Lecture 2
Basic Number Theory

Jason Lin

學習目標

- 回顧整數算術 (Integer Arithmetic)，特別是整除性 (Divisibility)，並利用輾轉相除法，又稱歐幾里德演算法 (Euclidean Algorithm)，來找出最大公因數 (Greatest Common Divisor)。
- 學習利用歐幾里德延伸演算法來解 Diophantine 線性不定方程式、線性同餘 (Congruence Modulo) 方程式，以及找出乘法反元素 (Multiplicative Inverse)。
- 主要著重在模數算術 (Modular Arithmetic) 和模運算子 (Modulo) 的學習，因為它們在密碼學中被大量地使用。

學習目標 (續)

- 強調並回顧矩陣 (Matrix) 和餘數矩陣 (Residual Matrix) 的運算，因為它們在密碼學中的應用非常廣泛。
- 學習利用餘數矩陣來解同餘 (Congruence) 方程組。

2.1 整數算術

- 在整數算術中，我們使用一個集合和一些運算。
- 或許你對這個集合和運算已經非常熟悉，但為了建立模數算術的背景知識，在此我們還是對整數算術做一個回顧。

2.1 整數算術 (續)

- 在本節討論的主題：
  - 整數集合 (The Set of Integer)
  - 二元運算 (Binary Operation)
  - 整數除法 (Division)
  - 整除性 (Divisibility)
  - 線性 Diophantine 方程式

2.1.1 整數集合

- 整數集合，標記為 *Z*，是從負無窮大到正無窮大的所有整數形成的集合 (圖 2.1)

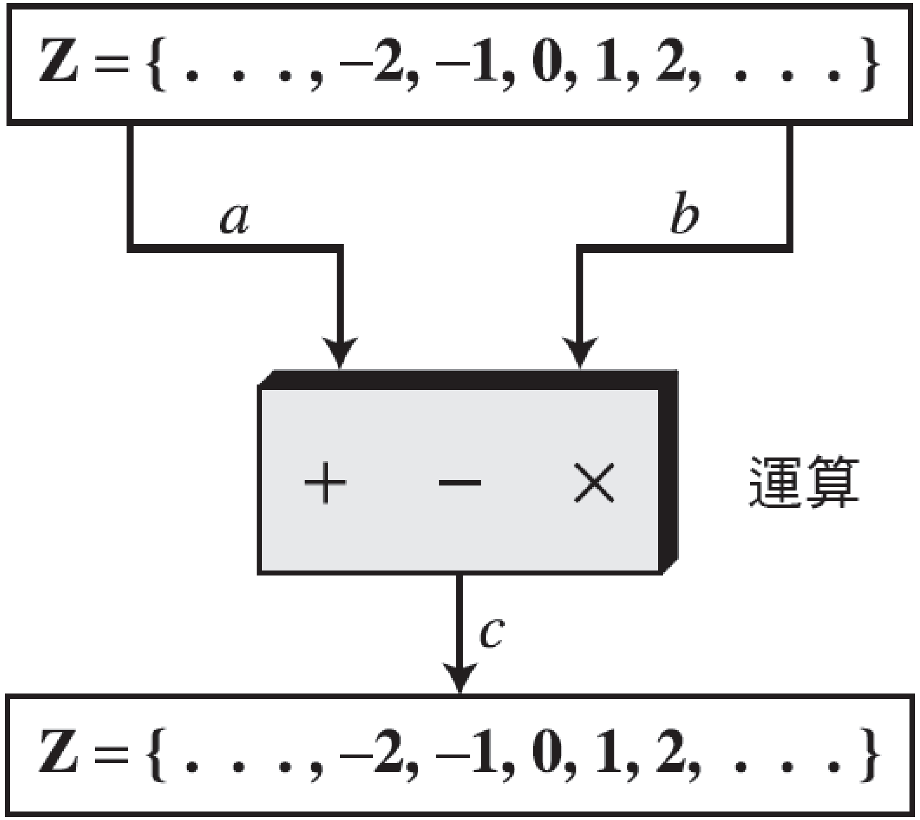
圖 2.1 整數集合

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

2.1.2 二元運算

- 在密碼學中，我們感興趣的是三種作用於整數集合的二元運算 (Binary Operation)。
- 二元運算可接受兩個輸入值 (Input)，然後產生一個輸出值 (Output)。

圖 2.2 三種作用在整數集合上的二元運算



範例 2.1

- 下列的例子顯示出三種二元運算作用於兩個整數後所產生的結果。由於每個輸入值均可為正值或負值，因此，對於每一種運算我們討論四種情形。

加：	$5 + 9 = 14$	$(-5) + 9 = 4$	$5 + (-9) = -4$	$(-5) + (-9) = -14$
減：	$5 - 9 = -4$	$(-5) - 9 = -14$	$5 - (-9) = 14$	$(-5) - (-9) = +4$
乘：	$5 \times 9 = 45$	$(-5) \times 9 = -45$	$5 \times (-9) = -45$	$(-5) \times (-9) = 45$

