Department of Software Engineering
BAHRIA UNIVERSITY
Discovering Knowledge

BAHRIA UNIVERSITY
Discovering Knowledge

Mathematics of Cryptography

Data Encryption & Security (CEN-451)

Spring 2025 (BSE-8A&B)

Mathematics of Cryptography

- Cryptography is based on some specific areas of mathematics, including number theory, linear algebra and matrices which are pervasive in cryptographic algorithms.
- **Outline of this lecture:**

I. Integer arithmetic.

II. Modular arithmetic.

III. Congruence equations.

IV. Matrices.

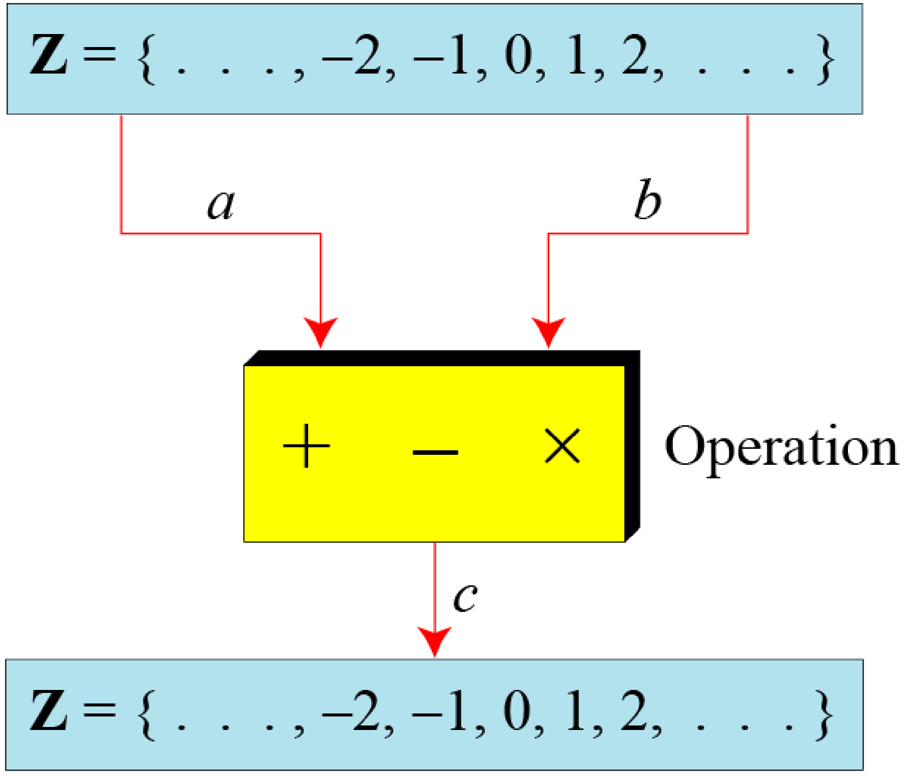
Integer Arithmetic

Set of Integers

- The set of integers, denoted by Z, contains all integer numbers from negative infinity to positive infinity.

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

- In cryptography, we are interested in three binary operations applied to the set of integers.



Set of Integers (Cont.)

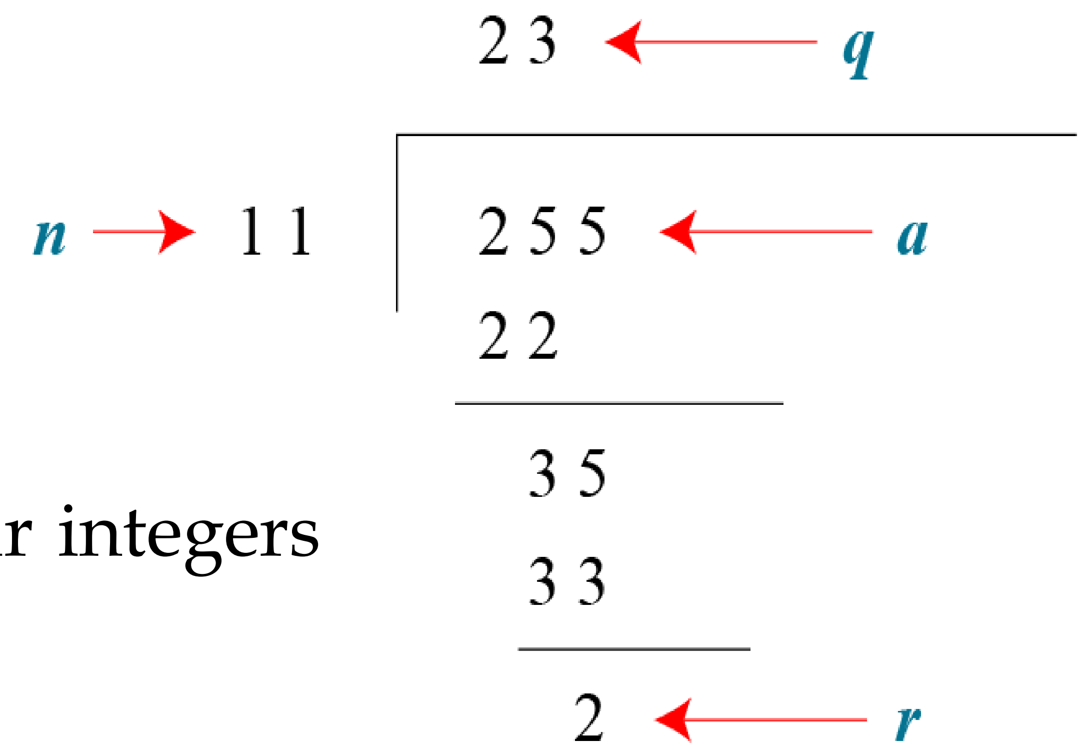
- The following example shows the results of the three binary operations on two integers.

