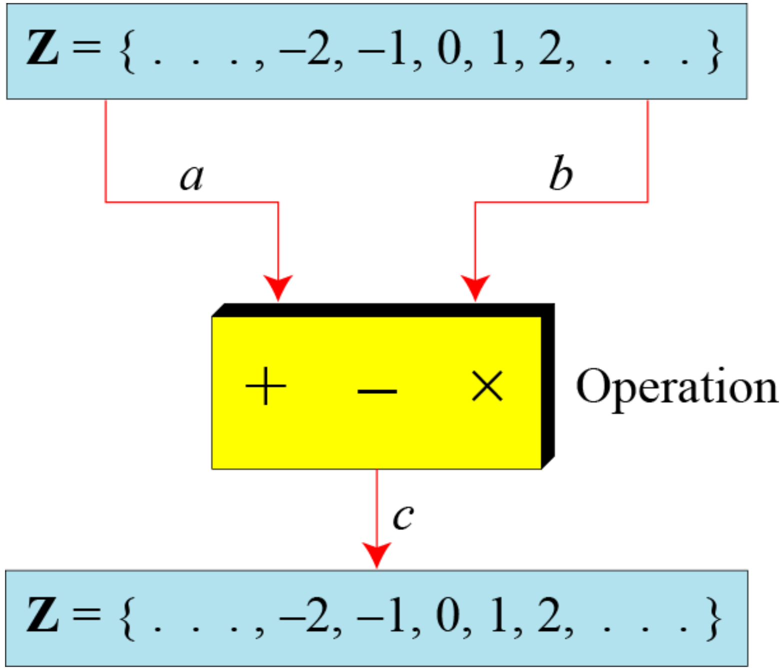
Set of Integers

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

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

Binary Operations on Integers

- 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**.



