

Chương 2

Mathematics of Cryptography Toán học mật mã

**Part I: Modular Arithmetic, Congruence,
and Matrices**

Số học mô-đun, đồng dư, ma trận

Chapter 2

Objectives

- To review integer arithmetic, concentrating on divisibility and finding the greatest common divisor using the Euclidean algorithm
- To understand how the extended Euclidean algorithm can be used to solve linear Diophantine equations, to solve linear congruent equations, and to find the multiplicative inverses
- To emphasize the importance of modular arithmetic and the modulo operator, because they are extensively used in cryptography
- To emphasize and review matrices and operations on residue matrices that are extensively used in cryptography
- To solve a set of congruent equations using residue matrices

Chapter 2

Objectives

- Để ôn lại số học số nguyên, tập trung vào tính chia hết và tìm ước số chung lớn nhất bằng cách sử dụng thuật toán Euclidean
- Để hiểu cách thuật toán Euclidean mở rộng có thể được sử dụng để giải các phương trình Diophantine tuyến tính, để giải các phương trình đồng dư tuyến tính và để tìm các nghịch đảo nhân
- Để nhấn mạnh tầm quan trọng của số học mô-đun và toán tử mô-đun, bởi vì chúng được sử dụng rộng rãi trong mật mã
- Để nhấn mạnh và xem xét các ma trận và hoạt động trên các ma trận dư được sử dụng rộng rãi trong mật mã
- Để giải một tập các phương trình đồng dư bằng cách sử dụng ma trận dư

2-1 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.

Topics discussed in this section:

- 2.1.1 Set of Integers**
- 2.1.2 Binary Operations**
- 2.1.3 Integer Division**
- 2.1.4 Divisibility**
- 2.1.5 Linear Diophantine Equations**

2.1.1 Set of Integers

The set of integers, denoted by Z, contains all integral numbers (with no fraction) from negative infinity to positive infinity (Figure 2.1).

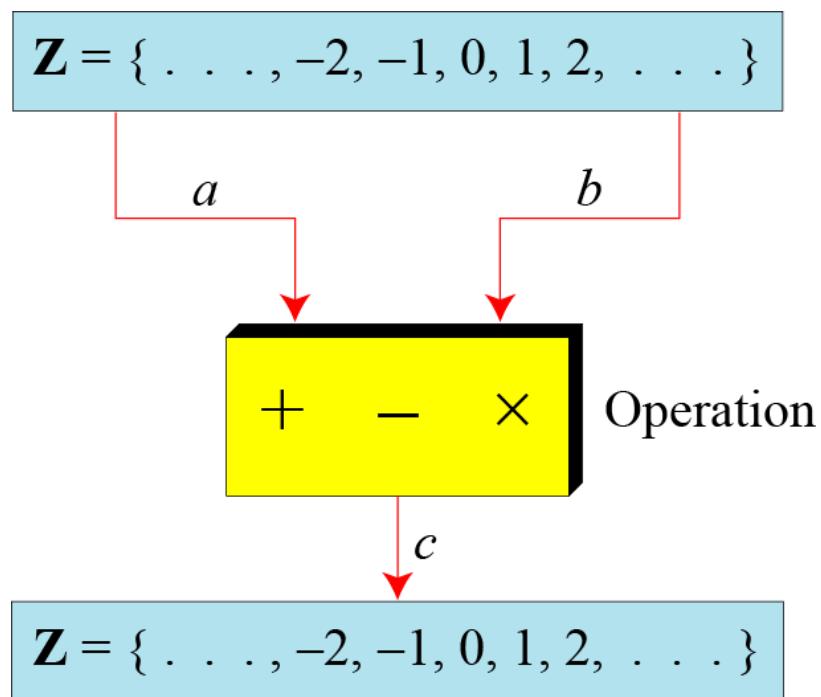
Figure 2.1 The set of integers

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

2.1.2 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.

Figure 2.2 Three binary operations for the set of integers



2.1.2 *Continued*

Example 2.1

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

2.1.3 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

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

Trong số học nguyên, nếu chúng ta chia a cho n , chúng ta có thể nhận được q và r . Mọi quan hệ giữa bốn số nguyên này có thể được hiển thị như trên

2.1.3 Continued

Example 2.2

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

Giả sử rằng $a = 255$ và $n = 11$. Chúng ta có thể tìm thấy $q = 23$ và $r = 2$ bằng cách sử dụng thuật toán chia.

Figure 2.3 Example 2.2, finding the quotient and the remainder

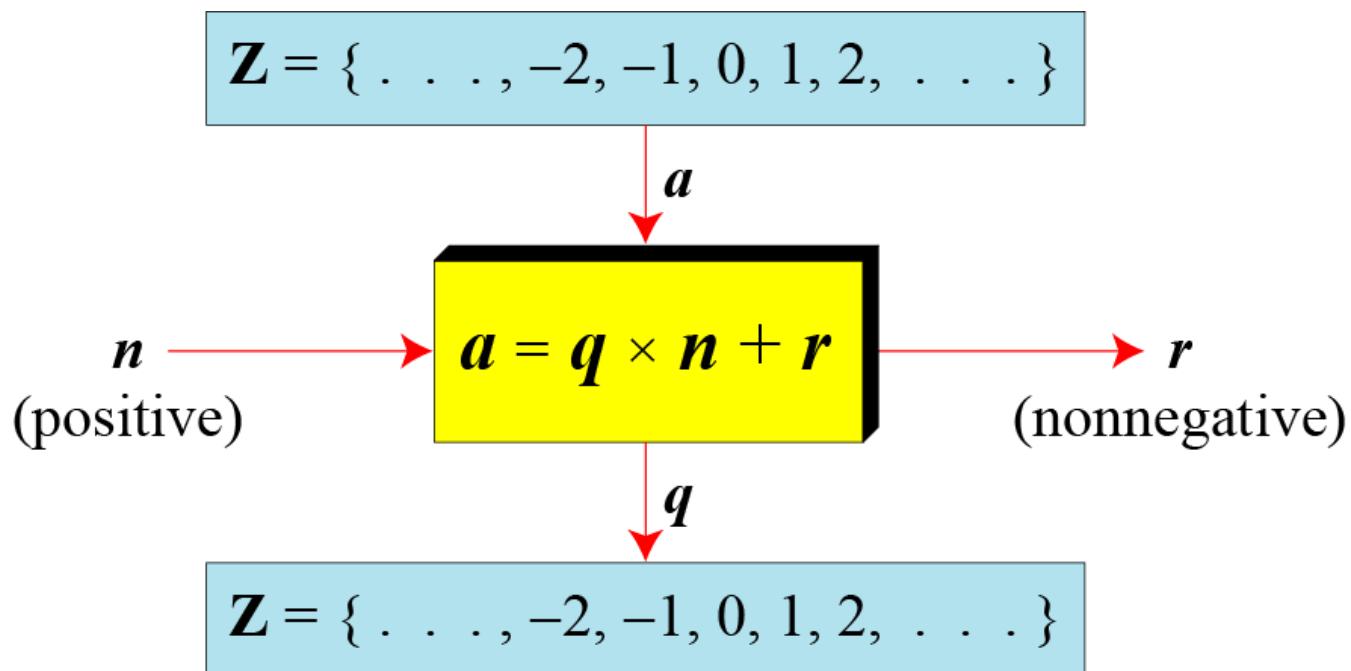
Hình 2.3 Ví dụ 2.2, tìm thương và phần dư

$$\begin{array}{r} 2\ 3 \quad \longleftarrow q \\ \hline 2\ 5\ 5 \quad \longleftarrow a \\ 2\ 2 \\ \hline 3\ 5 \\ 3\ 3 \\ \hline 2 \quad \longleftarrow r \end{array}$$

