第四部份

近世應用代數

第 14 章

環和模數算術

在這第 4 且是本書的最後部份，強調的將再度是結構問題，如我們開始探討元素集合時，且這些元素集合在兩個二元運算下是封閉的。結構和枚舉的概念，經常互相增援。本章我們將看到如在第 1，4，5 及 8 章所見到的概念再次來到最前線。

當我們檢視第 4 章的集合 **Z** 時，它是和封閉的加法及乘法二元運算結合在一起。在本章，我們以寫 **(Z, +, ·)** 代替 **Z** 來強調這些運算。在 **(Z, +, ·)** 的某些性質之後的模型，稱之為**環** (ring) 的代數結構將被定義。在還沒認識它之下，我們已在許多數學模組處理過環。現在我們將考慮有限環，其出現在數論及電腦科學應用裡。在電腦科學研究中，特別有興趣的是**雜湊函數** (hashing function)，我們發現它提供一個確認儲存在表中的記錄。

14.1 環結構：定義和例題

我們以定義環結構開始，明白我們所給的最抽象的定義，像定理，來自許多例題的學習，在定理中吾人認知共同的概念或由一個不相關物體所成的集合中所出現的概念。

定義 14.1

令 R 為一個非空集合，在 R 上我們有兩個封閉的二元運算，記為 + 和 · (它們可能和我們所熟悉的平常之加法和乘法有相當的不同)。則 R 是一個**環** (ring) 若對所有 $a, b, c \in R$，滿足下面條件：

a) $a+b=b+a$	＋的交換律
b) $a+(b+c)=(a+b)+c$	＋的結合律
c) $\exists\, z \in R$，滿足 $a+z=z+a=a$，對每個 $a \in R$。	＋法單位元素存在
d) 對每個 $a \in R$，存在元素 $b \in R$，滿足 $a+b=b+a=z$.	＋法反元素存在
e) $a \cdot (b \cdot c)=(a \cdot b) \cdot c$	・的結合律
f) $a \cdot (b+c)=a \cdot b+a \cdot c$ $(b+c) \cdot a=b \cdot a+c \cdot a$	・對＋的分配律

因為＋(環加法) 及・(環乘法) 的封閉二元運算均是可結合的，所以我們寫 $a+b+c$ 表 $(a+b)+c$ 或 $a+(b+c)$，或寫 $a \cdot b \cdot c$ 表 $(a \cdot b) \cdot c$ 或 $a \cdot (b \cdot c)$，而不會產生模稜兩可。當在處理 (封閉的) 環乘法二元運算時，我們將經常以 ab 代替 $a \cdot b$。而且，我們可擴大 (環定義中所給的) 結合律如我們在 4.2 節習題 8 和 9 裡所做的。利用數學歸納法，可證明出對所有 r，$n \in \mathbf{Z}^+$，其中 $n \geq 3$ 且 $1 \leq r < n$，

$$(a_1 + a_2 + \cdots + a_r) + (a_{r+1} + \cdots + a_n) = a_1 + a_2 + \cdots + a_r + a_{r+1} + \cdots + a_n,$$

且

$$(a_1 a_2 \cdots a_r)(a_{r+1} \cdots a_n) = a_1 a_2 \cdots a_r a_{r+1} \cdots a_n,$$

其中 a_1，a_2，…，a_r，a_{r+1}，…，a_n 為已知環 $(R, +, \cdot)$ 的元素。以一個相對應的方法，將分配律一般化如下：

$$a(b_1 + b_2 + \cdots + b_n) = ab_1 + ab_2 + \cdots + ab_n,$$
$$(b_1 + b_2 + \cdots + b_n)a = b_1 a + b_2 a + \cdots + b_n a,$$

對任意的環元素 a，b_1，b_2，…，b_n 及所有 $n \in \mathbf{Z}^+$，其中 $n \geq 3$。

下一節我們將學加法單位元素 (或零元素) 是唯一的，每一個環元素的加法反元素也是唯一的。現在讓我們考慮一些環的例題。

例題 14.1

在 (封閉的) 平常加法及乘法的二元運算之下，我們發現 $\mathbf{Z}$，$\mathbf{Q}$，$\mathbf{R}$ 和 $\mathbf{C}$ 均為環。在這些環中，其加法單位元素 z 是整數 0，且每個數 x 的加法反元素是熟悉的 $-x$。

例題 14.2

令 $M_2(\mathbf{Z})$ 表所有具整數元素的 2×2 矩陣所成的集合。[集合 $M_2(\mathbf{Q})$，

$M_2(\mathbf{R})$ 及 $M_2(\mathbf{C})$ 均類似定義。] 在 $M_2(\mathbf{Z})$ 上，兩個矩陣相等若它們的對應元素在 $\mathbf{Z}$ 上均相等。

這裡我們定義＋和・為

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} a+e & b+f \\ c+g & d+h \end{bmatrix}, \quad \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix}.$$

在這些 (封閉的) 二元運算之下，$M_2(\mathbf{Z})$ 是一個環。此處 $z = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ 且 $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ 的加法反元素是 $\begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$。

然而，有些事情在這裡發生，但不發生在例題 14.1 的環裡，例如，

$$\begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 3 & 7 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 5 & 7 \\ 4 & 7 \end{bmatrix} \neq \begin{bmatrix} 10 & 13 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 3 & 7 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix},$$

證明乘法在環裡未必是可交換的。那就是為什麼有兩個分配律，而且，

$$\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix},$$

甚至 $\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}$ 和 $\begin{bmatrix} 2 & 1 \\ 2 & 1 \end{bmatrix}$ 均不是加法單位元素。因此，一個環可能包含所謂的**眞零因子** (proper divisors of zero)，亦即，非零元素的乘積是環的零元素。

我們擴大環結構的研究於下面。

定義 14.2

令 $(R, +, \cdot)$ 是一個環。

a) 若 $ab = ba$ 對所有 $a, b \in R$，則稱 R 是一個**交換環** (commutative ring)。

b) 稱環 R 是沒有真零因子若對所有 $a, b \in R$，$ab = z \Rightarrow a = z$ 或 $b = z$。

c) 若元素 $u \in R$ 滿足 $u \neq z$ 且 $au = ua = a$ 對所有 $a \in R$，我們稱 u 是 R 的一個**么元** (unity)，或是 R 的**乘法單位元素** (multiplicative identity)。此時稱 R 是一個具有**么元的環** (ring with unity)。

由定義 14.2(c) 可知，每當我們有一個具么元的環 R 時，則 R 至少有兩個元素。更而，若環有一個么元，我們將在下一節學到么元是唯一的。

例題 14.1 的環均是交換環，且其么元是整數 1。那些環中沒有一個有任何的真零因子。同時，環 $M_2(\mathbf{Z})$ 是一個不可交換環，其么元是矩陣 $\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$。這個環確實含有零因子。

而且，每當我們想證明某個特別結構 $(R, +, \cdot)$是一個環時，我們可以證明 R 在兩個二元運算下是封閉的來開始，接著我們可繼續並證明定義 14.1 的條件 (a)-(e)。在我們試著建立分配律之前，然而，我們也許想先判斷乘法運算是否可交換。若我們應證明這個運算是可交換的，則我們僅需證明分配律中的一個即可 (因為另一個將自動成立)。而且，若我們能夠證明所有的前述條件，則我們將知道 $(R, +, \cdot)$ 不僅是一個環，它是一個交換環。

現在讓我們研究另一個例題，當我們想進一步探討定義 14.1 及 14.2 所設定的概念時。

例題 14.3

考慮集合 $\mathbf{Z}$ 及 $\oplus$ 和 $\odot$ 的二元運算，其被定義為

$$x \oplus y = x + y - 1, \qquad x \odot y = x + y - xy.$$

因此，我們發現，例如 $3 \oplus 7 = 3 + 7 - 1 = 9$ 且 $3 \odot 7 = 3 + 7 - 3 \cdot 7 = -11$。

因為平常的加法、減法，及乘法在 $\mathbf{Z}$ 上是封閉的二元運算，這些新的二元運算——即 $\oplus$ 和 $\odot$——亦在 $\mathbf{Z}$ 上封閉。事實上，我們將發現 $(\mathbf{Z}, \oplus, \odot)$ 是一個環。

a) 欲證明 $(Z, \oplus, \odot)$ 是一個環，我們必須證明定義 14.1 所給的六個條件。我們將檢視這些條件中的三個且將另外三個留在本節習題裡。

1) 首先，因為平常的加法在 $\mathbf{Z}$ 上是一個可交換的二元運算，我們發現對所有 $x, y \in \mathbf{Z}$，

$$x \oplus y = x + y - 1 = y + x - 1 = y \oplus x.$$

所以二元運算 $\oplus$ 在 $\mathbf{Z}$ 上亦是可交換的。

2) 當我們檢視條件 (c) 時，我們知道我們需找一個整數 z 滿足 $a \oplus z = z \oplus a = a$，對每個 $a \in \mathbf{Z}$。因此，我們必須解方程式 $a + z - 1 = a$，其給我們 $z = 1$。因此，非零整數 1 是 $\oplus$ 的零元素 (或加法單位元素)。

3) 加法反元素又是什麼呢？此刻若我們有一個 (任意的) 整數 a，我們想知道是否存在一個整數 b 滿足 $a \oplus b = b \oplus a = z$。由上面之 (2) 及