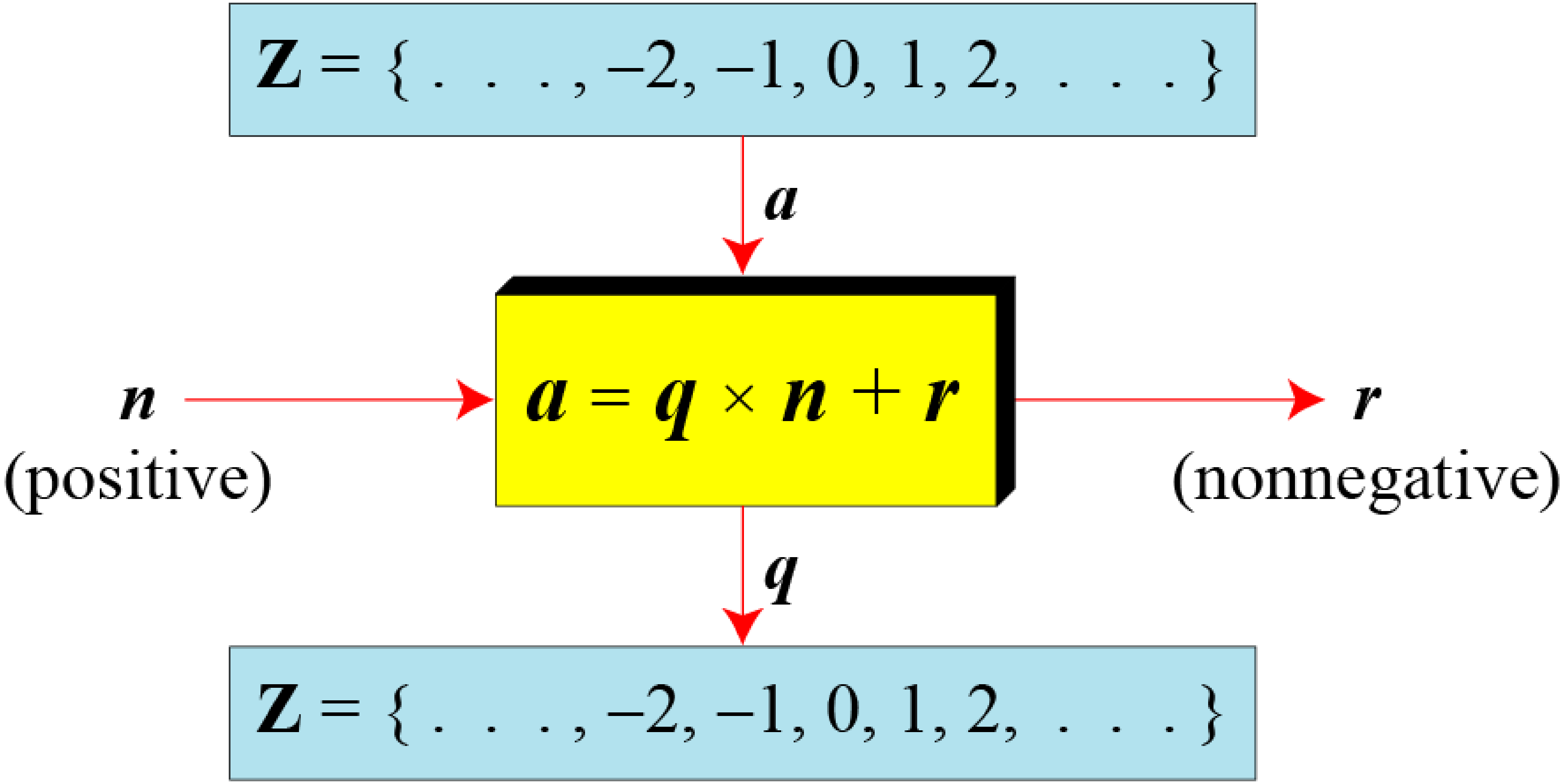
Integer Division

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

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

Division Algorithm for Integer



Observation

- When **a** is **negative** then **r and q** will be **negative.** How can we apply the restriction that **r needs to be positive**?

we **decrement the value of q by 1** and we **add the value of n to r to make it positive.**

–255

Modular Arithmetic

Modular Arithmetic

- Many **complex cryptographic algorithms** are actually based on fairly **simple modular arithmetic.**
- In modular arithmetic all **operations are performed** regarding a positive integer, i.e. **the modulus.**

Modular Arithmetic

- Given any integer a and a positive integer n, and given a division of **a by n** that leaves the remainder between **0 and n − 1**, both inclusive, we define