2.1.3 Continued

Figure 2.4 Division algorithm for integers

Thuật toán chia cho số nguyên



2.1.3 Continued

Example 2.3

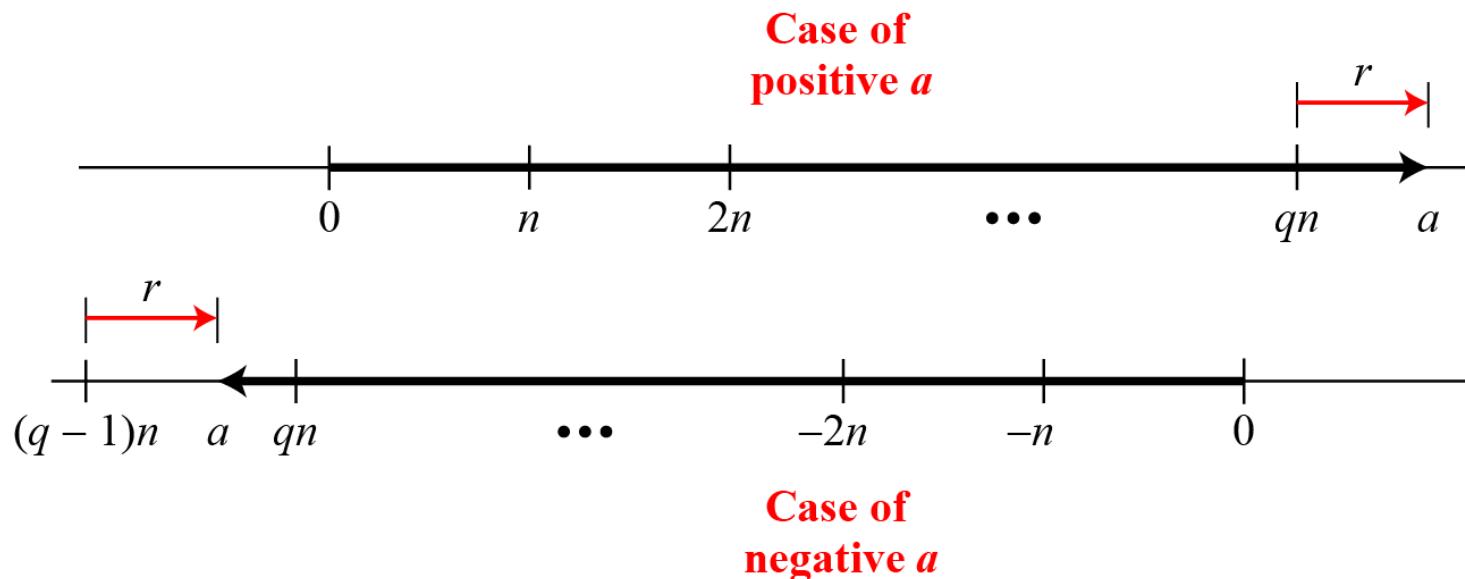
When we use a computer or a calculator, r and q are negative when a is negative. How can we apply the restriction that r needs to be positive? The solution is simple, we decrement the value of q by 1 and we add the value of n to r to make it positive.

Khi chúng ta sử dụng máy tính hoặc máy tính, r và q là số âm khi a là số âm. Làm thế nào chúng ta có thể áp dụng hạn chế mà r cần là số dương? Giải pháp rất đơn giản, chúng tôi giảm giá trị của q đi 1 và chúng tôi thêm giá trị của n vào r để làm cho nó dương.

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

2.1.3 Continued

Figure 2.5 Graph of division algorithm
Đồ thị của thuật toán chia



2.1.4 Divisibility (tính chia hết)

If a is not zero and we let $r = 0$ in the division relation, we get

Nếu a khác 0 và ta đặt $r = 0$ trong quan hệ chia, chúng ta nhận được

$$a = q \times n$$

If the remainder is zero: n/a

If the remainder is not zero: $n \nmid a$

2.1.4 *Continued*

Example 2.4

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

$$4|32$$

- 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

$$8\nmid 42$$

2.1.4 *Continued*

Example 2.5

- 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 $11\nmid (-32)$.

2.1.4 *Continued*

Properties

Property 1: if $a|1$, then $a = \pm 1$.

Property 2: if $b|a$ and $a|b$, then $a = \pm b$.

Property 3: if $b|a$ and $c|b$, then $c|a$.

***Property 4: if $a|b$ and $a|c$, then
 $a|(m \times b + n \times c)$, where m
and n are arbitrary integers***

2.1.4 *Continued*

Example 2.6

- 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 $3|66$.

2.1.4 *Continued*

Note

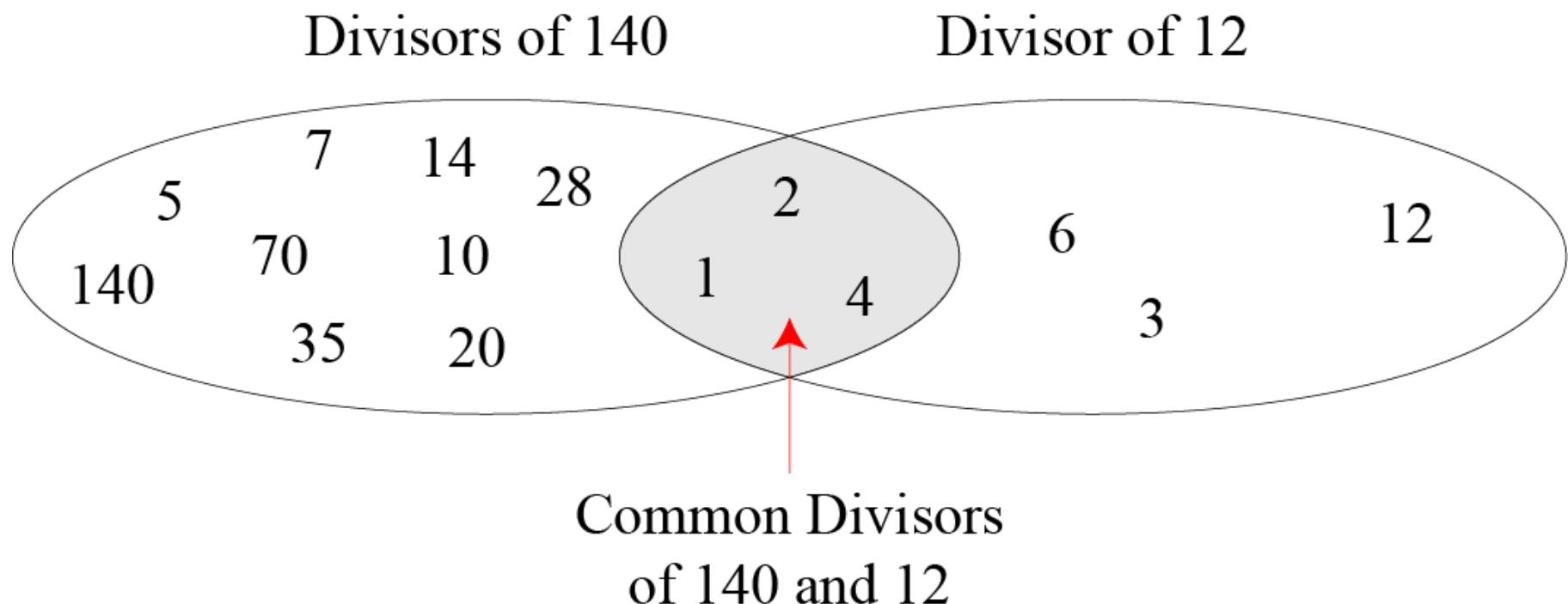
Fact 1: *The integer 1 has only one divisor, itself.* (Số nguyên 1 chỉ có một ước số là chính nó.)

