Number Theory

Introduction

- review integer arithmetic, concentrating on divisibility
- finding the greatest common divisor using the Euclidean algorithm

Integer Arithmetic

- In integer arithmetic, we use a set and a few operations.
- You are familiar with this set and the corresponding operations, but they are reviewed here to create a background for modular arithmetic.

- Set of Integers
- Binary Operations
- Integer Division
- Divisibility

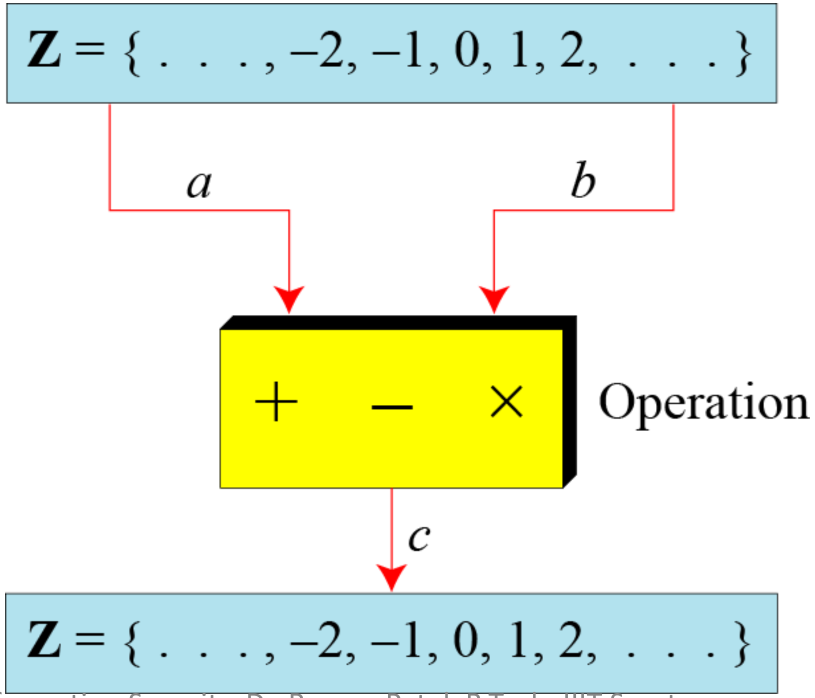
Set of Integers

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

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

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.



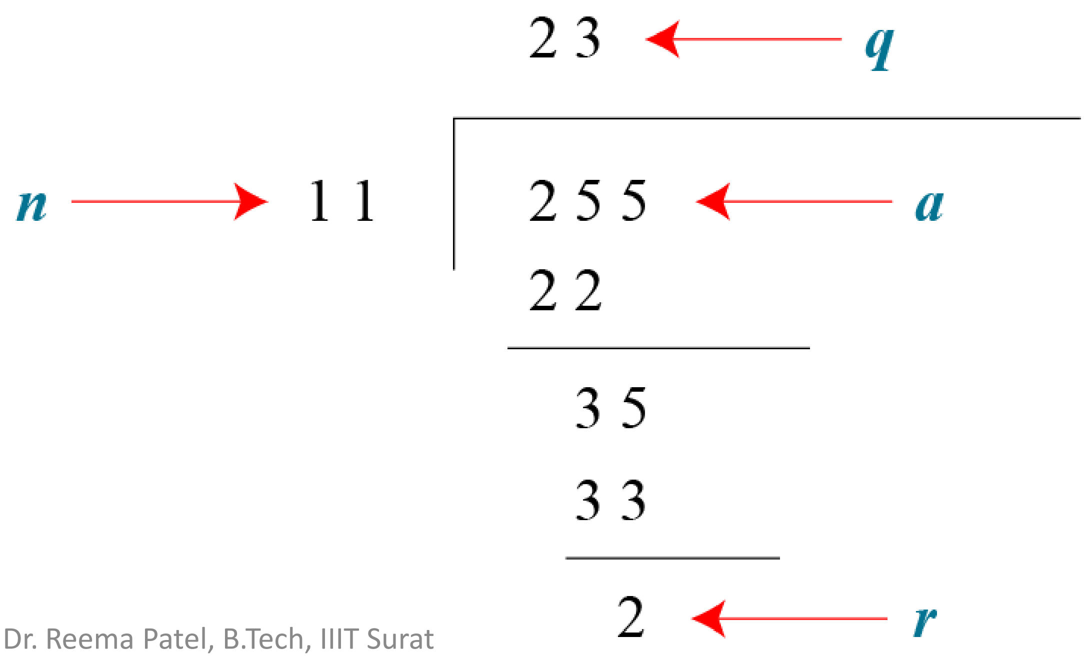
Binary Operations

- The following shows the results of the three binary operations on two integers.
- Because each input can be either positive or negative, we can have four cases for each operation.

