# Mathematics of Cryptography

Dr. B C Dhara

Department of Information Technology

Jadavpur University

# Objectives

- Review integer arithmetic, divisibility, finding the greatest common divisor using Euclidean algorithm
- Use of extended Euclidean algorithm to solve linear Diophantine equations, linear congruent equations, and find the multiplicative inverses
- Importance of modular arithmetic and the modulo operator
- Review matrices and operations on residue matrices
- To solve a set of congruent equations using residue matrices

# INTEGER ARITHMETIC

- In integer arithmetic, we use a set and a few operations, they are reviewed here to create a background for modular arithmetic
- Topics to be discussed
  - Set of Integers
  - Binary Operations
  - Integer Division
  - Divisibility
  - Linear Diophantine Equations

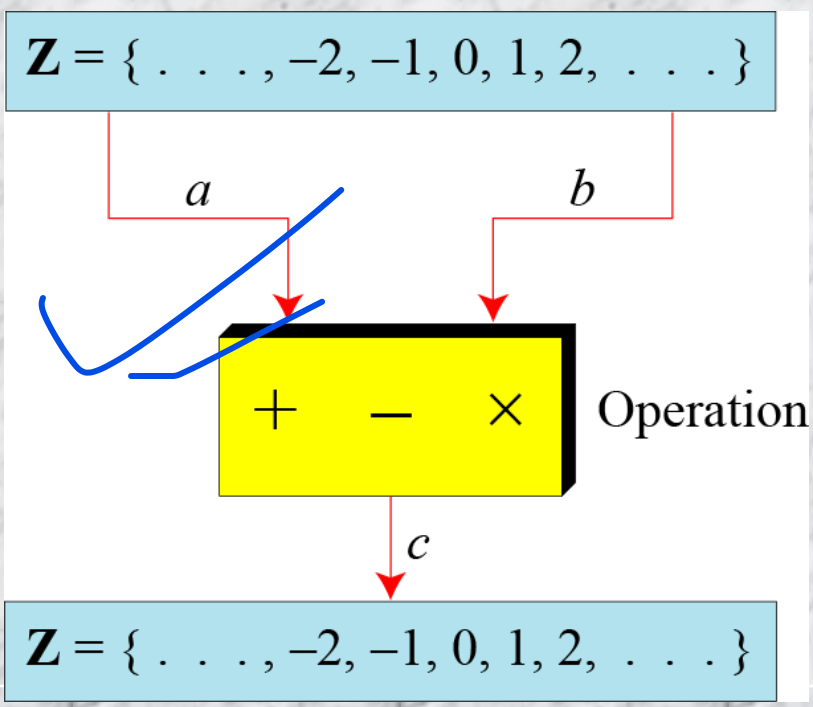
# Set of Integers

- 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

- 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 (Contd…)

- 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

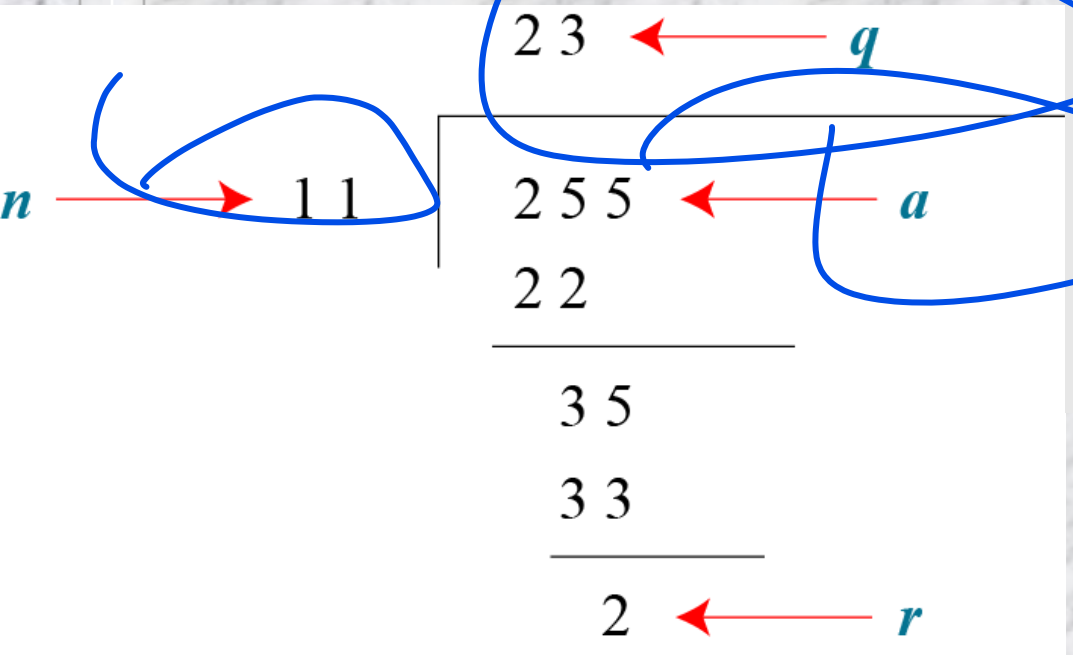
- In integer arithmetic, if we divide a by n, we can get q and r . The relationship between these four integers can be shown as

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

- ‘a’ is dividend, ‘q’ is quotient, ‘n’ is divisor and ‘r’ is remainder
- This is not an operation as get two outputs ‘q’ and ‘r’
  - This is called ***division relation***

# Integer Division (Contd…)

- Assume that a = 255 and n = 11. We can find q = 23 and R = 2 using the division algorithm