Fact 2: *Any positive integer has at least two divisors, 1 and itself (but it can have more).* (Bất kỳ số nguyên dương nào có ít nhất hai ước, 1 và chính nó (nhưng nó có thể có nhiều hơn)).

2.1.4 Continued

Figure 2.6 Common divisors of two integers

Các ước chung của hai số nguyên



2.1.4 Continued

Note

Greatest Common Divisor: ước số chung lớn nhất

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

Note

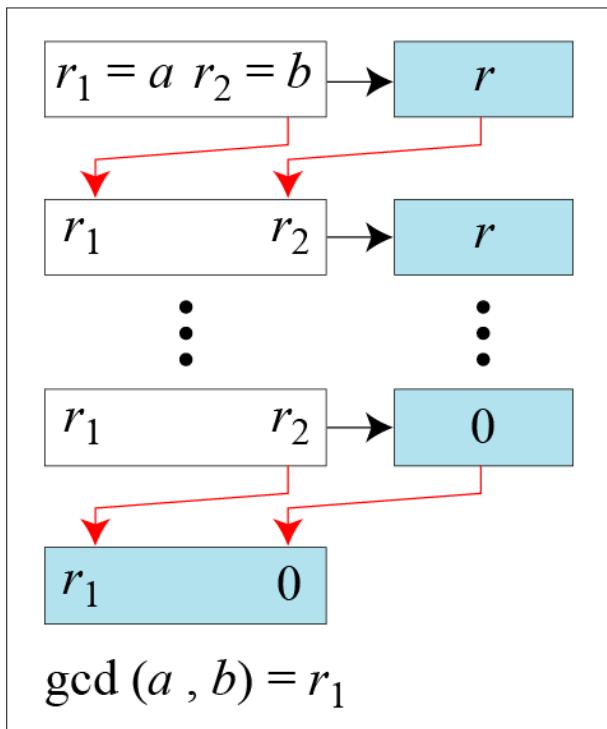
Euclidean Algorithm

Fact 1: $\gcd(a, 0) = a$

Fact 2: $\gcd(a, b) = \gcd(b, r)$, where r is the remainder of dividing a by b

2.1.4 Continued

Figure 2.7 Euclidean Algorithm



a. Process

```
r1 ← a;      r2 ← b;      (Initialization)  
while (r2 > 0)  
{  
    q ← r1 / r2;  
    r ← r1 - q × r2;  
    r1 ← r2; r2 ← r;  
}  
gcd (a, b) ← r1
```

b. Algorithm

Find the greatest common divisor of 2740 and 1760?
Tìm ước số chung lớn nhất của 2740 và 1760?

2.1.4 *Continued*

Example 2.7

Find the greatest common divisor of 2740 and 1760.
Tìm ước số chung lớn nhất của 2740 và 1760.

Solution

We have $\gcd(2740, 1760) = 20$.

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	

2.1.4 Continued

Note

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

- + Khi $\gcd(a, b) = 1$, ta nói rằng a và b nguyên tố của nhau.
- + Cho n là số tự nhiên, hai số $a=2n+1$ và $b=3n+1$ là nguyên tố của nhau, do $\gcd(a, b)=1$.

2.1.4 *Continued*

Example 2.8

Find the greatest common divisor of 25 and 60.
Tìm ước chung lớn nhất của 25 và 60.

Solution

We have $\gcd(25, 60) = 5$.

q	r_1	r_2	r
0	25	60	25
2	60	25	10
2	25	10	5
2	10	5	0
	5	0	

2.1.4 *Continued*

Extended Euclidean Algorithm

Thuật toán Euclid mở rộng

Given two integers a and b , we often need to find other two integers, s and t , such that

Cho hai số nguyên a và b , chúng ta thường cần tìm hai số nguyên khác, s và t , sao cho

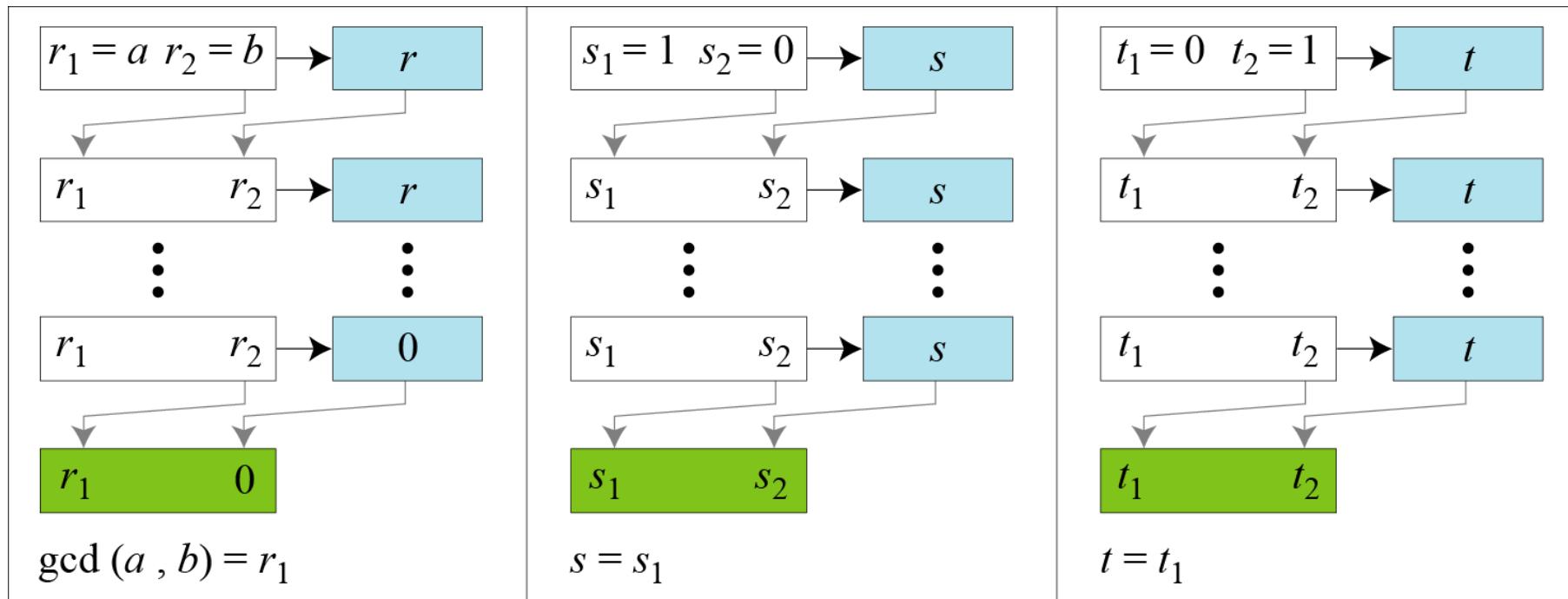
$$s \times a + t \times b = \gcd(a, b)$$

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

Thuật toán Euclid mở rộng có thể tính $\gcd(a, b)$ và đồng thời tính giá trị của s và t .

