HUST

TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI

HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY

ONE LOVE. ONE FUTURE.

TRƯỜNG ĐẠI HỌC
BÁCH KHOA HÀ NỘI
HANOI UNIVERSITY
OF SCIENCE AND TECHNOLOGY

LÝ THUYẾT MẬT MÃ

Cryptography Theory

ET3310

PGS. TS. Đỗ Trọng Tuấn
Trường Điện-Điện tử * Đại học Bách Khoa Hà Nội

ONE LOVE. ONE FUTURE.

Cơ sở toán học của Lý thuyết mật mã

Cơ sở toán học của Lý thuyết mật mã

Introduction to Number Theory

Divisibility and The Division Algorithm
- Divisibility
- The Division Algorithm

The Euclidean Algorithm
- Greatest Common Divisor
- Finding the Greatest Common Divisor

Modular Arithmetic
- The Modulus
- Properties of Congruences
- Modular Arithmetic Operations
- Properties of Modular Arithmetic
- Euclidean Algorithm Revisited
- The Extended Euclidean Algorithm

DIVISIBILITY AND THE DIVISION ALGORITHM

Divisibility

We say that a nonzero b **divides** a if $a = mb$ for some m, where a, b, and m are integers. That is, b divides a if there is no remainder on division. The notation $b|a$ is commonly used to mean b divides a. Also, if $b|a$, we say that b is a **divisor** of a.

The positive divisors of 24 are 1, 2, 3, 4, 6, 8, 12, and 24.

$13|182; -5|30; 17|289; -3|33; 17|0$

DIVISIBILITY AND THE DIVISION ALGORITHM

Subsequently, we will need some simple properties of divisibility for integers, which are as follows:

- If $a|1$, then $a = \pm 1$.
- If $a|b$ and $b|a$, then $a = \pm b$.
- Any $b \neq 0$ divides 0.
- If $a|b$ and $b|c$, then $a|c$:

$$11|66 \text{ and } 66|198 \Rightarrow 11|198$$

DIVISIBILITY AND THE DIVISION ALGORITHM

- If $b|g$ and $b|h$, then $b|(mg + nh)$ for arbitrary integers m and n.

To see this last point, note that

- If $b|g$, then g is of the form $g = b \times g_1$ for some integer g_1.
- If $b|h$, then h is of the form $h = b \times h_1$ for some integer h_1.

So

$$mg + nh = mbg_1 + nbh_1 = b \times (mg_1 + nh_1)$$

and therefore b divides $mg + nh$.

DIVISIBILITY AND THE DIVISION ALGORITHM

- If $b|g$ and $b|h$, then $b|(mg + nh)$ for arbitrary integers m and n.

$b = 7; g = 14; h = 63; m = 3; n = 2$

$7|14$ and $7|63$.

To show $7|(3 \times 14 + 2 \times 63)$,

we have $(3 \times 14 + 2 \times 63) = 7(3 \times 2 + 2 \times 9)$,
and it is obvious that $7|(7(3 \times 2 + 2 \times 9))$.

The Division Algorithm

Given any positive integer n and any nonnegative integer a, if we divide a by n, we get an integer quotient q and an integer remainder r that obey the following relationship:

$$a = qn + r \qquad 0 \leq r < n; q = \lfloor a/n \rfloor \tag{2.1}$$

where $\lfloor x \rfloor$ is the largest integer less than or equal to x. Equation (2.1) is referred to as the division algorithm.[1]

[1]Equation (2.1) expresses a theorem rather than an algorithm, but by tradition, this is referred to as the division algorithm.

Cơ sở toán học của Lý thuyết mật mã

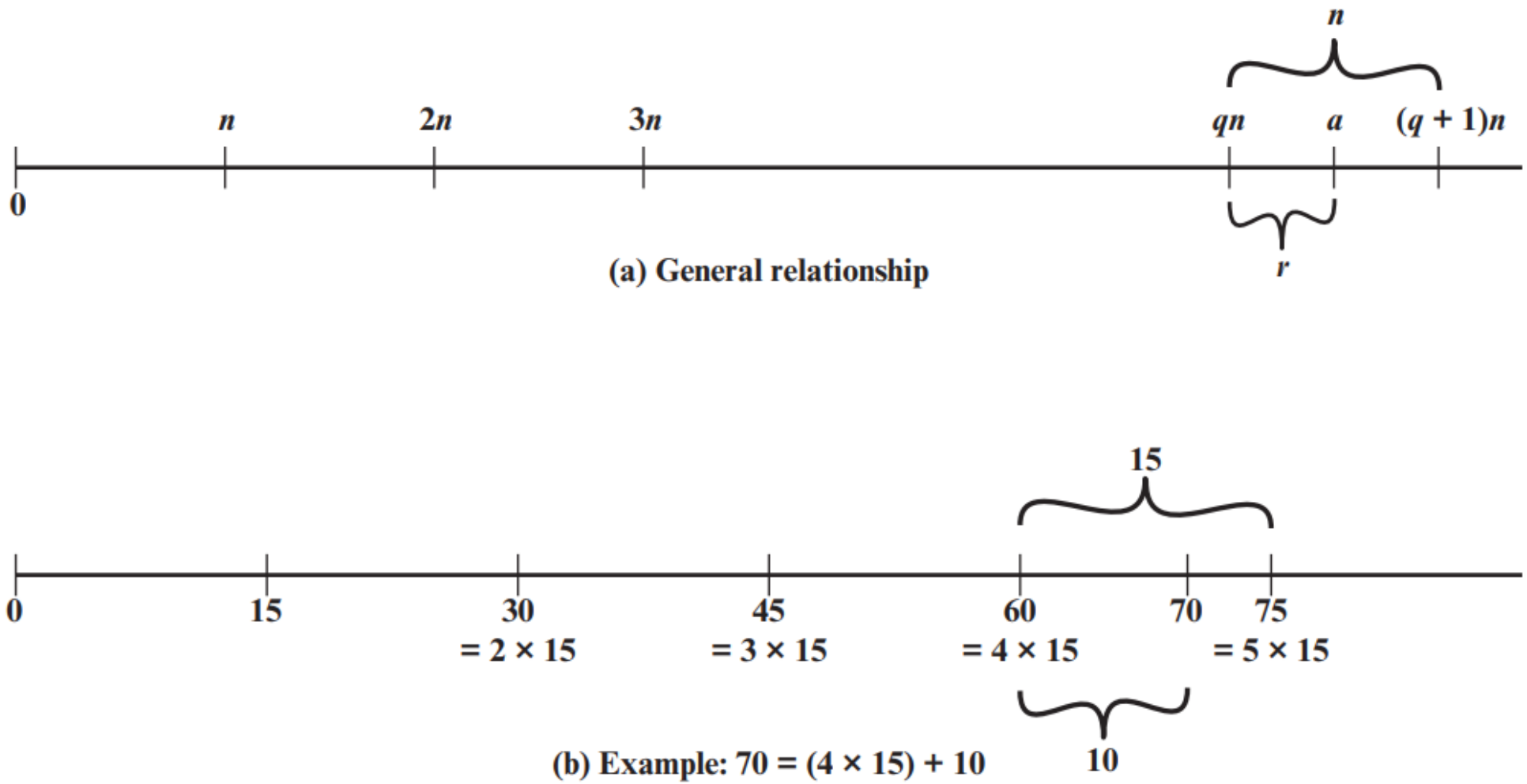
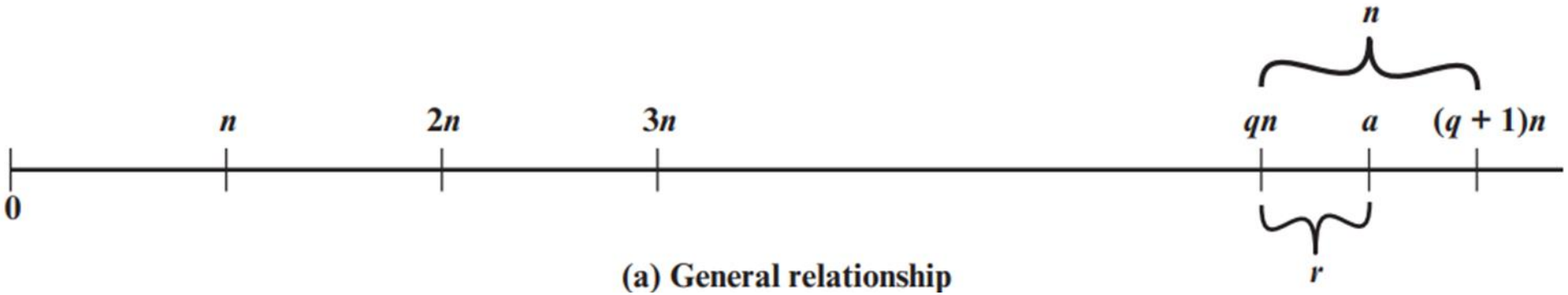


