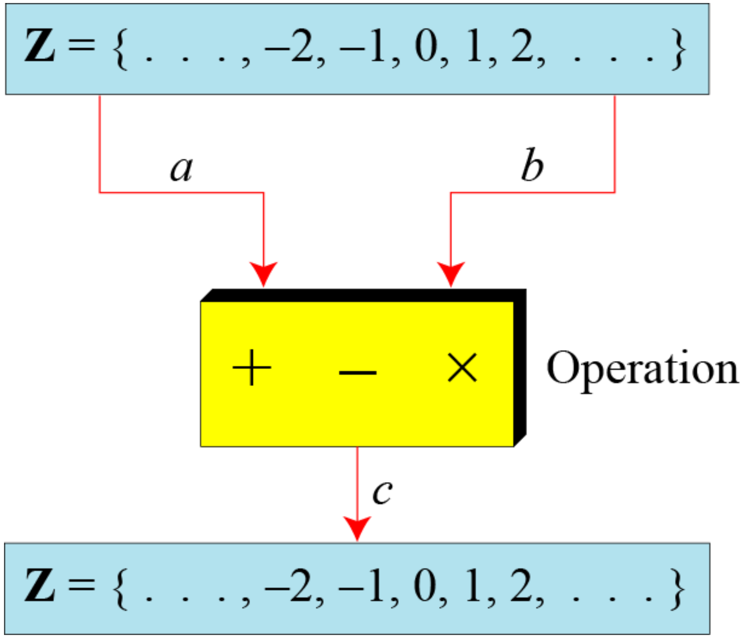
# Trường $Z_m$ (modulo)

# Tập số nguyên

- Tập số nguyên, ký hiệu là **Z,** chứa tất cả các số nguyên (không có phân số) từ âm vô cùng đến dương vô cùng.
- Trong mã hóa, có ba phép toán hai ngôi trong tập số nguyên được quan tâm. Một phép toán hai ngôi sử dụng hai giá trị đầu vào và cho kết quả là một giá trị đầu ra.

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



# Phép toán hai ngôi

- Mỗi giá trị đầu vào của phép toán hai ngôi trong tập số nguyên có thể là số dương hoặc số âm. Một ví dụ cụ thể như sau:

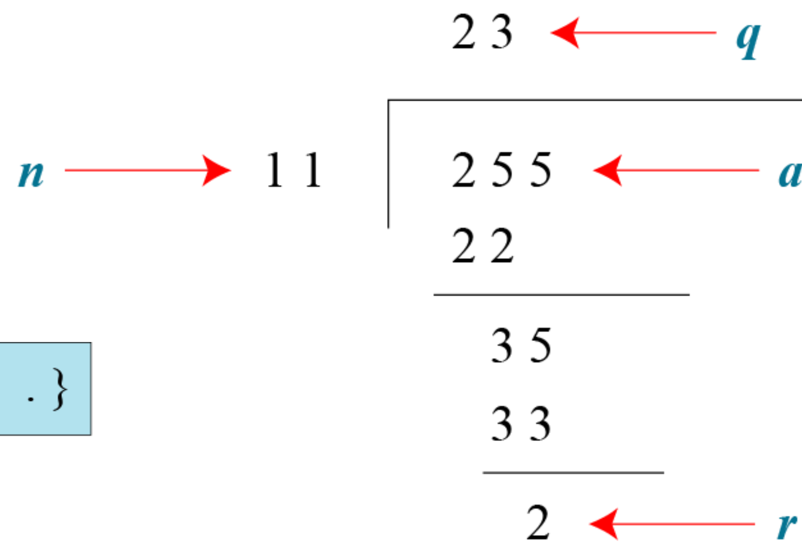
| | | | | |
|---|---|---|---|---|
| Add: | $5 + 9 = 14$ | $(-5) + 9 = 4$ | $5 + (-9) = -4$ | $(-5) + (-9) = -14$ |
| Subtract: | $5 - 9 = -4$ | $(-5) - 9 = -14$ | $5 - (-9) = 14$ | $(-5) - (-9) = +4$ |
| Multiply: | $5 \times 9 = 45$ | $(-5) \times 9 = -45$ | $5 \times (-9) = -45$ | $(-5) \times (-9)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