$\oplus$ 的定義，知 b 必滿足 $a+b-1=1$，且得 $b=2-a$。所以，例如，7 的加法反元素是 $2-7=-5$ 且 -42 的加法反元素是 $2-(-42)=44$。畢竟，在 7 的情形，我們發現 $7\oplus(-5)=7+(-5)-1=7-5-1=1$，其中 1 是加法單位元素。[注意：因為我們在 (1) 證明 $\oplus$ 是可交換的，我們亦知道 $(-5)\oplus 7=1$。]

b) 更而，環 $(\mathbf{Z}, \oplus, \odot)$ 亦具有定義 14.2 中額外的性質。特別的，這個環有一個么元 (亦即，乘法單位元素)。欲決定么元，令 a 為任一整數且考慮元素 u $(\neq z=1)$，其中

$$a\odot u=u\odot a=a.$$

因為 $a\odot u=a+u-au$，我們解 $a+u-au=a$，發現 $u(1-a)=0$。因為 a 是任意的，這個必成立甚至當 $a\neq 1$ 時。因此整數 $u=0$ 是環 $(\mathbf{Z}, \oplus, \odot)$ 的么元。

在這些無限環的例題之後，我們現在轉到具有限個元素的環。

例題 14.4

令 $\mathcal{U}=\{1, 2\}$ 且 $R=\mathcal{P}(\mathcal{U})$。定義 R 的元素上之 $+$ 及 $\cdot$ 為

$$A+B=A\,\Delta\,B=\{x|x\in A \text{ 或 } x\in B, \text{但 } x \text{ 不同時屬於 } A \text{ 和 } B\}$$
$$A\cdot B=A\cap B= \text{ 集合 } A, B\subseteq\mathcal{U} \text{ 的交集。}$$

對這些運算，我們得到表 14.1(a) 及 (b)。

由第 3 章的結果，吾人發現，對這些 (封閉的)“加法”及“乘法”二元運算 R 滿足定義 14.1 的條件 (a)，(b)，(e)，及 (f)。表中的“加法”說明 $\emptyset$ 是加法單位元素。對每個 $x\in R$，x 的加法反元素是 x 本身。乘法表由左上角至右下角依對角線成對稱，所以由表中所描述的，乘法是可交換的。表中亦說明 R 有么元 $\mathcal{U}$。所以 R 是一個具有么元的有限交換環。元素 $\{1\}$，$\{2\}$ 提供一個真零因子的例子。

表 14.1

$+$ (Δ)	$\emptyset$	$\{1\}$	$\{2\}$	$\mathcal{U}$
$\emptyset$	$\emptyset$	$\{1\}$	$\{2\}$	$\mathcal{U}$
$\{1\}$	$\{1\}$	$\emptyset$	$\mathcal{U}$	$\{2\}$
$\{2\}$	$\{2\}$	$\mathcal{U}$	$\emptyset$	$\{1\}$
$\mathcal{U}$	$\mathcal{U}$	$\{2\}$	$\{1\}$	$\emptyset$

(a)

$\cdot$ $(\cap)$	$\emptyset$	$\{1\}$	$\{2\}$	$\mathcal{U}$
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{1\}$	$\emptyset$	$\{1\}$	$\emptyset$	$\{1\}$
$\{2\}$	$\emptyset$	$\emptyset$	$\{2\}$	$\{2\}$
$\mathcal{U}$	$\emptyset$	$\{1\}$	$\{2\}$	$\mathcal{U}$

(b)

例題 14.5

對 $R=\{a, b, c, d, e\}$，我們以表 14.2(a) 及 (b) 來定義＋和・。

表 14.2

＋	a	b	c	d	e
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c
e	e	a	b	c	d

(a)

・	a	b	c	d	e
a	a	a	a	a	a
b	a	b	c	d	e
c	a	c	e	b	d
d	a	d	b	e	c
e	a	e	d	c	b

(b)

雖然我們在這裡不證明它們，但需要有 125 個等式來建立各個結合律及分配律均成立，所以 $(R, +, \cdot)$ 成為一個具么元的有限交換環，且它沒有真零因子。元素 a 是 R 的零 (即加法單位元素)，而 b 是其么元。這裡每個非零元素 x 有一個**乘法反元素** (multiplicative inverse) y，其中 $xy=yx=b$，即么元。元素 c 和 d 是互為乘法反元素；b 是自己的反元素，e 也是。

我們現在來考慮一般的環元素之乘法反元素概念。

定義 14.3

令 R 是一個具么元 u 的環。若 $a \in R$ 且存在 $b \in R$ 滿足 $ab=ba=u$，則稱 b 是 a 的一個**乘法反元素** (multiplicative inverse) 且稱 a 是 R 的一個**可逆元素** (unit)。(元素 b 亦是 R 的一個可逆元素。)

在 14.2 節，我們將看到，若一個環元素確有一個乘法反元素，則它僅有一個此類反元素。同時，我們將檢視兩種特殊的環結構。

定義 14.4

令 R 是一個具么元的交換環，則

a) 稱 R 是一個**整環** (integral domain) 若 R 沒有真零因子。
b) 稱 R 是一個**體** (field) 若 R 的每一個非零元素是一個可逆元素。

環 $(\mathbf{Z}, +, \cdot)$ 是一個整環但不是一個體，而 $\mathbf{Q}$，$\mathbf{R}$，$\mathbf{C}$，在平常的加法及乘法之下，是整環也是體。例題 14.5 中的環是一個整環也是一個體。

由定義 14.2(c) 知，若 R 是一個整環或是一個體，則 $|R| \geq 2$。

例題 14.6

對本節的最後一個環，我們令 $R=\{s, t, v, w, x, y\}$ 且以表 14.3(a) 及 (b) 來給＋和・。

表14.3

+	s	t	v	w	x	y
s	s	t	v	w	x	y
t	t	v	w	x	y	s
v	v	w	x	y	s	t
w	w	x	y	s	t	v
x	x	y	s	t	v	w
y	y	s	t	v	w	x

(a)

·	s	t	v	w	x	y
s	s	s	s	s	s	s
t	s	t	v	w	x	y
v	s	v	x	s	v	x
w	s	w	s	w	s	w
x	s	x	v	s	x	v
y	s	y	x	w	v	t

(b)

由這兩個表，我們看出 $(R, +, \cdot)$ 是一個具么元的交換環，但它既不是整環也不是體。元素 t 是么元，且 t 和 y 為 R 的可逆元素。

我們亦注意到 $vv = vy$，且甚至 v 不是 R 的零元素，我們不能將它消去而說 $v = y$。所以，一般的環不滿足乘法消去律，該消去律可能有時候需授權。我們將在下一節再次看到這個概念。

習題 14.1

1. 求例題 14.5 及 14.6 之環中的各個元素之加法反元素。
2. 決定下面各個數集在平常的加法及乘法之下是否是一個環。
   a) R＝正整數和零所成的集合。
   b) $R = \{kn \mid n \in \mathbf{Z}, k$ 是一個固定的正整數$\}$
   c) $R = \{a + b\sqrt{2} \mid a, b \in \mathbf{Z}\}$
   d) $R = \{a + b\sqrt{2} + c\sqrt{2} \mid a \in \mathbf{Z}, b, c \in \mathbf{Q}\}$
3. 令 $(R, +, \cdot)$ 是一個環含元素 a，b，c，d。試敘述需要用來證明下面各個結果的條件 (由環的定義)。
   a) $(a + b) + c = b + (c + a)$
   b) $d + a(b + c) = ab + (d + ac)$
   c) $c(d + b) + ab = (a + c)b + cd$
   d) $a(bc) + (ab)d = (ab)(d + c)$
4. 對例題 14.4 的集合 R，保留 $A \cdot B = A \cap B$，但定義 $A + B = A \cup B$，則 $(R, \cup, \cap)$ 是一個環嗎？
5. 考慮集合 $\mathbf{Z}$ 暨例題 14.3 所給的二元運算 $\oplus$ 及 $\odot$。(a) 證明 $\oplus$ 和 $\odot$ 的結合律及分配律以便完成例題 14.3(a) 的開始工作。[此建立 $(\mathbf{Z}, \oplus, \odot)$ 是一個環。] (b) 此環是可交換的嗎？(c) 在例題 14.3(b) 中，我們證明了 0 是 $(\mathbf{Z}, \oplus, \odot)$ 的么元，那麼這個環的可逆元素是什麼？(d) 此環是一個整環嗎？是一個體嗎？
6. 定義 $\mathbf{Z}$ 上的二元運算 $\oplus$ 及 $\odot$ 為 $x \oplus y = x + y - 7$，$x \odot y = x + y - 3xy$，對所有 $x, y \in \mathbf{Z}$。試解釋為何 $(\mathbf{Z}, \oplus, \odot)$ 不是一個環。
7. 令 k，m 為固定整數，求所有的 k，m 值使得 $(\mathbf{Z}, \oplus, \odot)$ 是一個環，在二元運

算 $x \oplus y = x+y-k$，$x \odot y = x+y-mxy$ 之下，其中 $x, y \in \mathbf{Z}$。

8. 表 14.4(a) 及 (b) 使 $(R, +, \cdot)$ 是一個環，其中 $R=\{s, t, x, y\}$。(a) 此環的零是什麼？(b) 各個元素的加法反元素是什麼？(c) $t(s+xy)$ 是什麼？(d) R 是一個交換環嗎？(e) R 有一個么元嗎？(f) 試找一對零因子。

表 14.4

+	s	t	x	y
s	y	x	s	t
t	x	y	t	s
x	s	t	x	y
y	t	s	y	x

(a)

·	s	t	x	y
s	y	y	x	x
t	y	y	x	x
x	x	x	x	x
y	x	x	x	x

(b)

9. 在集合 $\mathbf{Q}$ 上，分別定義加法和乘法，記為 $\oplus$ 及 $\odot$，如下：對 $a, b \in \mathbf{Q}$，$a \oplus b = a+b+7$，$a \odot b = a+b+(ab/7)$。(a) 證明 $(\mathbf{Q}, \oplus, \odot)$ 是一個環。(b) 此環是可交換的嗎？(c) 此環有一個么元嗎？可逆元素是什麼？(d) 此環是一個整環嗎？是一個體嗎？