Add:	$5 + 9 = 14$	$(-5) + 9 = 4$	$5 + (-9) = -4$	$(-5) + (-9) = -14$
Subtract:	$5 - 9 = -4$	$(-5) - 9 = -14$	$5 - (-9) = 14$	$(-5) - (-9) = +4$
Multiply:	$5 \times 9 = 45$	$(-5) \times 9 = -45$	$5 \times (-9) = -45$	$(-5) \times (-9) = 45$

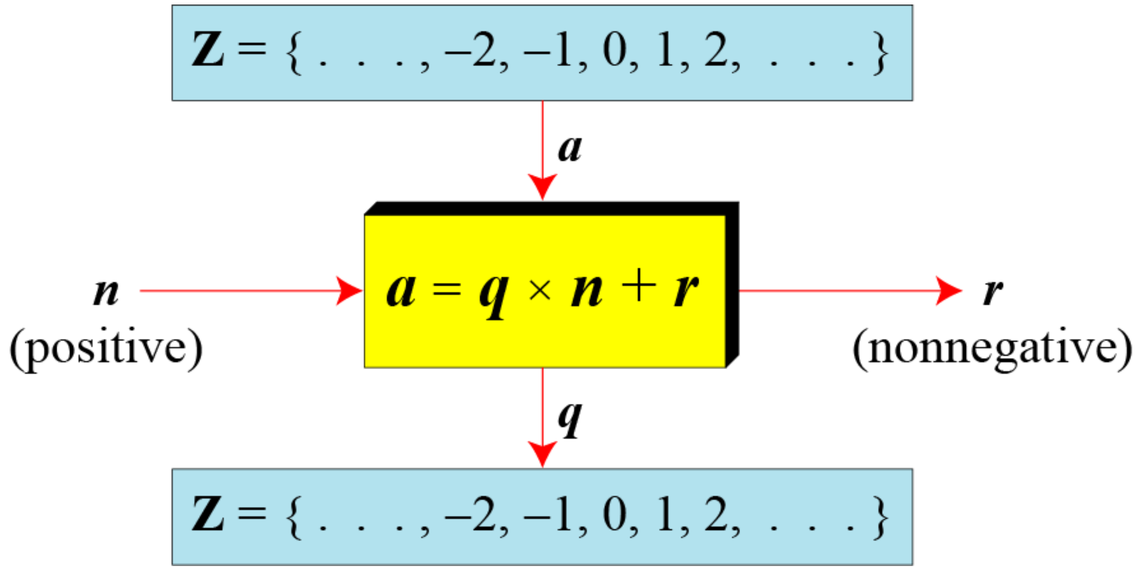
Integer Division

- In integer arithmetic, if we divide a by n, we can get q and r.
- $a = q \times n + r$
- Assume that a = 255 and n = 11. We can find q = 23 and r = 2 using the division algorithm.



Two Restrictions

- When we use division relationship in cryptography, we impose two restrictions
  - Divisor should be a positive integer (n>0)
  - Remainder should be a nonnegative integer (n>=0)



Two Restrictions

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

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

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, $a \mid n$

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

Divisibility

- The integer 4 divides the integer 32 because 32 = 8 × 4. We show this as

$$4 \mid 32$$

- The number 8 does not divide the number 42 because 42 = 5 × 8 + 2. There is a remainder, the number 2, in the equation. We show this as

$$8 \nmid 42$$

Properties

- Property 1: if $a|1$, then $a = \pm 1$.
- Property 2: if $a|b$ and $b|a$, then $a = \pm b$.
- Property 3: if $a|b$ and $b|c$, then $a|c$.
- Property 4: if $a|b$ and $a|c$, then
  $a|(m \times b + n \times c)$, where m
  and n are arbitrary integers

Divisibility

a. We have $13|78$, $7|98$, $-6|24$, $4|44$, and $11|(-33)$.

b. We have $13 \nmid 27$, $7 \nmid 50$, $-6 \nmid 23$, $4 \nmid 41$, and $11 \nmid (-32)$.

Divisibility

a. Since $3|15$ and $15|45$,

according to the third property, $3|45$.