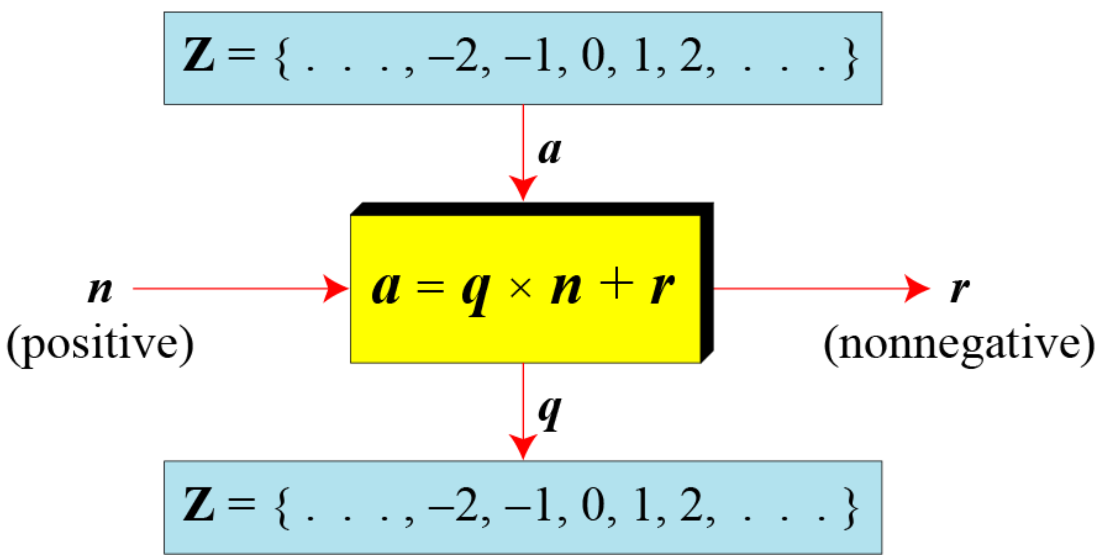
- Trong phép toán số nguyên, nếu chia *a* cho *n* thì cho ra được giá trị *q* và *r*.

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

# Phép chia

- Giả sử rằng *a* = 255 và *n* = 11, khi đó thương số *q*= 23 và phần dư *r* = 2.

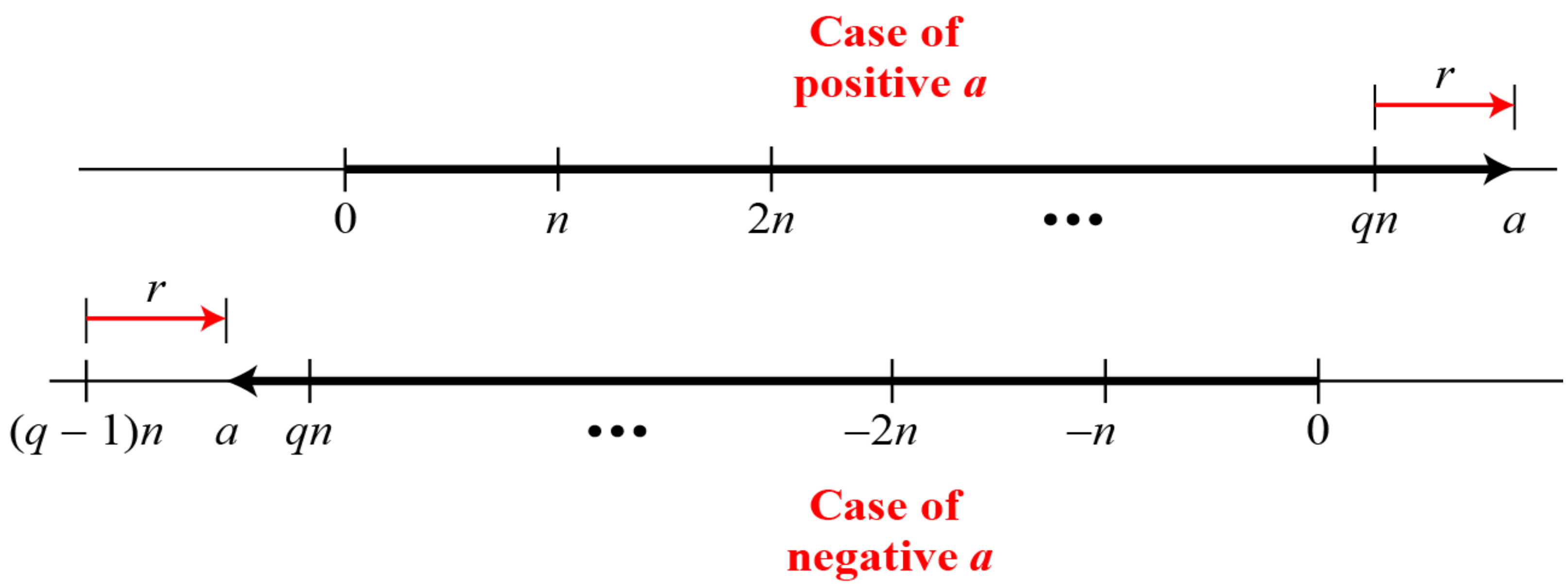


# Phép chia

- Nếu *a* là số âm thì thương số *q* và phần dư *r* là số âm. Để có phần dư *r* là số dương thì thương số *q* giảm 1, sau đó cộng thêm phần dư cho *n*.