10. 令 $(\mathbf{Q}, \oplus, \odot)$ 表一個體，其中 $\oplus$ 和 $\odot$ 被定義為 $a \oplus b = a+b-k$，$a \odot b = a+b+(ab/m)$，對固定的 $\mathbf{Q}$ 之元素 k，m $(\neq 0)$。在下面各小題中，決定 k 和 m 的值。

a) 體的零元素是 3。

b) 元素 6 的加法反元素是 -9。

c) 2 的乘法反元素是 1/8。

11. 令 $R=\{a+bi \mid a, b \in \mathbf{Z}, i^2=-1\}$，其中加法和乘法分別被定義為 $(a+bi)+(c+di)=(a+c)+(b+d)i$ 且 $(a+bi)(c+di)=(ac-bd)+(bc+ad)i$。(a) 證明 R 是一個整環。(b) 求 R 上的所有可逆元素。

12. (a) 求矩陣 $\begin{bmatrix} 1 & 2 \\ 3 & 7 \end{bmatrix}$ 於環 $M_2(\mathbf{Z})$ 中的乘法反元素，即求 a，b，c，d 使得

$$\begin{bmatrix} 1 & 2 \\ 3 & 7 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 3 & 7 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

(b) 證明 $\begin{bmatrix} 1 & 2 \\ 3 & 8 \end{bmatrix}$ 是環 $M_2(\mathbf{Q})$ 中的一個可逆元素，但不是 $M_2(\mathbf{Z})$ 上的可逆元素。

13. 若 $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbf{R})$，證明 $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ 是此環上的一個可逆元素若且唯若 $ad-bc \neq 0$。

14. 給一個含 8 個元素的環的例子。含 16 個元素的環呢？試一般化之。

15. 對 $R=\{s, t, x, y\}$ 利用表 14.5(a) 給 $+$ 且利用表 14.5(b) 的特別表給 $\cdot$，定義 $+$ 和 $\cdot$ 使 R 為一個環。

a) 使用結合律及分配律，決定乘法表中失落的元素。

b) 此環是可交換的嗎？

c) 它有一個么元嗎？有可逆元素嗎？

d) 此環是一個整環或是一個體嗎？

表 14.5

+	s	t	x	y
s	s	t	x	y
t	t	s	y	x
x	x	y	s	t
y	y	x	t	s

(a)

·	s	t	x	y
s	s	s	s	s
t	s	t	?	?
x	s	t	?	y
y	s	?	s	?

(b)

14.2　環性質及子結構

在 14.1 節的各個環裡，我們關心環的零元素及各個環元素的加法反元素。現在是時刻，併用其它性質，來證明這些元素真的是唯一的。

定理 14.1

在任一個環 $(R, +, \cdot)$ 裡，

a) 零元素 z 是唯一的，且
b) 各個環元素的加法反元素是唯一的。

證明：

a) 若 R 有多於一個的加法單位元素，令 z_1，z_2 表兩個加法單位元素，則

$$z_1 = z_1 + z_2 = z_2.$$

（z_2 是一個加法單位元素；z_1 是一個加法單位元素）

b) 對 $a \in R$，假設存在兩個元素 b，$c \in R$ 滿足 $a+b=b+a=z$ 及 $a+c=c+a=z$，則 $b=b+z=b+(a+c)=(b+a)+c=z+c=c$。(讀者應提出建立各個等式的條件。)

由於 (b) 中唯一性的結果，由此刻起，我們將把 $a \in R$ 的加法反元素表為 $-a$。更而，我們現在可談環中的**減法** (subtraction)，其中我們瞭解 $a-b=a+(-b)$。

由定理 14.1(b)，對任何環 R，我們亦得下面結果。

定理 14.2

加法消去律 (The Cancellation Laws of Addition)。對所有 a，b，$c \in R$。

a) $a+b=a+c \Rightarrow b=c$，且
b) $b+a=c+a \Rightarrow b=c$。

證明：

a) 因為 $a \in R$，得 $-a \in R$ 且我們有

$$a+b=a+c \Rightarrow (-a)+(a+b)=(-a)+(a+c)$$

$$\Rightarrow [(-a)+a]+b=[(-a)+a]+c$$
$$\Rightarrow z+b=z+c \Rightarrow b=c.$$

b) 我們將這個類似的證明留給讀者。

注意當我們檢視一個有限環的加法表時，我們發現環的每個元素在表的各列及各行中恰出現一次。這是定理 14.2 的一個直接結果，其中定理的 (a) 處理所有列且 (b) 處理所有行。

定理 14.3 對任一環 $(R, +, \cdot)$ 及任一 $a \in R$，我們有 $az=za=z$。

證明： 若 $a \in R$，則 $az=a(z+z)$，因為 $z+z=z$。因此，$z+az=az=az+az$。(為什麼？) 使用加法消去律，我們有 $z=az$。

$za=z$ 的證明同理可得。

讀者可能感覺定理 14.3 的結果是明顯的。但我們不僅是處理 **Z** 或 **Q** 或 $M_2(\mathbf{Z})$，我們的目標是證明任一個環滿足此一結果，且我們可能僅使用環定義中的條件及目前我們導給任意環的各種性質來得到這個結果。

[由定理 14.1(b) 知] 加法反元素的唯一性現在蘊涵下面結果。

定理 14.4 給一環 $(R, +, \cdot)$，對所有 $a, b \in R$，

a) $-(-a)=a$，
b) $a(-b)=(-a)b=-(ab)$，且
c) $(-a)(-b)=ab$.

證明：

a) 由定理 14.1 之後的俗約，$-(-a)$ 表 $-a$ 的加法反元素。因為 $(-a)+a=z$，所以 a 亦是 $-a$ 的加法反元素。因此，由反元素的唯一性，$-(-a)=a$。

b) 我們將證明 $a(-b)=-(ab)$ 且將另一部份證明留給讀者。我們知道 $-(ab)$ 表 ab 的加法反元素。然而，由定理 14.3，$ab+a(-b)=a[b+(-b)]=az=z$，所以由加法反元素的唯一性，$a(-b)=-(ab)$。

c) 此處我們將建立一個我們在代數中已使用的概念，因為我們第一次遇到**符號數** (signed numbers)。“減號乘上減號事實上是加號”，且由環的性質及定義，證明成立。由 (b)，我們有 $(-a)(-b)=-[a(-b)]=$

$-[-(ab)]$，且由 (a) 結果成立。

對乘法運算，我們亦發現下面結果，其可比擬定理 14.1。

定理 14.5

對一個環 $(R, +, \cdot)$，

a) 若 R 有一個么元，則這個么元是唯一的，且
b) 若 R 有一個么元，且 x 是 R 的一個可逆元素，則 x 的乘法反元素是唯一的。

證明：這些結果的證明留給讀者。

由於此定理之結果，當 $(R, +, \cdot)$ 是一個具有么元的環時，我們將表么元為 u。更而，在此一環中，每個可逆元素 x 的乘法反元素將被表為 x^{-1}。而且，我們現在可將體的定義重新敘述為一個具有么元的交換環 F 滿足對所有 $x \in F$，$x \neq z \Rightarrow x^{-1} \in F$。

有這些觀念幫助我們，我們將檢視體和整環間進一步的性質和關係。

定理 14.6

令 $(R, +, \cdot)$ 是一個含么元的交換環，則 R 是一個整環若且唯若對所有 $a, b, c \in R$ 滿足 $a \neq z$，$ab = ac \Rightarrow b = c$。(因此，滿足**乘法消去律** (the cancellation law of multiplication) 的含么元之交換環是一個整環。)

證明：若 R 是一個整環且 $x, y \in R$，則 $xy = z \Rightarrow x = z$ 或 $y = z$。現在若 $ab = ac$，則 $ab - ac = a(b - c) = z$，且因為 $a \neq z$，得 $b - c = z$ 或 $b = c$。反之，若 R 是具么元的環且 R 滿足乘法消去律，則令 $a, b \in R$ 滿足 $ab = z$。若 $a = z$，則我們完成。若否，由於 $az = z$，我們可寫 $ab = az$ 且得 $b = z$。所以，R 沒有真零因子且是一個整環。

在繼續之前，讓我們明白乘法消去律不蘊涵乘法反元素的存在。整環 $(\mathbf{Z}, +, \cdot)$ 滿足乘法消去律，但它僅含兩個元素，即 1 和 -1，為可逆元素。因此，一個整環未必是一個體。但體又是如何呢？體是否必為整環呢？

定理 14.7

若 $(F, +, \cdot)$ 是一個體，則它是一個整環。

證明：令 $a, b \in F$ 滿足 $ab = z$。若 $a = z$，我們就完成了。若否，a 有一個乘法反元素 a^{-1}，因為 F 是一個體。則

$$ab = z \Rightarrow a^{-1}(ab) = a^{-1}z \Rightarrow (a^{-1}a)b = a^{-1}z \Rightarrow ub = z \Rightarrow b = z.$$

因此，F 沒有真零因子且它是一個整環。

在第 5 章，我們發現函數 $f: A \to A$ 可能是一對一 (或映成) 而不必是映成 (或一對一)。然而，若 A 為有限，此一函數 f 是一對一若且唯若它是映成 (見定理 5.11)。同樣的情形發生於有限整環。一個整環未必是一個體，但當它是有限時，我們發現它是一個體。

定理 14.8

一個有限整環 $(D, +, \cdot)$ 是一個體。

證明：因為 D 為有限，我們可列出 D 的所有元素為 $\{d_1, d_2, \cdots, d_n\}$。對 $d \in D$，其中 $d \neq z$，我們有 $dD = \{dd_1, dd_2, \cdots, dd_n\} \subseteq D$，因為 D 在乘法之下是封閉的。現在 $|D| = n$ 且 $dD \subseteq D$，所以若我們能證明 dD 有 n 個元素，我們將有 $dD = D$。若 $|dD| < n$，則 $dd_i = dd_j$，對某些 $1 \leq i < j \leq n$。但因為 D 是一個整環且 $d \neq z$，我們有 $d_i = d_j$，當它們被假設為相異的。所以 $dD = D$ 且對某些 $1 \leq k \leq n$，$dd_k = u$，D 的么元。則 $dd_k = u \Rightarrow d$ 是 D 的一個可逆元素，且因為 d 為任意選的，得 $(D, +, \cdot)$ 是一個體。