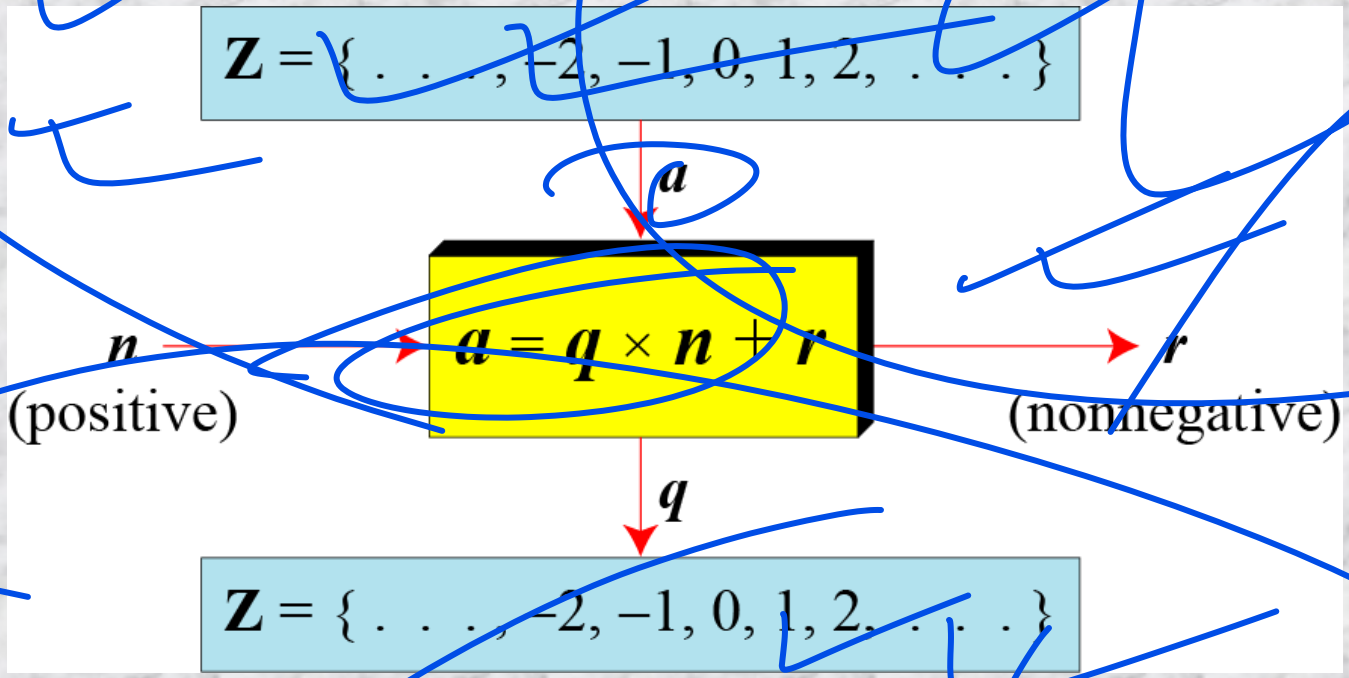



In cryptography two restrictions imposed:

i) Divisor be a positive (n>0)

ii) Remainder be a nonnegative integer ($r \geq 0$)

# Division algorithm for integers

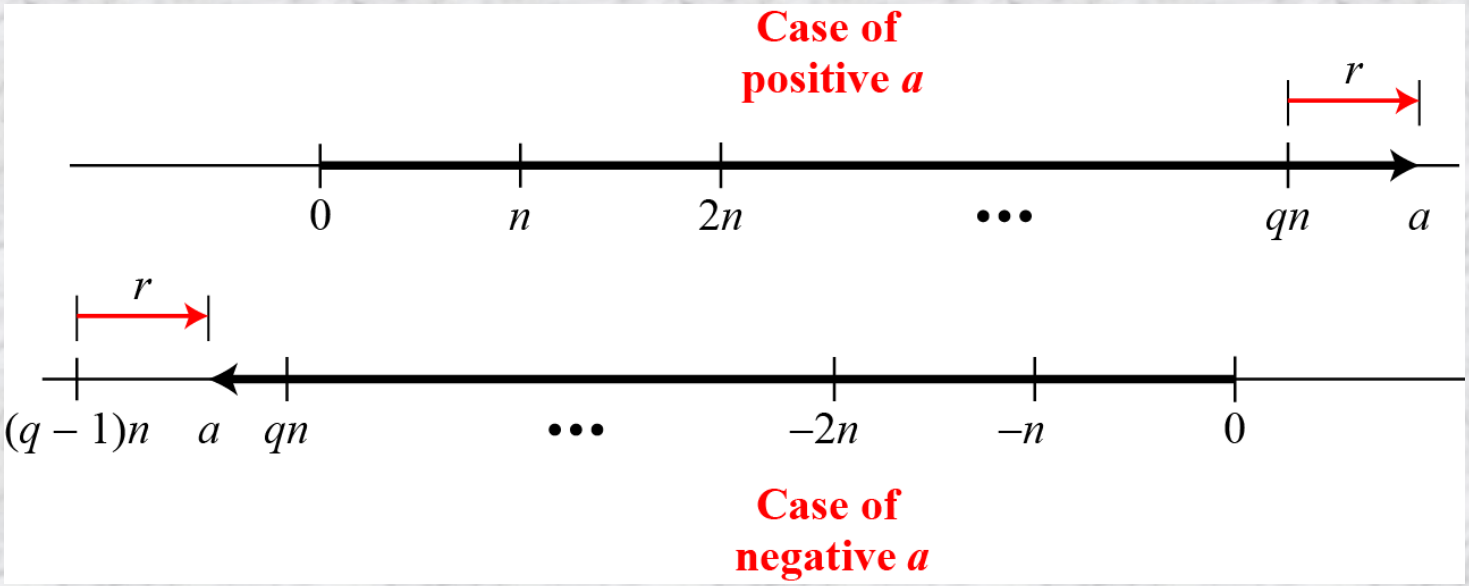


# Division algorithm for integers (contd…)

- 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?
- 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.

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

# Graph of division algorithm



# 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, **n|a (n divides a)**

If the remainder is not zero, $n \nmid a$ (n does not divides a)

# Divisibility (Contd…)

a. The integer 4 divides the integer 32 because $32 = 8 \times 4$. We show this as

$$4 \mid 32$$

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

$$8 \nmid 42$$

# Divisibility (Contd…)

- Property 1: if a|1, then a = ±1
- Property 2: if a|b and b|a, then a = ±b
- Property 3: if a|b and b|c, then a|c
- Property 4: if a|b and a|c, then a|(m × b + n × c), where m and n are arbitrary integers

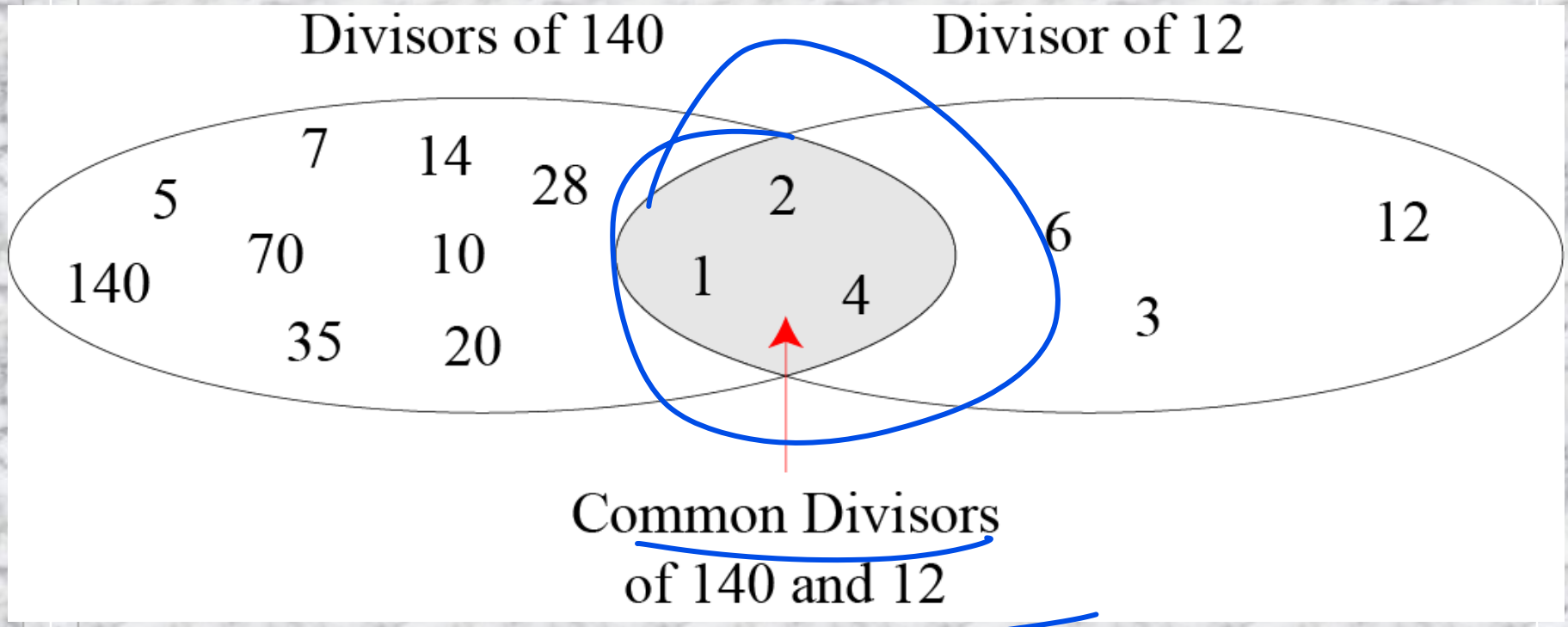
# Divisibility (Contd…)