b. Since $3|15$ and $3|9$,

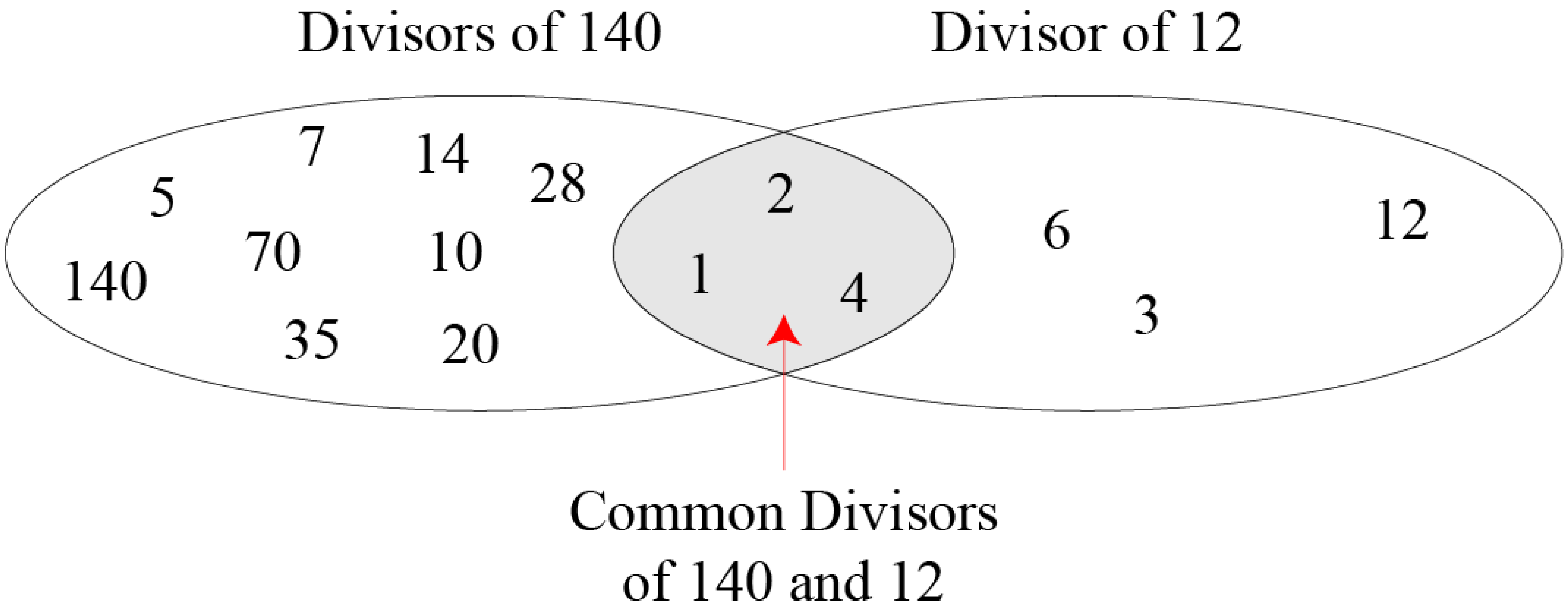
according to the fourth property,

$3|(15 \times 2 + 9 \times 4)$, which means $3|66$.

Divisibility

- Fact 1: The integer 1 has only one divisor, itself.
- Fact 2: Any positive integer has at least two divisors, 1 and itself (but it can have more).

Common divisors of two integers



Common divisors of two integers

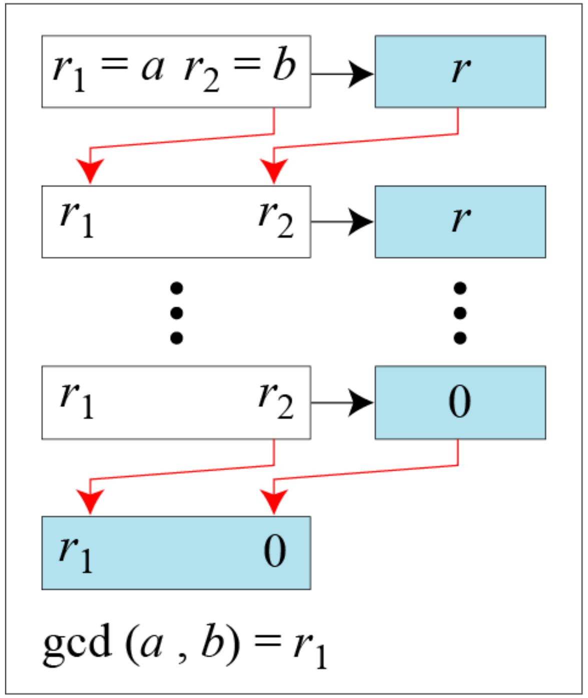
- Greatest Common Divisor
- The greatest common divisor of two positive integers is the largest integer that can divide both integers.

- 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

Euclidean Algorithm to Find GCD



a. Process

$r_1 \leftarrow a; \quad r_2 \leftarrow b;$ (Initialization)

while $(r_2 > 0)$

{

$q \leftarrow r_1 / r_2;$

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

$r_1 \leftarrow r_2; \quad r_2 \leftarrow r;$

}

$\gcd(a, b) \leftarrow r_1$

b. Algorithm

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

Euclidean Algorithm to Find GCD

- Find the greatest common divisor of 25 and 60.

Euclidean Algorithm to Find GCD

- Find the greatest common divisor of 25 and 60.
- We have gcd (25, 65) = 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	

Euclidean Algorithm to Find GCD

- Find the greatest common divisor of 2740 and 1760.

Euclidean Algorithm to Find GCD

- 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	

- We have gcd (2740, 1760) = 20.