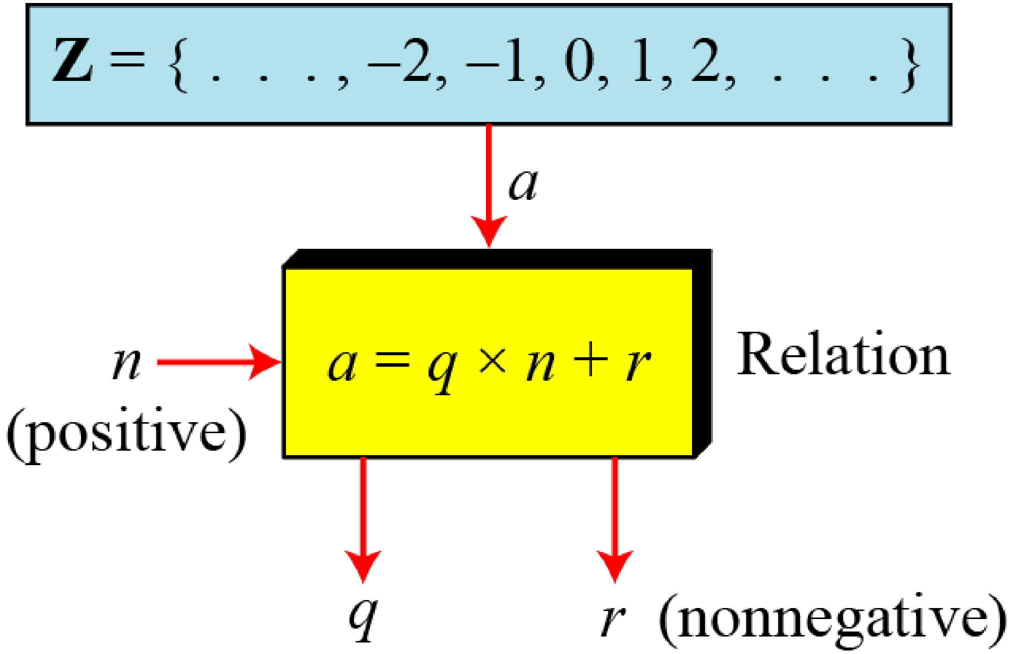
a mod n

Operations on Modular Arithmetic

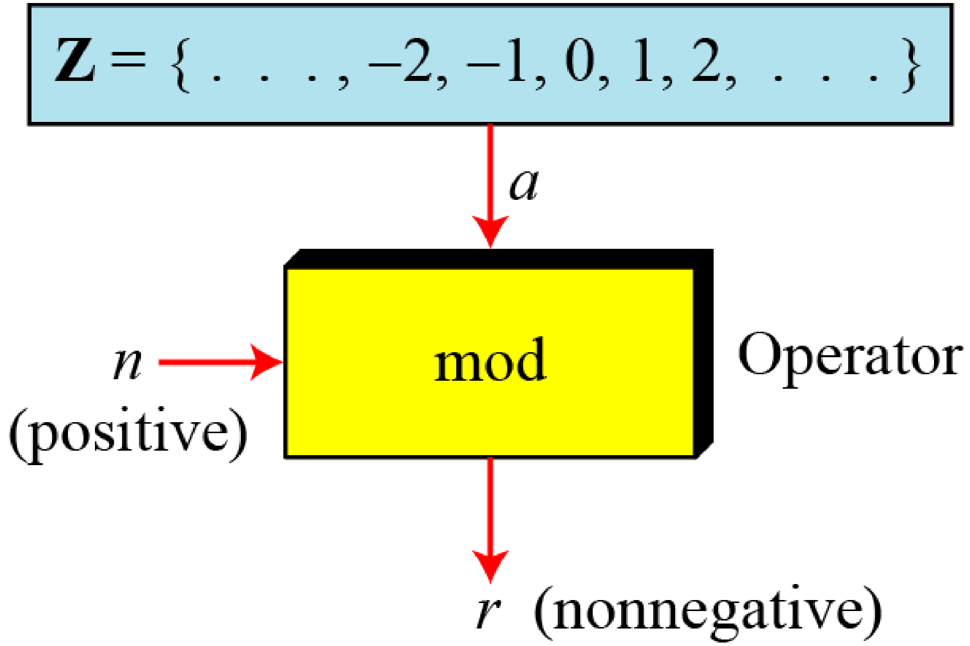
- In modular arithmetic, the numbers we are dealing with are just **integers** and the operations used are
  - ✓ **Addition,**
  - ✓ **Subtraction,**
  - ✓ **Multiplication** and
  - ✓ **Division.**

Division Modular Arithmetic

Modulo Operator



Division Algorithm



Modulo Operator

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

Modulo Operator : Examples

❖ Find the **result of the following operations:**

1. 27 mod 5

2. 36 mod 12

3. −18 mod 14

4. −7 mod 10

Modulo Operator : Examples

- Find the **result of the following operations:**

27 mod 5 ;

q = 5 ; r = 2 ;

27 mod 5 = 2

Modulo Operator : Examples

- Find the **result of the following operations:**

36 mod 12 ;

q = 3 ; r = 0 ;

36 mod 12 = 0

Modulo Operator : Examples

- Find the **result of the following operations**

  -18 mod 14 ;

  -18 Mod 14 = - 4 Which is a Negative

- To Make it **Positive**, We will **add the Modulus 14**

  -4 + 14 = 10

  Finally -18 Mod 14 = 10

Modulo Operator : Examples

- Find the **result of the following operations**

  −7 mod 10 ;