Figure 2.1 The Relationship $a = qn + r; 0 \leq r < n$



(a) General relationship

Figure 2.1a demonstrates that, given a and positive n, it is always possible to find q and r that satisfy the preceding relationship. Represent the integers on the number line; a will fall somewhere on that line (positive a is shown, a similar demonstration can be made for negative a). Starting at 0, proceed to n, $2n$, up to qn, such that $qn \leq a$ and $(q + 1)n > a$. The distance from qn to a is r, and we have found the unique values of q and r. The remainder r is often referred to as a **residue**.

$a = 11;$ $n = 7;$ $11 = 1 \times 7 + 4;$ $r = 4$ $q = 1$

$a = -11;$ $n = 7;$ $-11 = (-2) \times 7 + 3;$ $r = 3$ $q = -2$

Figure 2.1b provides another example.

THE EUCLIDEAN ALGORITHM

One of the basic techniques of number theory is the Euclidean algorithm, which is a simple procedure for determining the greatest common divisor of two positive integers. First, we need a simple definition: Two integers are **relatively prime** if and only if their only common positive integer factor is 1.

Greatest Common Divisor

Recall that nonzero b is defined to be a divisor of a if $a = mb$ for some m, where a, b, and m are integers. We will use the notation $\gcd(a, b)$ to mean the **greatest common divisor** of a and b. The greatest common divisor of a and b is the largest integer that divides both a and b. We also define $\gcd(0, 0) = 0$.

THE EUCLIDEAN ALGORITHM

More formally, the positive integer c is said to be the greatest common divisor of a and b if

1. c is a divisor of a and of b.
2. any divisor of a and b is a divisor of c.

An equivalent definition is the following:

$$\gcd(a, b) = \max[k, \text{such that } k|a \text{ and } k|b]$$

Because we require that the greatest common divisor be positive, $\gcd(a, b) = \gcd(a, -b) = \gcd(-a, b) = \gcd(-a, -b)$. In general, $\gcd(a, b) = \gcd(|a|, |b|)$.

$$\gcd(60, 24) = \gcd(60, -24) = 12$$

THE EUCLIDEAN ALGORITHM

Also, because all nonzero integers divide 0, we have $\gcd(a, 0) = |a|$.

We stated that two integers a and b are relatively prime if and only if their only common positive integer factor is 1. This is equivalent to saying that a and b are relatively prime if $\gcd(a, b) = 1$.

8 and 15 are relatively prime because the positive divisors of 8 are 1, 2, 4, and 8, and the positive divisors of 15 are 1, 3, 5, and 15. So 1 is the only integer on both lists.

THE EUCLIDEAN ALGORITHM

Finding the Greatest Common Divisor

We now describe an algorithm credited to Euclid for easily finding the greatest common divisor of two integers (Figure 2.2). This algorithm has broad significance in cryptography. The explanation of the algorithm can be broken down into the following points:

1. Suppose we wish to determine the greatest common divisor d of the integers a and b; that is determine $d = \gcd(a, b)$. Because $\gcd(|a|, |b|) = \gcd(a, b)$, there is no harm in assuming $a \geq b > 0$.
2. Dividing a by b and applying the division algorithm, we can state:

$$a = q_1 b + r_1 \qquad 0 \leq r_1 < b \tag{2.2}$$

THE EUCLIDEAN ALGORITHM

3. First consider the case in which $r_1 = 0$. Therefore b divides a and clearly no larger number divides both b and a, because that number would be larger than b. So we have $d = \gcd(a, b) = b$.
4. The other possibility from Equation (2.2) is $r_1 \neq 0$. For this case, we can state that $d \mid r_1$. This is due to the basic properties of divisibility: the relations $d \mid a$ and $d \mid b$ together imply that $d \mid (a - q_1 b)$, which is the same as $d \mid r_1$.
5. Before proceeding with the Euclidian algorithm, we need to answer the question: What is the $\gcd(b, r_1)$? We know that $d \mid b$ and $d \mid r_1$. Now take any arbitrary integer c that divides both b and r_1. Therefore, $c \mid (q_1 b + r_1) = a$. Because c divides both a and b, we must have $c \leq d$, which is the greatest common divisor of a and b. Therefore $d = \gcd(b, r_1)$.