- Since 3|15 and 15|45 ➔ 3|45 (by 3rd property)
- Since 3|15 and 3|9 ➔ 3|(15×2+9 ×4) i.e., 3|66 (by 4th property)

# Divisibility (Contd…)

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

# Common divisors of two integers



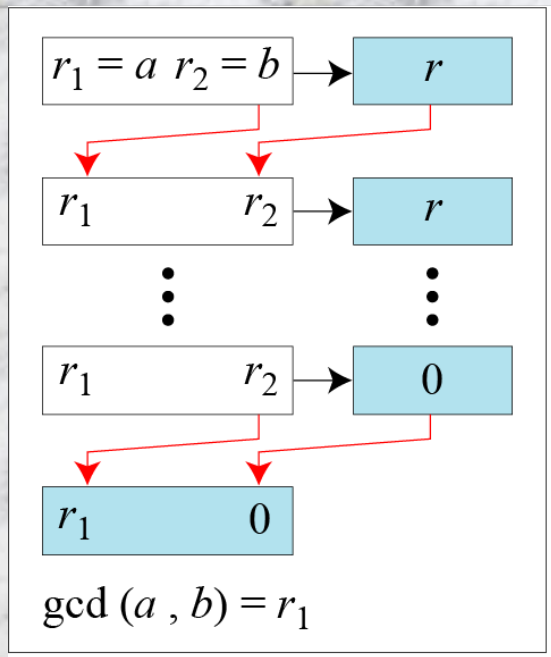
# Greatest Common Divisor

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




a. Process

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

while $(r_2 > 0)$

{

$q \leftarrow r_1 / r_2;$

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

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

}

gcd $(a, b) \leftarrow r_1$

b. Algorithm

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

# Euclidean Algorithm: example

- 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 | |

# Euclidean Algorithm: example

- Find the greatest common divisor of 25 and 60

| $q$ | $r_1$ | $r_2$ | $r$ |
|---|---|---|---|
| 0 | 25 | 60 | 25 |
| 2 | 60 | 25 | 10 |
| 2 | 25 | 10 | 5 |
| 2 | 10 | 5 | 0 |
| | **5** | 0 | |

# Extended Euclidean algorithm

- Property 4 of divisibility: if a|b and a|c, then a|(m × b + n × c), where m and n are arbitrary integers
- Given two integers a and b, we often need to find other two integers, s and t, such that

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

- The extended Euclidean algorithm can calculate the gcd (a, b) and at the same time calculate the value of s and t.

# Extended Euclidean algorithm (contd…)

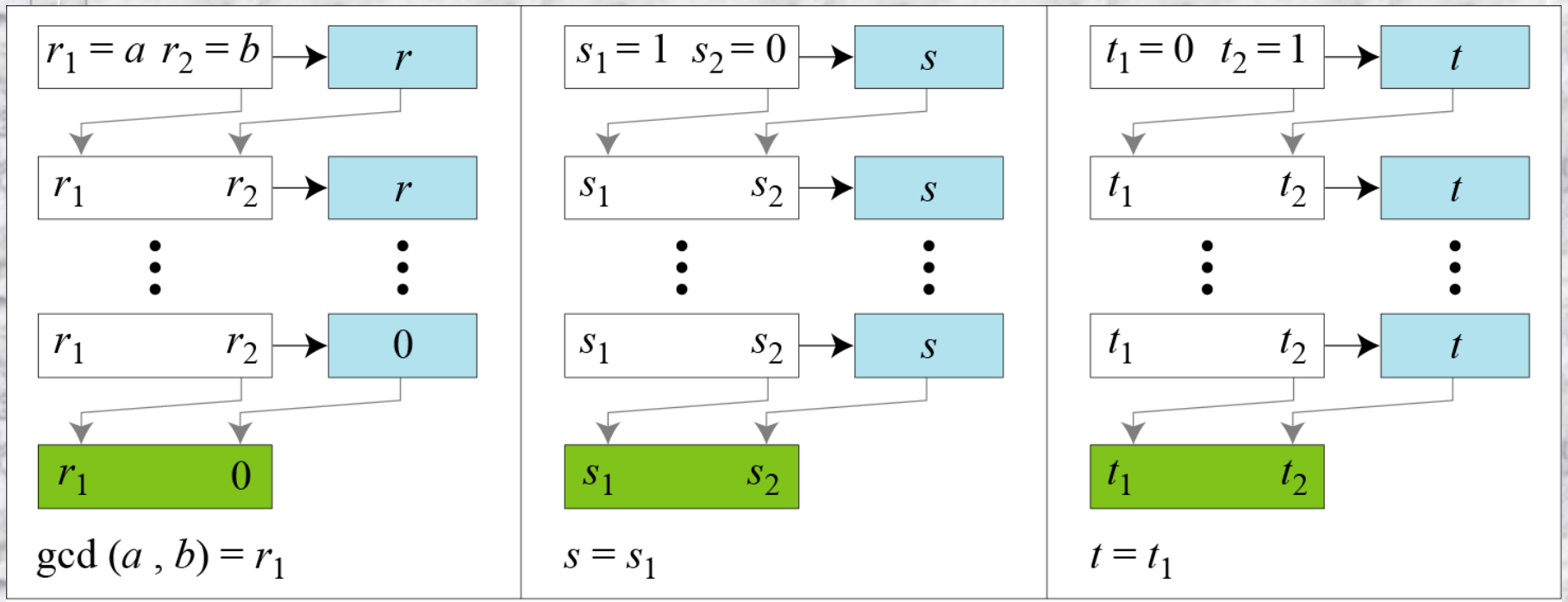
$$s \times a + t \times b = \gcd(a, b)$$

- Finding the gcd(81, 57) by the Euclidean Algorithm:

- 81 = 1(57) + 24
  57 = 2(24) + 9
  24 = 2(9) + 6
  9 = 1(6) + 3
  6 = 2(3) + 0

- **3** = 9 -1(6) [6 = 24 - 2(9)]
- **3** = 9 - 1(24 - 2(9))
- = 3(9) - 1(24) [9 = 57 - 2(24)]
- **3** = 3( 57 - 2(24)) - 1(24)
- = 3(57) - 7(24) [24 = 81 - 1(57)]
- **3** = 3(57) - 7( 81 - 1(57))
- = 10(57) -7(81)

# Extended Euclidean algorithm (Contd…)




a. Process

# Extended Euclidean algorithm (Contd…)

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

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

# Extended Euclidean algorithm (Contd…)

- Given a = 161 and b = 28, find gcd (a, b) and the values of s and t.