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:	$5 \times 9 = 45$	$(-5) \times 9 = -45$	$5 \times (-9) = -45$	$(-5) \times (-9) = 45$

Set of Integers (Cont.)

- In integer arithmetic, if we divide **a** by **n**, we can get **q** and **r**, where:
  - **a** is dividend
  - **n** is divisor
  - **q** is quotient
  - **r** is remainder
- The relationship between these four integers can be shown as:

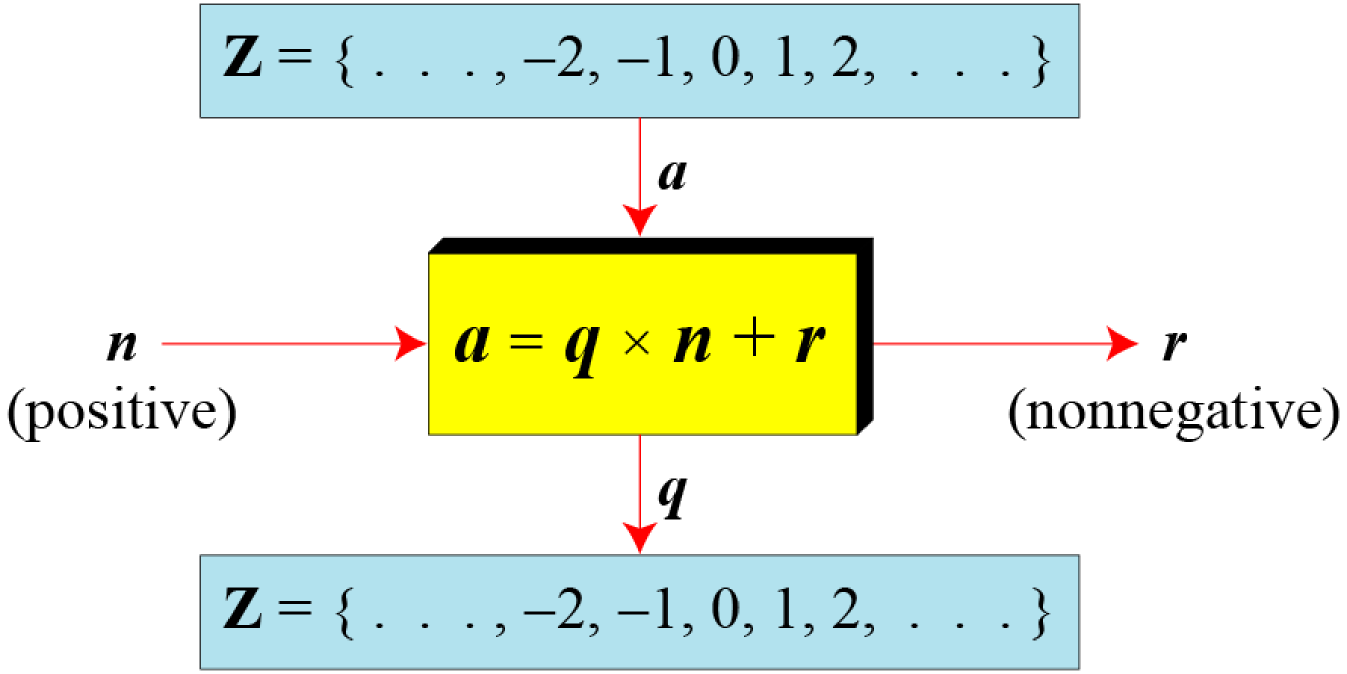
$$a = q \times n + r$$



Set of Integers (Cont.)

- In cryptography we often **impose two restrictions**:

n > 0 and r ≥ 0



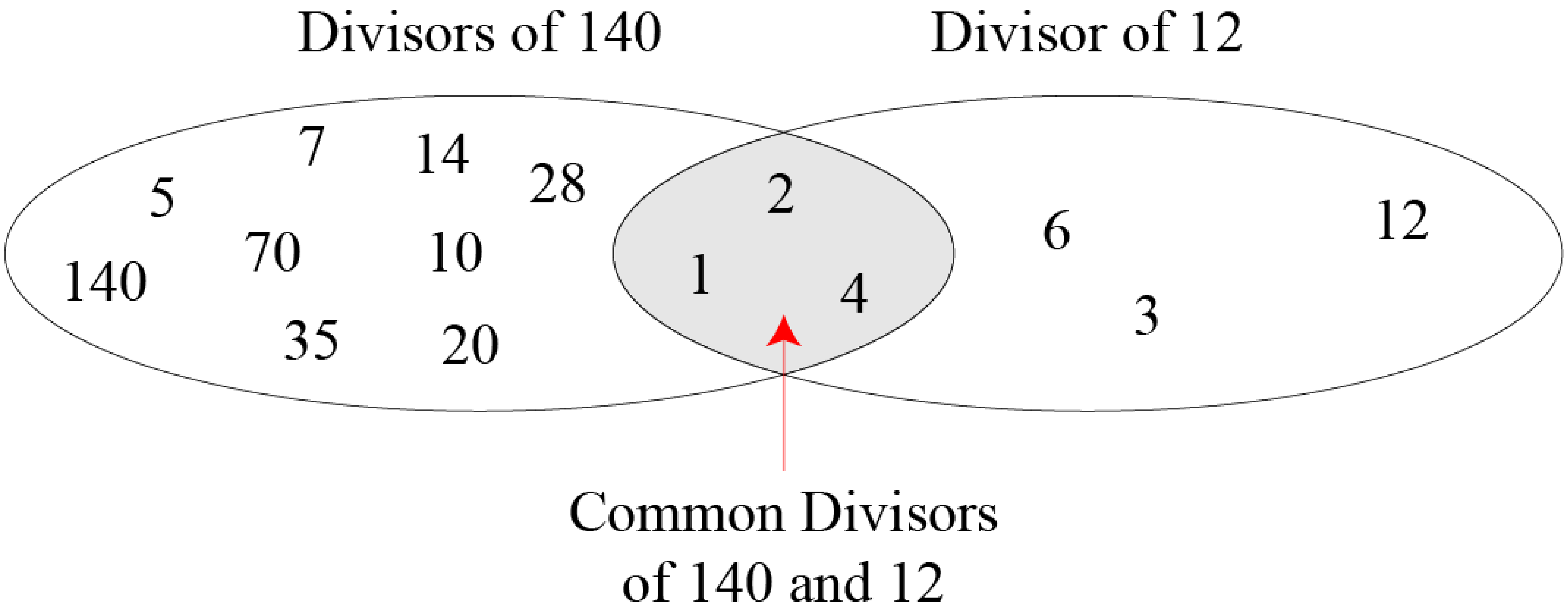
Set of Integers (Cont.)