2.1.3 整數除法

- 在整數算術中，如果我們使用 n 來除 a，可以得到 q 和 r。
- 這四個整數之間的關係可以表示為：

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

範例 2.2

- 假設 $a = 255$ 且 $n = 11$，利用過去所學的除法算術，我們可以得到 $q = 23$ 且 $r = 2$。

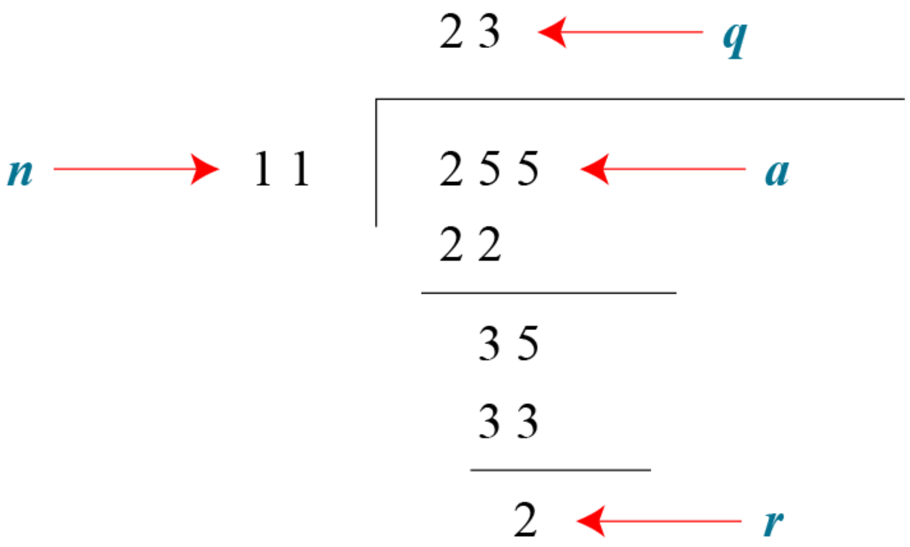
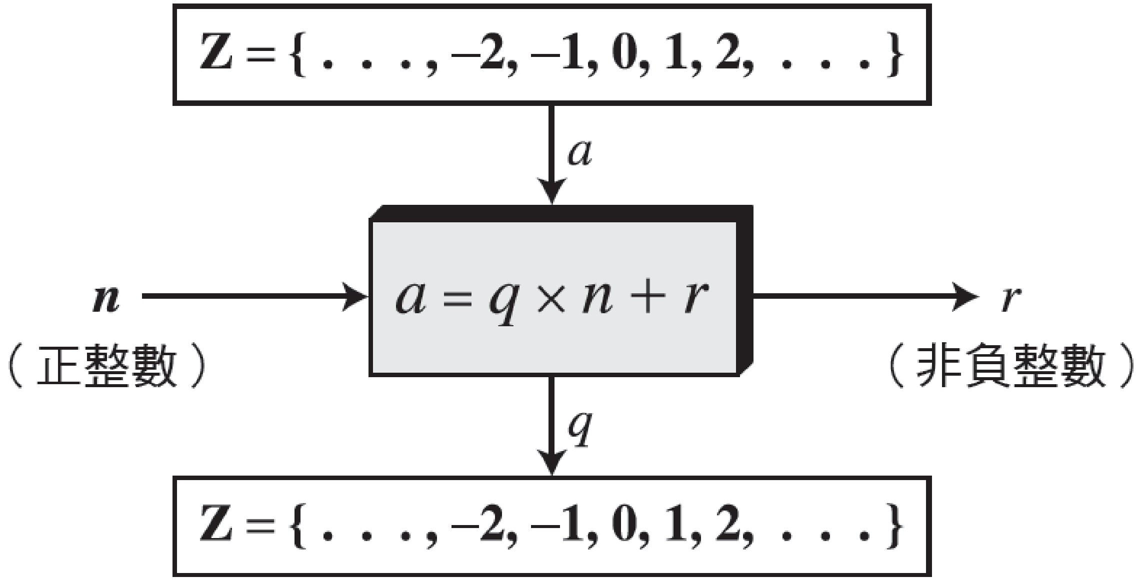


圖 2.3 整數的除法演算法

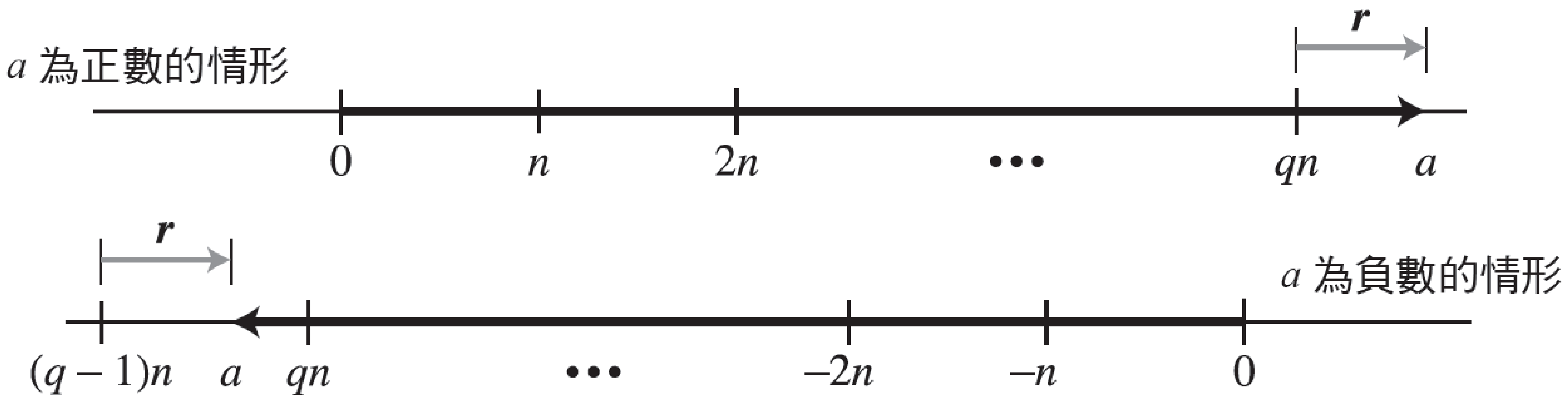


範例 2.3

- 當我們使用電腦或計算機計算除法時，若 a 為負數，則 r 和 q 也為負數。我們要如何根據限制讓 r 變為正數呢？
  - 很簡單，我們只要將 q 值減 1，並且將 r 值加 n ，就可以讓 r 變成正數。

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

圖 2.4 除法演算法的圖形



2.1.4 整除性

- 在一個除法關係中，如果 a 不為 0 且令 $r = 0$，則可以得到：

$$a = q \times n$$

若餘數為零，則 $n|a$

若餘數不為零，則 $n\nmid a$

範例 2.4

- 整數 4 可以整除 32，因為 $32 = 8 \times 4$。
  我們將此關係表示成 $4|32$

- 整數 8 無法整除 42，因為 $42 = 5 \times 8 + 2$，所以此方程式的餘數為 2。我們將此關係表示成 $8 \nmid 42$

範例 2.5

- 我們可以得到 $13|78, 7|98, -6|24, 4|44$ 以及 $11|(-33)$。
- 我們可以得到 $13 \nmid 27, 7 \nmid 50, -6 \nmid 23, 4 \nmid 41$ 以及 $11 \nmid (-32)$。

2.1.4 整除性 (續)

性質1：若 $a|1$，則 $a = \pm 1$。

性質2：若 $a|b$ 且 $b|a$，則 $a = \pm b$。

性質3：若 $a|b$ 且 $b|c$，則 $a|c$。

性質4：若 $a|b$ 且 $a|c$，則 $a|(m \times b + n \times c)$，
其中 m 和 n 為任意整數。

範例 2.6

- 因為 $3|15$ 且 $15|45$，根據**性質3**，我們得到 $3|45$。
- 因為 $3|15$ 且 $3|9$，根據**性質4**，$3|(15 \times 2 + 9 \times 4)$，亦即 $3|66$。