2.1.4 Continued

Figure 2.8.a Extended Euclidean algorithm, part a
Thuật toán Euclid mở rộng, phần a



a. Process

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

Cho $a = 161$ và $b = 28$, tìm $\gcd(a, b)$ và các giá trị của s và t .

2.1.4 Continued

Figure 2.8.b Extended Euclidean algorithm, part b
Thuật toán Euclid mở rộng, phần b

```
r1 ← a;      r2 ← b;  
s1 ← 1;      s2 ← 0;  
t1 ← 0;      t2 ← 1;
```

(Initialization)

while ($r_2 > 0$)

{

$q \leftarrow r_1 / r_2$;

```
  r ← r1 − q × r2;  
  r1 ← r2; r2 ← r;
```

(Updating r 's)

```
  s ← s1 − q × s2;  
  s1 ← s2; s2 ← s;
```

(Updating s 's)

```
  t ← t1 − q × t2;  
  t1 ← t2; t2 ← t;
```

(Updating t 's)

}

gcd(a, b) ← r₁; s ← s₁; t ← t₁

b. Algorithm

2.1.4 Continued

Example 2.9

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

Cho $a = 161$ và $b = 28$, tìm $\gcd(a, b)$ và các giá trị của s và 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
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	

2.1.4 Continued

Example 2.10

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

Cho $a = 17$ và $b = 0$, tìm $\gcd(a, b)$ và các giá trị của s và t .

Solution

We get $\gcd(17, 0) = 17$, $s = 1$, and $t = 0$.

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
	17	0		1	0		0	1	

2.1.4 Continued

Example 2.11

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

Cho $a = 0$ và $b = 45$, tìm $\gcd(a, b)$ và các giá trị của s và t .

Solution

We get $\gcd(0, 45) = 45$, $s = 0$, and $t = 1$.

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	

2-2 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 .

Topics discussed in this section:

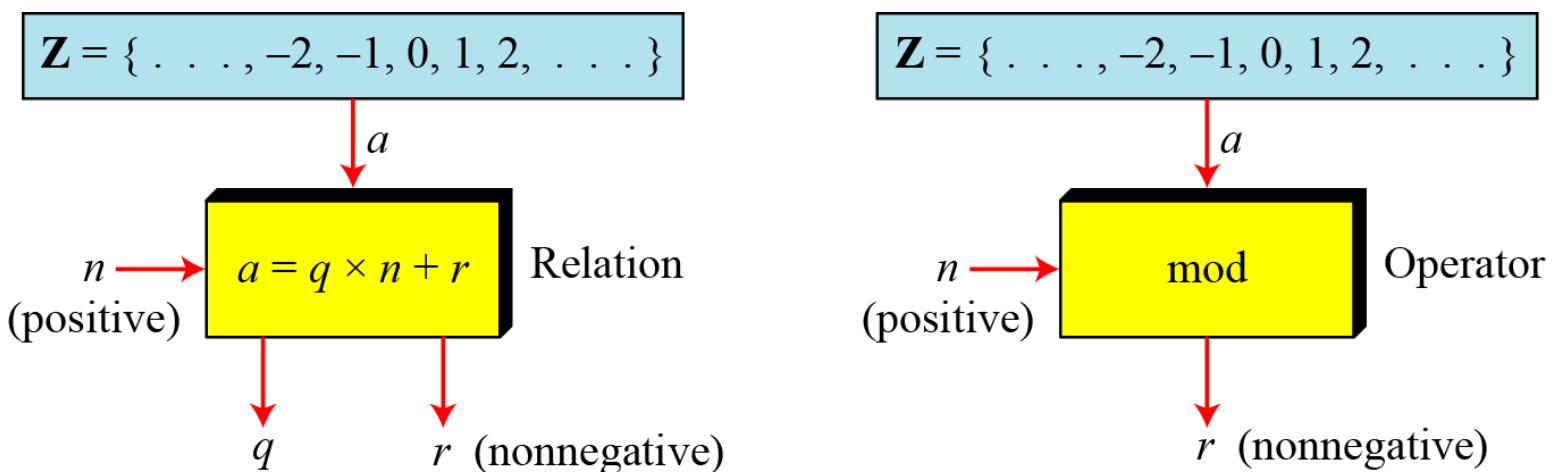
- 2.2.1 Modular Operator (phép toán mô-đun)**
- 2.2.2 Set of Residues (tập dư)**
- 2.2.3 Congruence (tính đồng dư)**
- 2.2.4 Operations in Z_n**
- 2.2.5 Addition and Multiplication Tables**
- 2.2.6 Different Sets (tập khác)**

2.2.1 Modulo Operator

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

Toán tử modulo được hiển thị dưới dạng **mod**. Đầu vào thứ hai (n) được gọi là môđun. Đầu ra r được gọi là số dư.

Figure 2.9 Division algorithm and modulo operator



2.1.4 Continued

Example 2.14

Tìm kết quả của các phép toán mô-đun sau đây:

- a. $27 \text{ mod } 5$
- b. $36 \text{ mod } 12$
- c. $-18 \text{ mod } 14$
- d. $-7 \text{ mod } 10$

Solution

- a. Chia 27 cho 5 ta được $r = 2$
- b. Chia 36 cho 12 được kết quả là $r = 0$.
- c. Chia -18 cho 14 ta được $r = -4$. Sau khi thêm môđun $r = 10$
- d. Chia -7 cho 10 ta được $r = -7$. Sau khi thêm môđun vào -7 , $r = 3$.

2.2.2 Tập dư

*The modulo operation creates a set, which in modular arithmetic is referred to as **the set of least residues modulo n, or Z_n** .*

Phép toán modulo tạo ra một tập hợp, trong số học môn được gọi là tập hợp có ít dư lượng nhất modulo n, hay còn gọi là Z_n .