  −7 Mod 10 = - 7 Which is a Negative

- To Make it **Positive**, We will **add the Modulus 10**

  -7 + 10 = 3

  Finally -7 Mod 10 = 3

Set of Residues in MA

Set of Residues

- For arithmetic modulo n, let Z_n denote the set

$$\boxed{\mathbf{Z}_n = \{ 0, 1, 2, 3, \ . \ . \ . \ , (n-1) \}}$$

- **$\mathbf{Z_n}$** is the **set of remainders** in arithmetic modulo n. It is officially called the **set of residues.**

$$\boxed{\mathbf{Z}_2 = \{ 0, 1 \}} \quad \boxed{\mathbf{Z}_6 = \{ 0, 1, 2, 3, 4, 5 \}} \quad \boxed{\mathbf{Z}_{11} = \{ 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 \}}$$

Congruence

Congruence

- In Cryptography, We often use the concept of **Congruence** (Instead of **Equality**).
- **For Example :**

2 Mod 10 = 2 ; 12 Mod 10 =2; 22 Mod 10 = 2; and so on

We Call {**2, 12, 22**} are called as **Congruent Mod 10**

Congruence Operator

- To show that two integers are **congruent**, we use the **congruence operator (≡).**

- We will call two integers **a and b** to be **congruent modulo n** if

$$(a \bmod n) = (b \bmod n)$$

- Symbolically, we will express such a congruence by

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

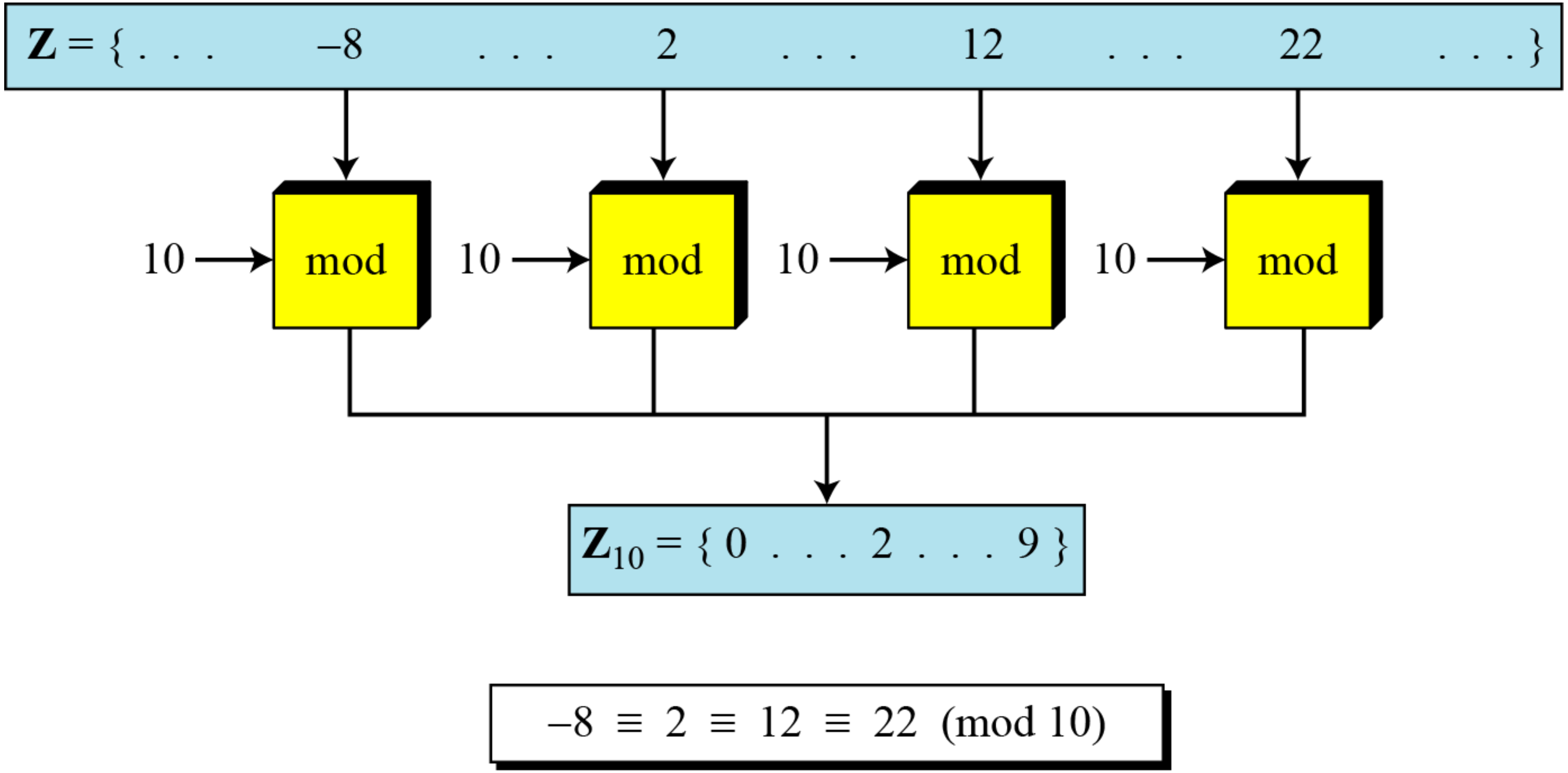
Congruence : Examples

❖ One way of seeing the **congruences (for mod 3 arithmetic):**