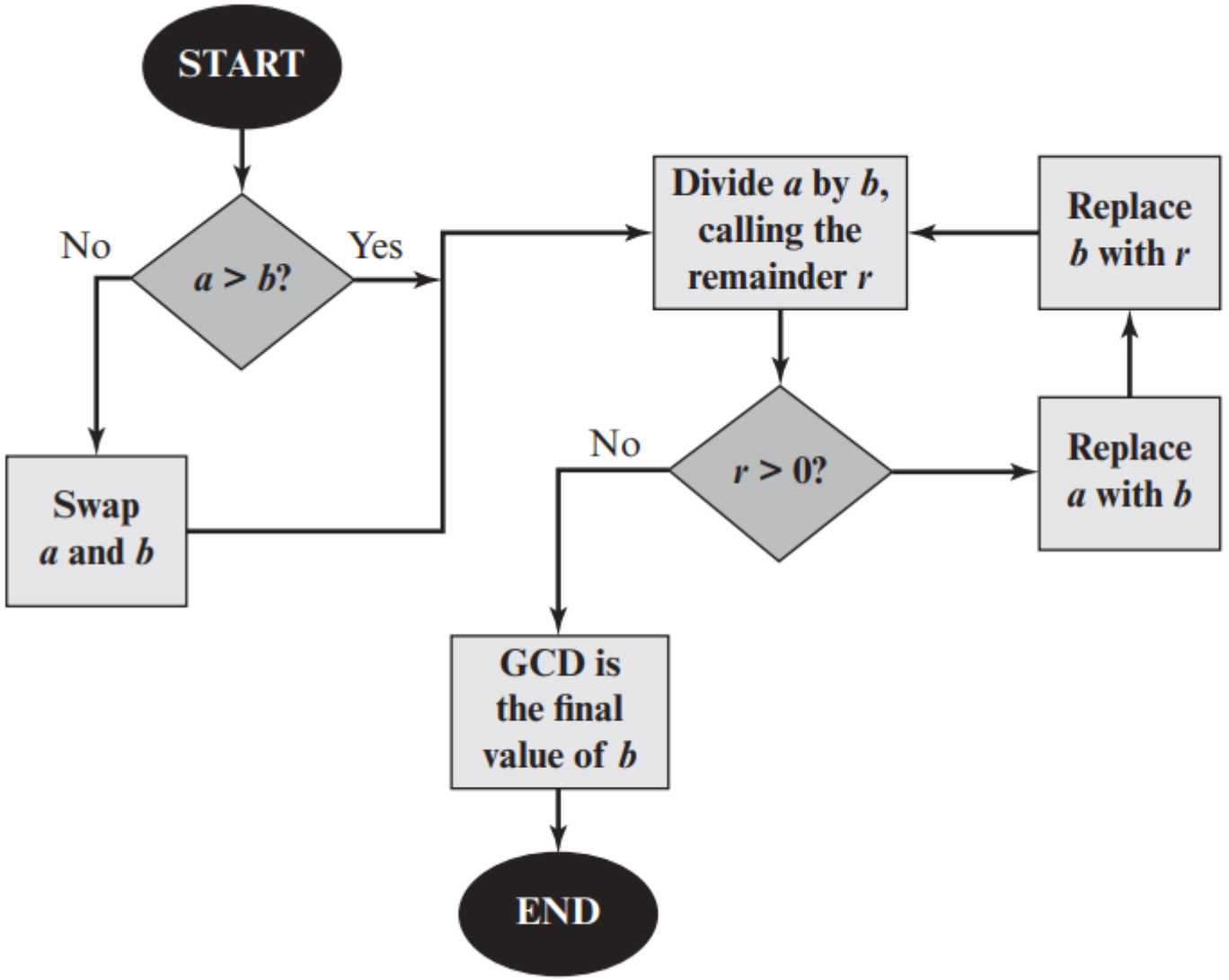


Figure 2.2 Euclidean Algorithm

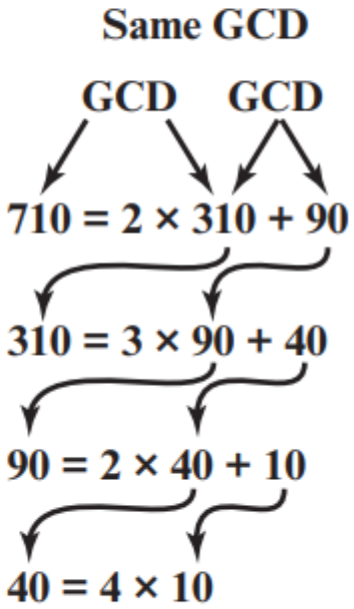


Figure 2.3 Euclidean Algorithm Example: gcd(710, 310)

MODULAR ARITHMETIC

The Modulus

If a is an integer and n is a positive integer, we define $a \bmod n$ to be the remainder when a is divided by n. The integer n is called the **modulus**. Thus, for any integer a, we can rewrite Equation (2.1) as follows:

$$a = qn + r \qquad 0 \leq r < n; q = \lfloor a/n \rfloor$$

$$a = \lfloor a/n \rfloor \times n + (a \bmod n)$$

$$11 \bmod 7 = 4; \qquad -11 \bmod 7 = 3$$

MODULAR ARITHMETIC

Two integers a and b are said to be **congruent modulo** n, if $(a \bmod n) = (b \bmod n)$. This is written as $a \equiv b \pmod{n}$.[2]

$$73 \equiv 4 \pmod{23}; \qquad 21 \equiv -9 \pmod{10}$$

Note that if $a \equiv 0 \pmod{n}$, then $n \mid a$.

[2] We have just used the operator *mod* in two different ways: first as a **binary operator** that produces a remainder, as in the expression $a \bmod b$; second as a **congruence relation** that shows the equivalence of two integers, as in the expression $a \equiv b \pmod{n}$. See Appendix 2A for a discussion.

MODULAR ARITHMETIC

Properties of Congruences

Congruences have the following properties:

1. $a \equiv b \pmod{n}$ if $n \mid (a - b)$.
2. $a \equiv b \pmod{n}$ implies $b \equiv a \pmod{n}$.
3. $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ imply $a \equiv c \pmod{n}$.

To demonstrate the first point, if $n \mid (a - b)$, then $(a - b) = kn$ for some k. So we can write $a = b + kn$. Therefore, $(a \bmod n)$ = (remainder when $b + kn$ is divided by n) = $(b \bmod n)$.

$23 \equiv 8 \pmod{5}$	because	$23 - 8 = 15 = 5 \times 3$
$-11 \equiv 5 \pmod{8}$	because	$-11 - 5 = -16 = 8 \times (-2)$
$81 \equiv 0 \pmod{27}$	because	$81 - 0 = 81 = 27 \times 3$

MODULAR ARITHMETIC

Modular Arithmetic Operations

Note that, by definition (Figure 2.1), the (mod n) operator maps all integers into the set of integers $\{0, 1, \ldots, (n - 1)\}$. This suggests the question: Can we perform arithmetic operations within the confines of this set? It turns out that we can; this technique is known as **modular arithmetic**.