Figure 2.10 Some Z_n sets

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

$$\mathbf{Z}_2 = \{ 0, 1 \}$$

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

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

2.2.3 Tính đồng dư (*congruence*)

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

Để chỉ ra rằng hai số nguyên là đồng dư, chúng ta sử dụng toán tử đồng dư (≡). Ví dụ, ta viết:

$$2 \equiv 12 \pmod{10}$$

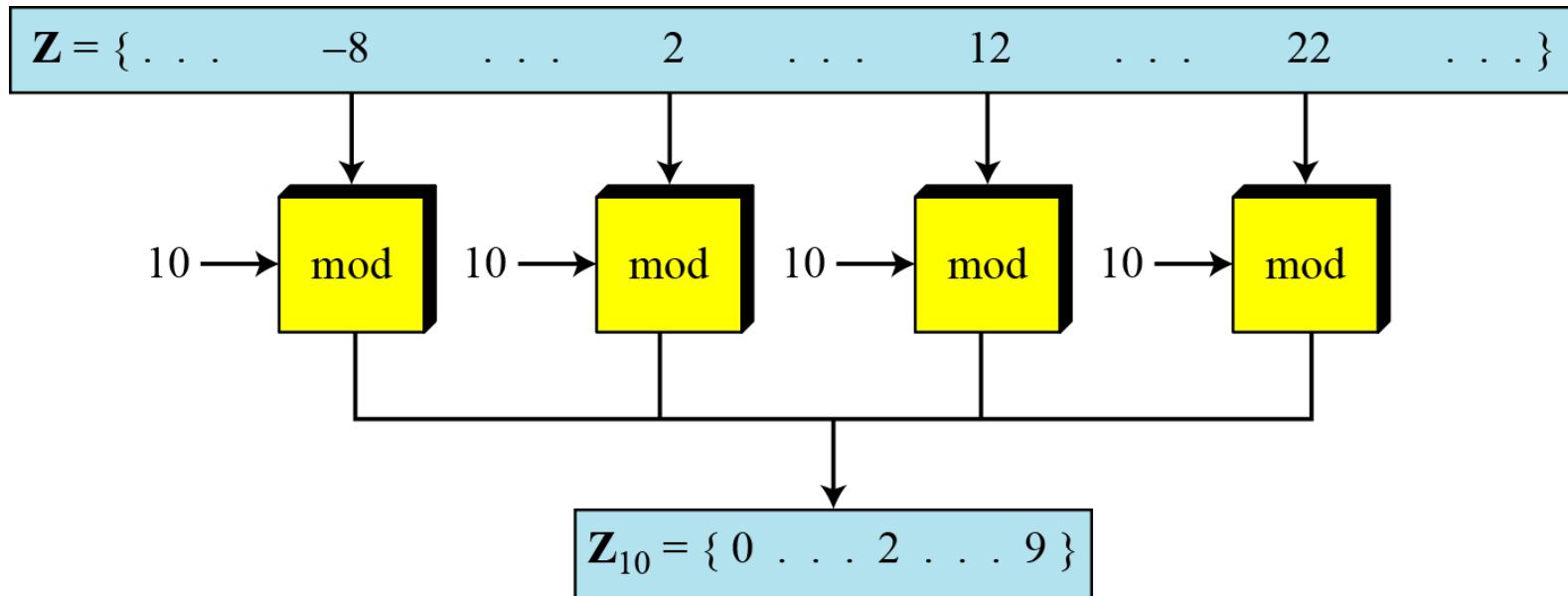
$$3 \equiv 8 \pmod{5}$$

$$13 \equiv 23 \pmod{10}$$

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

2.2.3 *Continued*

Figure 2.11 *Khái niệm về đồng dư*



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

Congruence Relationship

2.2.3 Continued

Residue Classes

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

Lớp dư $[a]$ hoặc $[a]_n$ là tập hợp các số nguyên đồng dư modulo n .

Ví dụ $n = 5$, chúng ta có 5 lớp dư sau đây:

$$[0] = \{ \dots, -15, -10, -5, 0, 5, 10, 15, \dots \}$$

$$[1] = \{ \dots, -14, -9, -4, 1, 6, 11, 16, \dots \}$$

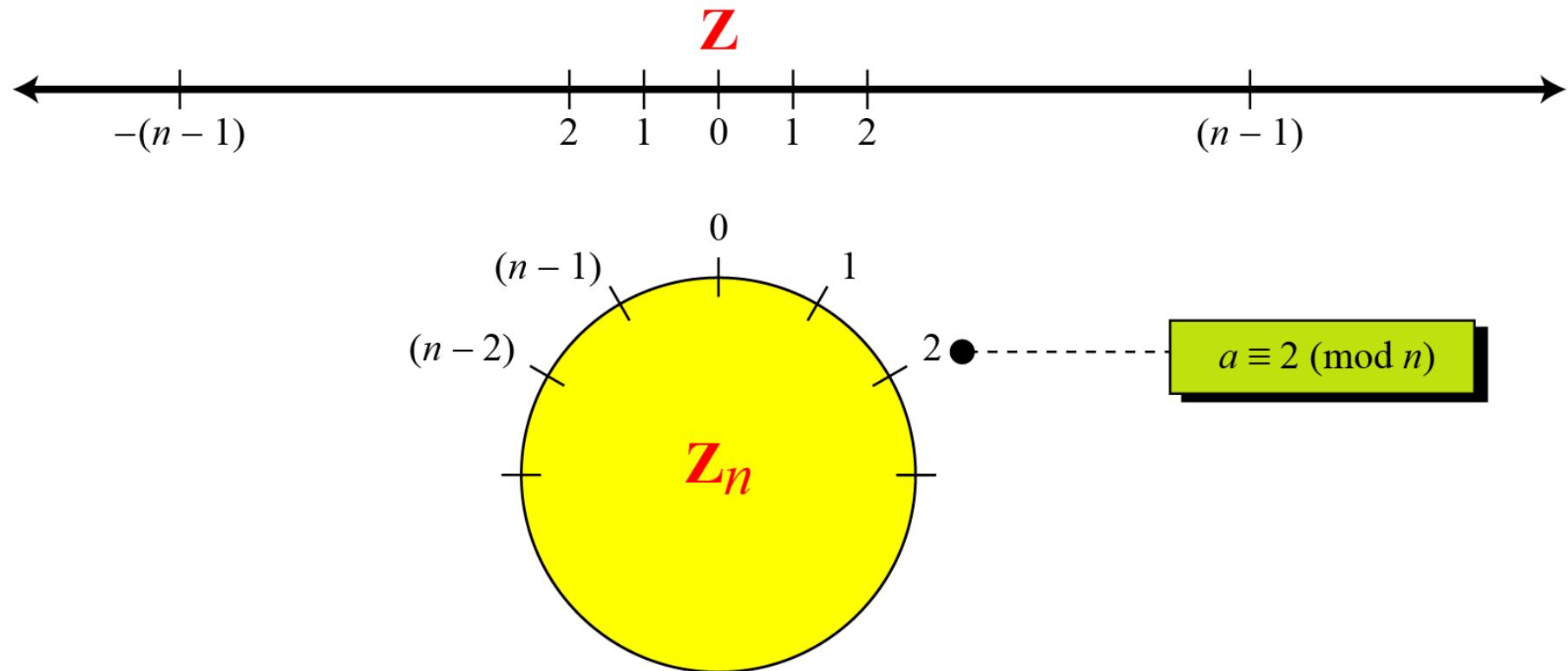
$$[2] = \{ \dots, -13, -8, -3, 2, 7, 12, 17, \dots \}$$