...	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	...
...-	9	-8	-7	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6	7	8	9	10	11	12	...

✓ Where the **top line is the output** of modulo 3 arithmetic and the **bottom line the set of all integers.**

Concept of Congruence



Congruence Relationship

Residue Classes

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

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

Congruence : Examples

- Some of the **congruence's modulo 3:**

1. $7 \equiv 1 \pmod{3}$
2. $-8 \equiv 1 \pmod{3}$
3. $-2 \equiv 1 \pmod{3}$
4. $7 \equiv -8 \pmod{3}$
5. $-2 \equiv 7 \pmod{3}$

Congruence : Examples

❖ Some of the **congruence's modulo 3:**

1. $7 \equiv 1 \pmod{3}$

   7 Mod 3 = 1 ;

   1 Mod 3 = 1 ; **we call as**

   $7 \equiv 1 \pmod{3}$

Congruence : Examples

- Some of the **congruence's modulo 3:**

$$-2 \equiv 1 \pmod{3}$$

a) - 2 Mod 3 = -2 ;

- 2 + 3 = 1 ;   -2 Mod 3 = 1 ;

b) 1 Mod 3 = 1 ; we write as

$$-2 \equiv 1 \pmod{3}$$

Congruence : Examples

- Some of the **congruence's modulo 3:**

$$-8 \equiv 1 \pmod{3}$$

a) $-8 \text{ Mod } 3 = -2$

$-2 + 3 = 1$; $-8 \text{ Mod } 3 = 1$;

b) $1 \text{ Mod } 3 = 1$; **we write as**

$$-8 \equiv 1 \pmod{3}$$

Congruence : Examples

- Some of the **congruence's modulo 3:**

$$7 \equiv -8 \pmod{3}$$

a) 7 Mod 3 = 1 ;