| $q$ | $r_1$ | $r_2$ | $r$ | $s_1$ | $s_2$ | $s$ | $t_1$ | $t_2$ | $t$ |
|---|---|---|---|---|---|---|---|---|---|
| 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 | |

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

# Extended Euclidean algorithm (Contd…)

- Given a = 17 and b = 0, find gcd (a, b) and the values of s and t

| $q$ | $r_1$ | $r_2$ | $r$ | $s_1$ | $s_2$ | $s$ | $t_1$ | $t_2$ | $t$ |
|---|---|---|---|---|---|---|---|---|---|
| | **17** | 0 | | **1** | **0** | | **0** | **1** | |

- We get gcd (17, 0) = 17, s = 1, and t = 0

# Extended Euclidean algorithm (Contd…)

- Given a = 0 and b = 45, find gcd (a, b) and the values of s and t

| $q$ | $r_1$ | $r_2$ | $r$ | $s_1$ | $s_2$ | $s$ | $t_1$ | $t_2$ | $t$ |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 45 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| | **45** | 0 | | 0 | 1 | | **1** | 0 | |

- We get gcd (0, 45) = 45, s = 0, and t = 1

# Linear Diophantine Equation

A linear Diophantine equation of two variables is ax + by = c.

- This equation has either no solution or infinite solutions
- Let, d= gcd(a,b)
  - If d divides c, then infinite solution (one particular solution and rest, general)
  - Otherwise, no solution

# Linear Diophantine Equation (contd…)

- Particular solution

1. $ax + by = c \rightarrow a_1x+b_1y = c_1$ [divided by d]
2. Solve $a_1s+b_1t = 1$ for s and t using extended Euclidean algorithm

$a_1s+b_1t = 1 \rightarrow (a/d)s + (b/d)t = 1$

$\rightarrow a(c/d)s+b(c/d)t = c$

Particular solution:
$x_0 = (c/d)s$ and $y_0 = (c/d)t$

# Linear Diophantine Equation (contd…)

Particular solution $(x_0, y_0)$, so

$$ax_0+by_0 = c$$

$$\Rightarrow a(x_0+k(b/d))+b(y_0 -k(a/d))= c$$

or

$$\Rightarrow a(x_0-k(b/d))+b(y_0 +k(a/d))= c$$

General solutions:

$x = x_0 + k\,(b/d)$ and $y = y_0 - k(a/d)$

or

$x = x_0 - k\,(b/d)$ and $y = y_0 + k(a/d)$

where k is an integer

# Linear Diophantine Equation: example

- Find the particular and general solutions to the equation 21x + 14y = 35

  [3x+2y=5 ➔ 3x+2y=1 (1, -1)]

  Particular solution:

  $x_0 = (c/d)s = 35/7*1=5;$

  $y_0 = (c/d)t = 35/7*(-1)=-5;$

  General solution:

x= 5+k*14/7= 5+2k
y=-5-k*21/7=-5-3k

or

x= 5-k*14/7= 5-2k
y=-5+k*21/7=-5+3k

# Example linear Diophantine

- For example, imagine we want to cash a Rs. 100 check and get some Rs. 20 and some Rs. 5 bills. We have many choices, which we can find by solving the corresponding Diophantine equation $20x + 5y = 100$
- Since $d = \gcd(20, 5) = 5$ and $5 \mid 100$, the equation has an infinite number of solutions, but only a few of them are acceptable in this case
- The general solutions with x and y nonnegative are (0, 20), (1, 16), (2, 12), (3, 8), (4, 4), (5, 0)

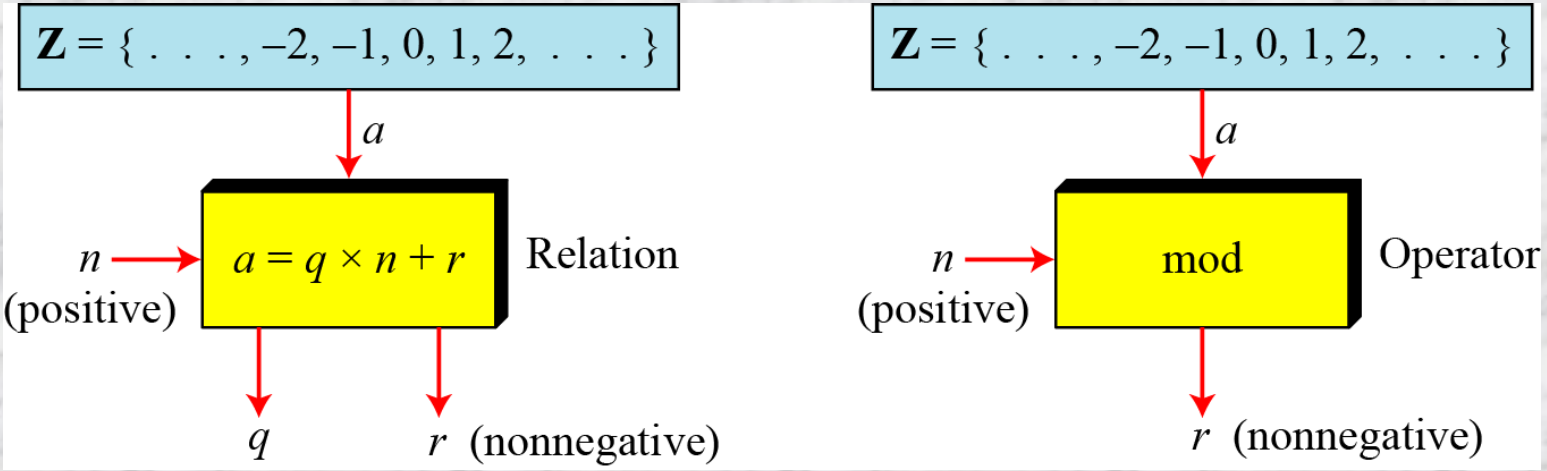
# MODULAR ARITHMETIC

- The division relationship ($a = q \times n + r$) discussed in the previous section 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

| | |
|---|---|
| Modular Operator | Operations in $Z_n$ |
| Set of Residues | Addition and Multiplication Tables |
| Congruence | Different Sets |