Modular arithmetic exhibits the following properties:

1. $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$
2. $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$
3. $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

MODULAR ARITHMETIC

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

We demonstrate the first property. Define $(a \bmod n) = r_a$ and $(b \bmod n) = r_b$. Then we can write $a = r_a + jn$ for some integer j and $b = r_b + kn$ for some integer k. Then

$$\begin{aligned}(a + b) \bmod n &= (r_a + jn + r_b + kn) \bmod n \\ &= (r_a + r_b + (k + j)n) \bmod n \\ &= (r_a + r_b) \bmod n \\ &= [(a \bmod n) + (b \bmod n)] \bmod n\end{aligned}$$

MODULAR ARITHMETIC

$11 \bmod 8 = ?$; $15 \bmod 8 = ?$

$[(11 \bmod 8) + (15 \bmod 8)] \bmod 8 = ?$

$(11 + 15) \bmod 8 = ?$

$[(11 \bmod 8) - (15 \bmod 8)] \bmod 8 = ?$

$(11 - 15) \bmod 8 = -4 \bmod 8 = ?$

$[(11 \bmod 8) \times (15 \bmod 8)] \bmod 8 = ?$

$(11 \times 15) \bmod 8 = ?$

Properties of Modular Arithmetic

Define the set Z_n as the set of nonnegative integers less than n:

$$Z_n = \{0, 1, \ldots, (n-1)\}$$

Table 2.2 Arithmetic Modulo 8

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

(a) Addition modulo 8

Properties of Modular Arithmetic

Define the set Z_n as the set of nonnegative integers less than n:

$$Z_n = \{0, 1, \ldots, (n-1)\}$$

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

(b) Multiplication modulo 8

w	$-w$	w^{-1}
0	0	—
1	7	1
2	6	—
3	5	3
4	4	—
5	3	5
6	2	—
7	1	7

(c) Additive and multiplicative inverse modulo 8

MODULAR ARITHMETIC

This is referred to as the **set of residues**, or **residue classes** (mod n). To be more precise, each integer in Z_n represents a residue class. We can label the residue classes (mod n) as $[0], [1], [2], \ldots, [n-1]$, where

$$[r] = \{a: a \text{ is an integer}, a \equiv r \pmod{n}\}$$

The residue classes (mod 4) are

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

MODULAR ARITHMETIC

Of all the integers in a residue class, the smallest nonnegative integer is the one used to represent the residue class. Finding the smallest nonnegative integer to which k is congruent modulo n is called **reducing k modulo n**.

If we perform modular arithmetic within Z_n, the properties shown in Table 2.3 hold for integers in Z_n. We show in the next section that this implies that Z_n is a commutative ring with a multiplicative identity element.

There is one peculiarity of modular arithmetic that sets it apart from ordinary arithmetic. First, observe that (as in ordinary arithmetic) we can write the following:

$$\textbf{if } (a + b) \equiv (a + c) \pmod{n} \textbf{ then } b \equiv c \pmod{n} \qquad \textbf{(2.4)}$$

$$(5 + 23) \equiv (5 + 7) \pmod{8};\ 23 \equiv 7 \pmod{8}$$

MODULAR ARITHMETIC

There is one peculiarity of modular arithmetic that sets it apart from ordinary arithmetic. First, observe that (as in ordinary arithmetic) we can write the following:

$$\textbf{if } (a + b) \equiv (a + c) \pmod{n} \textbf{ then } b \equiv c \pmod{n} \qquad \textbf{(2.4)}$$

$$(5 + 23) \equiv (5 + 7) \pmod{8}; 23 \equiv 7 \pmod{8}$$

Equation (2.4) is consistent with the existence of an additive inverse. Adding the additive inverse of a to both sides of Equation (2.4), we have

$$((-a) + a + b) \equiv ((-a) + a + c) \pmod{n}$$
$$b \equiv c \pmod{n}$$

MODULAR ARITHMETIC

Table 2.3 Properties of Modular Arithmetic for Integers in Z_n

Property	Expression
Commutative Laws	$(w + x) \bmod n = (x + w) \bmod n$ $(w \times x) \bmod n = (x \times w) \bmod n$
Associative Laws	$[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$ $[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$
Distributive Law	$[w \times (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$
Identities	$(0 + w) \bmod n = w \bmod n$ $(1 \times w) \bmod n = w \bmod n$
Additive Inverse $(-w)$	For each $w \in Z_n$, there exists a z such that $w + z \equiv 0 \bmod n$

MODULAR ARITHMETIC

However, the following statement is true only with the attached condition:

if $(a \times b) \equiv (a \times c) \pmod{n}$ **then** $b \equiv c \pmod{n}$ **if** a is relatively prime to n **(2.5)**

Recall that two integers are **relatively prime** if their only common positive integer factor is 1. Similar to the case of Equation (2.4), we can say that Equation (2.5) is consistent with the existence of a multiplicative inverse. Applying the multiplicative inverse of a to both sides of Equation (2.5), we have

$$((a^{-1})ab) \equiv ((a^{-1})ac) \pmod{n}$$
$$b \equiv c \pmod{n}$$

MODULAR ARITHMETIC

To see this, consider an example in which the condition of Equation (2.5) does not hold. The integers 6 and 8 are not relatively prime, since they have the common factor 2. We have the following:

$$6 \times 3 = 18 \equiv 2 (\text{mod } 8)$$
$$6 \times 7 = 42 \equiv 2 (\text{mod } 8)$$

Yet $3 \not\equiv 7 \ (\text{mod } 8)$.

The reason for this strange result is that for any general modulus n, a multiplier a that is applied in turn to the integers 0 through $(n - 1)$ will fail to produce a complete set of residues if a and n have any factors in common.

MODULAR ARITHMETIC

With $a = 6$ and $n = 8$,

Z_8	0	1	2	3	4	5	6	7
Multiply by 6	0	6	12	18	24	30	36	42
Residues	0	6	4	2	0	6	4	2

Because we do not have a complete set of residues when multiplying by 6, more than one integer in Z_8 maps into the same residue. Specifically, $6 \times 0 \bmod 8 = 6 \times 4 \bmod 8$; $6 \times 1 \bmod 8 = 6 \times 5 \bmod 8$; and so on. Because this is a many-to-one mapping, there is not a unique inverse to the multiply operation.

However, if we take $a = 5$ and $n = 8$, whose only common factor is 1,

Z_8	0	1	2	3	4	5	6	7
Multiply by 5	0	5	10	15	20	25	30	35
Residues	0	5	2	7	4	1	6	3

The line of residues contains all the integers in Z_8, in a different order.