b) -8 Mod 3 = -2

-2 + 3 = 1 ; 8 Mod 3 = 1 ; **we write as**

$$7 \equiv -8 \pmod{3}$$

Congruence : Examples

- Some of the **congruence's modulo 3:**

$$-2 \equiv 7 \pmod{3}$$

a) **-2 Mod 3 = -2**

-2 + 3 = 1 ; -2 Mod 3 = 1

b) **7 Mod 3 = 1**

$$-2 \equiv 7 \pmod{3}$$

Modulo Operator : Some More Examples

- Find the **Remainder of the following operations:**

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

$$3 \equiv 8 \pmod{5} \qquad 8 \equiv 13 \pmod{5}$$

Modulo Operator : Some More Examples

1. $38 \equiv 23 \bmod 15$ because $38 = 15*2 + 8$ and $23 = 15 + 8$;
2. $-1 \equiv 1 \bmod 2$ because $-1 = -1*2+1$ and $1 = 0*2+1$;
3. $8 \equiv 3 \bmod 5$ because $8 = 5+3$ and $3 = 0*5+3$;
4. $-8 \equiv 2 \bmod 5$ because $-8 = -2*5+2$ and $2 = 0*5+2$;
5. $8 \not\equiv -8 \bmod 5$ because $8 = 5+3$ and $-8 = -2*5+2$.

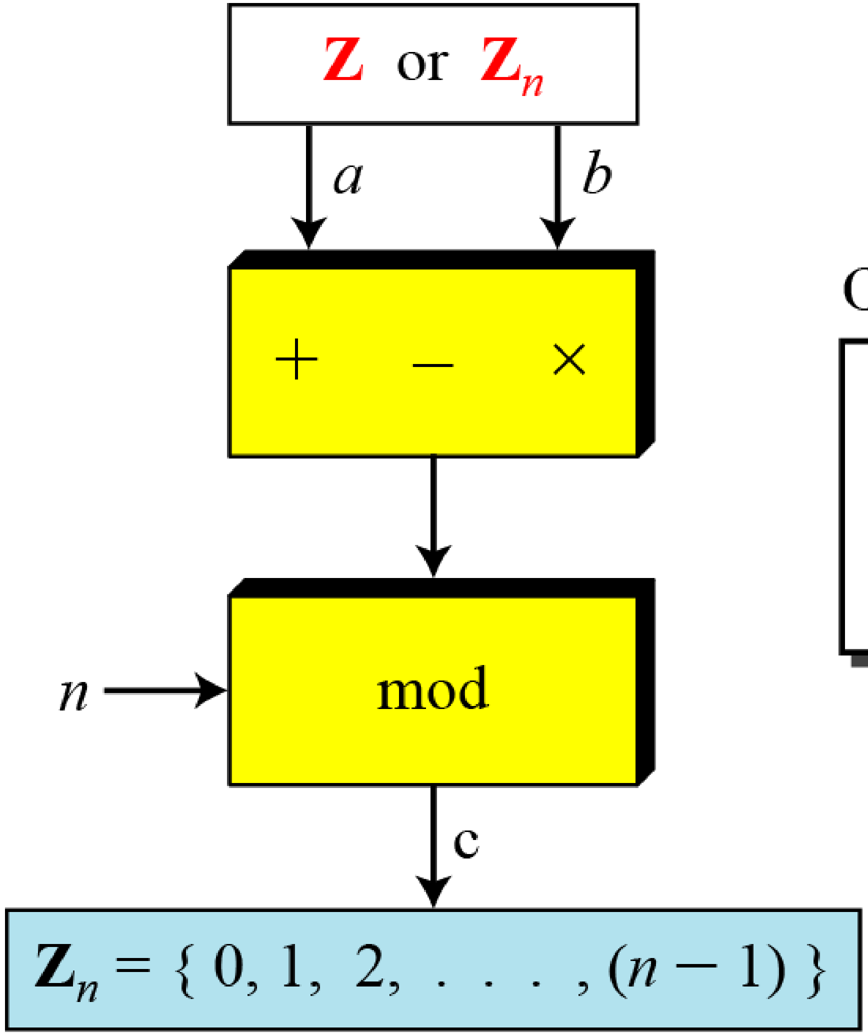
The remainders 3 and 2 are not the same.