$$[3] = \{ \dots, -12, -7, -5, 3, 8, 13, 18, \dots \}$$

$$[4] = \{ \dots, -11, -6, -1, 4, 9, 14, 19, \dots \}$$

2.2.3 Continued

**Figure 2.12 Comparison of Z and Z_n using graphs
So sánh Z và Z_n bằng đồ thị**



2.2.3 *Continued*

Example 2.15

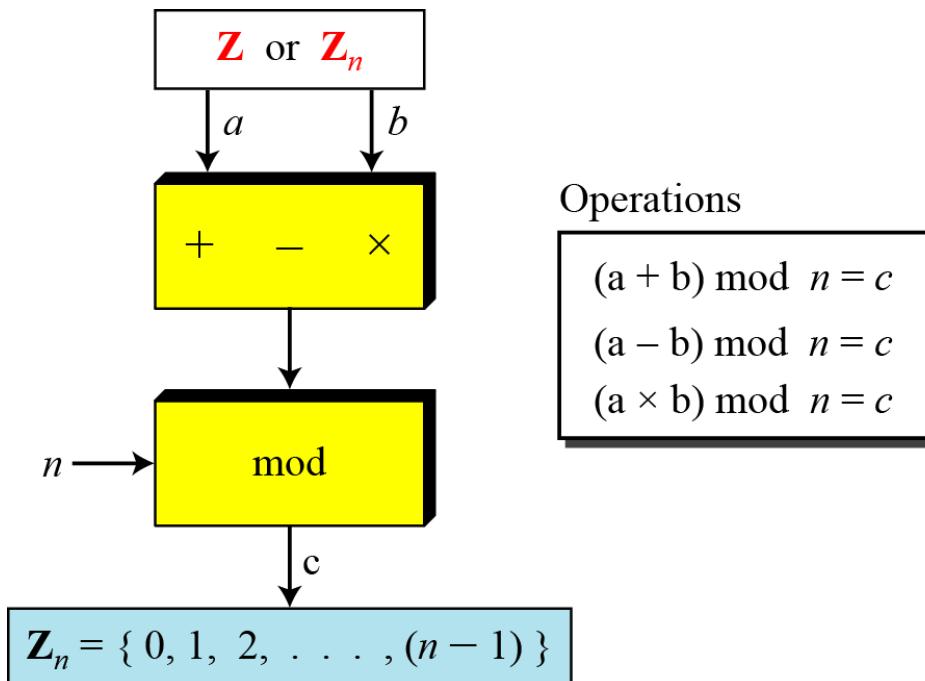
We use modular arithmetic in our daily life; for example, we use a clock to measure time. Our clock system uses modulo 12 arithmetic. However, instead of a 0 we use the number 12.

Chúng ta sử dụng số học mô-đun trong cuộc sống hàng ngày; ví dụ, chúng ta sử dụng đồng hồ để đo thời gian. Hệ thống đồng hồ sử dụng số học modulo 12. Tuy nhiên, thay vì số 0, chúng tôi sử dụng số 12.

2.2.4 Phép toán trong Z_n

Ba phép toán nhị phân mà chúng ta đã thảo luận cho tập Z cũng có thể được xác định cho tập Z_n . Kết quả có thể cần được ánh xạ tới Z_n bằng toán tử mod.

Figure 2.13 Binary operations in Z_n
Phép toán nhị phân trong Z_n



2.2.4 *Continued*

Example 2.16

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

- Add 7 to 14 in Z_{15} .
- Subtract 11 from 7 in Z_{13} .
- Multiply 11 by 7 in Z_{20} .

Solution

$$(14 + 7) \bmod 15 \rightarrow (21) \bmod 15 = 6$$

$$(7 - 11) \bmod 13 \rightarrow (-4) \bmod 13 = 9$$

$$(7 \times 11) \bmod 20 \rightarrow (77) \bmod 20 = 17$$

2.2.4 *Continued*

Example 2.17

Perform the following operations (the inputs come from either Z or Z_n):

- Add 17 to 27 in Z_{14} .
- Subtract 43 from 12 in Z_{13} .
- Multiply 123 by -10 in Z_{19} .

Solution

$$(14 + 7) \bmod 15 \rightarrow (21) \bmod 15 = 6$$

$$(7 - 11) \bmod 13 \rightarrow (-4) \bmod 13 = 9$$

$$(7 \times 11) \bmod 20 \rightarrow (77) \bmod 20 = 17$$

2.2.4 *Continued*

Tính chất

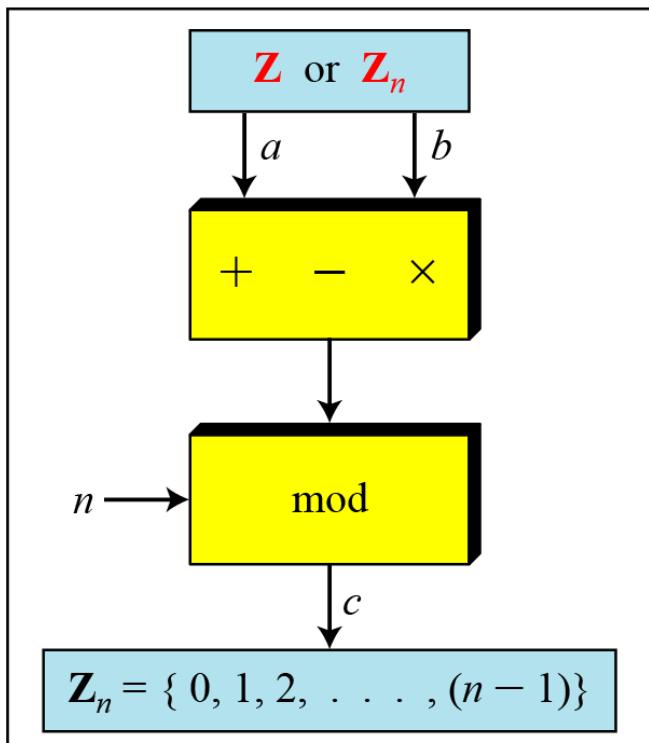
First Property: $(a + b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$

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

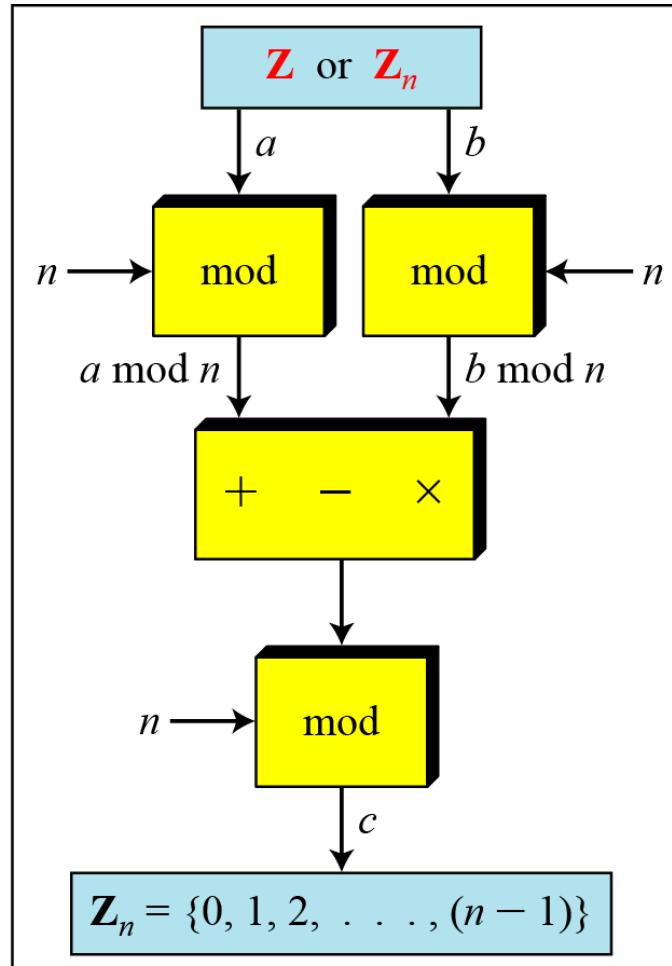
Third Property: $(a \times b) \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n$