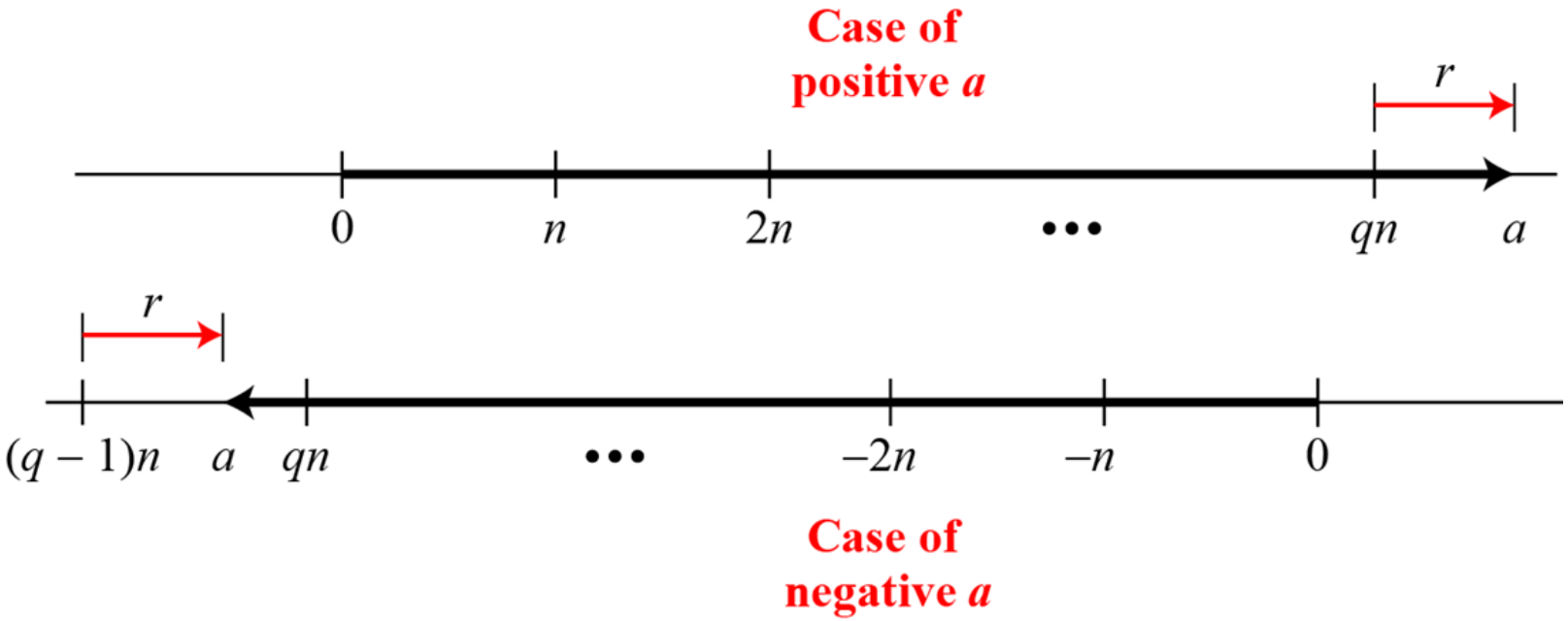
MODULAR ARITHMETIC

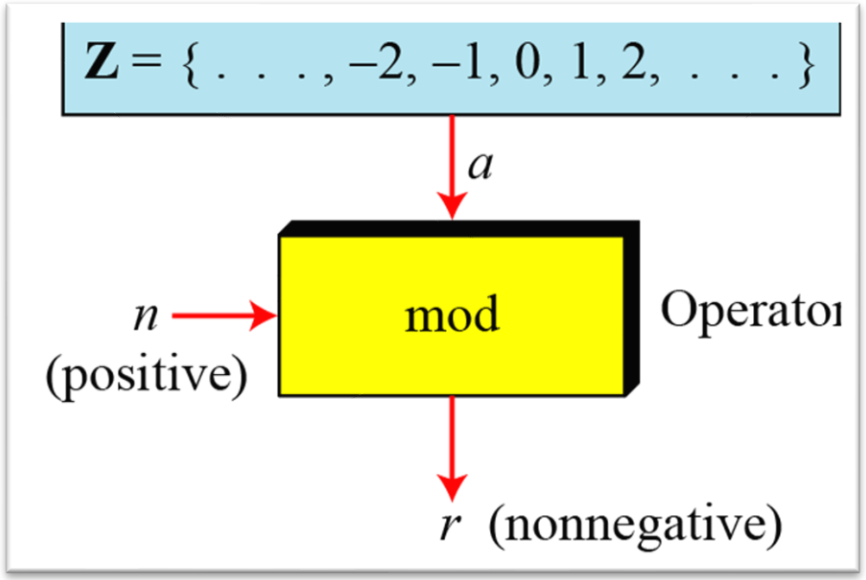
In general, an integer has a multiplicative inverse in Z_n if and only if that integer is relatively prime to n. Table 2.2c shows that the integers 1, 3, 5, and 7 have a multiplicative inverse in Z_8: but 2. 4. and 6 do not.

w	$-w$	w^{-1}
0	0	—
1	7	1
2	6	—
3	5	3
4	4	—
5	3	5
6	2	—
7	1	7

(c) Additive and multiplicative inverse modulo 8

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

Modulo Operator

Example

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

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

- Let a,b,c,n be integers with n≠0

(1) a≡0 (mod n) iff n|a

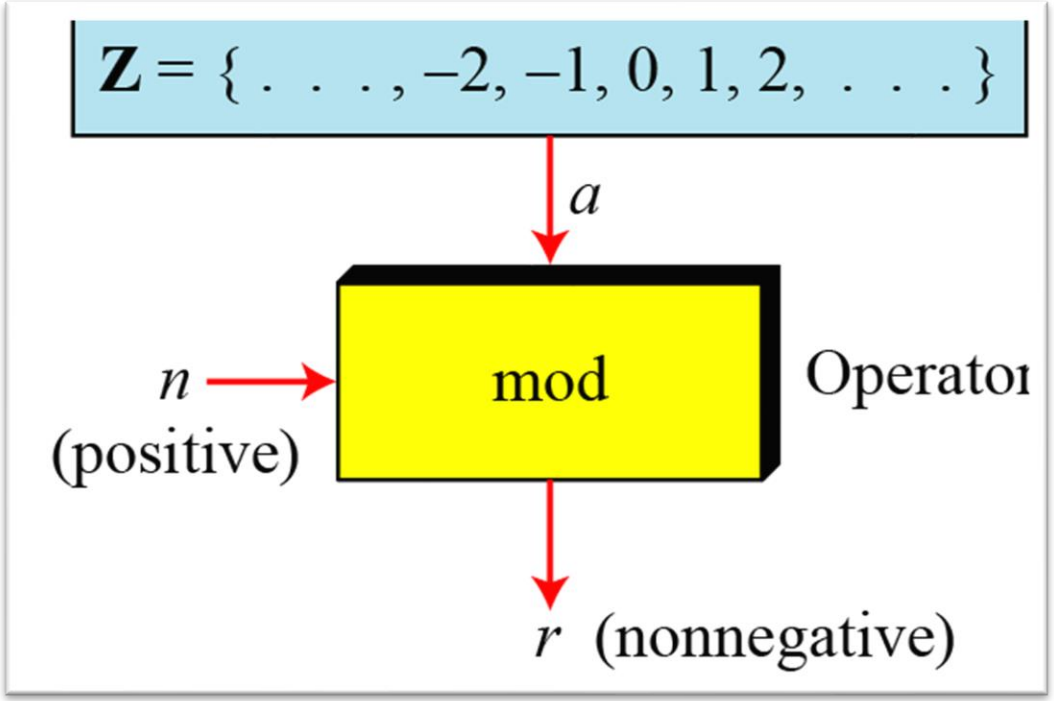
(2) a≡a (mod n)

(3) a≡b (mod n) iff b≡a (mod n)

(4) a≡b and b≡c (mod n) → a≡c (mod n)

(5) a≡b and c≡d (mod n) → a+c≡b+d,
a−c≡b−d, ac≡bd (mod n)

(6) ab≡ac (mod n) with n≠0, and gcd(a,n)=1, then b≡c (mod n)



Modulo Operator

Example

Find the result of the following operations:

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

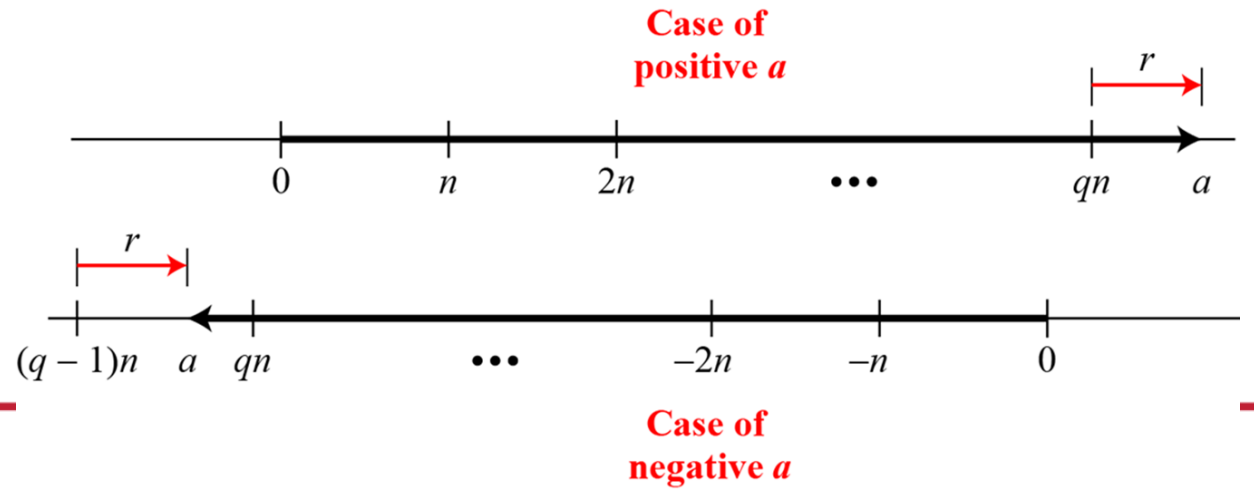
Solution

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.



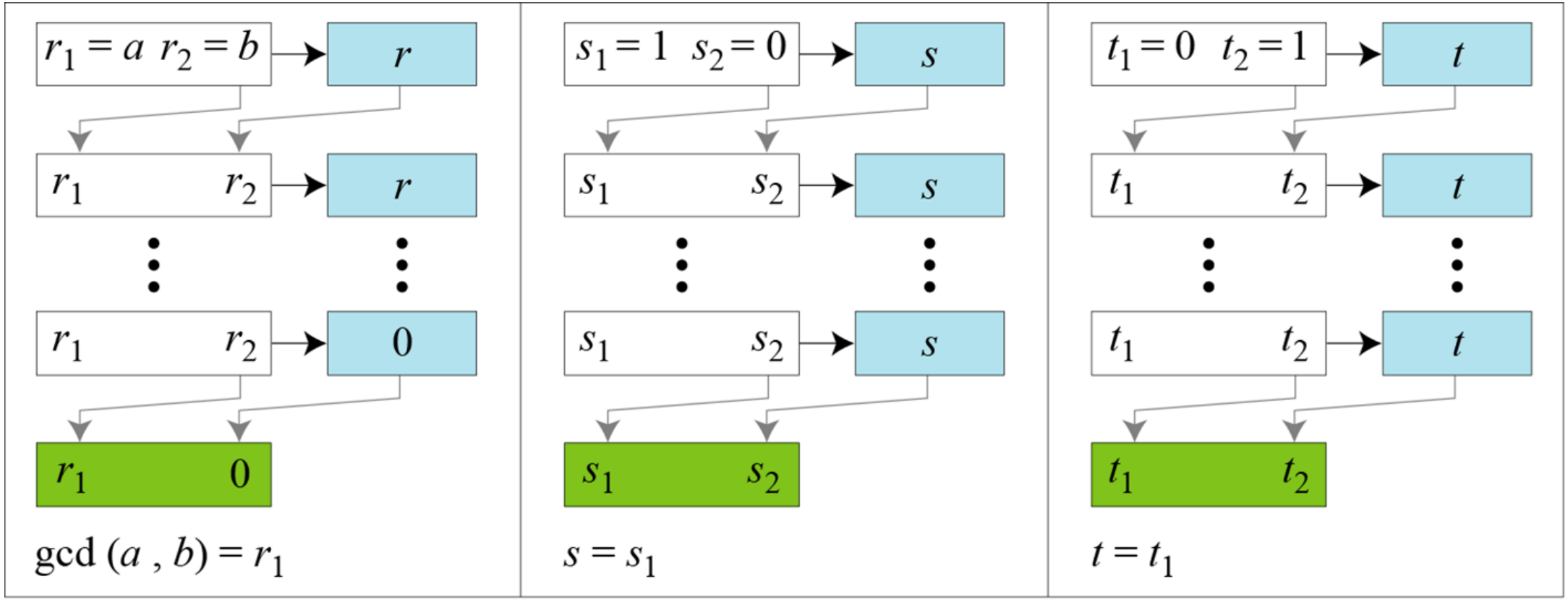
The Extended Euclidean Algorithm

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.

The Extended Euclidean Algorithm



a. Process

The Extended Euclidean Algorithm

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

b. Algorithm

The Extended Euclidean Algorithm

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

? GCD(a=161; b= 28), s, 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	

Extended Euclidean Algorithm

Example

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

Extended Euclidean Algorithm

s_1	s_2
1	0

t_1	t_2
0	1

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

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

q	r_1 r_2	r	s_1 s_2	s	t_1 t_2	t

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.