- When we use a computer or a calculator, **r** and **q** are negative when **a** is negative.
- **Q)** How can we apply the restriction that **r** needs to be positive?
- **A)** We decrement the value of **q** by 1 and we add the value of **n** to **r** to make **r** positive.

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

Divisibility: Common Divisor

- Common divisors of two integers:

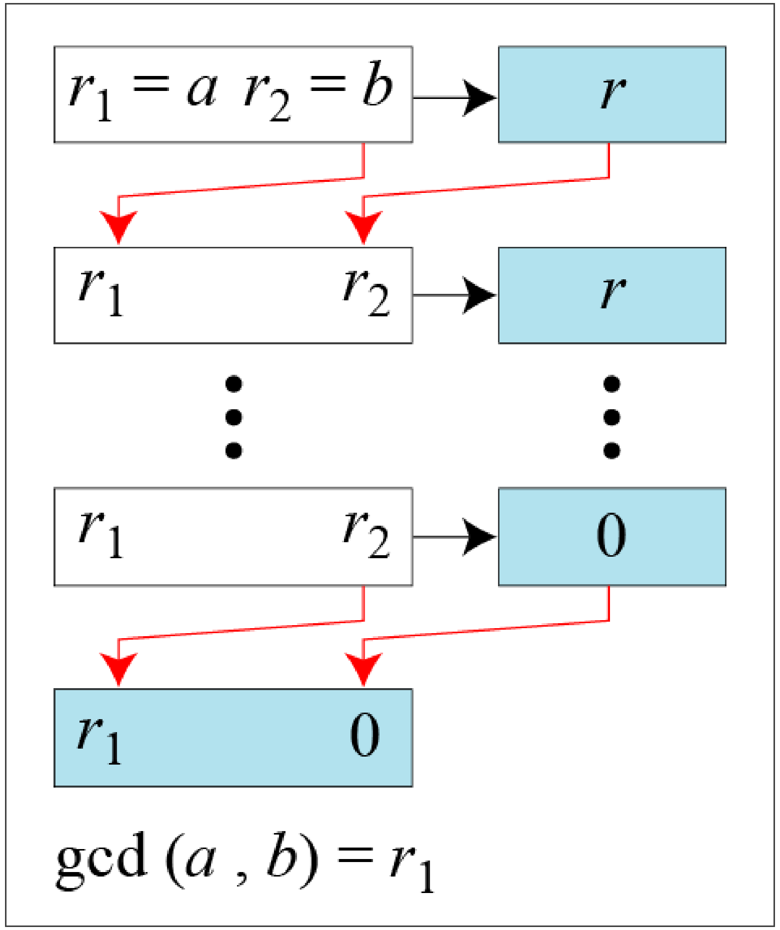


Divisibility: Common Divisor (Cont.)

- **Greatest Common Divisor (GCD)** of two positive integers is the largest integer that can divide both integers.
- The **Euclidean algorithm** can find the **GCD** on basis of the following two facts:
  - **gcd (a, 0) = a**
  - **gcd (a, b) = gcd (b, r)**, where **r** is the remainder of dividing **a** by **b**.
- **Example:**

$$\gcd(36,10) = \gcd(10,6) = \gcd(6,4) = \gcd(4,2) = \gcd(2,0) = 2$$

Divisibility: Common Divisor (Cont.)



Divisibility: Common Divisor (Cont.)

Example 01: 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	

Hence, we have gcd (2740, 1760) = 20.

Example 01: Find the greatest common divisor of 2740 and 1760.

q	r1	r2	r

Divisibility: Common Divisor (Cont.)

- **Example 02:** 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	

- Hence, we have gcd (25, 60) = 5.

Example 02: Find the greatest common divisor of 25 and 60.

q	r1	r2	r

Divisibility: Common Divisor (Cont.)

Relatively Prime:

- When gcd (a, b) = 1, we say that **a** and **b** are **relatively prime**.
- Two numbers are **relatively prime** if they have no common factors other than 1.
- **For example,** 7 and 20 are relatively prime.