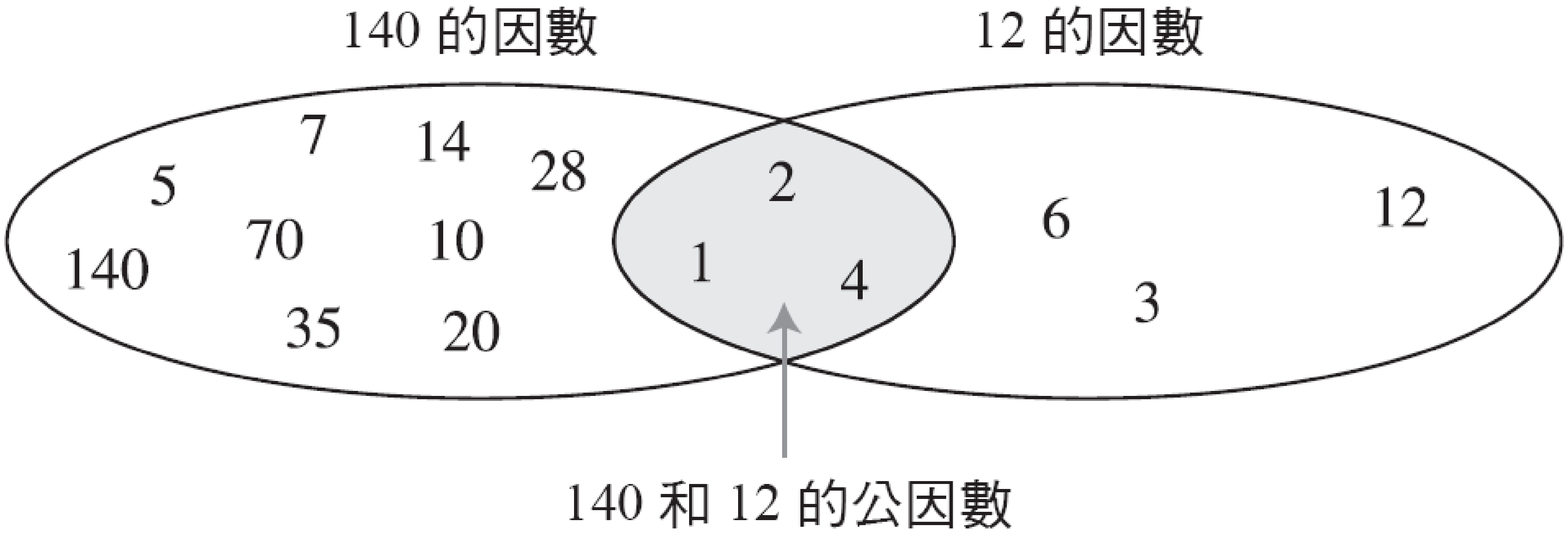
2.1.4 整除性 (續)

注意

事實1：整數 1 只有一個因數 (Divisor)，就是它自己

事實2：任何整數至少有 2 個因數，1 和它自己（但也可能有更多其他因數）

圖 2.5 兩個整數的公因數



2.1.4 整除性 (續)

注意　**最大公因數 (Greatest Common Divisor，GCD)**

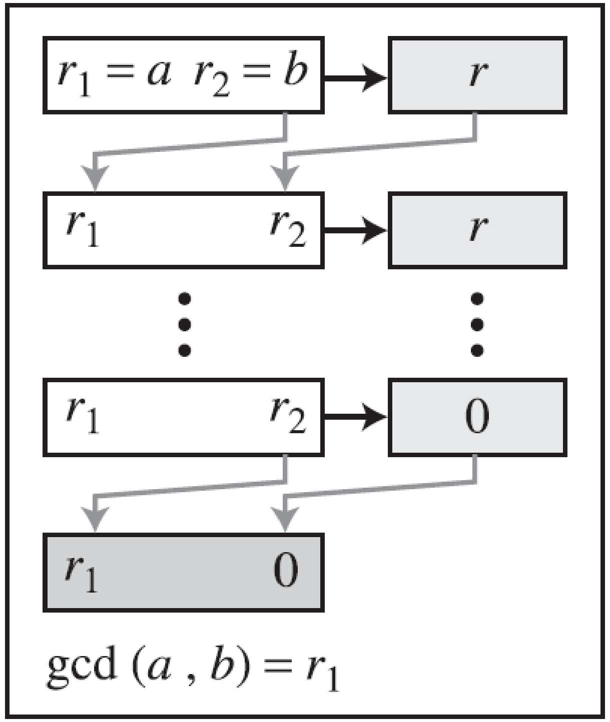
兩個整數的最大公因數為所有能整除這兩個整數之最大整數。

注意　**歐幾里德演算法 (Euclidean Algorithm)**

事實1：$\gcd(a, 0) = a$。

事實2：$\gcd(a, b) = \gcd(b, r)$, 其中 r 是 a 除以 b 的餘數。

圖 2.6 歐幾里德演算法



a. 流程

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

  gcd (a, b) ← r1
```

b. 演算法

2.1.4 整除性 (續)

注意

當 $\gcd(a, b) = 1$ 時，我們說 a 和 b 為互質 (Relatively Prime)。

範例 2.7

- 試求 2740 和 1760 的最大公因數。
- 解法：我們得到 $\gcd(2740, 1760) = 20$。

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	

範例 2.8

- 試求 25 和 60 的最大公因數。
- 解法：我們得到 $\gcd(25, 60) = 5$。

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

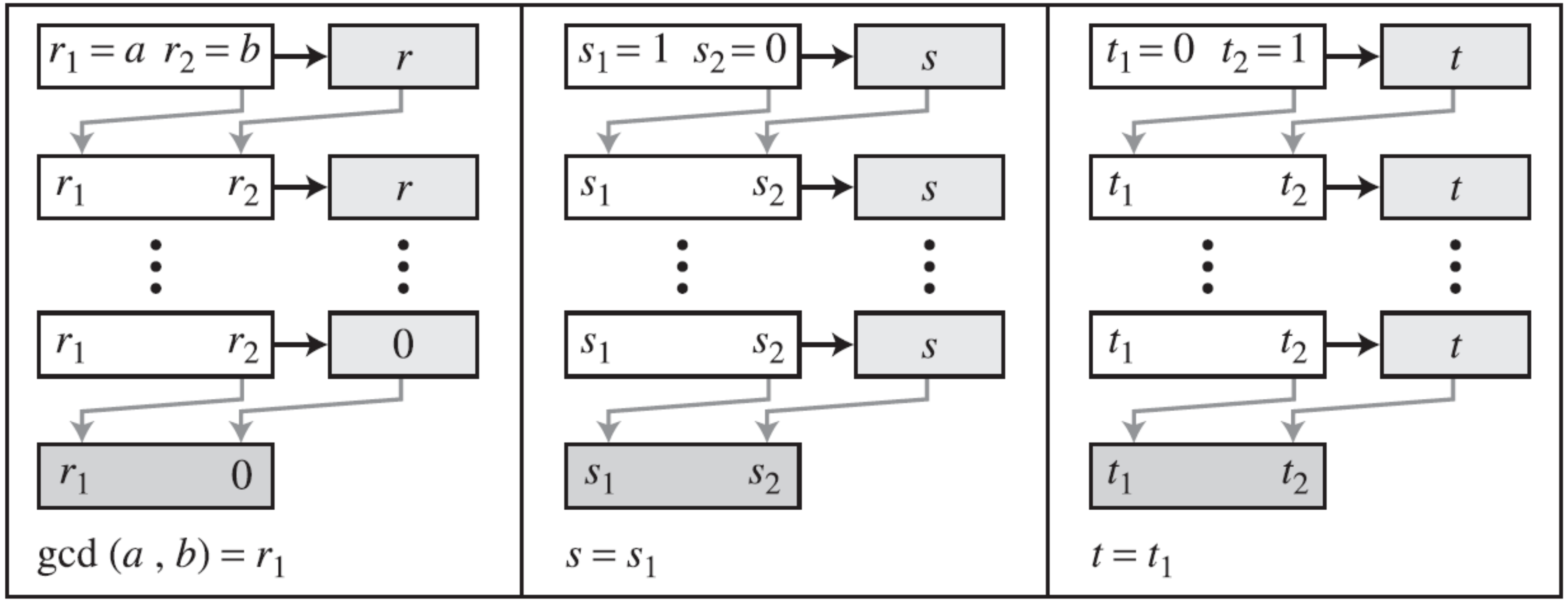
歐幾里德延伸演算法

- 給定兩個整數 a 和 b，我們時常需要去找出另外兩個整數 s 和 t，使得

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

- 歐幾里德延伸演算法可以同時計算出 $\gcd(a, b)$ 以及 s 和 t 的值。

圖 2.7 歐幾里德延伸演算法



a. 流程

圖 2.8 歐幾里德延伸演算法 (續)