# Modular 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***

# 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 $Z_n$

- Some $Z_n$

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

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

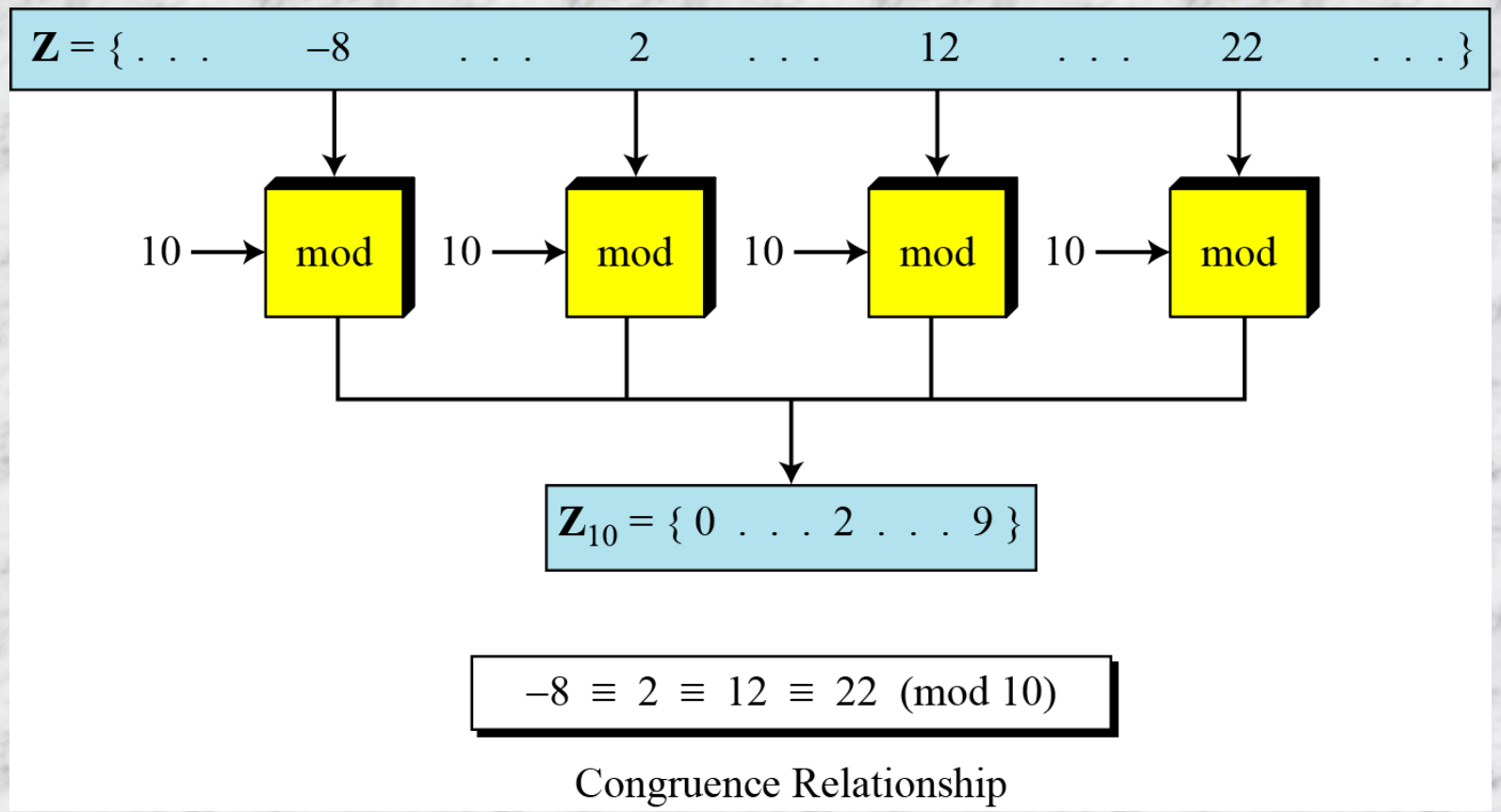
# Congruence

- $Z \rightarrow Z_n$, is not one-to-one mapping
  - Many members of Z map to one member of $Z_n$,
  - e.g., 2 mod 10=2, 12 mod 10=2, 22 mod 10=2
- 2, 12 and 22 are called **congruent** mod 10
- To show that two integers are congruent, we use the congruence operator ( $\equiv$ ). 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 (contd…)




Congruence Relationship

# Congruence (contd…)

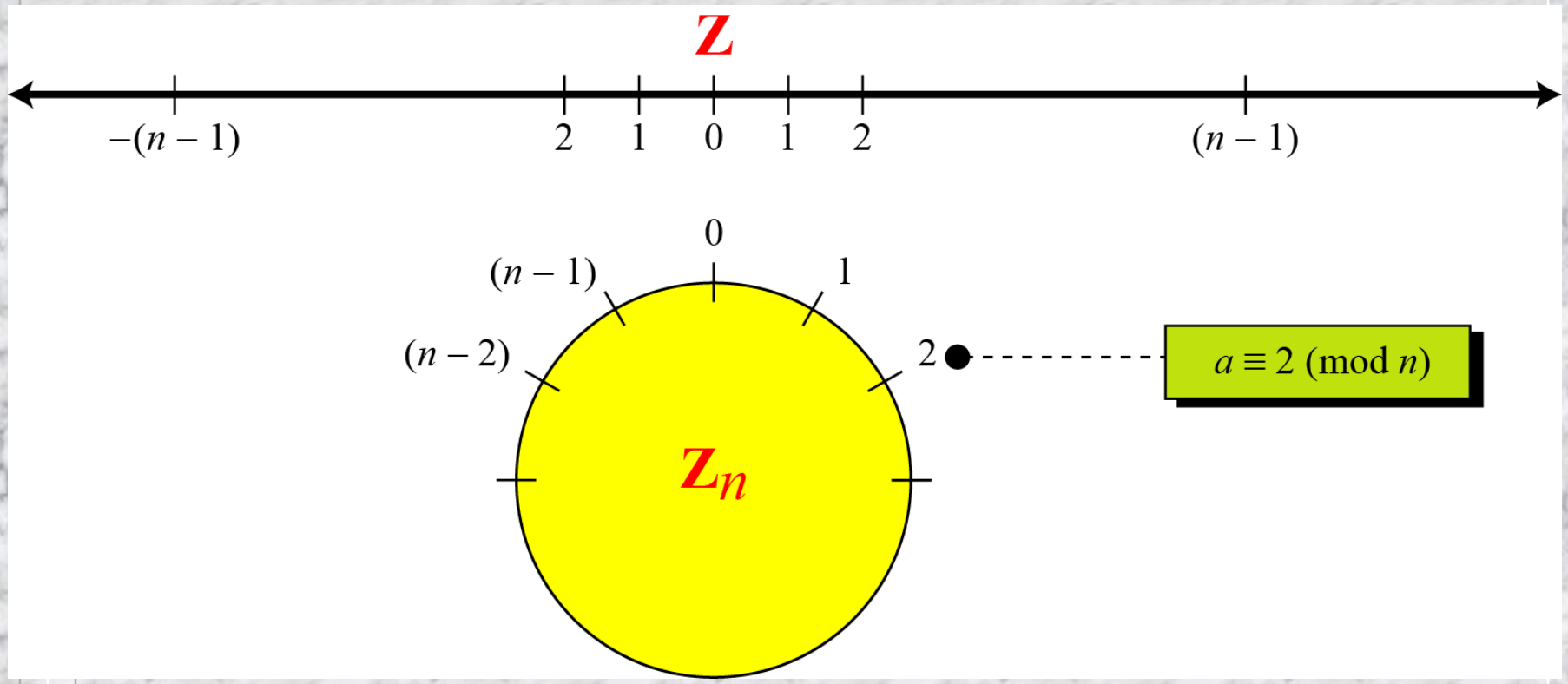
- Congruence looks like equal operator, but there are difference:
  - Equality operator maps a member of Z to itself
  - Congruence operator maps a member from Z to $Z_n$
  - Equality one-to-one mapping, congruence operator is many-to-one mapping
  - (mod n) is used to indicate the destination set $Z_n$

# Residue Classes

- A residue class [a] or $[a]_n$ is the set of integers congruent modulo n.
  - Set of all integers such that $x \equiv a \pmod{n}$
  - Residue classes (mod 5)