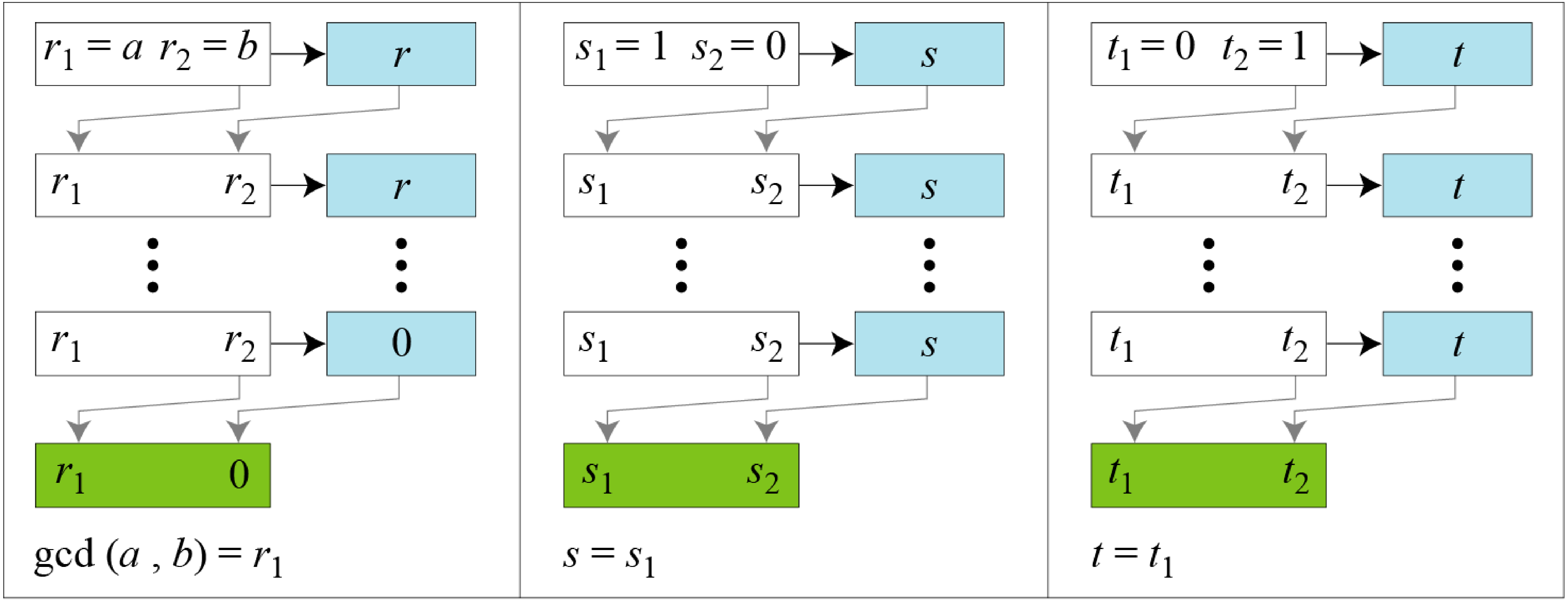
Divisibility: Extended Euclidean Algorithm

- 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**.

Divisibility: Extended Euclidean Algorithm (Cont.)



Divisibility: Extended Euclidean Algorithm (Cont.)

- **Example 01:** Given **a** = 161 and **b** = 28, find **gcd(a, b)** and the values of **s** and **t**.
- $\mathbf{r} = \boldsymbol{r_1} - (\boldsymbol{q} \times \boldsymbol{r_2})$ $\mathbf{s} = \boldsymbol{s_1} - (\boldsymbol{q} \times \boldsymbol{s_2})$ $\mathbf{t} = \boldsymbol{t_1} - (\boldsymbol{q} \times \boldsymbol{t_2})$

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.

Example 01: Given **a** = 161 and **b** = 28, find **gcd(a, b)** and the values of **s** and **t**.

$\mathbf{r} = r_1 - (q \times r_2)$ $\mathbf{s} = s_1 - (q \times s_2)$ $\mathbf{t} = t_1 - (q \times t_2)$

q	r1	r2	r	s1	s2	s	t1	t2	t

Divisibility: Extended Euclidean Algorithm (Cont.)

- **Example 02:** Given **a** = 17 and **b** = 0, find **gcd(a, b)** and 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.

Divisibility: Extended Euclidean Algorithm (Cont.)

- **Example 03:** 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.

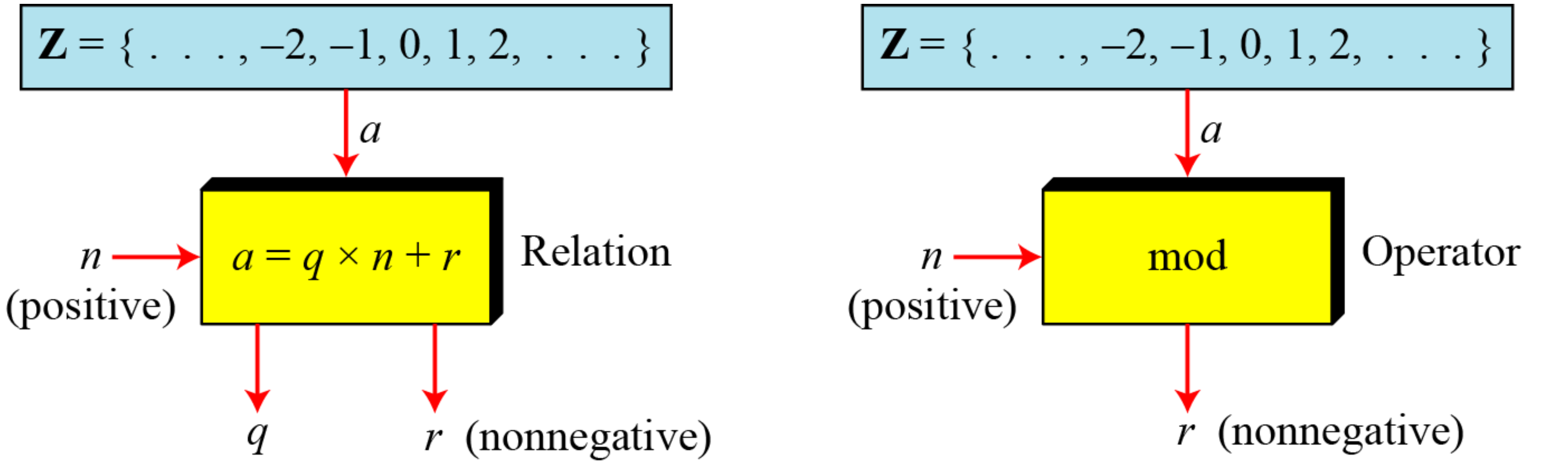
Modular Arithmetic

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, i.e. **r**. Hence, we don't care about **q**.
- This implies that we can change the above relation into a binary operator with two inputs **a** and **n**, and one output **r**.