```
r₁ ← a; r₂ ← b;
s₁ ← 1; s₂ ← 0;          (Initialization)
t₁ ← 0; t₂ ← 1;
while (r₂ > 0)
 {
  q ← r₁ / r₂;
   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. 演算法

範例 2.9

- 給定 $a = 161$ 和 $b = 28$，求出 $\gcd(a, b)$ 以及 s 和 t 的值。
- 解法：我們得到 $\gcd(161, 28) = 7$，$s = -1$ 和 $t = 6$。

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	

範例 2.10

- 給定 $a = 17$ 和 $b = 0$，求出 $\gcd(a, b)$ 以及 s 和 t 的值。
- 解法：我們得到 $\gcd(17, 0) = 17$，$s = 1$ 和 $t = 0$。

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

範例 2.11

- 給定 $a = 0$ 和 $b = 45$，求出 $\gcd(a, b)$ 以及 s 和 t 的值。
- 解法：我們得到 $\gcd(0, 45) = 45$，$s = 0$ 和 $t = 1$。

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	

2.1.5 線性 Diophantine 方程式

注意

雙變數之 Diophantine 方程式是一種形態為 $ax + by = c$ 的線性不定方程式。

注意

特解：

$x_0 = (c/d)s$ 和 $y_0 = (c/d)t$，其中 $d = \gcd(a, b)$

2.1.5 線性 Diophantine 方程式 (續)

注意

通解：

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

其中 k 為整數

範例 2.12

- 求出方程式 $21x + 14y = 35$ 的特解和通解。
- 解法：

特解：$x_0 = 5 \times 1 = 5$ 和 $y_0 = 5 \times (-1) = -5$	因為 $35/7 = 5$
通解：$x = 5 + k \times 2$ 和 $y = -5 - k \times 3$	其中 k 為整數

範例 2.13

- 舉例來說，我們要把 100 美元的支票兌換成一些由 20 美元和 5 美元的鈔票。利用求解線性 Diophantine 方程式 $20x + 5y = 100$ ，可以找出許多不同的兌換方式。因為 $d = \gcd(20, 5) = 5$，而且 $5|100$，此方程式有無限多解，但本例中，這些解中只有少數是合理的 (x 值和 y 值必須同時為非負整數解)。
  - 這條方程式之非負整數的通解為 (0, 20), (1, 16), (2, 12), (3, 8), (4, 4), (5, 0)

2.2 模數算術

- 前一節所討論的除法關係 ($a = q \times n + r$) 有兩個輸入值 (a 和 n) 以及兩個輸出值 (q 和 r)。
- 在模數算術中，我們只對其中一個輸出值餘數 r 感興趣。

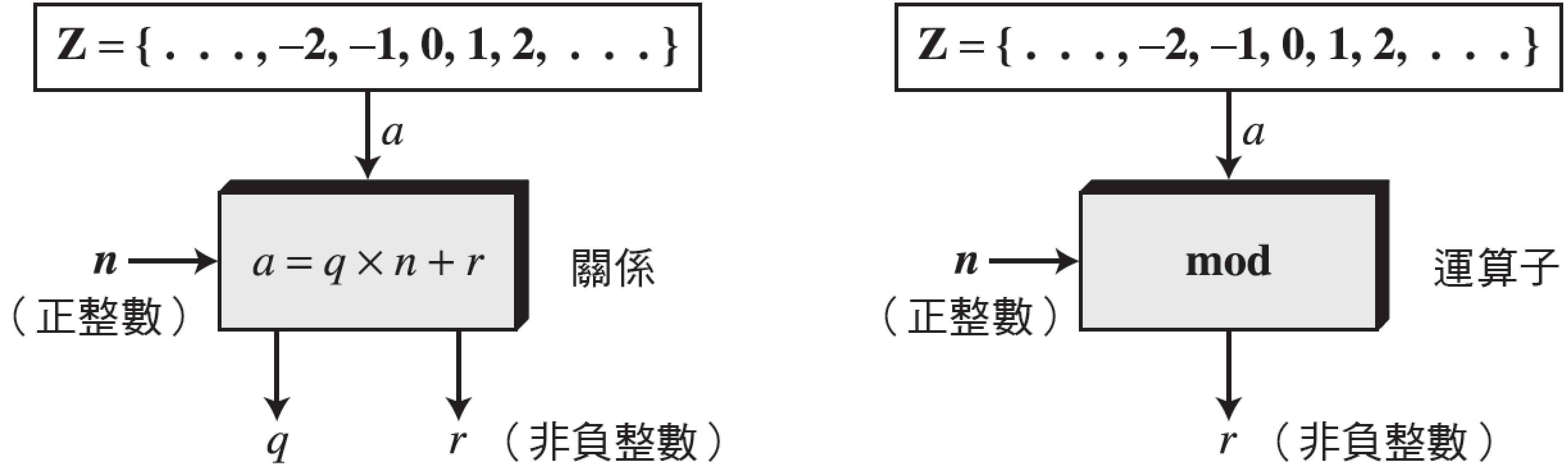
2.2 模數算術 (續)

- 本節所探討的主題包含：
  - 模運算子 (Modulo)
  - 餘數集合：Z_n
  - 同餘 (Congruence)
  - Z_n下的運算
  - 反元素 (Inverse)
  - 加法表和乘法表
  - 加法和乘法的不同集合
  - 另外兩種集合

2.2.1 模運算子

- 模運算子 (Modulo Operator)，符號為 **mod**。第二個輸入值 (n) 稱為模數 (Modulus) ，輸出值 r 則被稱為餘數 (Residue/Remainder)。

圖 2.9 除法關係與模運算子



範例 2.14

- 求解下列運算式：

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

■ 解法

- 27 除以 5 可得 $r = 2$。
- 36 除以 12 可得 $r = 0$ 。
- -18 除以 14 可得 $r = -4$，而 -4 加上模數之後，$r = 10$。
- -7 除以 10 可得 $r = -7$，而 -7 加上模數之後，$r = 3$。