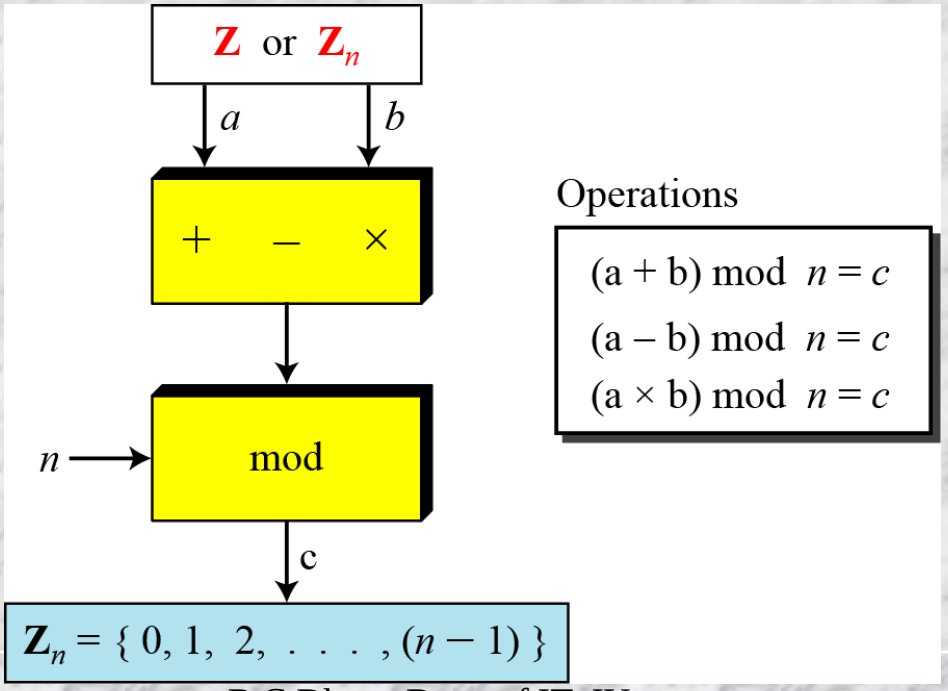
$$[0] = \{\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots\}$$
$$[1] = \{\ldots, -14, -9, -4, 1, 6, 11, 16, \ldots\}$$
$$[2] = \{\ldots, -13, -8, -3, 2, 7, 12, 17, \ldots\}$$
$$[3] = \{\ldots, -12, -7, -5, 3, 8, 13, 18, \ldots\}$$
$$[4] = \{\ldots, -11, -6, -1, 4, 9, 14, 19, \ldots\}$$

# Comparison of Z and $Z_n$ using graphs



# Operation in $Z_n$

- The three binary operations (addition, subtraction and multiplication) 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 $Z_n$ (contd…)*

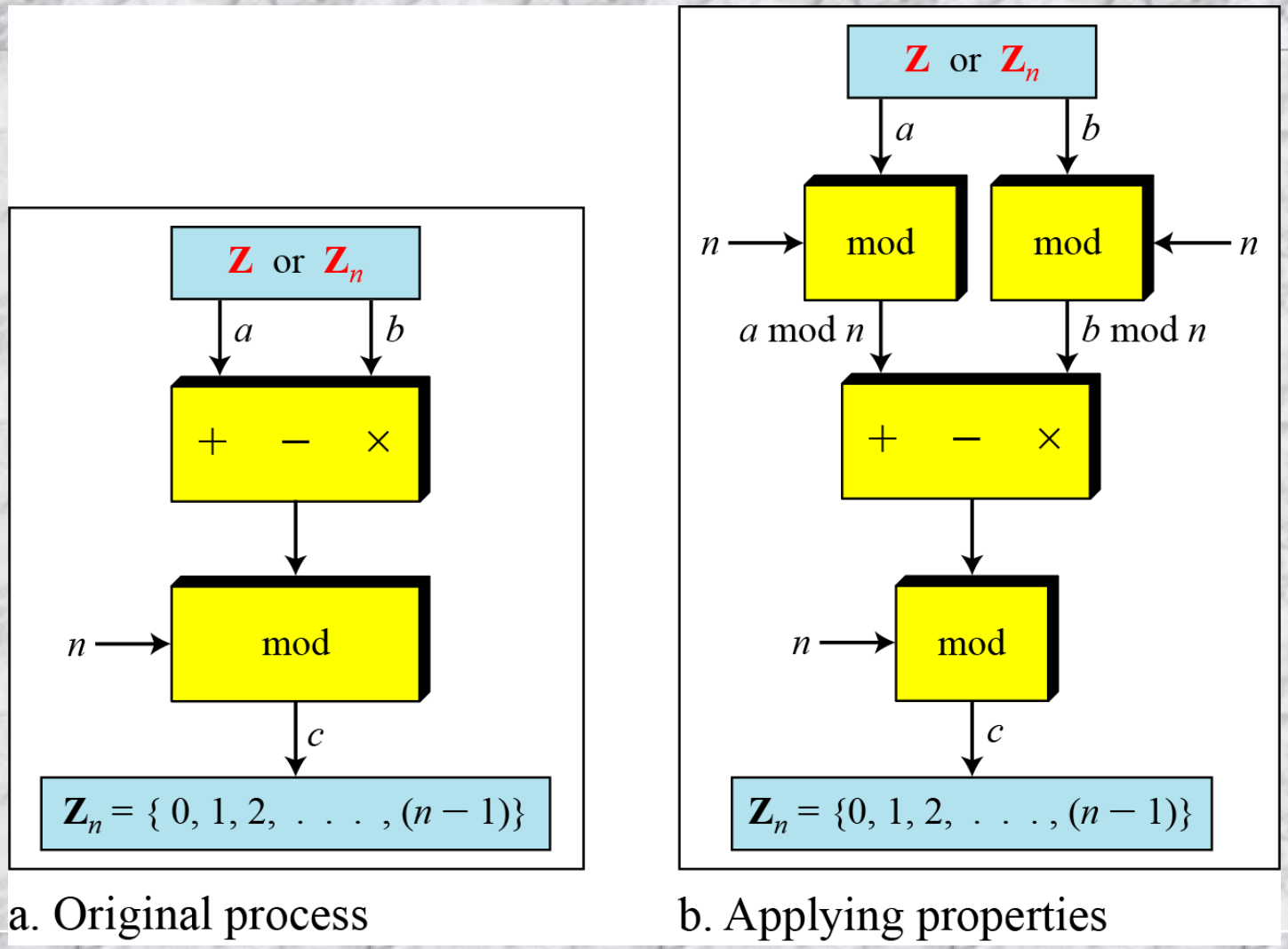
- Perform the following operations (the inputs come from $Z_n$):
- a. Add 7 to 14 in $Z_{15}$.
- b. Subtract 11 from 7 in $Z_{13}$.
- c. Multiply 11 by 7 in $Z_{20}$.

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

# Properties of modular arithmetic

| | |
|---|---|
| **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 modular arithmetic (contd…)



# Example

- The following shows the application of the above properties:
- $(1723345 + 2124945) \bmod 11 = (8 + 9) \bmod 11 = 6$
- $(1723345 - 2124945) \bmod 16 = (8 - 9) \bmod 11 = 10$
- $(1723345 \times 2124945) \bmod 16 = (8 \times 9) \bmod 11 = 6$

- $11^7 \bmod 13$ ?