由定理 14.8 的證明，我們亦明白我們正在處理一個有限體的非零元素，這些元素的乘法表滿足體的每個元素在各行及各列恰出現一次。

下一節，我們將注意對離散數學有用的有限體。然而，在結束本節之前，讓我們檢視環的一些特別的子集合。

當我們在第 6 章處理有限狀態機器時，我們看到內部狀態集的子集合給增加至它們自己的機器 (當原始機器的下一個狀態及輸出函數被適當地限制時)。這些被稱是子機器。因為封閉的二元運算是特別類型的函數，我們見到一個類似的概念於下面定義裡。

定義 14.5

給一個環 $(R, +, \cdot)$，R 的一個非空子集合 S 被稱是 R 的一個**子環** (subring) 若 $(S, +, \cdot)$ ——亦即 S 在 R 的加法及乘法之下——限制到 S 是一個環。

例題 14.7

對每個環 R，子集合 $\{z\}$ 和 R 永遠是 R 的子環。

例題 14.8

a) 所有偶數的集合是 $(\mathbf{Z}, +, \cdot)$ 的一個子環。事實上，對每個 $n \in \mathbf{Z}^+$，$n\mathbf{Z} = \{nx | x \in \mathbf{Z}\}$ 是 $(\mathbf{Z}, +, \cdot)$ 的一個子環。

b) $(\mathbf{Z}, +, \cdot)$ 是 $(\mathbf{Q}, +, \cdot)$ 的一個子環，$(\mathbf{Q}, +, \cdot)$ 是 $(\mathbf{R}, +, \cdot)$ 的一個子環，$(\mathbf{R}, +, \cdot)$ 是 $(\mathbf{C}, +, \cdot)$ 的一個子環。

在例題 14.6 裡，子集合 $S=\{s, w\}$ 和 $T=\{s, v, x\}$ 均為 R 的子環。 **例題 14.9**

下一個結果描述，某環之子環的那些子集合之特徵。

給一個環 $(R, +, \cdot)$，R 的一非空子集合 S 是 R 的一個子環若且唯若 **定理 14.9**

1) 對所有 a，$b \in S$，我們有 $a+b$，$ab \in S$ (亦即，S 在定義在 R 上的加法及乘法二元運算下是封閉的)，且
2) 對所有 $a \in S$，我們有 $-a \in S$。

證明：若 $(S, +, \cdot)$ 是 R 的一個子環，則在它自己的權限內，它滿足一個環的所有條件。因此，它滿足定理的條件 1 和 2。反之，令 S 為 R 的一非空子集合且滿足條件 1 和 2。環定義中的條件 (a)，(b)，(e)，及 (f) 由 S 的所有元素繼承，因為它們亦為 R 的元素。因此，這裡所有我們需證明的是 S 有一個加法單位元素。現在 $S \neq \emptyset$，所以有一元素 $a \in S$，且由條件 2，$-a \in S$。則由條件 1，$z=a+(-a) \in S$。

考慮我們已檢視在例題 14.3 及 14.1 節習題 5 的環 $(Z, \oplus, \odot)$。這裡我們有 $x \oplus y=x+y-1$ 且 $x \odot y=x+y-xy$。現在考慮所有奇數的子集合 $S=\{\cdots, -5, -3, -1, 1, 3, 5, \cdots\}$。因為，例如，3 和 5 在 S 裡，但平常的和 $3+5=8 \notin S$。這個集合 S 不是 $(\mathbf{Z}, +, \cdot)$ 的一個子環。然而，$3 \oplus 5=3+5-1=7 \in S$。事實上，對所有 a，$b \in S$，我們有 $a \oplus b=a+b-1$，其中 $a+b$ 是偶數且 $a+b-1$ 奇數，所以 $a \oplus b \in S$。而且 $a \oplus b=a+b-ab$，其中 $a+b$ 是偶數且 ab 是奇數，所以 $a \odot b \in S$。最後，$-a$ [a 在環 $(\mathbf{Z}, \oplus, \odot)$ 的加法反元素] 等於 $2-a$，其為奇數每當 a 是奇數時。因此，若 $a \in S$，則 $-a \in S$，且由定理 14.9 知 S 是 $(\mathbf{Z}, \oplus, \odot)$ 的一個子環。 **例題 14.10**

注意 $(\mathbf{Z}^+, +, \cdot)$ 滿足定理 14.9 的條件 1，但不滿足條件 2，所以它不是 $(\mathbf{Z}, +, \cdot)$ 的一個子環。

定理 14.9 的結果亦可被給如下。

對任一環 $(R, +, \cdot)$，若 $\emptyset \neq S \subseteq R$， **定理 14.10**

a) 則 $(S, +, \cdot)$ 是 R 的一個子環若且唯若對所有 a，$b \in S$，我們有 $a-b \in S$ 且 $ab \in S$；
b) 且若 S 是有限，則 $(S, +, \cdot)$ 是 R 的一個子環若且唯若對所有 a，$b \in S$，我們有 $a+b$，$ab \in S$。(再次，額外的幫助來自一個有限的條

件。)

證明：這些證明留給讀者。

下一個例題說明吾人可如何使用前面定理的第一部份。

例題 14.11

讓我們考慮環 $R=M_2(\mathbf{Z})$ 及 R 的子集合

$$S=\left\{\begin{bmatrix} x & x+y \\ x+y & x \end{bmatrix} \middle| \, x, y \in \mathbf{Z}\right\}$$

當 $x=y=0$ 得 $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in S$ 且 $S \neq \emptyset$。所以現在我們檢視 S 上的任兩個元素，即型如

$$\begin{bmatrix} x & x+y \\ x+y & x \end{bmatrix} \text{ 和 } \begin{bmatrix} v & v+w \\ v+w & v \end{bmatrix}$$

的兩個矩陣，其中 $x, y, v, w \in \mathbf{Z}$。我們發現

$$\begin{bmatrix} x & x+y \\ x+y & x \end{bmatrix}-\begin{bmatrix} v & v+w \\ v+w & v \end{bmatrix}=\begin{bmatrix} x-v & (x-v)+(y-w) \\ (x-v)+(y-w) & x-v \end{bmatrix}$$

所以 S 在減法之下是封閉的。轉向乘法，我們有

$$\begin{aligned}
&\begin{bmatrix} x & x+y \\ x+y & x \end{bmatrix}\begin{bmatrix} v & v+w \\ v+w & v \end{bmatrix} \\
&=\begin{bmatrix} xv+(x+y)(v+w) & x(v+w)+(x+y)v \\ (x+y)v+x(v+w) & (x+y)(v+w)+xv \end{bmatrix} \\
&=\begin{bmatrix} xv+xv+yv+xw+yw & xv+xw+xv+yv \\ xv+yv+xv+xw & xv+yv+xw+yw+xv \end{bmatrix} \\
&=\begin{bmatrix} xv+xv+yv+xw+yw & (xv+xv+yv+xw+yw)+(-yw) \\ (xv+xv+yv+xw+yw)+(-yw) & xv+xv+yv+xw+yw \end{bmatrix}
\end{aligned}$$

所以 S 在乘法之下亦是封閉的。

現訴諸於定理 14.10(a)，吾人發現 S 是 R 的一個子環。

我們現在將挑選出一個重要的子環類型。

定義 14.6

環 R 的一個非空子集合 I 被稱是 R 的一個**理想** (ideal) 若對所有 a，b

$\in I$ 且所有 $r \in R$，我們有 (a) $a-b \in I$ 且 (b) ar，$ra \in I$。

理想是一個子環，但反過來未必成立：$(\mathbf{Z}, +, \cdot)$ 是 $(\mathbf{Q}, +, \cdot)$ 的一個子環，但不是一個理想，因為，例子，$(1/2)9 \notin \mathbf{Z}$，對 $(1/2) \in \mathbf{Q}$，$9 \in \mathbf{Z}$。同時，例題 14.8(a) 的所有子環均是 $(\mathbf{Z}, +, \cdot)$ 的理想。

回看例題 14.10，我們看到若 $a \in S$，$x \in \mathbf{Z}$，則 $a \odot x = a + x - ax$ $(= x \odot a)$，且若 x 是偶數 (因為 x 是奇數的情形已被涵蓋在例題 14.10 裡)，則 $a + x$ 是奇數且 ax 是偶數，而使 $a + x - ax$ 為奇數。因此，對所有 $a \in S$ 且所有 $x \in \mathbf{Z}$，$a \odot x$ 及 $x \odot a$ 均在 S 上，所以 S 是環 $(\mathbf{Z}, \oplus, \odot)$ 的一個理想。

習題 14.2

1. 完成定理 14.2，14.4，14.5 及 14.10 的證明。
2. 若 a，b，和 c 是環 $(R, +, \cdot)$ 上的任意元素，證明 (a) $a(b-c) = ab - (ac) = ab - ac$ 且 (b) $(b-c)a = ba - (ca) = ba - ca$。
3. a) 若 R 是一個具么元的環且 a，b 為 R 的可逆元素，證明 ab 是一個 R 的可逆元素且 $(ab)^{-1} = b^{-1}a^{-1}$。

   b) 對環 $M_2(\mathbf{Z})$，求 A^{-1}，B^{-1}，$(AB)^{-1}$，$(BA)^{-1}$，及 $B^{-1}A^{-1}$，若

$$A = \begin{bmatrix} 4 & 7 \\ 1 & 2 \end{bmatrix}, \qquad B = \begin{bmatrix} 5 & 2 \\ 2 & 1 \end{bmatrix}.$$