2.2.2 餘數集合：Z_n

- 模數運算會產生一個集合，此集合在模數算數中被稱為模 n 之最小餘數集合 (Set of Least Residues Modulo n)，或記為 Z_n。

圖 2.10 一些 Z_n 的集合

$$\boxed{Z_n = \{ 0, 1, 2, 3, \ldots, (n-1) \}}$$

$$\boxed{Z_2 = \{ 0, 1 \}} \quad \boxed{Z_6 = \{ 0, 1, 2, 3, 4, 5 \}} \quad \boxed{Z_{11} = \{ 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 \}}$$

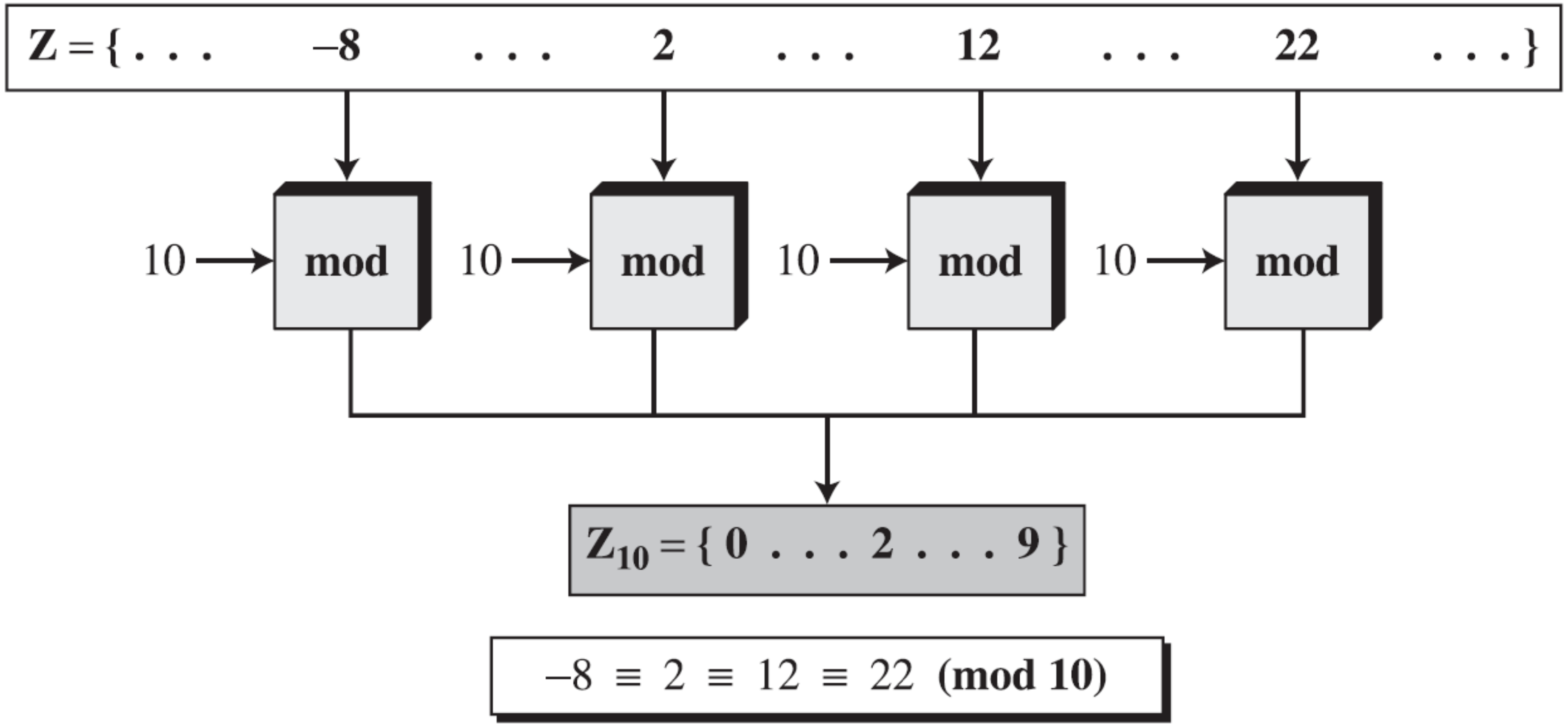
2.2.3 同餘

- 我們使用同餘運算子 (≡)來表示兩個整數是同餘的。舉例來說，我們寫出：

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

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

圖 2.11 同餘的概念



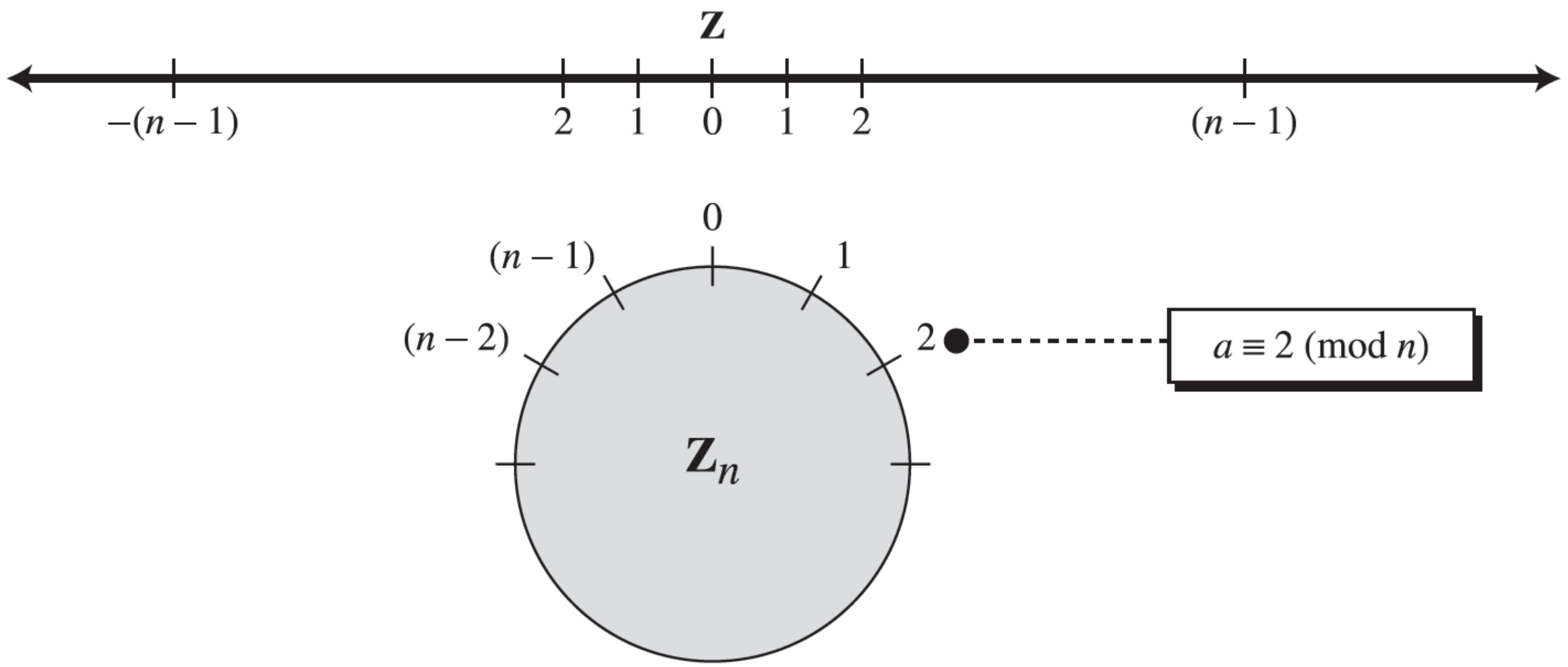
同餘關係

剩餘類

- 剩餘類 (Residue Class) $[a]$ 或 $[a]_n$，是一個在模 n 之下所有餘數為 a 的整數集合。

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