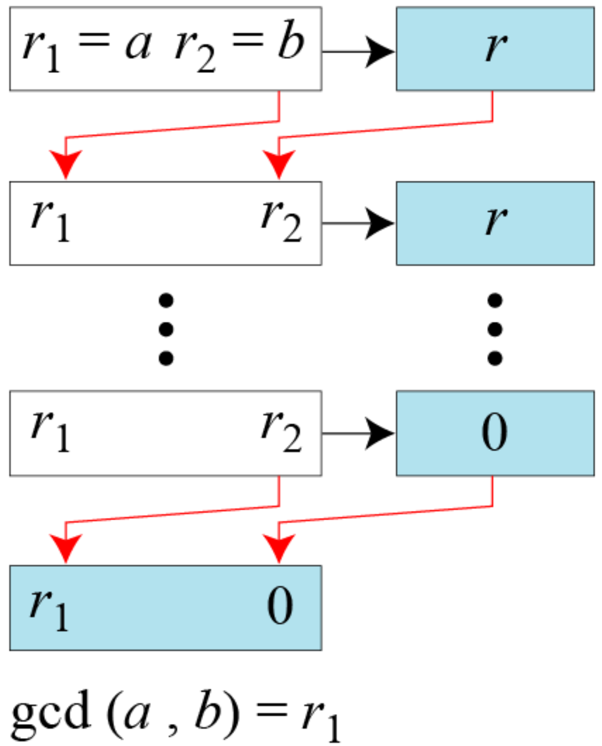
$$-255 = (-\mathbf{23} \times 11) + (\mathbf{-2}) \quad \leftrightarrow \quad -255 = (-\mathbf{24} \times 11) + \mathbf{9}$$



# Ước số chung lớn nhất (greatest common divisor)

- Ước số chung lớn nhất (*greatest common divisor*) của hai số nguyên dương *a* và *b* là một số nguyên lớn nhất là ước của cả hai số *a*, *b*, ký hiệu *gcd*(*a*, *b*).
- Thuật toán Euclid
  - *gcd(a, 0) = a*
  - *gcd(a, b) = gcd(b, r), với r là phần dư của phép chia a cho b*

# Thuật toán EUCLID




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

- Nếu $gcd(a, b) = 1$, thì *a* và *b* được gọi là ***hai số nguyên tố cùng nhau***.

# Thuật toán EUCLID

- Tìm ước số chung lớn nhất của 2740 và 1760

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

while ($r_2 > 0$)

{

$q \leftarrow r_1 / r_2;$

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

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

}

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

| $q$ | $r_1$ | $r_2$ | $r$ |
|---|---|---|---|
| 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 | |

- Kết quả *gcd*(2740, 1760) = 20

# Thuật toán EUCLID

- Tìm ước số chung lớn nhất của 25 và 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 | |

- Kết quả gcd(25, 60) = 5

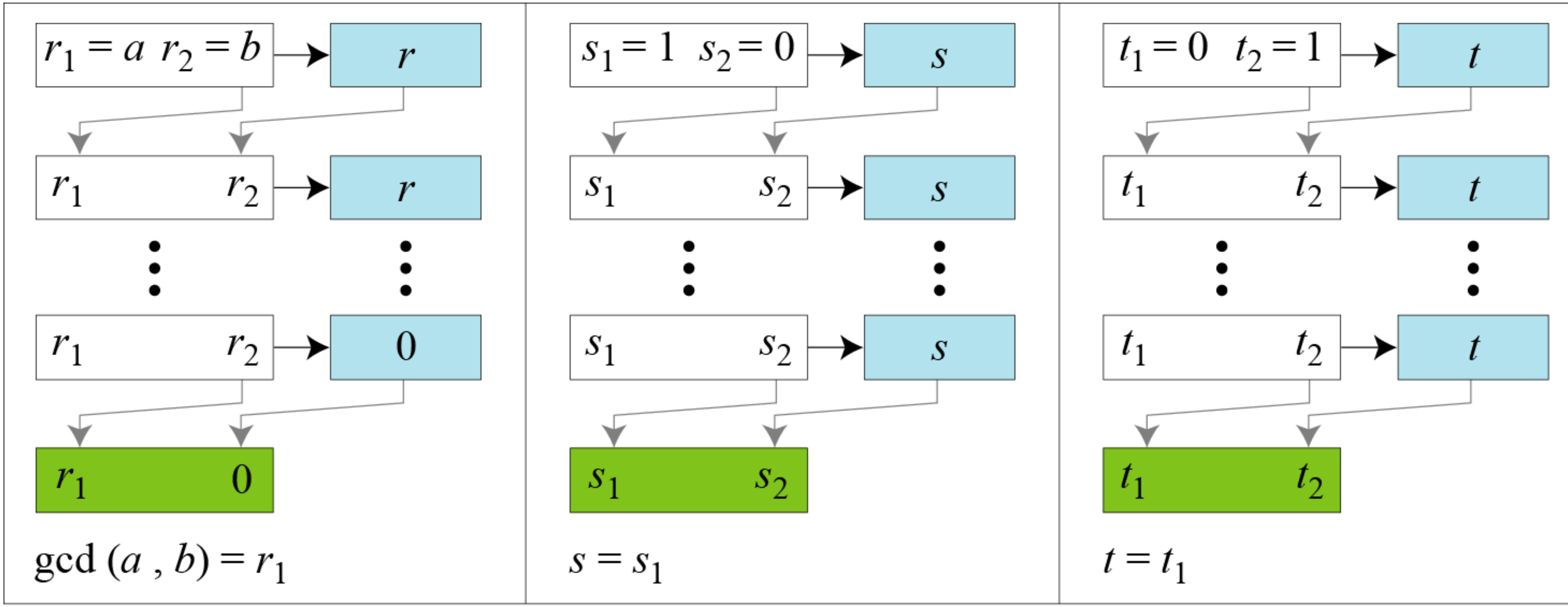
# Thuật toán EUCLID mở rộng

- Cho hai số nguyên a và b, hãy tìm hai số nguyên s và t sao cho

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

- Thuật toán Euclid mở rộng có thể tính được giá trị *gcd*(*a*, *b*) đồng thời tính được giá trị của hai số nguyên *s* và *t*.