Modulo Operator

- The modulo operator is shown as mod. The second input **n** is called the modulus. The output **r** is called the residue.
- The mod takes an integer **a** and positive modulus **n** as inputs. The operator creates a non-negative residue **r** → **a mod n = r**



Modulo Operator (Cont.)

- **Example 01:** Find the result of the following operations

a. 27 mod 5
b. 36 mod 12
c. −18 mod 14
d. −7 mod 10

- **Solution:** we divide **a** by **n** and find **q** and **r**. We then discard **q** and keep **r**.

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 to −4, **r = 10**.
d. Dividing −7 by 10 results in r = −7. After adding the modulus to −7, **r = 3**.

Set of Residues

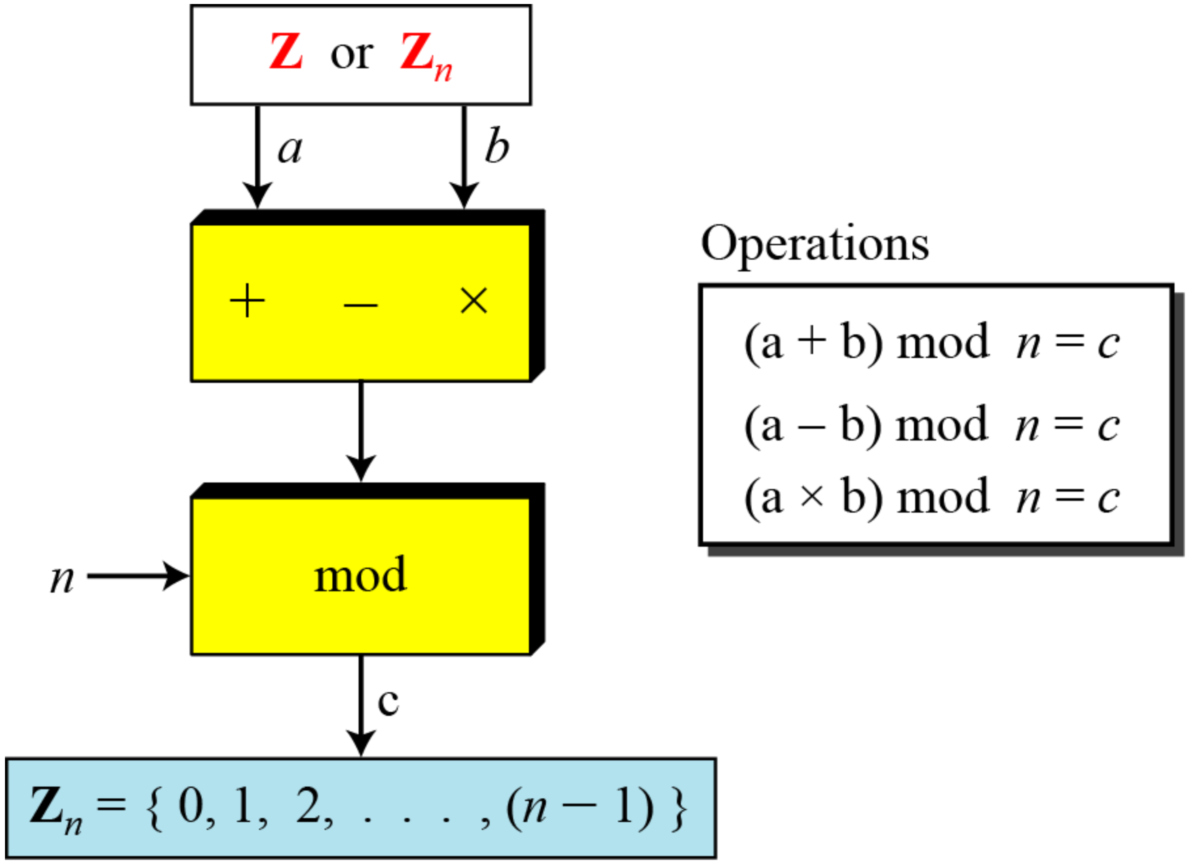
- The result of the modulo operation with modulus **n** is always an integer between **0 and n-1**.
- The modulo operation creates a set, which in modular arithmetic is referred to as the set of ***least residues*** modulo **n**, or $\mathbf{Z_n}$.

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

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

Operation in Z_n

- The three binary operations ***(addition, subtraction and multiplication)*** that we discussed for **Z** can also be defined for $\mathbf{Z_n}$.
- Result may need to be mapped to $\mathbf{Z_n}$ using the mod operator.



Operation in Z_n(Cont.)

- **Example 01:** 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}.
- **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(Cont.)

- **Example 02:** Perform the following operations ***(the inputs come from 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}.
- **Solution:** Home Work!