Modular Arithmetic Operations

Modular Arithmetic Operations

- The three binary operations (+,*,-) that can be performed on the set Z.
- These operation can also be defined for the **set Z_n.**
- To Achieve this
  - ✓ The result will be mapped to Z_n using the **mod operator.**

Modular Arithmetic Operations ($\mathbf{Z_n}$)



Operations

$$(a + b) \bmod n = c$$

$$(a - b) \bmod n = c$$

$$(a \times b) \bmod n = c$$

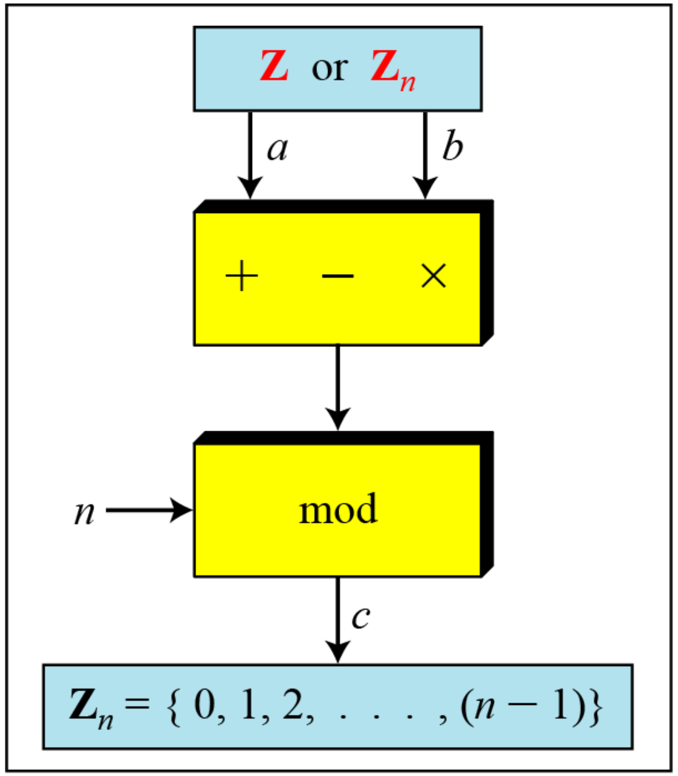
Modular Arithmetic Operations

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

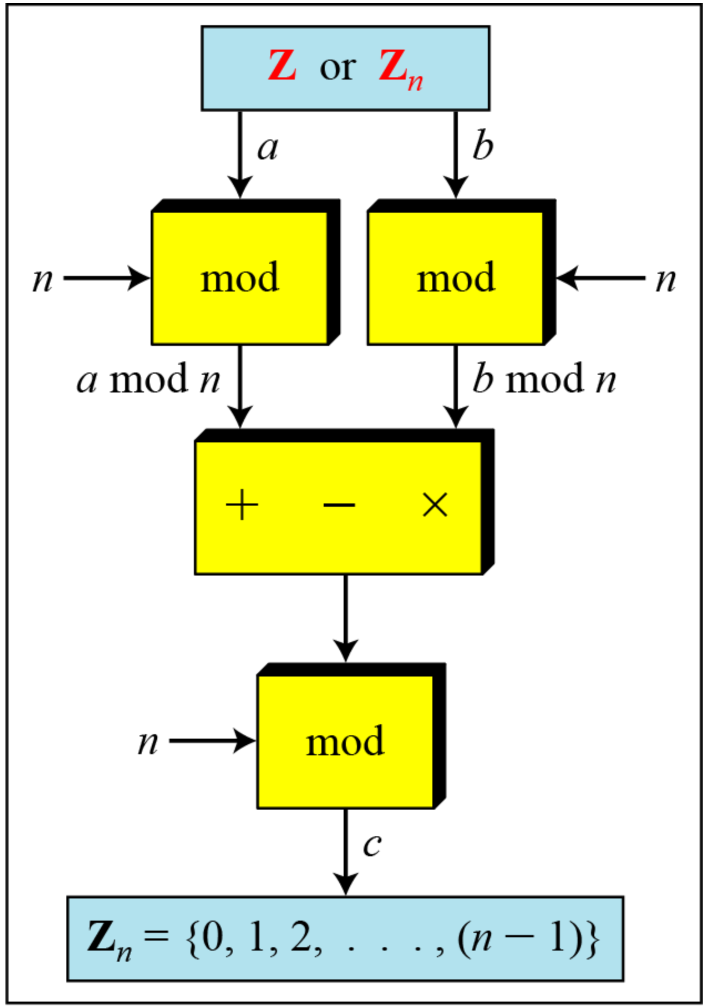
$$[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$$