# Thuật toán EUCLID mở rộng



# Thuật toán EUCLID mở rộng

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

while ($r_2 > 0$)

{

$q \leftarrow r_1 / r_2;$

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

}

$\gcd(a, b) \leftarrow r_1;$ $s \leftarrow s_1;$ $t \leftarrow t_1$

# Thuật toán EUCLID mở rộng

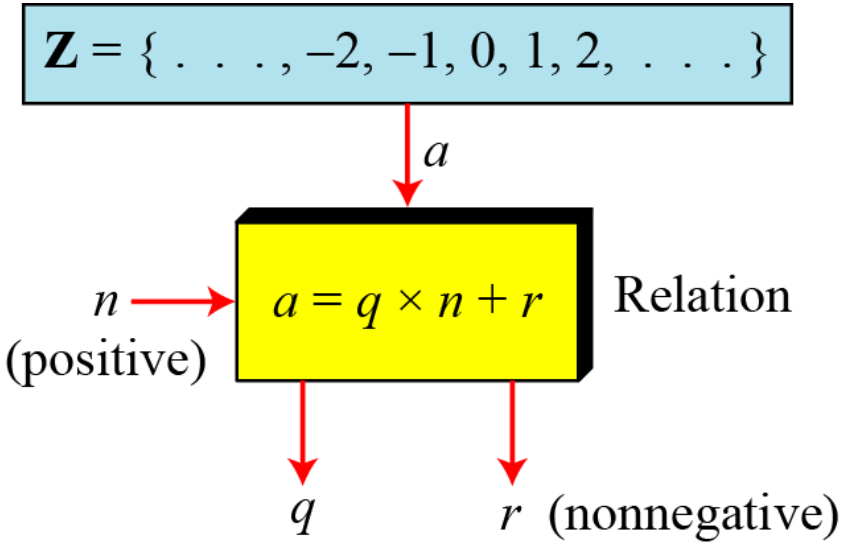
➢ Cho *a* = 161 và *b* = 28, hãy tìm gcd(*a*, *b*) và giá trị của *s* và *t.*

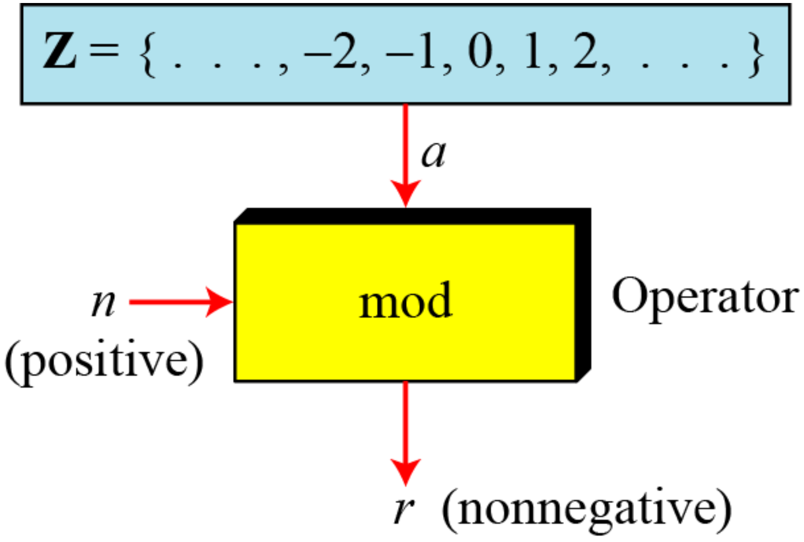
| $q$ | $r_1$ | $r_2$ | $r$ | $s_1$ | $s_2$ | $s$ | $t_1$ | $t_2$ | $t$ |
|---|---|---|---|---|---|---|---|---|---|
| 5 | 161 | 28 | 21 | 1 | 0 | 1 | 0 | 1 | −5 |
| 1 | 28 | 21 | 7 | 0 | 1 | −1 | 1 | −5 | 6 |
| 3 | 21 | 7 | 0 | 1 | −1 | 4 | −5 | 6 | −23 |
| | **7** | 0 | | **−1** | 4 | | **6** | −23 | |

➢ Kết quả *gcd*(161, 28) = 7, *s* = *-1* và *t* = *6.*

# Phép toán Modulo

- Phép toán modulo, được gọi là mod, là phép chia lấy phần dư.