Modular Arithmetic

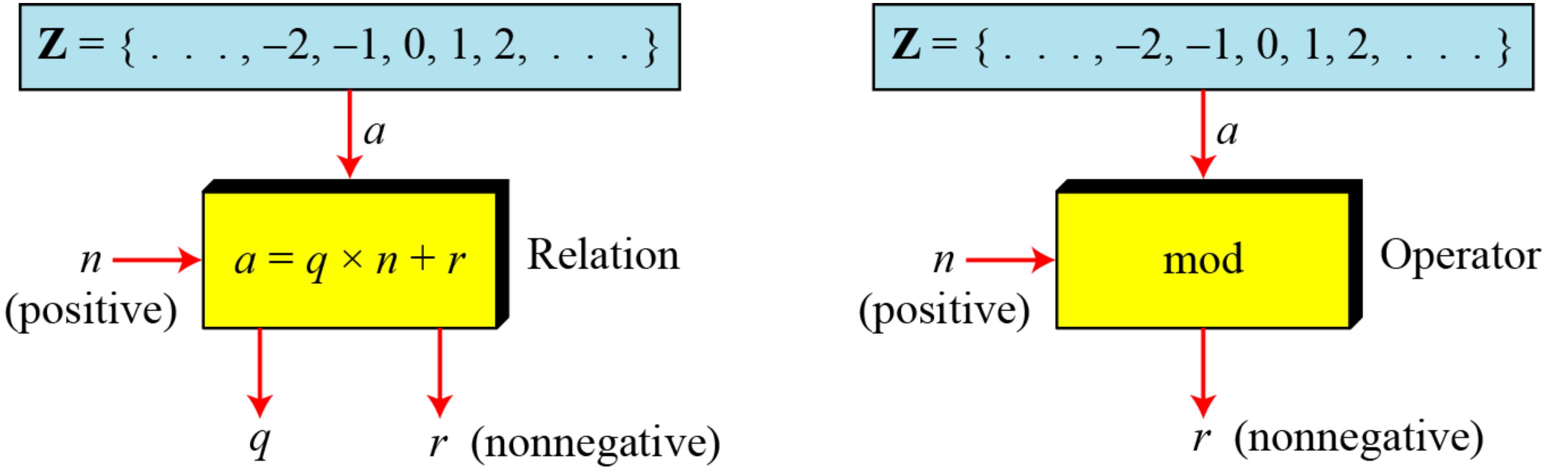
- The division relationship ($a = q \times n + r$) has two inputs (a and n) and two outputs (q and r).
- In modular arithmetic, we are interested in only one of the outputs, the remainder r.
- Topics:
  - Modular Operator
  - Set of Residues
  - Congruence
  - Operations in Z_n
  - Addition and Multiplication Tables
  - Different Sets

Modular Arithmetic

- 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.



Division algorithm and modulo operator

Modulo Operator

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

Modulo Operator

- 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.

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.

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

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

Some Z_n sets

Congruence

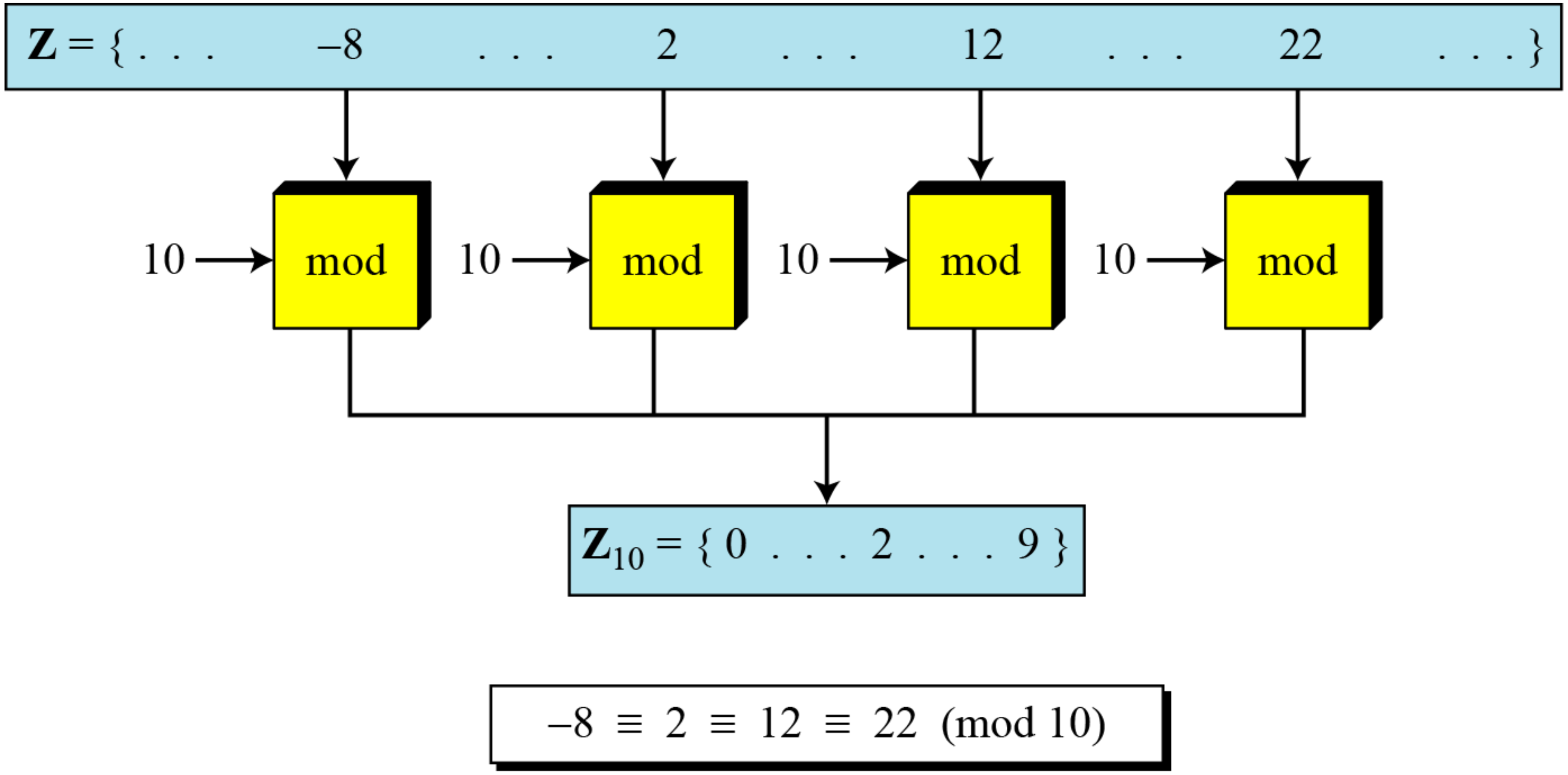
- To show that two integers are congruent, use the congruence operator ($\equiv$).