2.2.4 Continued

Figure 2.14 Properties of mode operator



a. Original process



b. Applying properties

2.2.4 *Continued*

Example 2.18

The following shows the application of the above properties:

1. $(1,723,345 + 2,124,945) \text{ mod } 11 = (8 + 9) \text{ mod } 11 = 6$
2. $(1,723,345 - 2,124,945) \text{ mod } 11 = (8 - 9) \text{ mod } 11 = 10$
3. $(1,723,345 \times 2,124,945) \text{ mod } 11 = (8 \times 9) \text{ mod } 11 = 6$

$$11^7 \text{ mod } 13 ?$$

2.2.4 *Continued*

Example 2.19

Trong số học, chúng ta thường cần tìm phần dư của các lũy thừa của 10 khi chia cho một số nguyên.

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

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

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

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

2.2.4 Continued

Example 2.20

Chúng ta đã được nói trong số học rằng phần dư của một số nguyên chia cho 3 cũng bằng phần dư của tổng các chữ số thập phân của nó. Chúng ta viết một số nguyên dưới dạng tổng các chữ số của nó nhân với các lũy thừa của 10.

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

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

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

2.2.5 *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).

Khi chúng ta làm việc trong số học mô-đun, chúng ta thường cần tìm nghịch đảo của một số liên quan đến một phép toán. Thông thường chúng ta đang tìm kiếm một phép *nghịch đảo cộng* (liên quan đến phép toán cộng) hoặc phép *nghịch đảo nhân* (liên quan đến phép nhân).

2.2.5 Continue

Additive Inverse: đảo cộng

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

Trong Z_n , hai số a và b là số nghịch đảo cộng của nhau nếu

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

Note

Trong số học mô-đun, mỗi số nguyên có một nghịch đảo cộng. Tổng của một số nguyên và nghịch đảo cộng của nó đồng dư với 0 modulo n.

2.2.5 *Continued*

Example 2.21

Find all additive inverse pairs in Z_{10} .

Tìm tất cả các cặp nghịch đảo cộng trong Z_{10} .

Solution

Sáu cặp đảo ngược cộng tính là:

(0, 0), (1, 9), (2, 8), (3, 7), (4, 6), và (5, 5).

2.2.5 Continue

Multiplicative Inverse: Đảo nhân

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

Trong Z_n , hai số a và b là số nghịch đảo của nhau nếu

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

Note

- Trong số học mô-đun, một số nguyên có thể có hoặc không có một phép nhân nghịch đảo. Khi đó, tích của số nguyên và phép nhân nghịch đảo của nó đồng dư với 1 modulo n .
- Một số nguyên a có nghịch đảo nhân trong Z_n khi và chỉ khi $\gcd(n, a)=1$, tức là a và n là nguyên tố của nhau

2.2.5 *Continued*

Example 2.22

Tìm nghịch đảo nhân của 8 trong Z_{10} .

Solution

Không có phép nhân nghịch đảo vì $\gcd(10, 8) = 2 \neq 1$. Nói cách khác, chúng ta không thể tìm thấy bất kỳ số nào từ 0 đến 9 sao cho khi nhân với 8, kết quả là đồng dư với 1.

Example 2.23

Tìm tất cả các nghịch đảo nhân trong Z_{10} .

Solution

Chỉ có ba cặp: $(1, 1)$, $(3, 7)$ và $(9, 9)$. Các số $0, 2, 4, 5, 6$ và 8 không có phép nhân nghịch đảo.

2.2.5 *Continued*

Example 2.24

Tìm tất cả các cặp nghịch đảo nhân trong Z_{11} .

Solution

We have seven pairs:

$(1, 1)$, $(2, 6)$, $(3, 4)$, $(5, 9)$, $(7, 8)$, $(9, 5)$, and $(10, 10)$.

2.2.5 *Continued*

Note

Thuật toán Euclide mở rộng tìm các nghịch đảo nhân của b trong Z_n khi n và b cho trước và $\gcd(n, b) = 1$.

Nghịch đảo nhân của b là giá trị của t sau khi được ánh xạ vào Z_n .

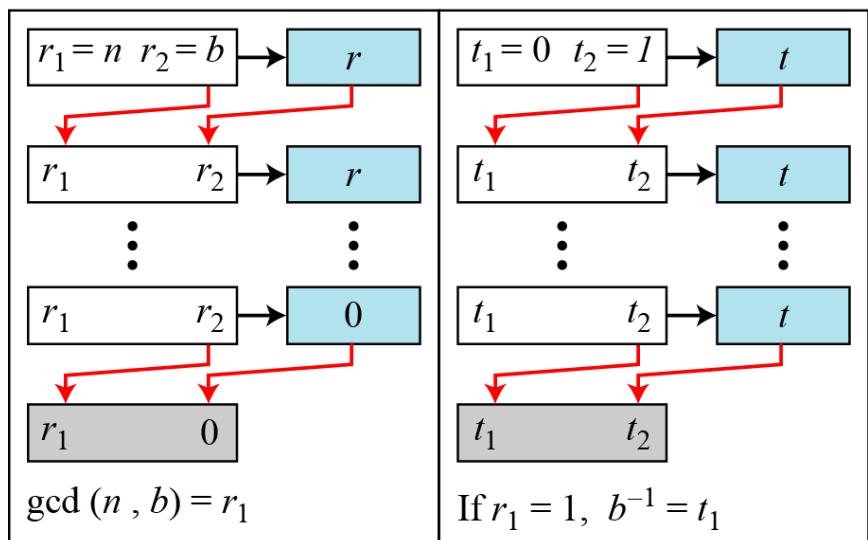
2.2.5 Continued

Figure 2.15

Sử dụng thuật toán Euclid mở rộng để tìm nghịch đảo nhân

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

Nếu tồn tại nghịch đảo nhân của b thì $\gcd(n, b) = 1$



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

2.2.5 *Continued*

Example 2.25

Tìm nghịch đảo nhân của 11 trong \mathbf{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	

Do gcd (26, 11) là 1; nghịch đảo của 11 là $-7 \bmod 26 = 19$.

11 và 19 là nghịch đảo nhân trong \mathbf{Z}_{26} .

Kiểm tra: $(11 \times 19) \bmod 26 = 209 \bmod 26 = 1$

2.2.5 *Continued*

Example 2.26

Find the multiplicative inverse of 23 in \mathbf{Z}_{100} .

Tìm nghịch đảo nhân của 23 trong \mathbf{Z}_{100} .

Solution

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 $-13 \bmod 100 = 87$.

2.2.5 *Continued*

Example 2.27

Find the inverse of 12 in \mathbb{Z}_{26} .

Solution

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.

2.2.6 Addition and Multiplication Tables

Figure 2.16 Addition and multiplication table for \mathbf{Z}_{10}

	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}

2.2.7 *Different Sets*

Figure 2.17 Some Z_n and Z_n^* sets

$$Z_6 = \{0, 1, 2, 3, 4, 5\}$$

$$Z_6^* = \{1, 5\}$$

$$Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$$

$$Z_7^* = \{1, 2, 3, 4, 5, 6\}$$

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

$$Z_{10}^* = \{1, 3, 7, 9\}$$

Note

We need to use Z_n when additive inverses are needed; we need to use Z_n^* when multiplicative inverses are needed.