# Phép toán Modulo

- Tìm kết quả của phép toán sau:

a. 27 mod 5 b. 36 mod 12

c. −18 mod 14 d. −7 mod 10

**Kết quả**:

a. Chia 27 cho 5, phần dư là r = 2

b. Chia 36 cho 102, phần dư là r = 0

c. Chia -18 cho 14, phần dư là r = -4, cộng thêm cho giá trị n=14, kết quả là r = 10

d. Chia -7 cho 10, phần dư là -7, cộng thêm cho giá trị n=10, kết quả là r = 3

# Tập hợp các phần dư

- Phép toán modulo cho *n* tạo ra một tập phần dư tối thiểu của *n*, được gọi là $Z_n$

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

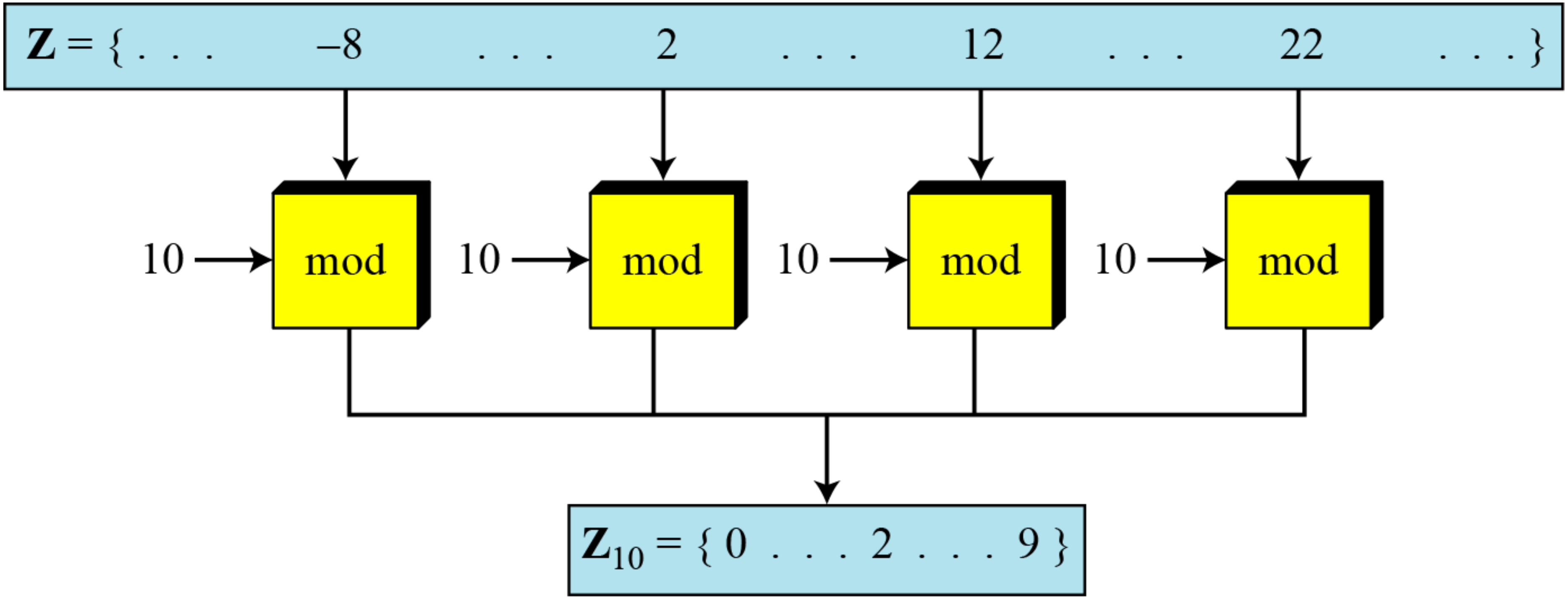
$$\mathbf{Z}_2 = \{\, 0, 1 \,\} \qquad \mathbf{Z}_6 = \{\, 0, 1, 2, 3, 4, 5 \,\} \qquad \mathbf{Z}_{11} = \{\, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 \,\}$$

- Để mô tả hai số nguyên là đồng dư, ta sử dụng phép toán đồng dư (≡), ví dụ:

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

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

# Tập hợp các phần dư




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

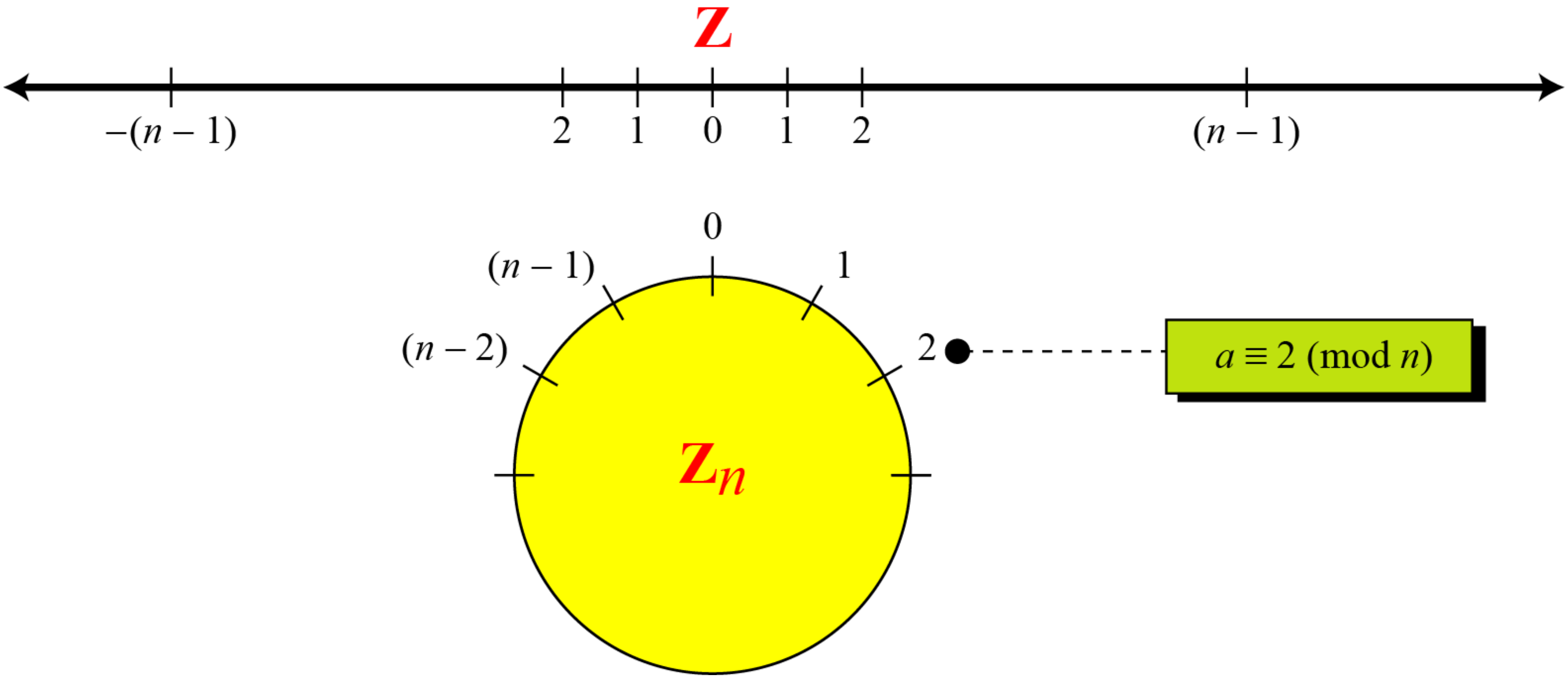
Congruence Relationship

# Tập hợp các phần dư

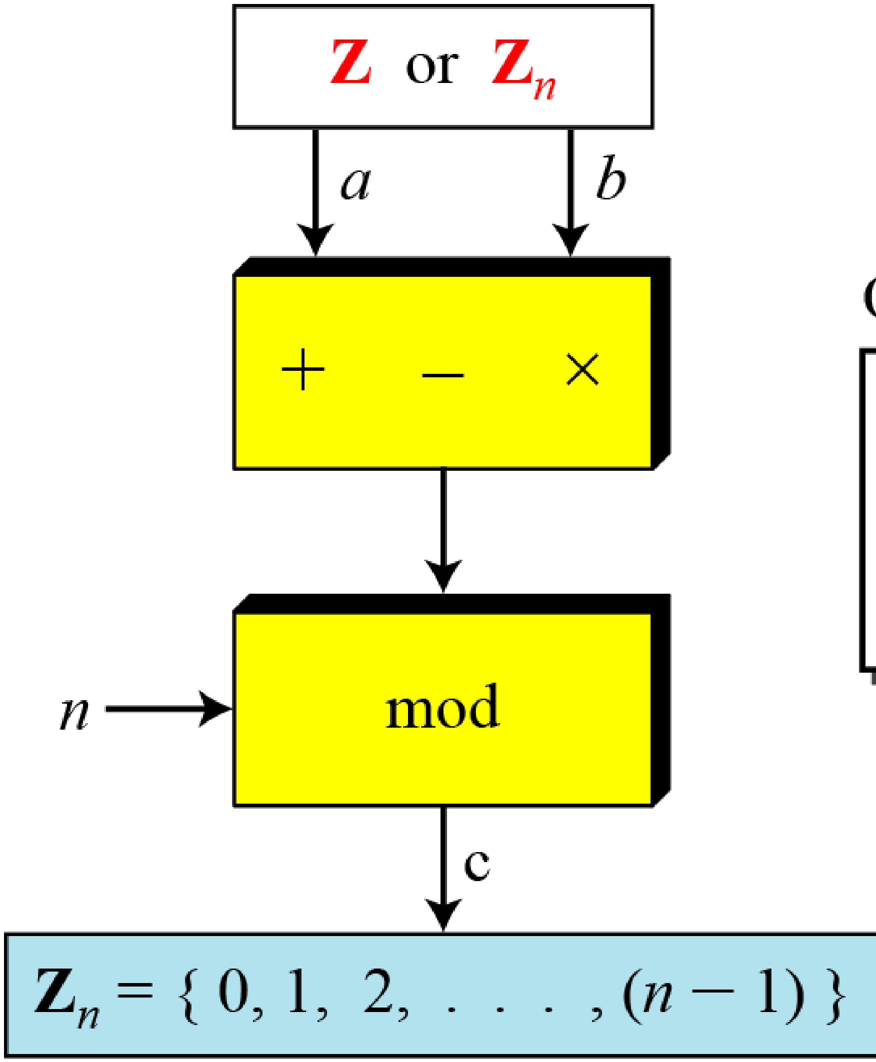
- Lớp phần dư [a] hoặc $[a]_n$ là tập số nguyên đồng dư khi chia cho *n.*
- Với $n$ = 5, ta có:

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

# Tập hợp các phần dư



# Tập hợp các phần dư




Operations

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

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

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

# Tính chất của phép toán MOD

- Ba tính chất của phép toán mod

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

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

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

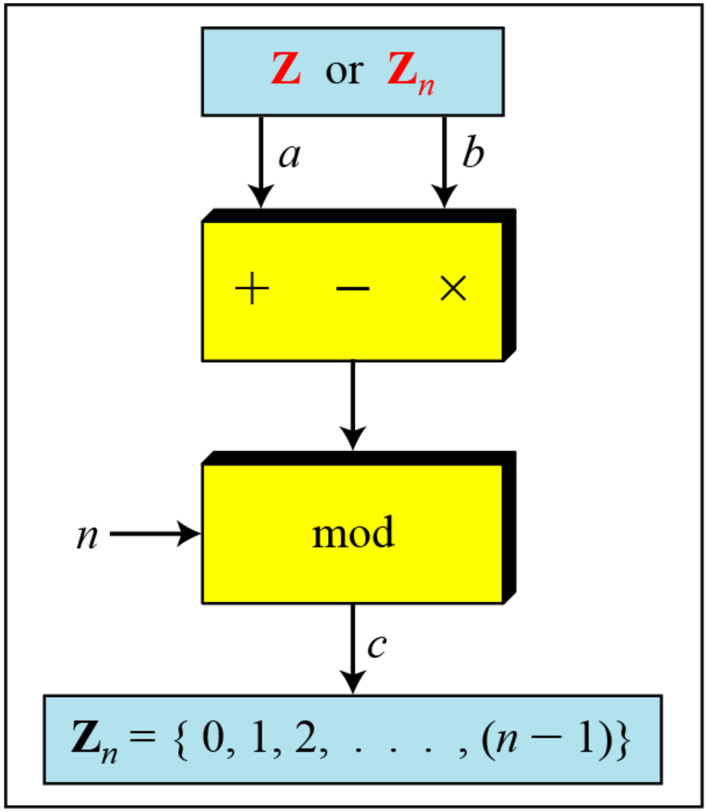
- Ví dụ:

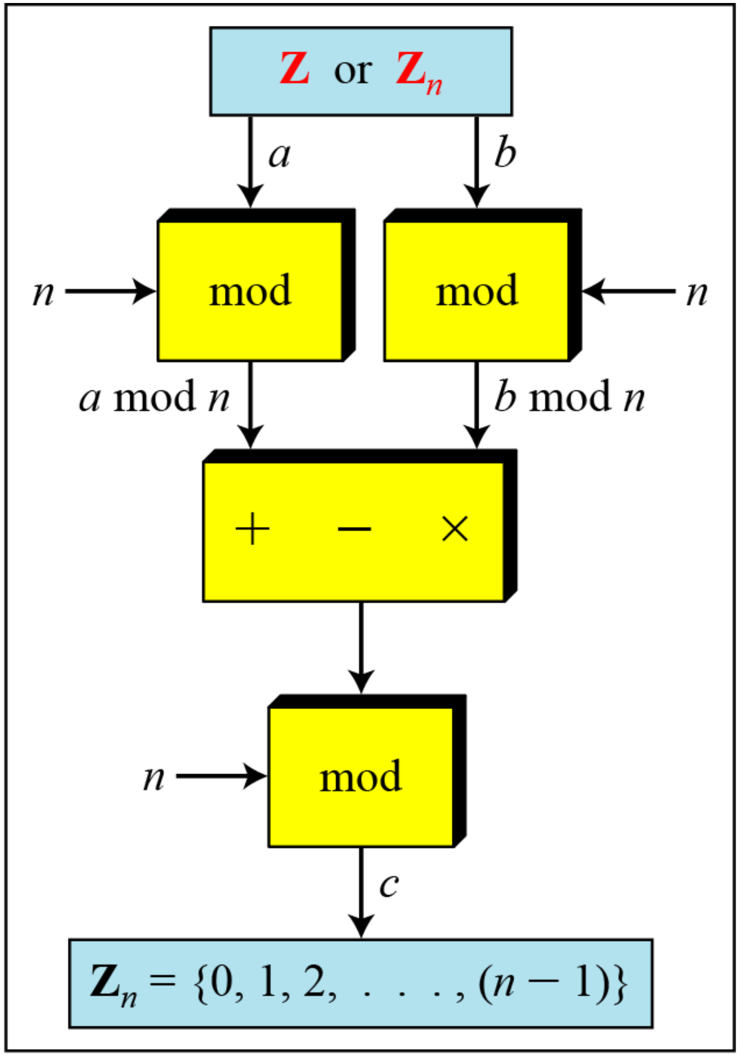
(1,723,345 + 2,124,945) mod 11 = (8 + 9) mod 11 = 6