Congruence

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

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

Congruence



Congruence Relationship

Congruence

- Properties of Congruence:
  1. $a \equiv b \pmod{n}$ if $n|(a - b)$.
  2. $a \equiv a \pmod{n}$ for all a **(Reflexive)**
  3. $a \equiv b \pmod{n}$ implies $b \equiv a \pmod{n}$ **(Symmetric)**
  4. $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ imply $a \equiv c \pmod{n}$.**(Transitive)**

- Examples: for 1st property
  - $23 \equiv (8 \bmod 5)$ because $(23 - 8) = 15 = 5 \times 3$
  - $-11 \equiv (5 \bmod 8)$ because $(-11 - 5) = -16 = 8 \times -2$

Congruence

- Some standard rules for congruence :

1. If $a \equiv a'$ mod n and $b \equiv b'$ mod n, then $(a + b) \equiv (a' + b')$ mod n
2. If $a \equiv a'$ mod n and $b \equiv b'$ mod n, then $(ab) \equiv (a'b')$ mod n

Congruence

- Examples:
  - Compute $1093028 \cdot 190301 \bmod 100$
  - $1093028 \equiv 28 \bmod 100$ and $190301 \equiv 1 \bmod 100$

Congruence

- Examples:
  - Compute $1093028 \cdot 190301 \bmod 100$

Congruence

- Examples:
  - Compute $1093028 \cdot 190301 \bmod 100$

- $1093028 \equiv 28 \bmod 100$ and $190301 \equiv 1 \bmod 100$

Congruence

last two digits of 1093028

- Examples:
  - Compute $1093028 \cdot 190301 \bmod 100$
  - $1093028 \equiv 28 \bmod 100$ and $190301 \equiv 1 \bmod 100$
- We can compute as
  - $1093028 \cdot 190301$

  $= [1093028 \bmod 100] \cdot [190301 \bmod 100] \bmod 100$

  $= 28 \cdot 1 \bmod 100$

  $= 28$

- Computing the product $1093028 \cdot 190301$ and then reducing the answer modulo 100 is very much time consuming.

Congruence

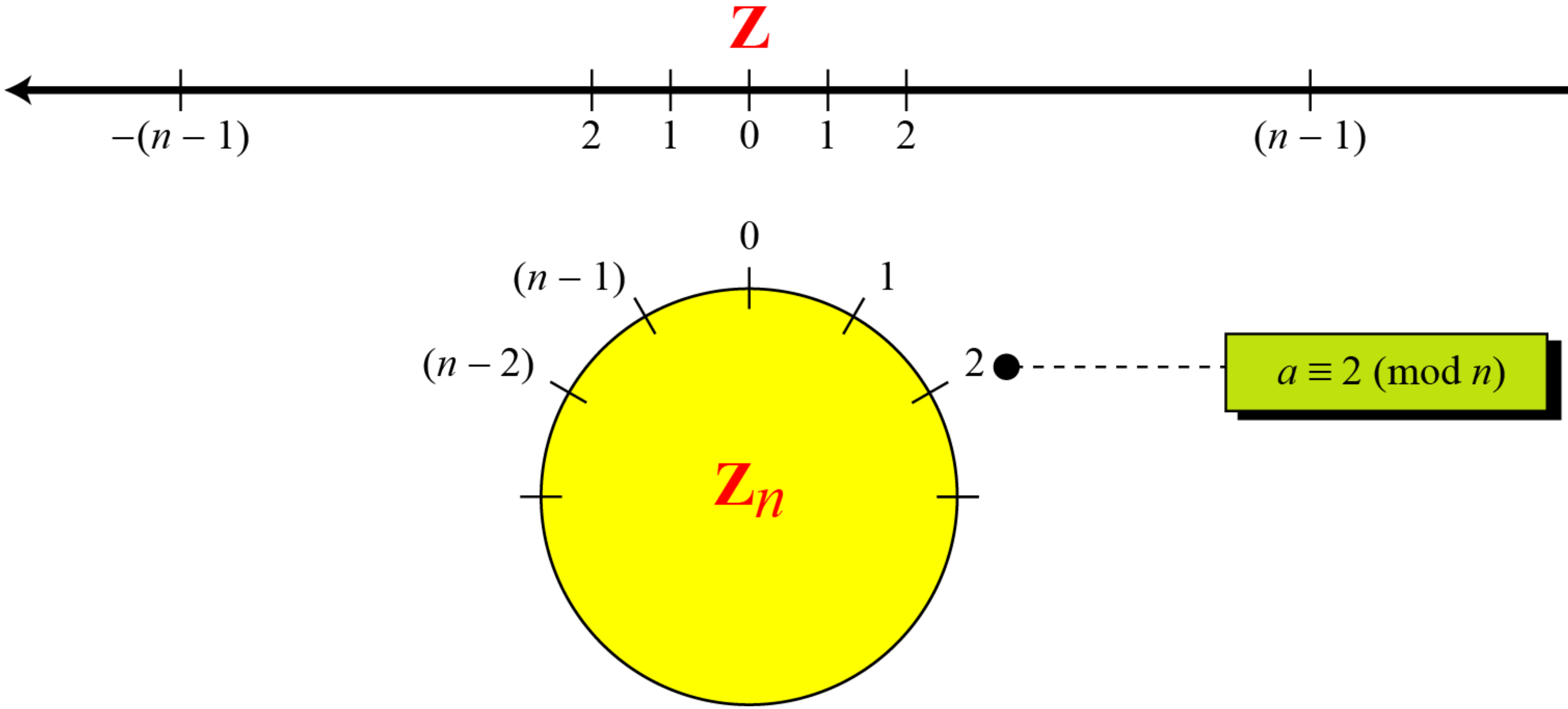
- Residue Classes
  - A residue class [a] or $[a]_n$ is the set of integers congruent modulo n.
  - It is the set of all integers such that $x \equiv a(\text{mod})n$
  - E.g. for n=5