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

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

Some Z_n sets

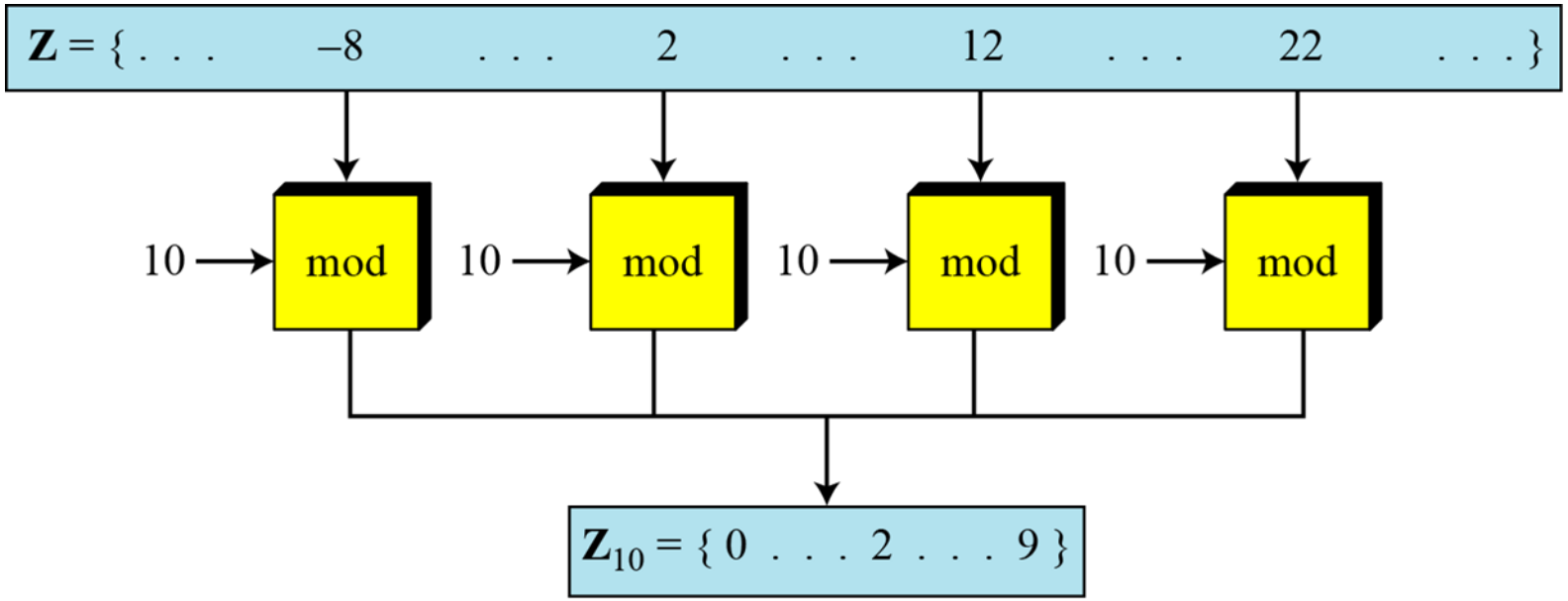
Congruence

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

Example

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

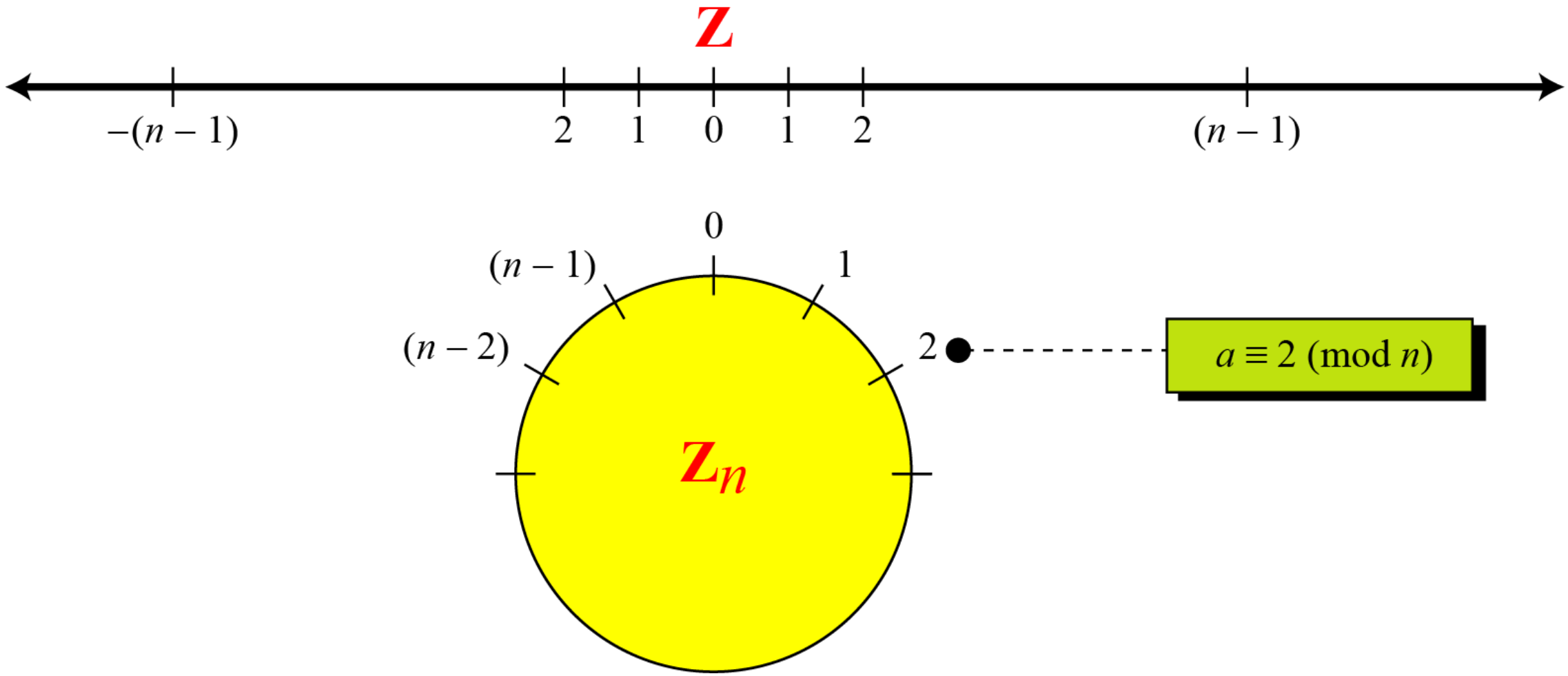
$3 \equiv 8 \pmod{5}$ $\quad 8 \equiv 13 \pmod{5}$



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

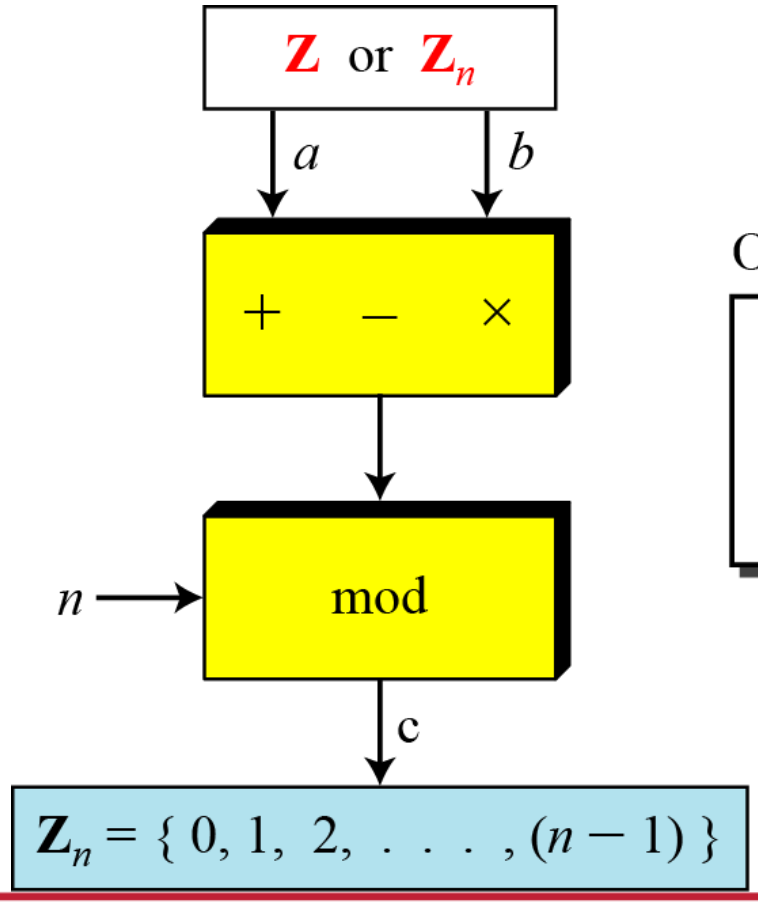
Congruence Relationship

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.