4. 證明環 R 上的一可逆元素不能為一個真零因子。
5. 若 a 是環 R 上的一可逆元素，證明 $-a$ 亦是 R 的一可逆元素。
6. a) 證明子集合 $S = \{s, w\}$ 和 $T = \{s, v, x\}$ 是例題 14.6 中環 R 的子環。(S，T 的元素的二元運算是給在表 14.3 的二元運算。)

   b) (a) 中的子環是 R 的理想嗎？
7. 令 S 和 T 是環 R 的子環。證明 $S \cap T$ 是 R 的子環。
8. 令 $R = M_2(\mathbf{Z})$ 且令 S 為 R 的子集合，其中

$$S = \left\{ \begin{bmatrix} x & x-y \\ x-y & y \end{bmatrix} \middle| \, x, y \in \mathbf{Z} \right\}.$$

   證明 S 是 R 的一個子環。
9. 令 $(R, +, \cdot)$ 是一個環。若 S，T_1，及 T_2 是 R 的子環，且 $S \subseteq T_1 \cup T_2$，證明 $S \subseteq T_1$ 或 $S \subseteq T_2$。
10. a) 令 $(R, +, \cdot)$ 是一個具么元 u 的有限交換環。若 $r \in R$ 且 r 不是 R 的零元素，證明 r 不是一個可逆元素就是一個真零因子。

    b) (a) 的結果是否仍然成立當 R 是無限時？
11. a) 對 $R = M_2(\mathbf{Z})$，證明

$$S = \left\{ \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \middle| \, a \in \mathbf{Z} \right\}$$

    是 R 的一個子環。

b) R 的么元是什麼。

c) S 有一個么元嗎？

d) S 有任何 R 沒有的性質嗎？

e) S 是 R 的一個理想嗎？

12. 令 S 和 T 為環 $R=M_2(\mathbf{Z})$ 的下面子集合：

$$S=\left\{\begin{bmatrix}a & 0\\ b & c\end{bmatrix}\middle| a,b,c\in\mathbf{Z}\right\},$$

$$T=\left\{\begin{bmatrix}2a & 2b\\ 2c & 2d\end{bmatrix}\middle| a,b,c,d\in\mathbf{Z}\right\}.$$

a) 證明 S 是 R 的一個子環，它是一個理想嗎？

b) 證明 T 是 R 的一個子環，它是一個理想嗎？

13. 令 $(R, +, \cdot)$ 是一個交換環，且令 z 表 R 的零元素。對一固定的元素 $a\in R$，定義 $N(a)=\{r\in R|ra=z\}$。證明 $N(a)$ 是 R 的一個理想。

14. 令 R 是一個具有么元 u 的交換環，且令 I 是 R 的一個理想。(a) 若 $u\in I$，證明 $I=R$。(b) 若 I 包含 R 的一個可逆元素，證明 $I=R$。

15. 若 R 是一個體，則 R 有多少個理想呢？

16. 令 $(R, +, \cdot)$ 是被給在表 14.6(a) 及 (b) 具有么元的 (有限) 交換環。

表 14.6

+	z	u	a	b
z	z	u	a	b
u	u	z	b	a
a	a	b	z	u
b	b	a	u	z

(a)

·	z	u	a	b
z	z	z	z	z
u	z	u	a	b
a	z	a	b	u
b	z	b	u	a

(b)

a) 證明 R 是一個體。

b) 找一個 R 的子環但其不是一個理想。

c) 令 x 和 y 為未知，解下面 R 上的線性方程組：$bx+y=u$；$x+by=z$。

17. 令 R 是一個具么元 u 的交換環。

a) 對任一 (固定的) $a\in R$，證明 $aR=\{ar|r\in R\}$ 是 R 的一個理想。

b) 若 R 的唯一理想是 $\{z\}$ 和 R，證明 R 是一個體。

18. 令 $(S, +, \cdot)$ 和 $(T, +', \cdot')$ 為兩個環。對 $R=S\times T$，定義加法 "$\oplus$" 及乘法 "$\odot$" 為

$$(s_1,t_1)\oplus(s_2,t_2)=(s_1+s_2,\ t_1+' t_2),$$
$$(s_1,t_1)\odot(s_2,t_2)=(s_1\cdot s_2,\ t_1\cdot' t_2).$$

a) 證明在這些封閉二元運算之下，R 是一個環。

b) 若 S 和 T 均為可交換的，證明 R 是可交換的。

c) 若 S 有么元 u_S 且 T 有么元 u_T，則 R 的么元是什麼？

d) 若 S 和 T 是體，R 也是一個體嗎？

19. 令 $(R, +, \cdot)$ 是一個具么元 u 的環，且 $|R|=8$。在 $R^4=R\times R\times R\times R$ 上，定義 $+$ 和 $\cdot$ 為習題 18 所建議的。(a) 有多少個元素恰有兩個非零分量？(b) 有多少個元素所有分量均非零？(c) 是否有一個么元？(d) 有多少個可逆元素若 R 有 4 個可逆元素？

20. 令 $(R, +, \cdot)$ 是一個環，且 $a\in R$。定義 $0a=z$，$1a=a$，且 $(n+1)a=na+a$，對所有 $n\in\mathbf{Z}^+$。(這裡我們以 $\mathbf{Z}$ 的元素來乘 R 的元素，所以我們暫時有一個不同於 $\mathbf{Z}$ 或 R 上之乘法的運算。) 對 $n>0$，我們定義 $(-n)a=n(-a)$，所以，例如，$(-3)a=3(-a)=2(-a)+(-a)=[(-a)+(-a)]+(-a)=[-(a+$

$a)]+(-a)=-[(a+a)+a]=-[2a+a]$
$=-(3a)$.

對所有 $a, b \in R$ 及所有 $m, n \in \mathbf{Z}$，證明

a) $ma+na=(m+n)a$

b) $m(na)=(mn)a$

c) $n(a+b)=na+nb$

d) $n(ab)=(na)b=a(nb)$

e) $(ma)(nb)=(mn)(ab)=(na)(mb)$

21. a) 對環 $(R, +, \cdot)$ 及每個 $a \in R$，我們定義 $a^1=a$，及 $a^{n+1}=a^n a$ 對所有 $n \in \mathbf{Z}^+$。證明對所有 $m, n \in \mathbf{Z}^+$，$(a^m)(a^n)=a^{m+n}$ 且 $(a^m)^n=a^{mn}$。

b) 您能建議我們可如何定義 a^0 或 a^{-n}, $n \in \mathbf{Z}^+$，包含任何 R 必須滿足的必要條件，以使這些定義有意義？

14.3　整數模 n

足夠抽象一會兒！我們現在將集中在特殊有限環和體的結構及使用。

定義 14.7

令 $n \in \mathbf{Z}^+$，$n>1$。對 $a, b \in \mathbf{Z}$，我們稱 ***a* 和 *b* 同餘模 *n*** (a is congruent to b modulo n)，且我們記 $a \equiv b \pmod{n}$，若 $n|(a-b)$，或等價地，$a=b+kn$ 對某些 $k \in \mathbf{Z}$。

例題 14.12

i) 我們發現 $17 \equiv 2 \pmod 5$，因為 $17-2=15=3(5)$，或 $17=2+3(5)$。

ii) 因為 $-7+49=-7-(-49)=42=7(6)$ [或，$-7=-49+7(6)$]，我們有 $-7 \equiv -49 \pmod 6$。

iii) 因為 $11-(-5)=16=2(8)$ [或 $11=-5+2(8)$]，得 $11 \equiv -5 \pmod 8$。

在檢視第一個定理之前，讓我們對同餘模 n 這個新概念做三個觀察。這裡，如上，我們有 $a, b, n \in \mathbf{Z}$，其中 $n>1$。

i) 利用除法演算法，我們可寫 $a=q_1 n+r_1$，及 $b=q_2 n+r_2$，其中 $0 \le r_1 < n$，$0 \le r_2 < n$。所以 $a-b=(q_1-q_2)n+(r_1-r_2)$。則若 $a \equiv b \pmod n$，得 $n|(a-b)$，且因此，$n|(r_1-r_2)$。但由於 $0 \le |r_1-r_2| < n$，我們發現 $r_1=r_2$。

因此，若 $a \equiv b \pmod n$，則 a，b 在除以 n 之下有相同的餘數。

ii) (i) 中結果的逆亦為真。亦即，若 $a=q_1 n+r_1$ 且 $b=q_2 n+r_2$，滿足 $r_1=r_2$，則 $a-b=(q_1-q_2)n$，且 $a \equiv b \pmod n$。

iii) 雖然 $a=b \Rightarrow a\equiv b \pmod n$，但我們不能期望 $a\equiv b \pmod n \Rightarrow a=b$。然而，若 $a\equiv b \pmod n$，且 $a, b \in \{0, 1, 2, \cdots, n-1\}$，則 $a=b$。

定理 14.11 同餘模 n 是 $\mathbf{Z}$ 上的一個等價關係。

證明：證明留給讀者。

因為集合上的等價關係導出該集合的一個分割，對 $n \geq 2$，同餘模 n 將 $\mathbf{Z}$ 分割成 n 個等價類。

$$[0]=\{\cdots, -2n, -n, 0, n, 2n, \cdots\}=\{0+nx | x \in \mathbf{Z}\}$$
$$[1]=\{\cdots, -2n+1, -n+1, 1, n+1, 2n+1, \cdots\}=\{1+nx | x \in \mathbf{Z}\}$$
$$[2]=\{\cdots, -2n+2, -n+2, 2, n+2, 2n+2, \cdots\}=\{2+nx | x \in \mathbf{Z}\}$$
$$\vdots$$
$$[n-1]=\{\cdots, -n-1, -1, n-1, 2n-1, 3n-1, \cdots\}$$
$$=\{(n-1)+nx | x \in \mathbf{Z}\}.$$