Properties of Mod Operator

- First Property:

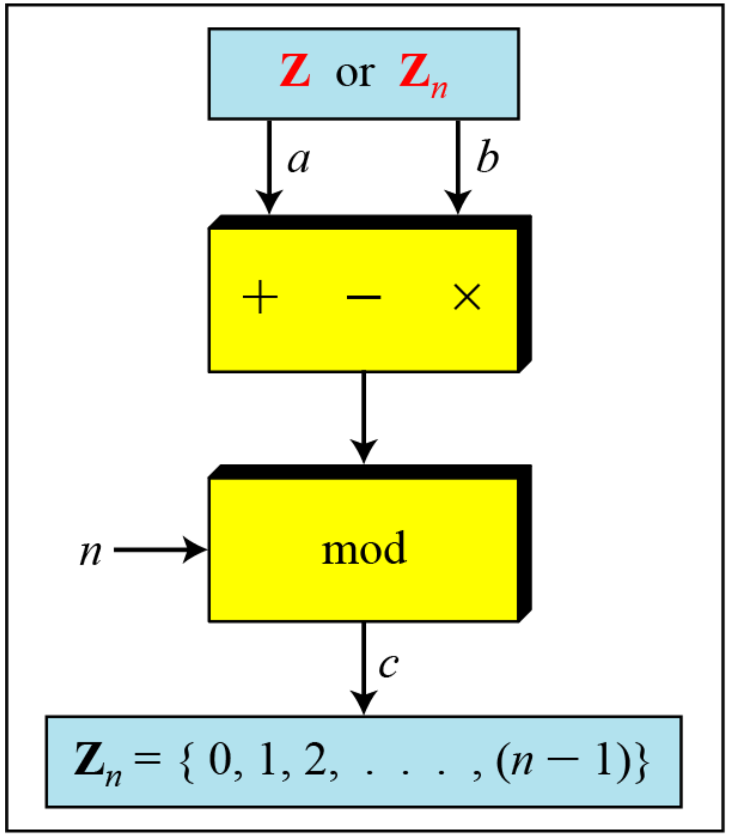
$$(a + b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$$

- Second Property:

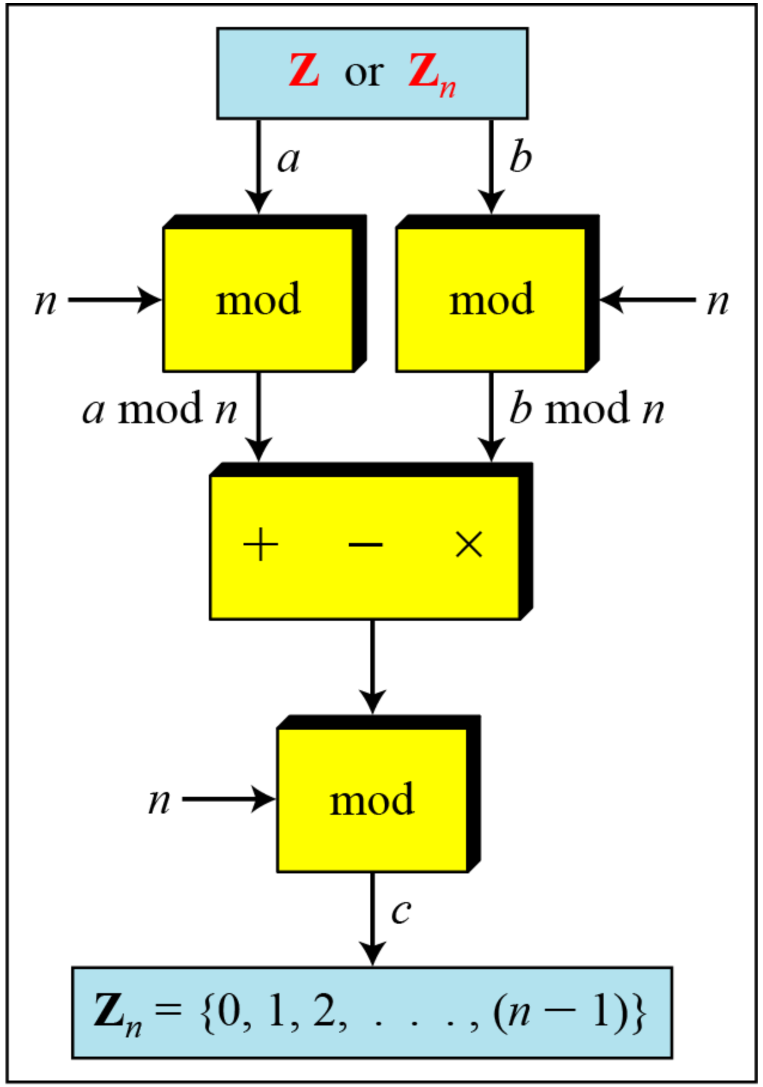
$$(a - b) \bmod n = [(a \bmod n) - (b \bmod n)] \bmod n$$

- Third Property:

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



a. Original process



b. Applying properties

Properties of Mod Operator (Cont.)

Benefits of Mod Properties:

- In cryptography, we deal with very large integers.
- If we multiple a very large integers by another, we may have an integer that is too large to be stored in the computer.
- Applying the Mod properties make the first two operands smaller before the multiplication is applied.

Properties of Mod Operator (Cont.)

- **Example 01:** the following shows an application of mod properties:

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

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

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

Properties of Mod Operator (Cont.)

- **Example 02:** in arithmetic, we often need to find the remainder of powers of 10 when divided by an integer.

mod x

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

Congruence

Congruence

- In cryptography, we often use the concept of **congruence** instead of equality.
- The congruence operator maps a member from **Z** to a member of $\mathbf{Z_n}$, where equality operator is **one-to-one** while congruence is **many-to-one**.
- To show that two integers are congruent, we use the congruence operator **(≡)**.

Congruence (Cont.)