# Example (contd…)

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

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

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

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

# Inverse

- 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

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

- 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 (contd…)

- Find all additive inverse pairs in $Z_{10}$
- The six pairs of additive inverses are (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

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

gcd(a, n) = 1

- 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 (contd…)

- ‘a’ has multiplicative inverse in $Z_n$ if and only if gcd(n,a)=1
  - ‘a’ and ‘n’ said to be relatively prime

# Multiplicative inverse (contd…)

- 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

# Multiplicative inverse (contd…)

- 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
- Find all multiplicative inverse pairs in $Z_{11}$
  - We have six pairs: (1, 1), (2, 6), (3, 4), (5, 9), (7, 8), and (10, 10)

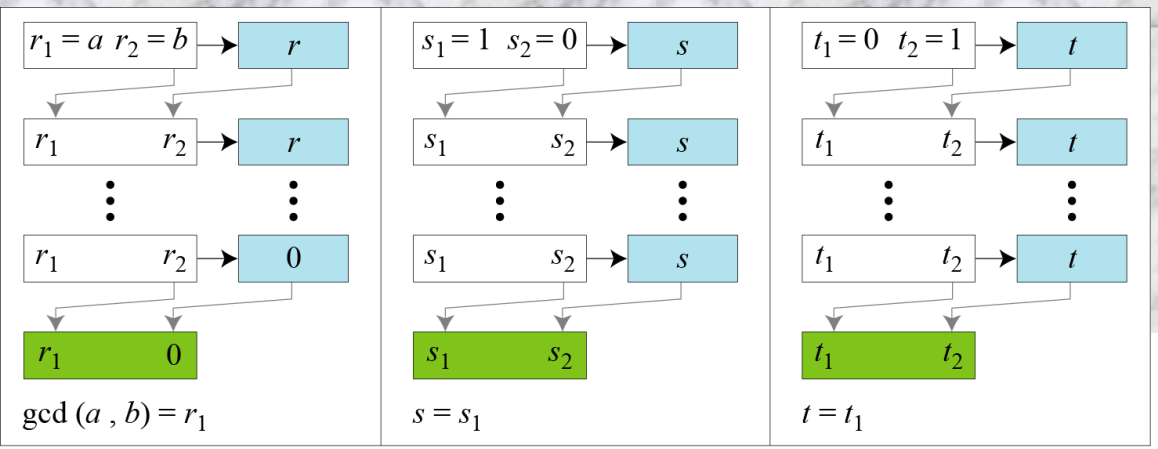
# Multiplicative inverse (contd…)

- The extended Euclidean algorithm finds the multiplicative inverses of b in $Z_n$ when n and b are given and gcd (n, b) = 1

  For number ‘b’ and ‘n’, we have $s \times n + b \times t = \gcd(n,b)$
  Incase of multiplicative inverse $\gcd(n,b)=1$, So,
  $s \times n + b \times t = 1$
  $(s \times n + b \times t) \bmod n = 1 \bmod n$
  $[(s \times n) \bmod n + (b \times t) \bmod n] = 1 \bmod n$
  $0 + (b \times t) \bmod n = 1 \bmod n$
  $(b \times t) \bmod n = 1$

- The multiplicative inverse of b is the value of t after being mapped to $Z_n$.

# Extended Euclidean algorithm for multiplicative inverse




a. Process

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

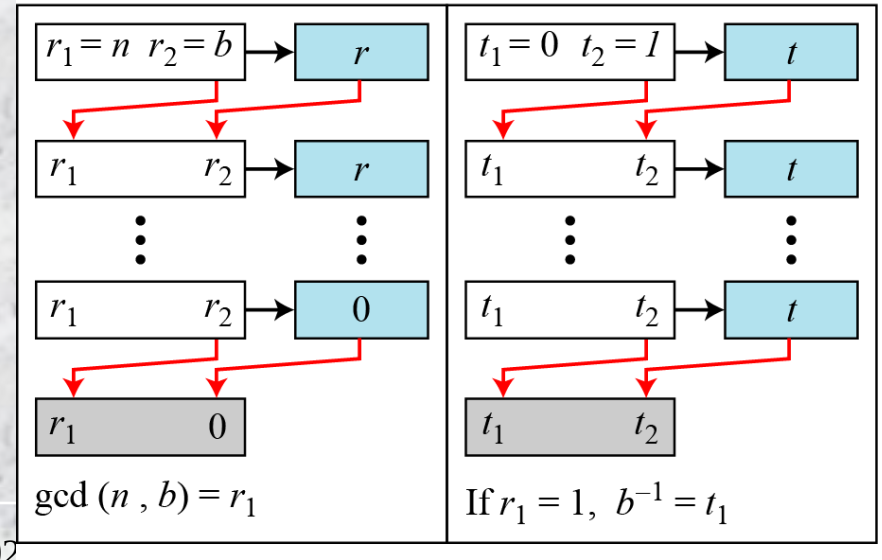
while $(r_2 > 0)$
{
$q \leftarrow r_1 / r_2;$

$r \leftarrow r_1 - q \times r_2;$
$r_1 \leftarrow r_2; \; r_2 \leftarrow r;$ (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 $(a, b) \leftarrow r_1; \; s \leftarrow s_1; \; t \leftarrow t_1$




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

# Extended Euclidean algorithm for multiplicative inverse (contd…)

- 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

# Extended Euclidean algorithm for multiplicative inverse (contd…)

- 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 | 9 |
| 1 | 8 | 7 | 1 | −4 | 9 | −13 |
| 7 | 7 | 1 | 0 | 9 | −13 | 100 |
| | 1 | 0 | | −13 | 100 | |

- The gcd (100, 23) =1; the inverse of 23 is −13 or 87.

# Extended Euclidean algorithm for multiplicative inverse (contd…)

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

# Different sets

- In cryptography very often inverse is used
  - In decryption process inverse of the encryption key is used
- If the operation is addition $Z_n$ can be used as set of keys
- When operation is multiplication, $Z_n$ cannot be used as set of keys since some does not have multiplicative inverse
  - We have to consider a subset $Z_n^*$ , which includes the integers that have inverse

# Different sets (contd…)

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

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

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

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

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

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

- Cryptography often uses two more sets: $Z_p$ and $Z_p^*$, the number p is a prime number
  - $Z_p = \{0,1,\ldots,p-1\}$ and $Z_p^* = \{1,2,\ldots,p-1\}$

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

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

# Matrices

- In cryptography we need to handle matrices. Although this topic belongs to a special branch of algebra called linear algebra, the following brief review of matrices is necessary preparation for the study of cryptography.

# Definition

Matrix **A**:

$$\begin{array}{c} \\ l \text{ rows} \end{array} \overbrace{\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & & \vdots \\ a_{l1} & a_{l2} & \cdots & a_{lm} \end{bmatrix}}^{m \text{ columns}}$$

$$\begin{bmatrix} 2 & 1 & 5 & 11 \end{bmatrix}$$

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

- Addition/subtraction

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

$$\mathbf{C = A + B}$$

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

$$\mathbf{D = A - B}$$

# Operations and relations (contd…)

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

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

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

Scalar multiplication

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

# *Determinant*

- The determinant of a square matrix A of size m × m denoted as det (A) is a scalar calculated recursively as shown below:

1. If $m = 1$, $\det(\mathbf{A}) = a_{11}$
2. If $m > 1$, $\det(\mathbf{A}) = \sum_{i=1\ldots m} (-1)^{i+j} \times a_{ij} \times \det(\mathbf{A}_{ij})$

Where $\mathbf{A}_{ij}$ is a matrix obtained from $\mathbf{A}$ by deleting the $i$th row and $j$th column.