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

Modular Arithmetic Operations(Z_n)



a. Original process



b. Applying properties

Modular Arithmetic Operations(Z_n): Some More Examples

1. $(1{,}723{,}345 + 2{,}124{,}945) \bmod 11$
2. $(1{,}723{,}345 - 2{,}124{,}945) \bmod 16$
3. $(1{,}723{,}345 \times 2{,}124{,}945) \bmod 16$

Modular Arithmetic Operations (Z_N) And Its Properties

THE SET Z_n AND ITS PROPERTIES

- Let's now consider the set **Z_n** along with the following **two binary operators** defined for the set:

1. **Modulo n addition; and**
2. **Modulo n multiplication.**

THE SET Z_n AND ITS PROPERTIES

❖ The **elements of Z_n** obey the following properties:

1. **Commutativity:**

   ✓ $(w + x) \bmod n = (x + w) \bmod n$

THE SET Z_n AND ITS PROPERTIES

❖ The **elements of Z_n** obey the following properties:

2. Associativity:

✓ $[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$

THE SET Z_n AND ITS PROPERTIES

❖ The **elements of Z_n** obey the following properties:

3. **Distributivity of Multiplication over Addition:**

   ✓ $[w \times (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$

4. **Existence of Identity Elements:**

   ✓ $(0 + w) \bmod n = (w + 0) \bmod n$

THE SET Z_n AND ITS PROPERTIES

❖ The **elements of Z_n** obey the following properties:

5. Existence of Additive Inverses:

For each $w \in Z_n$, there exists a $z \in Z_n$ such that

$w + z = 0 \bmod n$

Inverses of Z_n

Modulo Addition and Modulo Multiplication Over Z_n

- 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
  1. **Additive Inverse**
  2. **Multiplicative Inverse**

Modulo Addition Over Z_n

- For every element of Z_n, there exists an **additive inverse** in Z_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.**

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

Modulo Addition Over Z_n : Example

- Find all additive inverse pairs in Z_{10}.

Modulo Multiplicative Over Z_n

- Like, every non-zero element of Z_n. There exist an additive inverse in Z_n.
  - ✓ But there does **not exist a multiplicative inverse** for every **non-zero element of Z_n.**
- In modular arithmetic, an **integer may or may not have a multiplicative inverse.**

Modulo Multiplicative Over Z_n

- The product of the integer and its **multiplicative inverse is congruent to 1** modulo n.
- In Z_n, two numbers **a and b are the multiplicative inverse** of each other if

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

Modulo Multiplicative Over Z_n : Example

- Find the **Additive and Multiplicative inverse in Z_8**

Modulo Multiplicative Over Z_n : Example

❖ Find the **Multiplicative inverse in Z_6 and Z_5**

Multiplication modulo 6

*	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

Multiplication modulo 5

*	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Modulo Multiplicative Over Z_n : Example

- 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.**

Observation....

The **multiplicative inverses exist for only those elements** of Z_n that are **relatively prime/Coprime** to n.

Two Integers are said to be **relatively prime/Coprime,** iff the only two integers that **divides both of them should be only 1**

Observation....

Two integers are relatively prime to each other if the **integer 1 is the only common positive divisor.**

More formally, **two integers a and b are relatively prime to each other if gcd(a, b) = 1** where GCD denotes the **Greatest Common Divisor.**

Finally….

- The existence of the **multiplicative inverse** for an element 'a' of Z_n is predicated on a being **relatively prime to n**

Two integers are relatively prime to each other depends on their **greatest common divisor (GCD),**

Thank U