- **Example 01:**

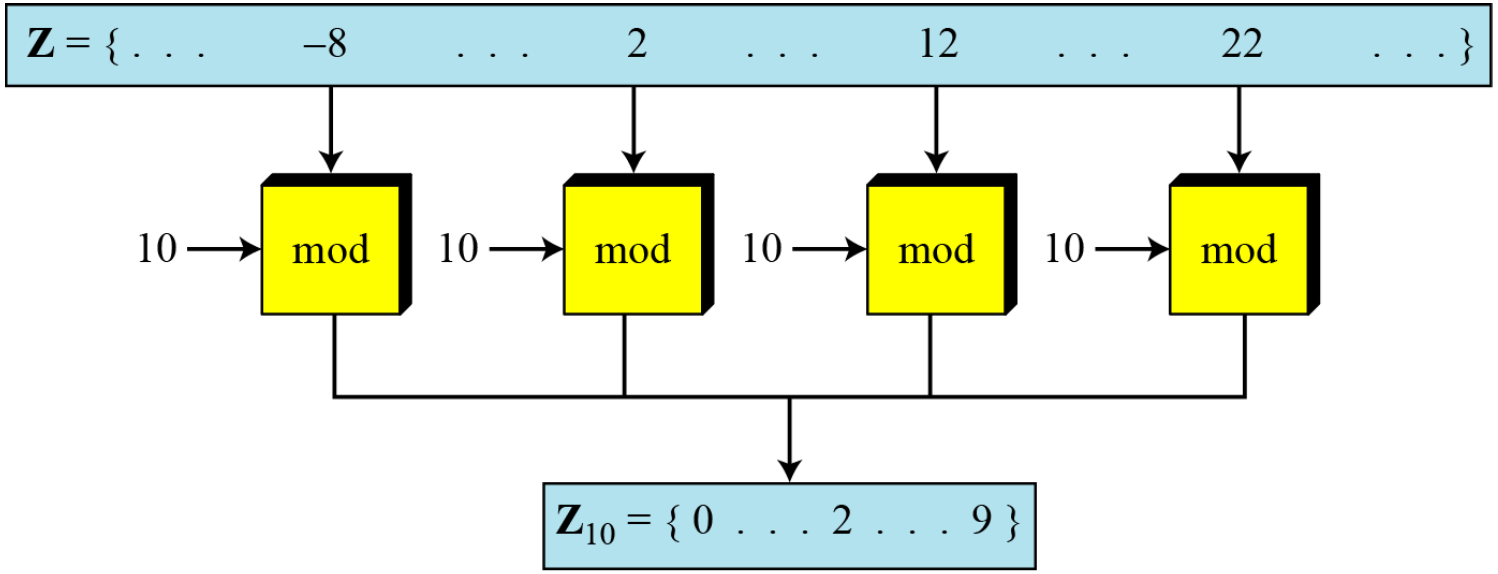
$$2 \equiv 12 \pmod{10} \qquad 13 \equiv 23 \pmod{10}$$
$$3 \equiv 8 \pmod{5} \qquad 8 \equiv 13 \pmod{5}$$

- **Example 02:**

$$34 \equiv 24 \pmod{10} \qquad -8 \equiv 12 \pmod{10}$$
$$23 \equiv 33 \pmod{5} \qquad -8 \equiv 2 \pmod{5}$$

Congruence (Cont.)

- The phrase **(mod 10)** in **2 ≡ 12 (mod 10)**, means that the destination set is $\mathbf{Z}_{10}$.



$$-8 \equiv 2 \equiv 12 \equiv 22 \pmod{10}$$

Congruence Relationship

Inverses

- In cryptography, we often work with inverses.
- If sender uses an integer as encryption key, the receiver uses the ***inverse*** of that integer as decryption key.

Multiplicative Inverse

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

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

- **E.g.** in modulus 10, the multiplicative inverse of 3 is 7,

i.e. **(3 ×7) mod 10 = 1**

Multiplicative Inverse (Cont.)

- It can be proved that **a** has a multiplicative inverse in Z_n if and only if **gcd(n, a) = 1**, i.e. **a** and **n** are relatively prime.
- The integer **a** in Z_n has a multiplicative inverse if and only if **gcd(n, a) ≡ 1 (mod n)**.
- **Example 01:** find the multiplicative inverse of 8 in Z_{10}.
- **Solution:**
  - There is no multiplicative inverse because **gcd (10, 8) = 2 ≠ 1**.

Multiplicative Inverse (Cont.)

- **Example 02:** find all multiplicative inverses in $\mathbf{Z_{10}}$.
- **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.
  - We can see that:

$$(1 \times 1) \bmod 10 \equiv 1$$
$$(3 \times 7) \bmod 10 \equiv 1$$
$$(9 \times 9) \bmod 10 \equiv 1$$