The determinant is defined only for a square matrix.

# *Determinant (contd…)*

- How we can calculate the determinant of a 2 × 2 matrix based on the determinant of a 1 × 1 matrix

$$\det\begin{bmatrix} 5 & 2 \\ 3 & 4 \end{bmatrix} = (-1)^{1+1} \times 5 \times \det[\,4\,] + (-1)^{1+2} \times 2 \times \det[\,3\,] \longrightarrow 5 \times 4 - 2 \times 3 = 14$$

or

$$\det\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = a_{11} \times a_{22} - a_{12} \times a_{21}$$

$$\det\begin{bmatrix} 5 & 2 & 1 \\ 3 & 0 & -4 \\ 2 & 1 & 6 \end{bmatrix} = (-1)^{1+1} \times 5 \times \det\begin{bmatrix} 0 & -4 \\ 1 & 6 \end{bmatrix} + (-1)^{1+2} \times 2 \times \det\begin{bmatrix} 3 & -4 \\ 2 & 6 \end{bmatrix} + (-1)^{1+3} \times 1 \times \det\begin{bmatrix} 3 & 0 \\ 2 & 1 \end{bmatrix}$$

$$= (+1) \times 5 \times (+4) \quad + \quad (-1) \times 2 \times (24) \quad + \quad (+1) \times 1 \times (3) = -25$$

# Multiplicative inverse

- Multiplicative inverse of a square matrix A is another square matrix B such that $A \times B = B \times A = I$
- Multiplicative inverse exists only if $\det(A) \neq 0$

# *Residue Matrices*

- 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

$$\mathbf{A} = \begin{bmatrix} 3 & 5 & 7 & 2 \\ 1 & 4 & 7 & 2 \\ 6 & 3 & 9 & 17 \\ 13 & 5 & 4 & 16 \end{bmatrix} \qquad \mathbf{A}^{-1} = \begin{bmatrix} 15 & 21 & 0 & 15 \\ 23 & 9 & 0 & 22 \\ 15 & 16 & 18 & 3 \\ 24 & 7 & 15 & 3 \end{bmatrix}$$

$$\det(\mathbf{A}) = 21 \qquad n=26 \qquad \det(\mathbf{A}^{-1}) = 5$$

# Congruence matrices

- Two matrices are congruent modulo n, written as $A \equiv B \pmod{n}$
  - If the matrices are of same dimension
  - $a_{i,j} \equiv b_{i,j} \pmod{n}$ for all i and j

# LINEAR CONGRUENCE

- Cryptography often involves solving an equation or a set of equations of one or more variables with coefficient in $Z_n$. This section shows how to solve equations when the power of each variable is 1 (linear equation).
  - Single-Variable Linear Equations
  - Set of Linear Equations

# *Single-Variable Linear Equations*

- Equations of the form $ax \equiv b \pmod{n}$ might have no solution or a limited number of solutions.

Assume that the gcd $(a, n) = d$.

If $d \nmid b$, there is no solution.

If $d \mid b$, there are $d$ solutions.

# *Single-Variable Linear Equations (contd…)*

- Solve the equation $10x \equiv 2 \pmod{15}$
  - First we find the gcd (10 and 15) = 5. Since 5 does not divide 2, we have no solution

If $d|b$, there are $d$ solutions.

# *Single-Variable Linear Equations (contd…)*

- Reduce the equation by dividing both sides of the equation by *d*
  - $a_1 x \equiv b_1 \pmod{n_1}$
  - multiply both sides by $a_1^{-1} \bmod n_1$ )and find particular solution $x_0$
  - General solutions are: $x = x_0 + k(n/d)$, $0 \leq k \leq d-1$
- Solve the equation $14x \equiv 12 \pmod{18}$

$$14x \equiv 12 \pmod{18} \rightarrow \quad 7x \equiv 6 \pmod{9} \quad \rightarrow \quad x \equiv 6\,(7^{-1}) \pmod{9}$$

$$x_0 = (6 \times 7^{-1}) \bmod 9 = (6 \times 4) \pmod{9} = 6$$

$$x_1 = x_0 + 1 \times (18/2) = 15$$

# *Single-Variable Linear Equations (contd…)*

- Solve the equation $3x + 4 \equiv 6 \pmod{13}$.
  - First we change the equation to the form $ax \equiv b \pmod{n}$.
  - We add $-4$ (i.e. 9) to both sides
    - $3x \equiv 2 \pmod{13}$
    - Because gcd (3, 13) = 1, the equation has only one solution, which is $x_0 = (2 \times 3^{-1}) \bmod 13 = 18 \bmod 13 = 5$
  - We can see that the answer satisfies the original equation: $3 \times 5 + 4 \equiv 6 \pmod{13}$.

# *Set of linear equations*

- We can also solve a set of linear equations with the same modulus if the matrix formed from the coefficients of the variables is invertible

$$
\begin{aligned}
a_{11}x_1 &+ a_{12}x_2 &+ \ldots &+ a_{1n}x_n &\equiv b_1 \\
a_{21}x_1 &+ a_{22}x_2 &+ \ldots &+ a_{2n}x_n &\equiv b_2 \\
\vdots & \vdots & & \vdots & \vdots \\
a_{n1}x_1 &+ a_{n2}x_2 &+ \ldots &+ a_{nn}x_n &\equiv b_n
\end{aligned}
$$

a. Equations

$$
\begin{bmatrix}
a_{11} & a_{12} & \ldots & a_{1n} \\
a_{21} & a_{22} & \ldots & a_{2n} \\
\vdots & \vdots & & \vdots \\
a_{n1} & a_{n2} & \ldots & a_{nn}
\end{bmatrix}
\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}
\equiv
\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}
$$

b. Interpretation

$$
\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}
\equiv
\begin{bmatrix}
a_{11} & a_{12} & \ldots & a_{1n} \\
a_{21} & a_{22} & \ldots & a_{2n} \\
\vdots & \vdots & & \vdots \\
a_{n1} & a_{n2} & \ldots & a_{nn}
\end{bmatrix}^{-1}
\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}
$$

c. Solution

# *Set of linear equations (contd…)*

- Solve the set of following three equations:

$$3x + 5y + 7z \equiv 3 \pmod{16}$$
$$x + 4y + 13z \equiv 5 \pmod{16}$$
$$2x + 7y + 3z \equiv 4 \pmod{16}$$

- $A = \begin{matrix} 3 & 5 & 7 \\ 1 & 4 & 13 \\ 2 & 7 & 3 \end{matrix}$ $\det(A) \bmod 16 = 15$
  - gcd(15,16)=1
- $A^{-1} = \begin{matrix} 15 & 14 & 11 \\ 9 & 5 & 0 \\ 1 & 11 & 9 \end{matrix}$
- The result is $x \equiv 15 \pmod{16}$, $y \equiv 4 \pmod{16}$, and $z \equiv 14 \pmod{16}$