Congruence

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

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

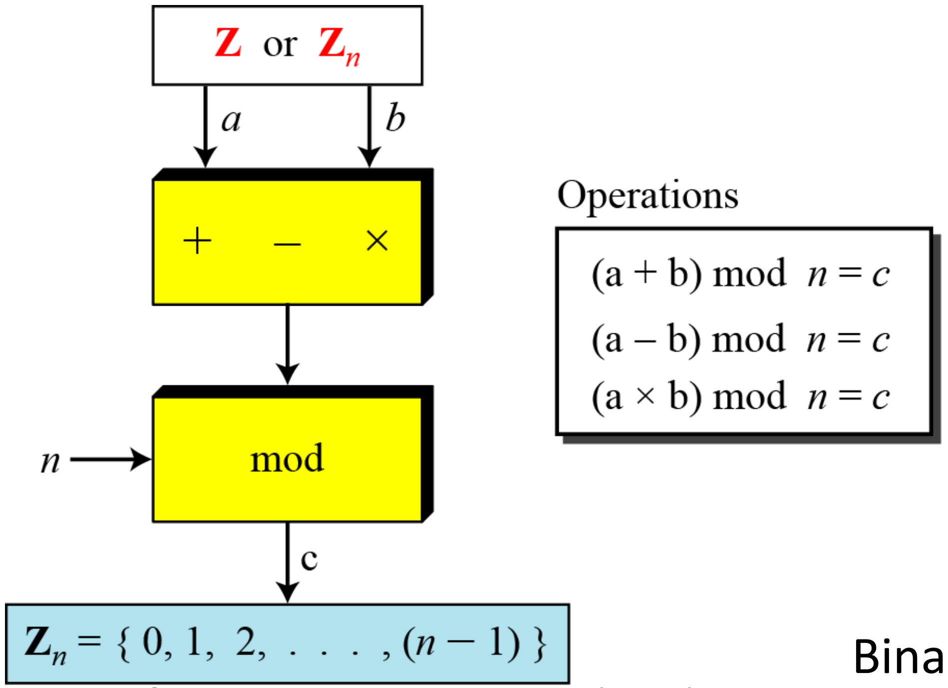
Congruence



Comparison of Z and 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 Zn. The result may need to be mapped to Zn using the mod operator.



Binary operations in Z_n

Operation in Z_n

- Perform the following operations (the inputs come from Zn):
- a. Add 7 to 14 in Z15.
- b. Subtract 11 from 7 in Z13.
- c. Multiply 11 by 7 in Z20.

Operation in Z_n

- Solution:

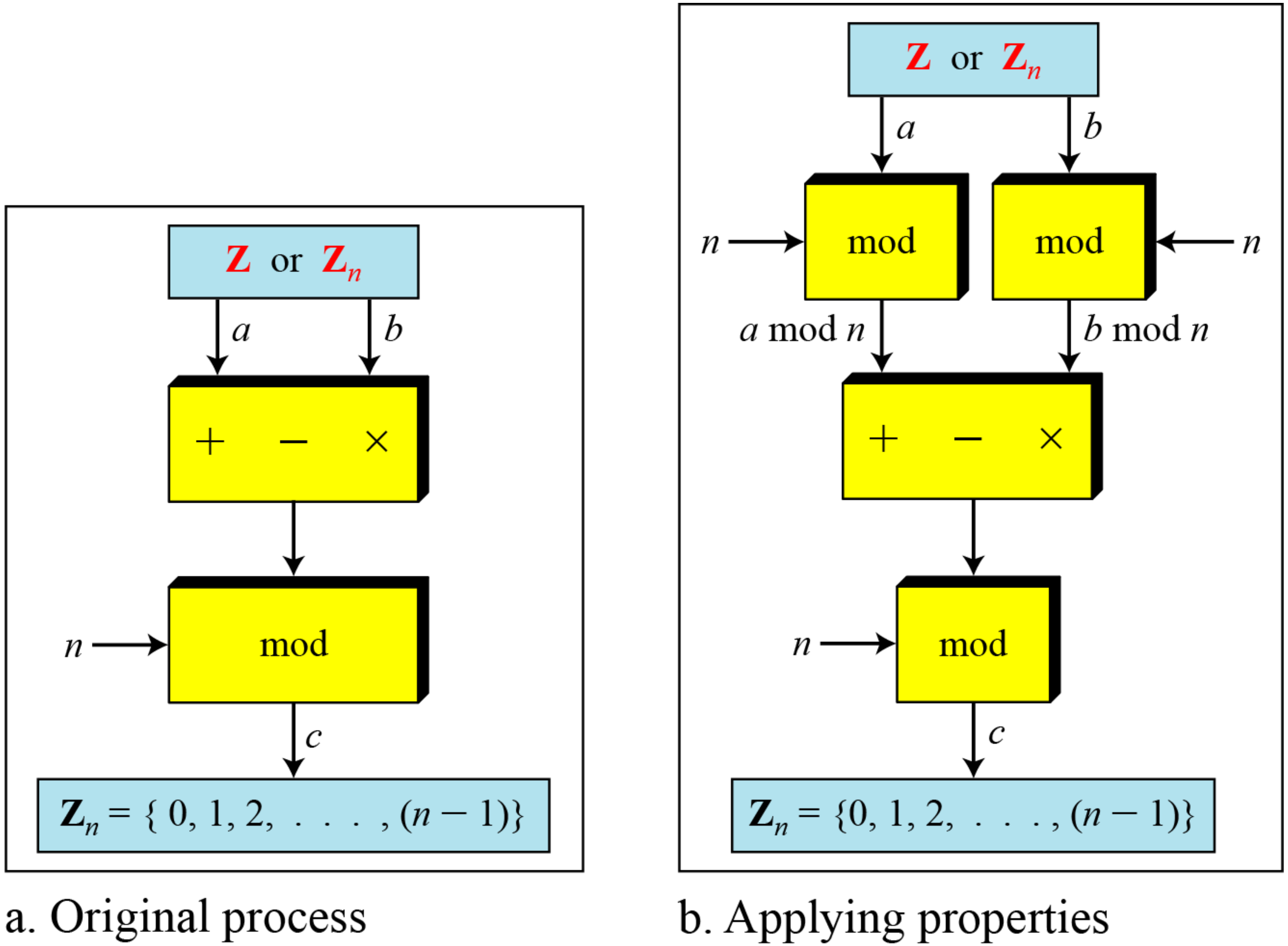
$$(14 + 7) \bmod 15 \rightarrow (21) \bmod 15 = 6$$
$$(7 - 11) \bmod 13 \rightarrow (-4) \bmod 13 = 9$$
$$(7 \times 11) \bmod 20 \rightarrow (77) \bmod 20 = 17$$

Operation in Z_n

- 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}.

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



Properties of mode operator

Operation in Z_n

- The following shows the application of the above properties:

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

2. $(1{,}723{,}345 - 2{,}124{,}945) \bmod 16 = (8 - 9) \bmod 11 = 10$

3. $(1{,}723{,}345 \times 2{,}124{,}945) \bmod 16 = (8 \times 9) \bmod 11 = 6$

Operation in Z_n

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

Operation in Z_n

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

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

$$\begin{array}{lcl} 10 \bmod 3 = 1 & \rightarrow & 10^n \bmod 3 = (10 \bmod 3)^n = 1 \\ 10 \bmod 9 = 1 & \rightarrow & 10^n \bmod 9 = (10 \bmod 9)^n = 1 \\ 10 \bmod 7 = 3 & \rightarrow & 10^n \bmod 7 = (10 \bmod 7)^n = 3^n \bmod 7 \end{array}$$

Operation in Z_n

- 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. We write an integer as the sum of its digits multiplied by the powers of 10.

Operation in Z_n

- 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. We write an integer as the sum of its digits multiplied by the powers of 10.

$$a = a_n \times 10^n + \cdots + a_1 \times 10^1 + a_0 \times 10^0$$

For example: $6371 = 6 \times 10^3 + 3 \times 10^2 + 7 \times 10^1 + 1 \times 10^0$

$$\begin{aligned}
a \bmod 3 &= (a_n \times 10^n + \cdots + a_1 \times 10^1 + a_0 \times 10^0) \bmod 3 \\
&= (a_n \times 10^n) \bmod 3 \ + \cdots + (a_1 \times 10^1) \bmod 3 \ + (a_0 \times 10^0) \bmod 3 \\
&= (a_n \bmod 3) \times (10^n \bmod 3) + \cdots + (a_1 \bmod 3) \times (10^1 \bmod 3) + \\
&\quad (a_0 \bmod 3) \times (10^0 \bmod 3) \\
&= a_n \bmod 3 + \cdots + a_1 \bmod 3 \ + a_0 \bmod 3 \\
&= (a_n \ + \cdots + a_1 + a_0) \bmod 3
\end{aligned}$$