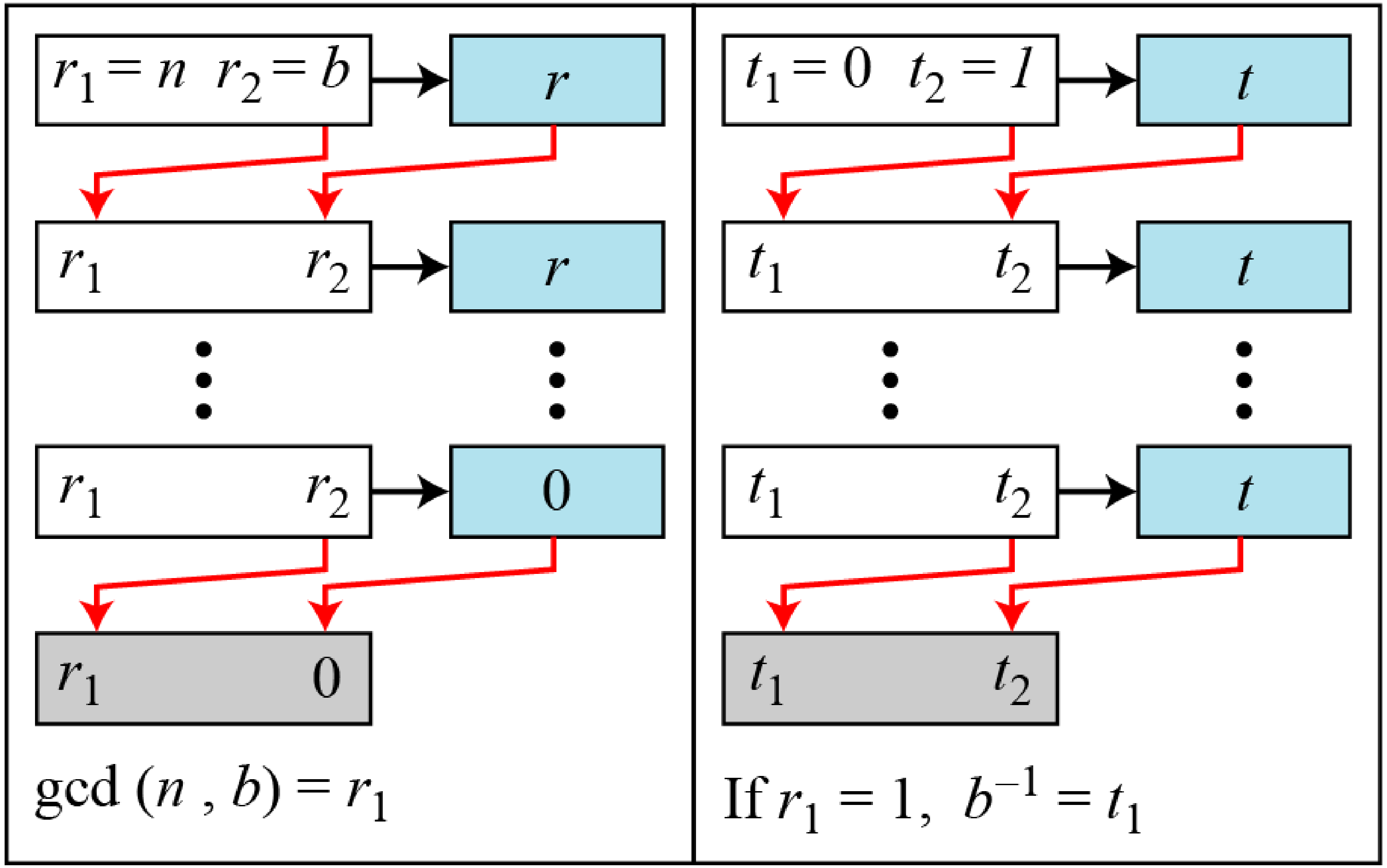
Multiplicative Inverse (Cont.)

- **Example 03:** find all multiplicative inverse pairs in $\mathbf{Z}_{11}$.
- **Solution:**
  - We have the pairs: (1, 1), (2, 6), (3, 4), (5, 9), (7, 8), and (10, 10).
  - In moving from $\mathbf{Z}_{10}$ to $\mathbf{Z}_{11}$ the number of pairs doubles.
  - In $\mathbf{Z}_{11}$, the **gcd(11, a)** is 1 for all values of a except 0. Hence, all integers 1 to 10 have multiplicative inverses.

Extended Euclidean Algorithm for Multiplicative Inverse

- The extended Euclidean algorithm can find the multiplicative inverses of **b** in $\mathbf{Z_n}$ when **gcd (n, b) = 1**.
- The multiplicative inverse of **b** is the value of **t** after being mapped to $\mathbf{Z_n}$.

Extended Euclidean Algorithm for Multiplicative Inverse (Cont.)



Extended Euclidean Algorithm for Multiplicative Inverse (Cont.)

- **Example 01:** 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.

Example 01: Find the multiplicative inverse of 11 in Z_{26}.

$$\mathbf{r} = r_1 - (q \times r_2) \qquad \mathbf{t} = t_1 - (q \times t_2)$$

q	r1	r2	r	t1	t2	t
	26	11		0	1	

Extended Euclidean Algorithm for Multiplicative Inverse (Cont.)

- **Example 02:** 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.

Extended Euclidean Algorithm for Multiplicative Inverse (Cont.)

- **Example 03:** 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) is 2; the inverse does not exist.

Matrices (Do it Yourself!)

Matrices

- In cryptography we need to handle matrices. The following brief review of matrices is necessary preparation for the study of cryptography.

$$\text{Matrix } \mathbf{A}: \begin{array}{cc} & m \text{ columns} \\ l \text{ rows} & \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & & \vdots \\ a_{l1} & a_{l2} & \cdots & a_{lm} \end{bmatrix} \end{array}$$

Matrices (Cont.)

- Examples of matrices:

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

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

Matrices (Cont.)

- Example of addition and subtraction:

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

C = A + B

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

D = A − B

Matrices (Cont.)

- Example for product of a row matrix (1 × 3) by a column matrix (3 × 1). The result is a matrix of size 1 × 1.

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

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

Matrices (Cont.)

- Example for product of a 2 × 3 matrix by a 3 × 4 matrix. The result is a 2 × 4 matrix.

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

Matrices (Cont.)

- Example of scalar multiplication:

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

Determinant

- The determinant of a square matrix **A** of size **m × m** denoted as **det(A)** is a scalar calculated recursively.
- The determinant is defined only for a square matrix.
- Example for 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

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

Determinant (Cont.)

- Example for the calculation of the determinant of a 3 × 3 matrix:

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

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

Matrices Inverse

- Multiplicative inverses are **only** defined for **square matrices**.
- Cryptography uses residue matrices, i.e. matrices where all elements are in $\mathbf{Z_n}$.
- A residue matrix has a multiplicative inverse if the determinant of the matrix has a multiplicative inverse in $\mathbf{Z_n}$.
- In other words, a residue matrix has a multiplicative inverse if **gcd (det(A), n) = 1**.

Matrices Inverse (Cont.)

- We focus our concern in matrix arithmetic modulo 26.
- The inverse of a matrix does not always exist, but when it does, it satisfies the equation $A^{-1}A = I$.
- **Example:** a residue matrix **A** in Z_{26}.

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

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

Thank You!