對所有 $t \in \mathbf{Z}$，由 (4.3 節的) 除法演算法，我們可寫 $t=qn+r$，其中 $0 \leq r < n$，所以 $t \in [r]$，或 $[t]=[r]$。我們使用記號 $\mathbf{Z}_n$ 來表 $\{[0], [1], [2], \cdots\cdots, [n-1]\}$。(當沒有模稜兩可的危險時，我們經常以 a 代 $[a]$ 且記 $\mathbf{Z}_n=\{0, 1, 2, \cdots, n-1\}$。) 現在我們的目標是定義等價類集合 $\mathbf{Z}_n$ 上封閉的加法及乘法二元運算使得我們可得一環。

對 $[a], [b] \in \mathbf{Z}_n$，定義＋和・為

$$[a]+[b]=[a+b] \text{ 且 } [a]\cdot[b]=[a][b]=[ab].$$

例如，若 $n=7$，則 $[2]+[6]=[2+6]=[8]=[1]$，且 $[2][6]=[12]=[5]$。

在這些定義被接受前，我們必須探討這些 (封閉的二元) 運算是否為**良好定義的** (well-defined) 即若 $[a]=[c]$，$[b]=[d]$，則 $[a]+[b]=[c]+[d]$ 且 $[a][b]=[c][d]$。因為 $a \neq c$ 可得 $[a]=[c]$，我們的加法和乘法結果取決於由等價類所選出的代表嗎？我們將證明這兩個運算的結果和等價類代表的選擇無關且兩個運算是非常良好定義的。

首先，我們觀察 $[a]=[c] \Rightarrow a=c+sn$，對某些 $s \in \mathbf{Z}$，且 $[b]=[d] \Rightarrow b=d+tn$ 對某些 $t \in \mathbf{Z}$。因此

$$a+b=(c+sn)+(d+tn)=c+d+(s+t)\,n,$$

所以 $(a+b)\equiv(c+d) \pmod n$ 且 $[a+b]=[c+d]$。而且，

$$ab = (c + sn)(d + tn) = cd + (sd + ct + stn)\, n$$

且 $ab \equiv cd \pmod{n}$，或 $[ab] = [cd]$

此結果引導我們至下面結果。

定理 14.12

對 $n \in \mathbf{Z}^+$，$n > 1$，在上面所定義的封閉二元運算之下，$\mathbf{Z}_n$ 是一個具么元 [1] (及加法單位元素 [0]) 的交換環。

證明：證明留給讀者。由 $\mathbf{Z}_n$ 上加法及乘法定義及由環 $(\mathbf{Z}, +, \cdot)$ 相對應的性質，得環 $\mathbf{Z}_n$ 的性質。

在敘述任何進一步結果之前，讓我們檢視兩個特殊例子，$\mathbf{Z}_5$ 及 $\mathbf{Z}_6$。在表 14.7(a) 和 (b) 及 14.8(a) 和 (b)，我們以 a 簡化 $[a]$。

表 14.7

$\mathbf{Z}_5$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

(a)

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

(b)

在 $\mathbf{Z}_5$ 上，每個非零元素有一個乘法反元素，所以 $\mathbf{Z}_5$ 是一個體。然而，對 $\mathbf{Z}_6$，1 和 5 是唯一的可逆元素且 2，3，4 是真零因子。同時，在 $\mathbf{Z}_9$，$3 \cdot 3 = 3 \cdot 6 = 0$，所以 3 和 6 是真零因子。因此，對 $\mathbf{Z}_n$，$n > 2$，欲成為一個體，我們僅需多一個奇數模。

表 14.8

$\mathbf{Z}_6$

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

(a)

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

(b)

定理 14.13

$\mathbf{Z}_n$ 是一個體若且唯若 n 是一個質數。

證明：令 n 為一質數，且假設 $0<a<n$。則 $\gcd(a, n)=1$，所以如我們在 4.4 節所學的，存在整數 s，t 滿足 $as+tn=1$。因此 $as\equiv 1 \pmod{n}$，或 $[a][s]=[1]$，且 $[a]$ 是 $\mathbf{Z}_n$ 的一個可逆元素，因此 $\mathbf{Z}_n$ 是一個體。

反之，若 n 不是一個質數，則 $n=n_1n_2$，其中 $1<n_1$，$n_2<n$。所以 $[n_1]\neq[0]$ 且 $[n_2]\neq[0]$，但 $[n_1][n_2]=[n_1n_2]=[0]$，且 $\mathbf{Z}_n$ 甚至不是一個整環，所以 $\mathbf{Z}_n$ 不可能是一個體。

在 $\mathbf{Z}_6$ 裡，[5] 是一個可逆元素且 [3] 是一個零因子。我們找一個方法來辨認何時 $[a]$ 會是 $\mathbf{Z}_n$ 上的一個可逆元素，其中 n 是合成數。

定理 14.14

在 $\mathbf{Z}_n$ 上，$[a]$ 是一個可逆元素若且唯若 $\gcd(a, n)=1$。

證明：若 $\gcd(a, n)=1$，如定理 14.13 的證明，結果成立。反之，令 $[a]\in\mathbf{Z}_n$ 且 $[a]^{-1}=[s]$，則 $[as]=[a][s]=[1]$，所以 $as\equiv 1 \pmod{n}$ 且 $as=1+tn$ 對某些 $t\in\mathbf{Z}$。但 $1=as+n(-t)\Rightarrow \gcd(a, n)=1$。

例題 14.13

在 $\mathbf{Z}_{72}$ 上求 $[25]^{-1}$。

因為 $\gcd(25, 72)=1$，歐幾里得演算法引導我們

$$\begin{aligned} 72&=2(25)+22, & 0<22<25,\\ 25&=1(22)+3, & 0<3<22,\\ 22&=7(3)+1, & 0<1<3. \end{aligned}$$

因為 1 是最後的非零餘數，我們有

$$\begin{aligned} 1&=22-7(3)=22-7[25-22]=(-7)(25)+(8)(22)\\ &=(-7)(25)+8[72-2(25)]=8(72)-23(25). \end{aligned}$$

但是

$$1=8(72)-23(25)\Rightarrow 1\equiv(-23)(25)\equiv(-23+27)(25)\pmod{72},$$

所以 $[1]=[49][25]$ 且 $[25]^{-1}=[49]$ 於 $\mathbf{Z}_{72}$ 上。

此外，由此結果，我們現在能解下面的線性同餘給 x：

1) 若 $25x\equiv 1 \pmod{27}$，則 $x\equiv 49 \pmod{72}$。
2) 若 $5x\equiv 3 \pmod{27}$，則 $x\equiv 49\cdot 3 \pmod{72}\equiv 3 \pmod{72}$。

現在 [25] 是 $\mathbf{Z}_{72}$ 上的一個可逆元素，但是否存在任何方法來知道這個環上有多少個可逆元素？由定理 14.14，若 $1\le a<72$，則 $[a]^{-1}$ 存在且唯

若 gcd(a, 72)＝1。因此，$\mathbf{Z}_{72}$ 上的可逆元素個數是整數 a 的個數，滿足 $1 \le a < 72$ 且 gcd(a, 72)＝1。使用尤拉 ϕ 函數 (例題 8.8)，我們發現這是

$$\phi(72) = \phi(2^3 3^2) = (72)[1-(1/2)][1-(1/3)] = (72)(1/2)(2/3) = 24.$$

一般來講，對任意 $n \in \mathbf{Z}^+$，$n > 1$，$\mathbf{Z}_n$ 有 $\phi(n)$ 個可逆元素及 $n-1-\phi(n)$ 個真零因子。

在我們繼續進行一些例子之前，其中同餘扮演一個角色，我們想回看早先定義在例題 4.36 及 10.8 的二元運算 **mod**。在那些例題裡，我們考慮 $x, y \in \mathbf{Z}^+$ 且定義 x **mod** y 為當我們以 y 來除以 x 所得的餘數。此刻，我們將擴大這個概念至包含 $x \le 0$ 的情形。因此，對 $x \in \mathbf{Z}$ 及 $y \in \mathbf{Z}^+$，x **mod** y 是 x 除以 y 所得的餘數。

但是，現在，這個 **mod** 和定義 14.7 的 mod 有什麼關係呢？在這裡，我們發現若 a，b，$n \in \mathbf{Z}$，其中 $n > 1$，則 $a \equiv b \pmod{n}$ 若且唯若 a **mod** $n = b$ **mod** n。(此由定理 14.11 之前我們所做的觀察可得。)

現在是給一些另加例題的時候了。

例題 14.14

隨機產生數出現在許多應用裡。特別地，它們經常被使用在太貴、太危險，或在真實世界實在顯然不可能的模擬實驗裡。

使用電腦來產生隨機數的概念首先由 John von Neumann (1903-1957) 於 1946 年發展的。然而，雖然這些數可能出現為隨機，但它們並不是，因此，**擬隨機** (pseudorandom) 數的標題出現。

由 Derrick H. Lehmer (1905-1991) 於 1949 年所推荐的，最常被用的生產此類擬隨機數的方法是引用同餘的觀念。對**線性同餘生成器** (linear congruential generator)，吾人以四個整數開始：乘數 a，增右量 c，模數 m，及種子 x_0，其中

$$2 \le a < m, \qquad 0 \le c < m, \qquad \text{且} \quad 0 \le x_0 < m.$$

這些非負數被用來以

$$x_{n+1} = (ax_n + c) \textbf{ mod } m$$

來遞回產生一個擬隨機數數列 x_1，x_2，x_3，…。所以 $0 \le x_{n+1} < m$，對 $n \ge 0$。例如，若 $a = 3$，$c = 2$，$m = 11$，及 $x_0 = 1$，則

$x_1 = (ax_0 + c)$ **mod** $m = [3(1) + 2]$ **mod** $11 = 5$，所以 $x_1 = 5$。

同理，$x_2 = (ax_1 + 0)$ **mod** $m = [3(5) + 2]$ **mod** $11 = 17$ **mod** $11 = 6$，所以 $x_2 = 6$。