Operation in Z_n

- Example:
  - 8756 mod 3
  - 9878 mod 3
  - 1095676 mod 3

Modular Arithmetic Operations

- Exponentiation is performed by repeated multiplication.
- Example:
- Find 11^7 mod 13

Modular Arithmetic Operations

- Exponentiation is performed by repeated multiplication.
- Example:
- Find 11^7 mod 13
  - $11^2 = 121 \equiv 4 \pmod{13}$
  - $11^4 = (11^2)^2 \equiv 4^2 \equiv 3 \pmod{13}$
  - $11^7 = 11 \times 4 \times 3 \equiv 132 \equiv 2 \pmod{13}$

Modular Arithmetic Operations

- Example: $17^{10} \bmod 14$

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 Inverse

- In Z_n, two numbers a and b are additive inverses of each other if

Additive Inverse

- 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 Inverse

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

Additive Inverse

- 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 Inverse

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

Multiplicative Inverse

- In Zn, 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 Inverse

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

Multiplicative Inverse

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

- **Solution:**
- In other words, we cannot find any number between 0 and 9 such that when multiplied by 8, the result is congruent to 1.
- There is no multiplicative inverse because gcd (10, 8) = 2 ≠ 1.

Multiplicative Inverse

- Find all multiplicative inverses in Z_{10}.

Multiplicative Inverse

- 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.

Multiplicative Inverse

- Find all multiplicative inverses in Z_{11}.

Multiplicative Inverse

- Find all multiplicative inverses in Z_{11}.

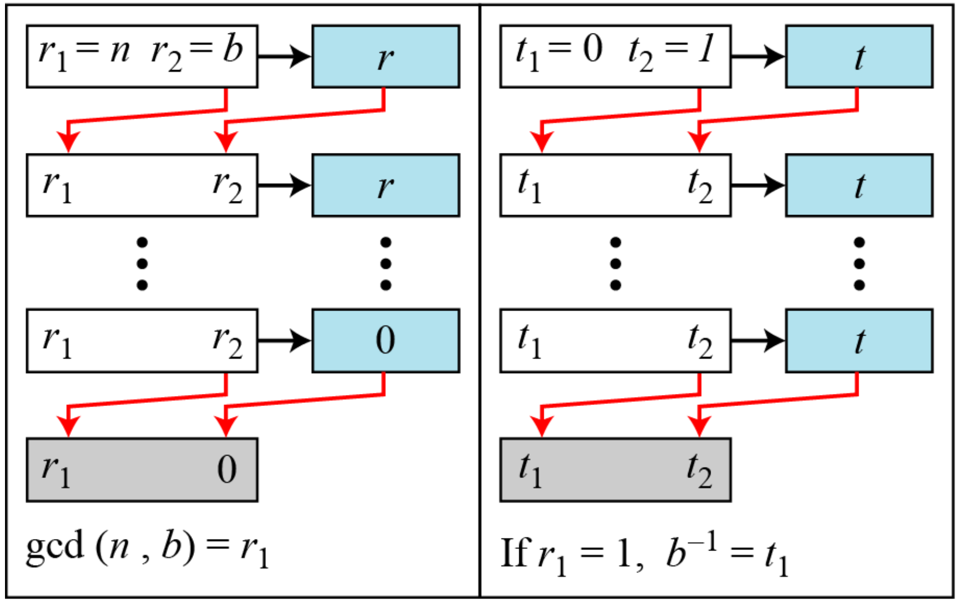
- Solution:
- We have seven pairs: (1, 1), (2, 6), (3, 4), (5, 9), (7, 8), (9, 5), and (10, 10).

Multiplicative Inverse

- 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 Zn.

Multiplicative Inverse



a. Process

$r_1 \leftarrow n; \qquad r_2 \leftarrow b;$

$t_1 \leftarrow 0; \qquad t_2 \leftarrow 1;$

while ($r_2 > 0$)

{

$q \leftarrow r_1 \; / \; r_2;$

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

$r_1 \leftarrow r_2; \qquad r_2 \leftarrow r;$

$t \leftarrow t_1 - q \times t_2;$

$t_1 \leftarrow t_2; \qquad t_2 \leftarrow t;$

}

if ($r_1 = 1$) then $b^{-1} \leftarrow t_1$

b. Algorithm

Using extended Euclidean algorithm to find multiplicative inverse

Multiplicative Inverse

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

Multiplicative Inverse

- Find the multiplicative inverse of 11 in Z26.

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 Inverse

- Find the multiplicative inverse of 23 in Z_{100}.

Multiplicative Inverse

- 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.

Multiplicative Inverse

- Find the inverse of 12 in Z_{26}.

Multiplicative Inverse

- Find the inverse of 12 in Z26.

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

	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 $\mathbf{Z}_{10}$

Addition and multiplication table for Z10

Different Sets

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

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

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

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

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

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

Some Z_n and Z_{n^*} sets

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

Different Sets

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

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

Multiplicative Inverse

- Find the multiplicative inverse of 50 in Z_{71}

- Find the multiplicative inverse of 43 in Z_{64}