(1,723,345 − 2,124,945) mod 11 = (8 − 9) mod 11 = 10

(1,723,345 × 2,124,945) mod 11 = (8 × 9) mod 11 = 6

# Tính chất của phép toán MOD



# Tính chất của phép toán MOD

- Phần dư của phép chia một số lũy thừa 10

$$10^n \bmod x = (10 \bmod x)^n$$

$$10 \bmod 3 = 1 \quad \rightarrow \quad 10^n \bmod 3 = (10 \bmod 3)^n = 1$$
$$10 \bmod 9 = 1 \quad \rightarrow \quad 10^n \bmod 9 = (10 \bmod 9)^n = 1$$
$$10 \bmod 7 = 3 \quad \rightarrow \quad 10^n \bmod 7 = (10 \bmod 7)^n = 3^n \bmod 7$$

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

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

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

# Phần tử đối ngẫu

- Trong $Z_n$, hai số a và b được gọi là đối ngẫu nhau nếu:

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

- Trong $Z_n$, mỗi số nguyên đều có phần tử đối ngẫu. Tổng của một phần tử và phần tử đối ngẫu thì đồng dư với 0 mod *n.*
- Trong $Z_n$ mọi phần tử *a* đều có phần tử đối ngẫu là *n-a.*
- Các cặp phần tử đối ngẫu trong $Z_{10}$ là: (0,0), (1,9), (2,8), (3,7), (4,6), (5,5).

# Phần tử nghịch đảo

- Trong $Z_n$, hai số a và b được gọi là nghịch đảo nhau nếu:

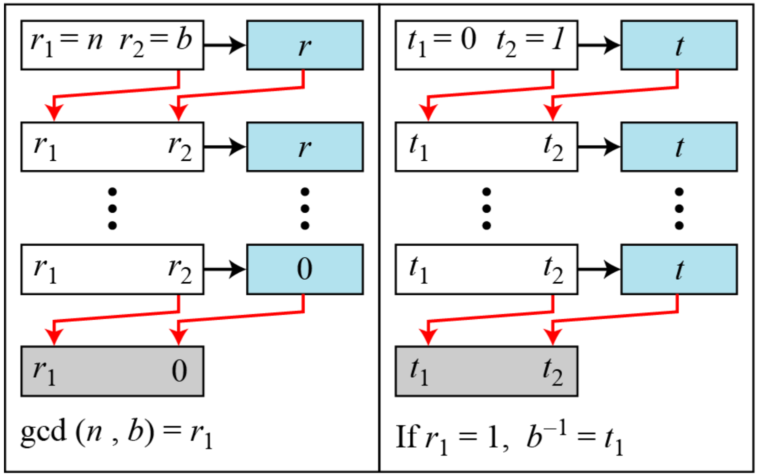
$$a \times b \equiv 1 \pmod{n}$$

- Trong $Z_n$, mỗi số nguyên có hoặc không có phần tử nghịch đảo. Tích của một phần tử và phần tử nghịch đảo thì đồng dư với 1 mod *n.*
- Vì gcd(10, 8) = 2 ≠ 1 nên 8 không có phần tử nghịch đảo trong $Z_{10}$.
- Các cặp phần tử nghịch đảo nhau trong $Z_{10}$ là: (1,1), (3,7), (9,9); các số 0, 2, 4, 5, 6 và 8 không có phần tử nghịch đảo.

# Phần tử nghịch đảo

- Thuật toán euclid mở rộng để tìm phần tử nghịch đảo của *b* trong $Z_n$ khi *n* và *b* là cặp số nguyên tố cùng nhau, nghĩa là: *gcd*(*n*, *b*) = 1.
- Các cặp số nghịch đảo trong $Z_{11}$ gồm:

(1,1), (2,6), (3,4), (5,9), (7,8), (9,5), và (10,10)




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

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

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 $b^{-1} \leftarrow t_1$

# Phần tử nghịch đảo

- Tìm phần tử nghịch đảo của 11 trong $Z_{26}$

| $q$ | $r_1$ | $r_2$ | $r$ | $t_1$ | $t_2$ | $t$ |
|---|---|---|---|---|---|---|
| 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 | |

gcd(11,26) = 1,

phần tử nghịch đảo của 11 trong $Z_{26}$ là -7 hoặc 19.

# Phần tử nghịch đảo

- Tìm phần tử nghịch đảo của 23 trong $Z_{100}$

| $q$ | $r_1$ | $r_2$ | $r$ | $t_1$ | $t_2$ | $t$ |
|---|---|---|---|---|---|---|
| 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 | |

gcd(23,100) = 1, phần tử nghịch đảo của 23 trong $Z_{100}$ là -13 hoặc 87.

# Phần tử nghịch đảo

- Tìm phần tử nghịch đảo của 12 trong $Z_{26}$

| $q$ | $r_1$ | $r_2$ | $r$ | $t_1$ | $t_2$ | $t$ |
|---|---|---|---|---|---|---|
| 2 | 26 | 12 | 2 | 0 | 1 | −2 |
| 6 | 12 | 2 | 0 | 1 | −2 | 13 |
| | 2 | 0 | | −2 | 13 | |

gcd(12,26) = 2,

Không tồn tại phần tử nghịch đảo của 12 trong $Z_{26}$

# Tập phần tử khả nghịch

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

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

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

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

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

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

- Tập $Z_n$ được dùng để tìm cặp phần tử đối ngẫu.
- Tập $Z_n^*$ được dùng để tìm cặp phần tử nghịch đảo.