圖 2.12 利用圖形來比較 Z 和 Z_n



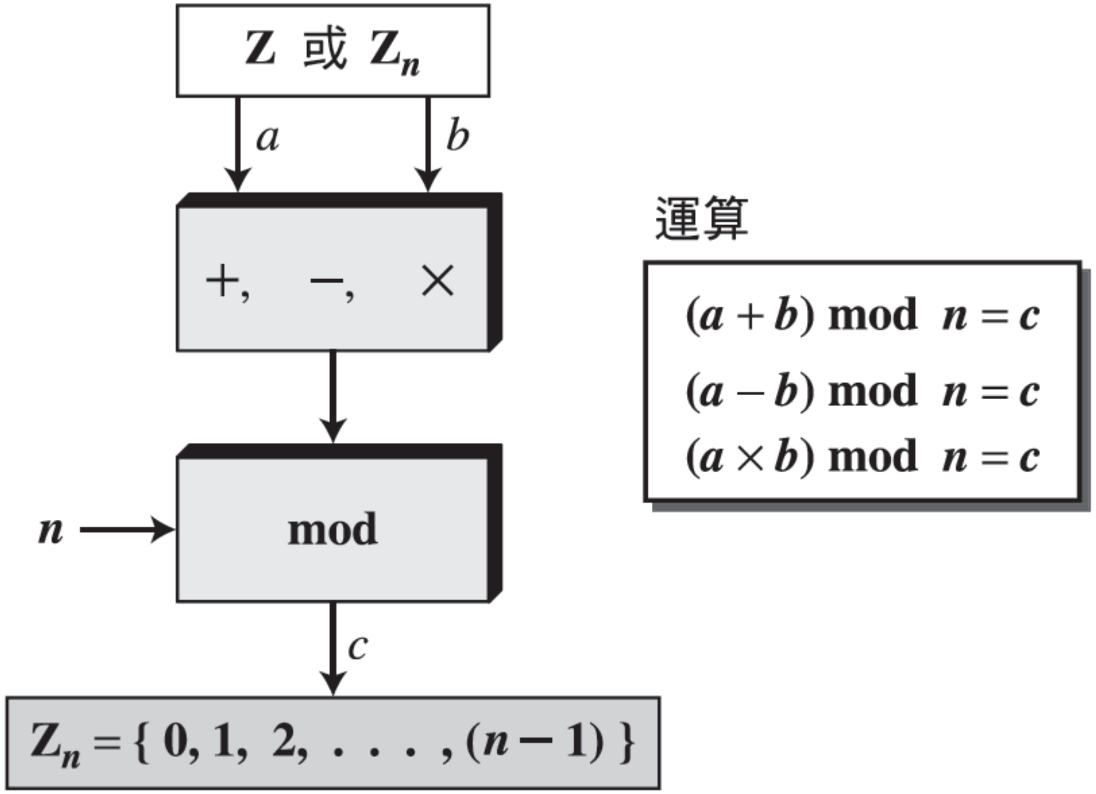
範例 2.15

- 日常生活都會用到模數算術，例如使用時鐘來測量時間，其系統是模數為 12 的算術。然而，在時鐘系統中，我們會使用數字 12 來代替 0，所以時鐘系統會從 0 (或 12) 開始前進，直到 11 為止。因為一天是 24 小時，因此會沿著時鐘的圓形循環兩次，並且把第一次的循環記為 A.M.，然後把第二次的循環記為 P.M.。

2.2.4 Z_n下的運算

- 我們之前討論集合 Z 中的三個運算 (加法、減法和乘法) 也可以在集合 Z_n 中定義。
- 這些運算的結果可能需要使用模運算子將其對應到 Z_n 中。

圖 2.13 Z_n 中的二元運算



範例 2.16

- 計算下列各運算式 (輸入值為 Z_n 中的元素)：
  a. 在 Z_{15} 中計算 14 加 7。
  b. 在 Z_{13} 中計算 7 減 11。
  c. 在 Z_{20} 中計算 7 乘 11。
- 解法

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

範例 2.17

- 計算下列各運算式 (輸入值為 Z 或 Z_n 中的元素)：
  a. 在 Z_{14} 中計算 17 加 27。
  b. 在 Z_{13} 中計算 12 減 43。
  c. 在 Z_{19} 中計算 123 乘 -10。
- 解法