依此法繼續，吾人發現 $x_3 = 9$，$x_4 = 7$，且 $x_5 = 1$，即為種子。因此，這個線性同餘生產器在重複之前產生五個相異整數。所得的擬隨機數數列是 1，5，6，9，7，1，5，6，…。

以 $a = 3$，$c = 5$，$m = 12$，及 $x_0 = 6$，我們首先得到 $x_1 = [3(6) + 5]$ **mod** $12 = 11$，所以 $x_1 = 11$。其次，$x_2 = [3(11) + 5]$ **mod** $12 = 38$ **mod** $12 = 2$，所以 $x_2 = 2$。進一步計算得 $x_3 = 11$。此次線性同餘生產器僅產生三個相異整數，在重複之前。這種所產生的擬隨機數數列是 6，11，2，11，2，11，2，…，其中的種子不重複。

實際上大值的 a 和 m 被使用，尤其對危險的模擬。對 $a = 16{,}807 (= 7^5)$，$c = 0$，$m = 2{,}147{,}483{,}647 (= 2^{31} - 1$，一個質數)，且 $x_0 = 1$，吾人得到一個 2,147,483,647 個擬隨機數的數列，在一個重複整數出現之前。

例題 14.15

a) 不管是海軍准尉使用密碼譯解環或是軍事領袖派作戰計畫給軍隊，在整個歷史，各種人希望保有某種令人無法瞭解的資訊，而它將變成錯誤的訊息。

早在西元前第一世紀，羅馬將軍 Gaius Julius Caesar (100 B.C.-44 B.C.) 使用一種**密碼推移** (cipher shift) 來使某種訊息的內容僅給那些他想傳遞訊息者瞭解。欲描述這個早先的**密碼系統** (cryptosystem)——經常被稱為 *Caesar* 密碼——我們將使某種約俗簡化呈現。首先，我們將寫原始訊息，**明語** (plaintext)，僅使用小寫字母，沒有標點符號或空格。接著把明語譯成密碼，每個小寫字母，由 a 到 w，使字母順序分別被向前推移三個字母位置，且最後三個字母，即 x，y，和 z，被推移到前三個字母。我們以大寫字母表所得的**密語** (ciphertext)。因此，a 被譯成 D，b 為 E，c 為 F，…，j 為 M，…，m 為 P，…，y 為 B，且 z 為 C。

若 Caesar 想告知羅馬的參議員一個最近的勝利，他可能寄出訊息 “I came, I saw, I conquered”。這個訊息將如下譯成密碼：

明語	*i*	*c*	*a*	*m*	*e*	*i*	*s*	*a*	*w*	*i*	*c*	*o*	*n*	*q*	*u*	*e*	*r*	*e*	*d*
密語	*L*	*F*	*D*	*P*	*H*	*L*	*V*	*D*	*Z*	*L*	*F*	*R*	*Q*	*T*	*X*	*H*	*U*	*H*	*G*

一旦接到這個密語，只要這位參議員知道推移的大小和方向，他可以掉換過程。將密語裡的每個大寫字母，由 D 到 Z，依字母順序

以倒回三個字母位置的小寫字母取代，且以 x 取代 A，y 取代 B，及以 z 取代 C，可破解密語。在破解密語之後，接著人們可插入適當的空格及標點符號於明語裡。(注意移走明語裡的空格，而得沒有空格的密語，有助於令訊息更加難以瞭解。若吾人不知破解密語的推移之大小和方向，空格的出現可對原始訊息的結構建議某種訊息。)

b) Caesar 密碼的概念可被一般化及使用同餘概念來做數字模擬。首先將明語的 26 個字母的每個字母指定一個非負整數如下：

a	b	c	d	$\cdots$	k	l	m	n	$\cdots$	w	x	y	z
0	1	2	3	$\cdots$	10	11	12	13	$\cdots$	22	23	24	25

密語的 26 個字母亦被指定相同的整數，亦即，A 被指定為 0，B 被指定為 1，$\cdots$，Y 被指定為 24，且 Z 被指定為 25。

現在選一個非負整數 κ，其中 $0 \le \kappa \le 25$。例如，Caesar 選 $\kappa = 3$。這個整數 κ 被稱是**鍵** (key) 且幫我們定義譯成密碼函數 E: $\mathbf{Z}_{26} \to \mathbf{Z}_{26}$ 如下。給明語的一個字母，令 θ 為它所對應的非負整數，則 $E(\theta) = (\theta + \kappa)$ **mod** 26 且此結果決定由指定非負整數 θ 的明語字母所對應的密語字母。欲破解密碼，我們應用反函數 D: $\mathbf{Z}_{26} \to \mathbf{Z}_{26}$，其中我們記 $D(\theta) = (\theta - \kappa)$ **mod** 26。將各個非負整數取代為其所對應的明語字母，吾人可捕捉原始訊息的明語版。

若我們不知道鍵值，一個試驗及誤差法可被使用。共有 26 種可能——每一個對 26 個可能的 κ 值中的一個。一個更有效的攻擊方法是取在 26 個字母中最常出現的字母及在密語中最常出現的字母。在英語裡，字母 e 最常出現，及接著四個最常出現的字母是 t，a，o 和 i。

現在若一個父母由一個學院學生接到密語 $Z\ L\ U\ K\ T\ V\ Y\ L\ T\ V\ U\ L\ F$，且不知道鍵值，則父母能做什麼？因為在密語裡最常出現的字母是 L，父母在譯成密碼下，可以 L 對應 e。此建議 E: $\mathbf{Z}_{26} \to \mathbf{Z}_{26}$ 被定義為 $E(\theta) = (\theta + 7)$ **mod** 26，因為依字母順序，L 在 e 之後 7 個位置。所以這裡的鍵值 κ，是 7，且破解密碼函數是 D: $\mathbf{Z}_{26} \to \mathbf{Z}_{26}$，其中 $D(\theta) = (\theta - 7)$ **mod** 26。

譯解父母所接到的密語訊息可被分析如下：

(1)	Z	L	U	K	T	V	Y	L	T	V	U	L	F
(2)	25	11	20	10	19	21	24	11	19	21	20	11	5
(3)	18	4	13	3	12	14	17	4	12	14	13	4	24
(4)	s	e	n	d	m	o	r	e	m	o	n	e	y

這裡 (1) 提供已知的 (譯成密碼的) 密語。在 (2) 每個密語字母被指定給它的非負整數取代。一旦應用破解函數 D，(2) 中的結果提供 (3) 中的指定值。將 (3) 中的每個非負整數取代為其所對應的明語字母，得到原始訊息。

"Send more money."

c) (b) 中的推移密碼的安全性可利用**仿射密碼** (affine cipher) 來稍加加強。明語和密語的所有字母被指定為非負整數，如 (b) 中。然而，這裡的譯成密碼函數 E 被給為 $E(\theta)=(\alpha\theta+\kappa)$ **mod** 26，其中 $0 \le \alpha, \kappa \le 25$ 且 $\gcd(\alpha, 26)=1$。

若 $\theta_1, \theta_2 \in \mathbf{Z}_{26}$，則 $E(\theta_1)=E(\theta_2) \Rightarrow (\alpha\theta_1+\kappa)$ **mod** $26=(\alpha\theta_2+\kappa)$ **mod** $26 \Rightarrow \alpha\theta_1$ **mod** $26=\alpha\theta_2$ **mod** $26 \Rightarrow \theta_1=\theta_2$，由定理 14.14。所以 E 是一對一。更而，E 亦是映成且為可逆，由定理 5.11，因為 $\mathbf{Z}_{26}$ 是有限的。

讓我們考慮一個特別的例子。假設 $\alpha=11$ 且 $\kappa=7$，則明語字母 g 的譯成密碼進行如下：

i) g 被指定非負整數 6；
ii) 應用 E，我們有 $E(6)=(11 \cdot 6+7)$ **mod** $26=73$ **mod** $26=21$；且
iii) 非負整數 21 決定密語字母 V。

[所以使用這個仿射密碼，其中 $E(\theta)=(11\theta+7)$ **mod** 26，明語字母 g 被譯成密碼為密語字母 V。]

現在假設我們有下面的密語，其係某個訊息經由一個仿射密語轉譯而來的：

QYYFGCULBLKYZVOSTCOYPURGCULYZYWKYOSTCOYL

由於不知 α 或 κ 值，吾人可能必須檢視 $[\phi(26)](26) = \left[26\left(1-\frac{1}{2}\right)\left(1-\frac{1}{13}\right)\right](26) = \left[26\left(\frac{1}{2}\right)\left(\frac{12}{13}\right)\right](26) = (12)(26) = 312$ 個情形給鍵值 α，κ。然而，讓我們以某些方式來說——或許可考慮明語及密語中字母出現的頻率——我們導出兩種對應。明確地，我們知道 e 和 Y 對應，及 t 和 R 對應。而且，非負整數 4 和 19 分別取代明語字母 e 與 t，而 24 和 17 分別取代 Y 和 R 於密語裡，所以譯成密碼函數被決定如下：

1) $e(4)$ 和 $Y(24)$ 的對應告訴我們 $E(4)=(4\alpha+\kappa)$ **mod** $26=24$。
2) $t(19)$ 和 $R(17)$ 的對應告訴我們 $E(19)=(19\alpha+\kappa)$ **mod** $26=17$。

因此，$E(19)-E(4)=[(19\alpha+\kappa)-(4\alpha+\kappa)]$**mod** $26=15\alpha$ **mod** $26=(17-24)$ **mod** $26=-7$ **mod** $26=19$。因為 $15\cdot 7=105=1+104=1+4(26)$，我們 $15\cdot 7=1$ **mod** 26，$15^{-1}=7$ (於 $\mathbf{Z}_{26}$)。則 $15\alpha=19$ **mod** $26\Rightarrow \alpha=15^{-1}\cdot 19$ **mod** $26=7\cdot 19$ **mod** $26=133$ **mod** $26=3$，如 $133=3+5(26)$。