2.2.8 Two More Sets

Mật mã học thường sử dụng thêm hai tập: Zp và Zp^ .
Môđun trong hai tập hợp này là một số nguyên tố.*

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

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

2-3 MATRICES

Trong mật mã, chúng ta cần xử lý các ma trận. Mặc dù chủ đề này thuộc về một nhánh đặc biệt của đại số gọi là đại số tuyến tính, việc xem xét ngắn gọn về ma trận sau đây là sự chuẩn bị cần thiết cho việc nghiên cứu mật mã.

Topics discussed in this section:

- 2.3.1 Definitions: định nghĩa**
- 2.3.2 Operations and Relations: phép toán**
- 2.3.3 Determinants: định thức**
- 2.3.4 Residue Matrices: ma trận dư**

2.3.1 Definition

Figure 2.18 A matrix of size $\textcolor{red}{l} \times m$

Matrix A:

m columns

$$\begin{matrix} & & & & \\ & & & & \\ & & & & \\ & & & & \\ \textcolor{red}{l} \text{ rows} & \left[\begin{array}{cccc} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \vdots & \vdots & & \vdots \\ \vdots & \vdots & & \vdots \\ a_{l1} & a_{l2} & \dots & a_{lm} \end{array} \right] \end{matrix}$$

2.3.1 *Continued*

Figure 2.19 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

2.3.2 Operations and Relations

Example 2.28

Figure 2.20 shows an example of addition and subtraction.

Figure 2.20 Addition and subtraction of matrices

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

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

2.3.2 Continued

Example 2. 29

Figure 2.21 shows the product of a row matrix (1×3) by a column matrix (3×1). The result is a matrix of size 1×1 .

Figure 2.21 Multiplication of a row matrix by a column matrix

$$\begin{matrix} \text{C} & \text{A} & \text{B} \\ \left[\begin{matrix} 5 & 3 \end{matrix} \right] & = & \left[\begin{matrix} 5 & 2 & 1 \end{matrix} \right] \times \left[\begin{matrix} 7 \\ 8 \\ 2 \end{matrix} \right] \end{matrix}$$


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

2.3.2 *Continued*

Example 2. 30

Figure 2.22 shows the product of a 2×3 matrix by a 3×4 matrix. The result is a 2×4 matrix.

Figure 2.22 *Multiplication of a 2×3 matrix by a 3×4 matrix*

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

2.3.2 *Continued*

Example 2. 31

Figure 2.23 shows an example of scalar multiplication (nhân vô hướng).

Figure 2.23 *Scalar multiplication*

$$\begin{matrix} \mathbf{B} & & \mathbf{A} \\ \left[\begin{matrix} 15 & 6 & 3 \\ 9 & 6 & 12 \end{matrix} \right] & = & 3 \times \left[\begin{matrix} 5 & 2 & 1 \\ 3 & 2 & 4 \end{matrix} \right] \end{matrix}$$

2.3.3 Determinant: định thức

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

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

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

Note

The determinant is defined only for a square matrix.

2.3.3 Continued

Example 2.32

Figure 2.24 shows how we can calculate the determinant of a 2×2 matrix based on the determinant of a 1×1 matrix.

Figure 2.24 Calculating the determinant of a 2×2 matrix

Tính định thức của ma trận 2×2

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

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

2.3.3 Continued

Example 2.33

Figure 2.25 shows the calculation of the determinant of a 3×3 matrix.

Figure 2.25 Calculating the determinant of a 3×3 matrix

$$\det \begin{bmatrix} 5 & 2 & 1 \\ 3 & 0 & -4 \\ 2 & 1 & 6 \end{bmatrix} = (-1)^{1+1} \times 5 \times \det \begin{bmatrix} 0 & -4 \\ 1 & 6 \end{bmatrix} + (-1)^{1+2} \times 2 \times \det \begin{bmatrix} 3 & -4 \\ 2 & 6 \end{bmatrix} + (-1)^{1+3} \times 1 \times \det \begin{bmatrix} 3 & 0 \\ 2 & 1 \end{bmatrix}$$
$$= (+1) \times 5 \times (+4) \quad + \quad (-1) \times 2 \times (24) \quad + \quad (+1) \times 1 \times (3) = -25$$

2.3.4 Inverses: *Nghịch đảo*

Note

Multiplicative inverses are only defined for square matrices.

2.3.5 Residue Matrices: ma trận dư

Cryptography uses residue matrices: matrices where all elements are in Z_n . A residue matrix has a multiplicative inverse if $\gcd(\det(A), n) = 1$.

Mật mã học sử dụng ma trận dư: ma trận trong đó tất cả các nguyên tố đều có trong Z_n . Một ma trận dư có một nghịch đảo nhân nếu $\gcd(\det(A), n) = 1$.

Example 2.34

Figure 2.26 A residue matrix and its multiplicative inverse

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

$$\det(A) = 21$$

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

2-4 LINEAR CONGRUENCE

Mật mã học thường liên quan đến việc giải một phương trình hoặc một hệ phương trình của một hoặc nhiều biến trong Z_n . Phần này chỉ ra cách giải phương trình khi lũy thừa của mỗi biến là 1 (phương trình tuyến tính).

Topics discussed in this section:

- 2.4.1 Single-Variable Linear Equations**
- 2.4.2 Set of Linear Equations**

2.4.1 Phương trình tuyến tính một biến

Phương trình có dạng $ax \equiv b \pmod{n}$ có thể không có nghiệm hoặc có một số nghiệm hữu hạn.

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

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

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

2.4.1 *Continued*

Example 2.35

Solve the equation $10x \equiv 2 \pmod{15}$.

Solution

First we find the gcd (10 and 15) = 5. Since 2 does not divide 5, we have no solution.

Example 2.36

Solve the equation $14x \equiv 12 \pmod{18}$.

Solution

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

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

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

2.4.1 *Continued*

Example 2.37

Solve the equation $3x + 4 \equiv 6 \pmod{13}$.

Solution

First we change the equation to the form $ax \equiv b \pmod{n}$. We add -4 (the additive inverse of 4) to both sides, which give $3x \equiv 2 \pmod{13}$.

Because $\gcd(3, 13) = 1$, the equation has only one solution, which is $x_0 = (2 \times 3^{-1}) \pmod{13} = 18 \pmod{13} = 5$.

We can see that the answer satisfies the original equation:
 $3 \times 5 + 4 \equiv 6 \pmod{13}$.

2.4.2 Single-Variable Linear Equations

Chúng ta cũng có thể giải một hệ các phương trình tuyến tính với cùng một môđun nếu ma trận được tạo thành từ các hệ số của các biến là khả nghịch.

Figure 2.27 Set of linear equations

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

a. Equations

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

b. Interpretation

c. Solution

2.4.2 *Continued*

Example 2.38

Giải bộ ba phương trình sau:

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

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

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

Solution

The result is $x \equiv 15 \pmod{16}$, $y \equiv 4 \pmod{16}$, and $z \equiv 14 \pmod{16}$.

We can check the answer by inserting these values into the equations.