2.2.4 Z_n下的運算 (續)

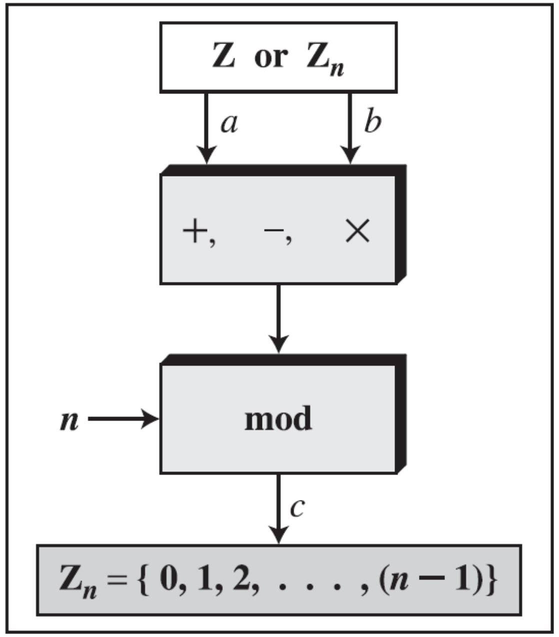
- 性質

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

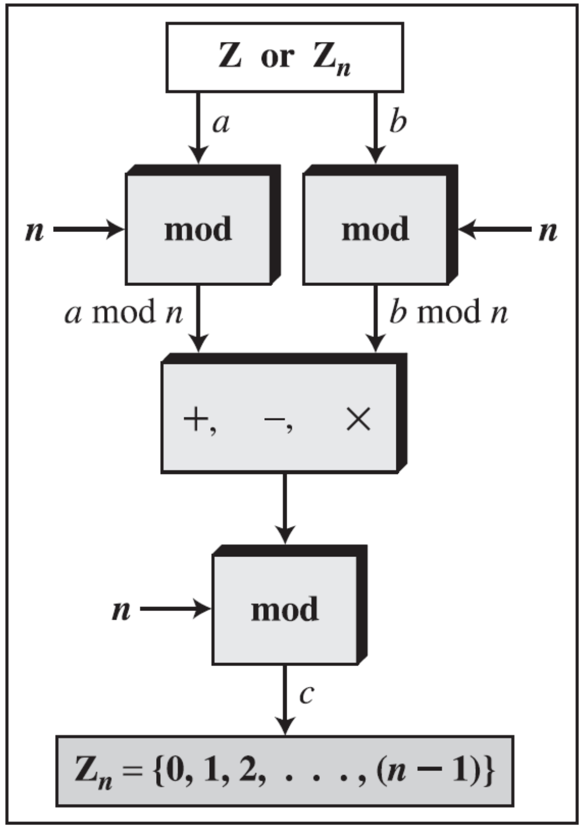
性質 2： $(a - b) \bmod n = [(a \bmod n) - (b \bmod n)] \bmod n$

性質 3： $(a \times b) \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n$

圖 2.14 模運算子的性質



a. 原始的計算流程



b. 應用性質後的計算流程

範例 2.18

- 下列運算式顯示出如何應用上述性質：

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

範例 2.19

- 在算術中，我們經常需要計算10 的冪次方除以某個整數所得之餘數。

$10^n \bmod x = (10 \bmod x)^n$ 使用 n 次性質 3。

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

範例 2.20

- 我們在過去被教導過，算術中一個整數除以 3 的餘數，和其每一位數之總和除以 3 的餘數是相同的。我們可以使用模運算子的性質來證明這個宣稱。我們先將整數改寫成每一個位數乘以 10 的冪次方之總和。

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

舉例來說：$6371 = 6 \times 10^3 + 3 \times 10^2 + 7 \times 10^1 + 1 \times 10^0$

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

2.2.5 反元素

- 當使用模數算術時，我們經常需要在某種運算下求出一個數值的反元素 (Inverse)。
- 通常會在加法運算之下尋找某數的加法反元素 (Additive Inverse)，或者在乘法運算之下尋找某數的乘法反元素 (Multiplicative Inverse)。

加法反元素

- 在 Z_n 中，兩數 a 和 b 互為對方的加法反元素若 $a + b \equiv 0 \pmod{n}$

注意

在模數算術中，每個整數都有加法反元素。
一個整數和其加法反元素之和，在模 n 下與 0 同餘。

範例 2.21

- 試求出 Z_{10} 中所有互為加法反元素的數對。
- 解法：加法反元素的六個數對分別為 (0, 0), (1, 9), (2, 8), (3, 7), (4, 6), 和 (5, 5)。

乘法反元素

- 在 Z_n 中，兩數 a 和 b 互為對方的乘法反元素若

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

注意

在模數算術中，一個整數不一定有乘法反元素。
若一個整數有乘法反元素，則該整數和其乘法反元素的乘積必定在模 n 下與 1 同餘。

範例 2.22

- 試求 8 在 Z_{10} 中的乘法反元素。
- 解法：
  - 乘法反元素是不存在的，因為 $\gcd(10,8)=2\neq 1$。換句話說，在 0 到 9 之間，我們無法找出一個整數使其和 8 相乘後，結果和 1 同餘。

範例 2.23

- 試求在 Z_{10} 中所有的乘法反元素。
- 解法：
  - 在 Z_{10} 中只有三對乘法反元素：(1, 1), (3, 7) 和 (9, 9)。數值 0, 2, 4, 5, 6, 和 8 沒有乘法反元素。

範例 2.24

- 試求在 Z_{11} 中所有的乘法反元素。
- 解法：
  - 我們得到 6 對乘法反元素：(1, 1), (2, 6), (3, 4), (5, 9), (7, 8), 和 (10, 10)。

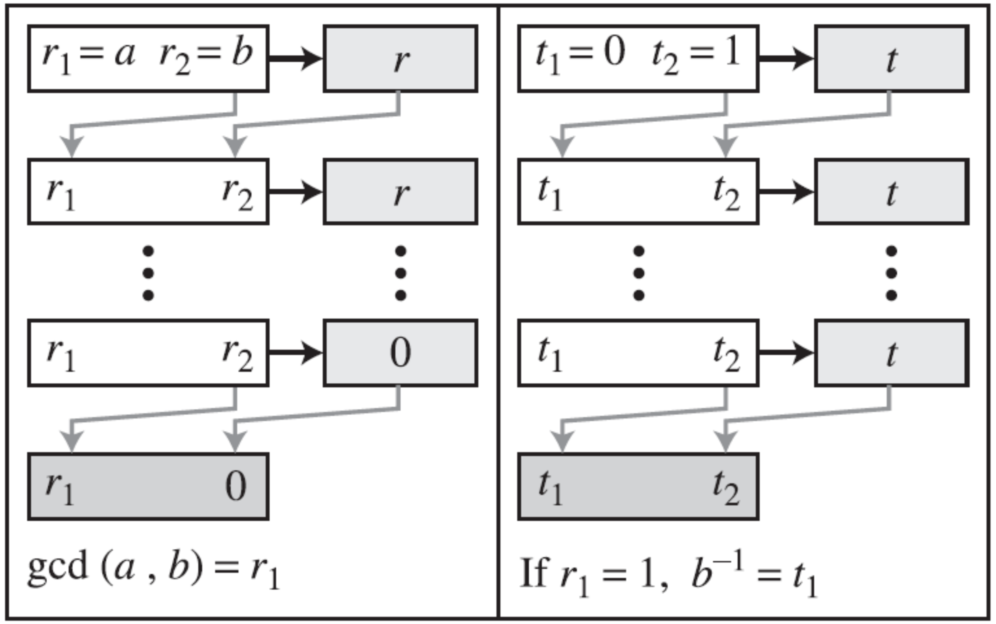
2.2.5 反元素 (續)