Operations

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

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

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

Operation in Z_n

Example

Perform the following operations (the inputs come from Zn):

a. Add 7 to 14 in Z_{15}.

b. Subtract 11 from 7 in Z_{13}.

c. Multiply 11 by 7 in Z_{20}.

Operation in Z_n

Example

Perform the following operations (the inputs come from Zn):

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

$$(14 + 7) \bmod 15$$

$$(7 - 11) \bmod 13$$

$$(7 \times 11) \bmod 20$$

Operation in Z_n

Example

Perform the following operations (the inputs come from Zn):

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

$$(14 + 7) \bmod 15$$
$$(7 - 11) \bmod 13$$
$$(7 \times 11) \bmod 20$$

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

Operation in Z_n

Example

Perform the following operations

a. Add 17 to 27 in Z_{14}.

b. Subtract 43 from 12 in Z_{13}.

c. Multiply 123 by −10 in Z_{19}.

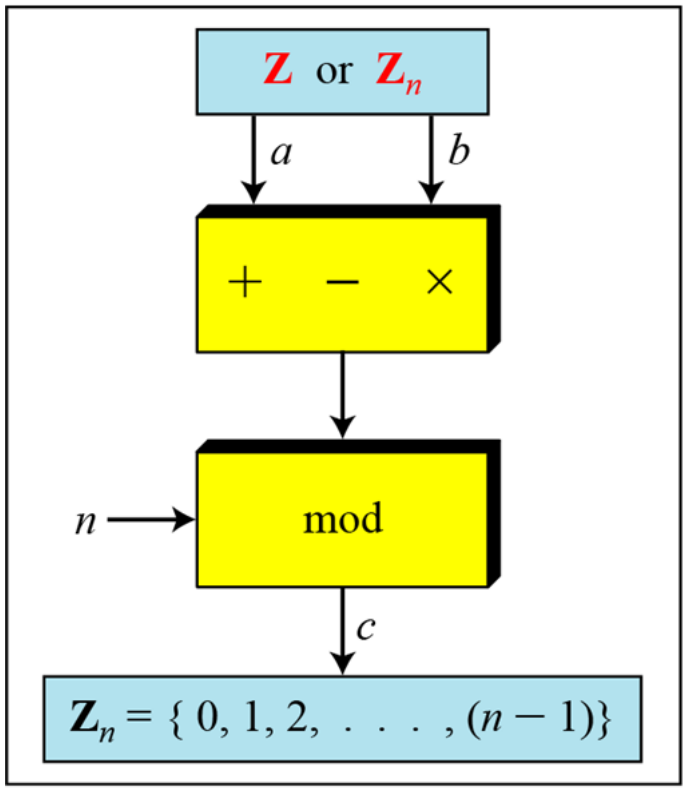
Operation in Z_n

Additive Inverse

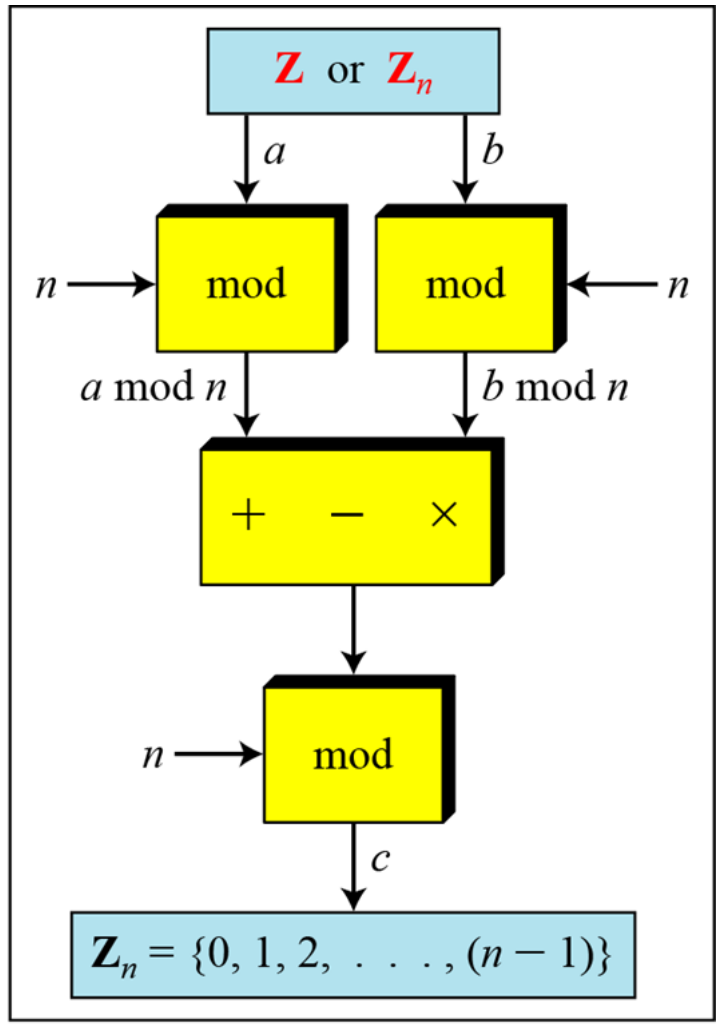
$$a + b \equiv 0 \pmod{n}$$

Multiplicative Inverse

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



a. Original process



b. Applying properties

Operation in Z_n

Additive Inverse

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

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

Multiplicative Inverse

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

$$\begin{aligned}(a + b) \bmod n &= [(a \bmod n) + (b \bmod n)] \bmod n \\ (a - b) \bmod n &= [(a \bmod n) - (b \bmod n)] \bmod n \\ (a \times b) \bmod n &= [(a \bmod n) \times (b \bmod n)] \bmod n\end{aligned}$$

Extended Euclidean Algorithm

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

Extended Euclidean Algorithm

Example

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

t_1	t_2
0	1

Solution

q	r_1	r_2	r	t_1	t_2	t

Extended Euclidean Algorithm

t_1	t_2
0	1

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

Solution

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.

Zn and Zn* sets

Use Z_n when additive inverses are needed

Use Z_n^* when multiplicative inverses are needed

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

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

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

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

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

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

Linear Diophantine Equation

A linear Diophantine equation of two variables is

$$ax + by = c.$$

Particular solution:

$x_0 = (c/\gcd(a,b))s$ and $y_0 = (c/\gcd(a,b))t$

General solutions:

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

where k is an integer

Linear Diophantine Equation

Find the particular and general solutions to the equation

$$21x + 14y = 35.$$

Particular: $x_0 = 5 \times 1 = 5$ and $y_0 = 5 \times (-1) = -5$

General: $x = 5 + k \times 2$ and $y = -5 - k \times 3$

Linear Diophantine Equation

For example, imagine we want to cash a $100 check and get some $20 and some $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)

Lập trình ứng dụng di động

HUST

hust.edu.vn fb.com/dhbkhn

THANK YOU !