注意

給定整數 n 和 b，且 $\gcd(n, b) = 1$，歐幾里德延伸演算法可以求出 b 在 Z_n 中的乘法反元素。

b 的乘法反元素為 t 對應到 Z_n 後所得到的數值。

圖 2.15 利用歐幾里德延伸演算法來求出乘法反元素



a. 流程

```
r₁ ← n; r₂ ← b;
t₁ ← 0; t₂ ← 1;

while (r₂ > 0)
 {
  q ← r₁ / r₂;

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

   t  ← t₁ − q × t₂;
   t₁ ← t₂;   t₂ ← t;
 }
  if (r₁ = 1) then b⁻¹ ← t₁
```

b. 演算法

範例 2.25

- 試求 11 在 Z_{26} 中的乘法反元素。
- 解法：

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	

$\gcd(26, 11) = 1$; 11 的乘法反元素為 -7 或 19。

範例 2.26

- 試求 23 在 Z_{100} 中的乘法反元素。
- 解法：

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	

$\gcd(100, 23) = 1;\ 23$的乘法反元素為 -13 或 87。

範例 2.27

- 試求 12 在 Z_{26} 中的乘法反元素。
- 解法：

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	

$\gcd(26, 12) = 2$; 乘法反元素不存在。

圖 2.16 Z_{10} 的加法表和乘法表

+	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

Z_{10} 的加法表

×	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

Z_{10} 的乘法表

圖 2.17 一些 Z_n 和 Z_{n^*} 的集合

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

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

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

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

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

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

2.2.7 加法和乘法的不同集合

注意

當需要加法反元素時，我們使用集合 Z_n；
當需要乘法反元素時，我們使用集合 Z_{n^*}。

2.2.8 另外兩種集合

- 密碼學常常使用另外兩種集合：Z_p 和 Z_{p^*}。
- 這兩種集合所使用的模數都是質數 (prime)。

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

2.3 矩陣

- 在密碼學中，我們有時會用到矩陣（Matrix）。雖然這個主題是屬於代數中的一個分支—線性代數，但為了有助於學習矩陣在密碼學中的應用，以下將簡單地回顧矩陣。

2.3 矩陣 (續)

- 本節所探討的主題包含：
  - 定義
  - 運算和關係式
  - 行列式
  - 反矩陣
  - 餘數矩陣

圖 2.18 一個大小為 $l \times m$ 的矩陣

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

圖 2.19 一些矩陣的範例

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

列矩陣

$$\begin{bmatrix} 2 \\ 4 \\ 12 \end{bmatrix}$$

行矩陣

$$\begin{bmatrix} 23 & 14 & 56 \\ 12 & 21 & 18 \\ 10 & 8 & 31 \end{bmatrix}$$

方陣

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}$$

$\mathbf{0}$

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$\mathbf{I}$

範例 2.28

- 圖 2.20 顯示出一些加法和減法的範例。

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

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

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

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

範例 2.29

- 圖 2.21 顯示一個 (1 × 3) 矩陣和一個 (3 × 1) 矩陣的乘積，結果是一個大小為 1 × 1 的矩陣。

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

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

範例 2.30

- 圖 2.22 顯示一個 (2 × 3) 矩陣和一個 (3 × 4) 矩陣的乘積，結果是一個大小為 2 × 4 的矩陣。

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

範例 2.31

- 圖 2.23 顯示純量乘法的一個範例。

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

2.3.3 行列式

- 一個大小為 $m \times m$ 的方陣 A ，其行列式 (determinant) 標記為 $\det(A)$，是一個可利用下列遞迴式計算所得之純量：
  1. 若 $m = 1$，則 $\det(A) = a_{11}$
  2. 若 $m > 1$，則 $\det(A) = \sum_{j=1\ldots m}(-1)^{i+j} \times a_{ij} \times \det\left(A_{ij}\right)$

其中，A_{ij} 是一個由 A 刪除掉第 i 列和第 j 行所得的矩陣。

2.3.3 行列式 (續)

注意

只有方陣具有行列式。

範例 2.32

- 圖 2.24 顯示我們如何利用上述的遞迴式和 1 × 1 矩陣的行列式，來計算 2 × 2 矩陣的行列式。

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

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

範例 2.33

- 圖 2.25 顯示如何計算 3×3 矩陣的行列式。

$$\det\begin{bmatrix}5 & 2 & 1\\3 & 0 & -4\\2 & 1 & 6\end{bmatrix} = (-1)^{1+1} \times 5 \times \det\begin{bmatrix}0 & -4\\1 & 6\end{bmatrix} + (-1)^{1+2} \times 2 \times \det\begin{bmatrix}3 & -4\\2 & 6\end{bmatrix} + (-1)^{1+3} \times 1 \times \det\begin{bmatrix}3 & 0\\2 & 1\end{bmatrix}$$
$$= (+1) \times 5 \times (+4) + (-1) \times 2 \times (26) + (+1) \times 1 \times (3) = -29$$

2.3.4 反矩陣 (Inverse Matrix)

- 如果矩陣 A 可逆，則存在 A 的反矩陣 A^{-1}，使得 $A^{-1}A = AA^{-1} = I$，其中 I 為單位矩陣。
- Ex.,

$$A = \begin{bmatrix} 3 & 2 \\ 1 & -1 \end{bmatrix}, A^{-1} = \frac{1}{-5}\begin{bmatrix} -1 & -2 \\ -1 & 3 \end{bmatrix}$$

注意

乘法反矩陣只在方陣有定義。

2.3.5 餘數矩陣 (Residual Matrix)

- 在密碼學上我們使用餘數矩陣：所有元素皆定義在 Z_n 中的矩陣。
- 若 $\gcd(\det(A), n) = 1$，則該餘數矩陣具有乘法反矩陣。

圖 2.26 一個餘數矩陣和其乘法反矩陣

- 令 A 是定義在 Z_{26} 中的矩陣。

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

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

2.4 線性同餘

- 在密碼學中，我們常常會需要在 Z_n 中去解單變數或者多變數的方程式或是方程組。
- 本節將討論如何解變數為 1 次方的線性方程式。

2.4.1 單變數線性方程式

- 型式為 $ax \equiv b \pmod{n}$ 的方程式可能為無解或是有限個數的解。

- 假設 $\gcd(a, n) = d$
  - 如果 $d \nmid b$，則無解。
  - 如果 $d \mid b$，則有 d 個解。

- 若 x_0 為方程式的一個解，則所有的解可表示如下：
  - $\{x_0 + k\frac{n}{d} \mid k \in \mathbb{Z}\}$。

範例 2.35

- 求解方程式 $10x \equiv 2 \pmod{15}$。
- 解法：
  - 首先求出 $\gcd(10, 15) = 5$。
  - 因為 5 不能整除 2，所以此方程式無解。

範例 2.36

- 試解出方程式 $14x \equiv 12 \pmod{18}$。
- 解法：

$$14x \equiv 12 \pmod{18} \rightarrow \quad 7x \equiv 6 \pmod{9} \quad \rightarrow \; x \equiv 6\ (7^{-1}) \pmod{9}$$
$$x_0 = (6 \times 7^{-1}) \bmod 9 = (6 \times 4) \pmod{9} = 6$$
$$x_1 = x_0 + 1 \times (18/2) = 15$$

範例 2.37

- 求解方程式 $3x + 4 \equiv 6 \pmod{13}$。
- 解法：
  - 首先將方程式轉換成 $ax \equiv b \pmod{n}$ 的型式：我們在等號的兩邊同時加 -4 (4 的加法反元素)，讓方程式變成$3x \equiv 2 \pmod{13}$。
  - 因為 $\gcd(3, 13) = 1$，此方程式只有一個解，也就是 $x_0 = (2 \times 3^{-1}) \bmod 13 = 18 \bmod 13 = 5$。
  - 我們可以發現這個解滿足原方程式：$3 \times 5 + 4 \equiv 6 \pmod{13}$。