由於 $\alpha=3$ **mod** 26，現在由 (1) $\kappa=(24-4\alpha)$ **mod** $26=(24-12)$ **mod** $26=12$。[或由 (2)，$\kappa=(17-19\alpha)$ **mod** $26=(17-57)$ **mod** $26=-40$ **mod** $26=12$]。

因此，E: $\mathbf{Z}_{26}\to\mathbf{Z}_{26}$ 被稱定義為 $E(\theta)=(3\theta+12)$ **mod** 26 且破解密碼函數 D: $\mathbf{Z}_{26}\to\mathbf{Z}_{26}$ 被給為 $D(\theta)=(9\theta+22)$ **mod** 26，因為 $E^{-1}(\theta)=3^{-1}(\theta-12)$ **mod** $26=9(\theta-12)$ **mod** $26=(9\theta-108)$ **mod** $26=(9\theta+22)$ **mod** 26。函數 D 被應用於下面，可由列 2 的整數 (代替密語字母) 得到列 3 的結果。

(1) 密語	*Q*	*Y*	*Y*	*F*	*G*	*C*	*U*	*L*	*B*	*L*	*K*	*Y*	*Z*	*V*	*O*	*S*	*T*	*C*	*O*	*Y*
(2)	16	24	24	5	6	2	20	11	1	11	10	24	25	21	14	18	19	2	14	24
(3)	10	4	4	15	24	14	20	17	5	17	8	4	13	3	18	2	11	14	18	4
(4) 明語	*k*	*e*	*e*	*p*	*y*	*o*	*u*	*r*	*f*	*r*	*i*	*e*	*n*	*d*	*s*	*c*	*ℓ*	*o*	*s*	*e*

(1) 密語	*P*	*U*	*R*	*G*	*C*	*U*	*L*	*Y*	*Z*	*Y*	*W*	*K*	*Y*	*O*	*S*	*T*	*C*	*O*	*Y*	*L*
(2)	15	20	17	6	2	20	11	24	25	24	22	10	24	14	18	19	2	14	24	11
(3)	1	20	19	24	14	20	17	4	13	4	12	8	4	18	2	11	14	18	4	17
(4) 明語	*b*	*u*	*t*	*y*	*o*	*u*	*r*	*e*	*n*	*e*	*m*	*i*	*e*	*s*	*c*	*ℓ*	*o*	*s*	*e*	*r*

此處，例如，密語字母 *Q* 被非負整數 16 取代。應用破解密碼函數 D 至 16，我們有 $D(16)=(9\cdot 16+22)$ **mod** $26=166$ **mod** $26=10$，且 10 是對應至明語字母 *k* 的非負整數。

破解的訊息顯示 (Mario Puzo 的教父) Don Vito Corleone 給他最小兒子 Michael 的智慧忠告“保持親近您的朋友，但應更親近您的敵人”。

例題 14.15 中各個密碼系統的安全性依賴鍵值 [(a) 的 $\kappa=3$，(b) 的 κ，及 (c) 中的 α，κ]。對此類隱遁的**鍵值密碼系統** (private key cryptosystems)，有兩位想使用這個系統來安心地改變鍵值。若任何有權限的人發現鍵值，則這個人可容易地將訊息譯成密碼或破解密碼。

下一個例題處理模指數。

例題 14.16

在密碼學† 的研究裡，吾人經常需要執行模數來計算諸如 b^e **mod** n 的

† 欲知更多的密碼學 (及相關主題)，讀者應找找由 T. H. Barr [3], P. Garrett [6]，及 W. Trappe 和 L. C. Washington [13] 所提供的參考資料。

結果，其中 b，e，及 n 為大的整數。欲說明這個——以一個稍小的大小——讓我們決定 5^{143} **mod** 222。我們明白實際計算 5^{143} (一個非常大的整數) 及求這個結果 (5^{143}) 除以 222 的餘數是頗沒效率的。一個更有效率的方法是以指數，即 143 的二進位表示式開始。因

$$\begin{aligned}143 &= 1(128)+0(64)+0(32)+0(16)+1(8)+1(4)+1(2)+1(1)\\ &= 1(2^7)+0(2^6)+0(2^5)+0(2^4)+1(2^3)+1(2^2)+1(2^1)+1(2^0)\\ &= (10001111)_2,\end{aligned}$$

我們以反向使用 (143 的) 二進位表示式，亦即由右至左，來計算 5^{143} **mod** 222。圖 14.1 的擬編碼程序提供這個計算的必要步驟。這裡的輸入是整數 b，正整數 n (模數)，及指數 e，另一個正整數的二進位表示式 $(a_m a_{m-1}\cdots a_2 a_1 a_0)_2$。輸出的 x 等於 b^e **mod** n。

```
procedure 模指數(b: 整數;
                 n, e = (a_m a_{m-1}···a_2 a_1 a_0)_2: 正整數)
begin
  x := 1
  power := b mod n
  for i = 0 to m do
    begin
      if a_i = 1 then x := (x * power) mod n
      power := (power * power) mod n
    end
end
```

圖 14.1

對我們的例子，$b=5$，$e=143=(10001111)_2=(a_7a_6a_5\cdots a_2a_1a_0)_2$ [所以 $m=7$]，且 $n=222$。表 14.9 的結果告訴我們在執行 **for** 迴圈的所有步驟。這是初始指定值：x 是 1 且冪次方 b **mod** n，亦即 5 **mod** 222 = 5，之後的

表 14.9

i	a_i	x	冪次方
0	1	$1*5=5$	5^2 (= 25) **mod** 222 = 25
1	1	$5*25$ **mod** 222 = 125	25^2 (= 625) **mod** 222 = 181
2	1	$125*181$ **mod** 222 = 203	181^2 (= 32761) **mod** 222 = 127
3	1	$203*127$ **mod** 222 = 29	127^2 (= 16129) **mod** 222 = 145
4	0	29	145^2 (= 21025) **mod** 222 = 157
5	0	29	157^2 (= 24649) **mod** 222 = 7
6	0	29	7^2 (= 49) **mod** 222 = 49
7	1	$29*49$ **mod** 222 = 89	49^2 (= 2401) **mod** 222 = 181

結果。

隨著這個程序的執行，x 欄的最後元素告訴我們 5^{143} **mod** 222 是 89。

下一個例題提供模同餘在資訊恢復上的一個應用。

例題 14.17

當我們搜尋一個儲存在電腦裡的記錄表時，每個記錄被指定一個記憶位置或位址於電腦的記憶體。記錄本身經常是由體 (環結構無法處理) 所組成。例如學校的註冊組長保有每位學生的記錄，而該記錄含有學生社會保險號碼、名字，及主修，總共三個體的資料。

在搜尋某一個學生的記錄時，我們可使用他的或她的社會保險號碼做為該記錄的鍵值，因為它唯一的確認該記錄。所以，我們發展一個由鍵值所成的集合映到由表中位址所成的集合的函數。

若學院是足夠小，我們可發現社會保險的前 4 碼足夠來做確認。我們發展一個**雜湊** (hashing or scattering) 函數 h 由鍵值 (仍然是社會保險號碼) 集映到位址集，由鍵值的前 4 碼決定。例如，h(081-37-6495) 確認在位址為 0813 的記錄。依此法，我們可儲存該表而至多使用 10,000 個位址。所有的事情將進行的很好，主要 h 是一對一函數。若有第三位學生的社會保險號碼是 081-39-0207，則 h 將不再唯一確認學生的記錄。當這個情形發生，吾人稱一個**碰撞** (collision) 發生。因為增加儲存表的大小經常導致更多的未使用儲存，我們必須平衡這個儲存的費用對抗處理此類碰撞的費用。溶解碰撞的方法已被發明，它們依賴那些被用來儲存記錄的資料結構 (諸如向量或線性連結表目)。

不同的雜湊函數已被發展，包含下面。

a) **除法** (division)：此處我們限制位址的個數，我們想使用一個固定整數 n。對任意鍵值 k (一個正整數)，我們定義 $h(k)=r$，其中 $r=k$ **mod** n，亦即 $r \equiv k \pmod{n}$ 且 $0 \le r < n$。

b) 經常被執行的是**折迭法** (folding method)，其中鍵值被分成幾個部份，並將這幾個部份加在一起而得 h(key)。例如，h(081-37-6495)＝081＋37＋6495＝6613 個使用折迭，且若我們僅想要三數字位址，刪除第一個數字 6，我們可有 h(081-37-6495)＝613。

選取一個適切的雜湊函數的重要性不可能被過度強調，當我們試著以較大的速率及較少未使用的儲存來改進效率時。

利用模概念，我們可發展一個雜湊函數 h，使用和上面相同的鍵值，其中

$$h(x_1x_2x_3\text{-}x_4x_5\text{-}x_6x_7x_8x_9) = y_1y_2y_3,$$

且

$$y_1 = (x_1 + x_2 + x_3) \bmod 5$$
$$y_2 = (x_4 + x_5) \bmod 3$$
$$y_3 = (x_6 + x_7 + x_8 + x_9) \bmod 7.$$

此處，例如，h(081-37-6495)＝413。

本節的最後一個例題提供一個再見 (1.5 及 10.5 節的) Catalan 數的例題。

例題 14.18

有多少種方法我們可由 {0, 1, 2, 3} 選出三個元素 a，b，c，若允許重複且想要 $a+b+c\equiv 0 \pmod 4$？所有的選法被列在表 14.10 的欄 1。(此處各個選擇的和為 0，4，或 8，且順序是無關的。例如，a＝0，b＝1，c＝3 被考慮為和 a＝1，b＝0，c＝3 的選法相同。) 我們看到共有五種此類選法且我們記得 $5 = \left(\frac{1}{3+1}\right)\binom{2\cdot 3}{3}$，第三個 Catalan 數。更而，將選法 0，0，0 (在列 1 及欄 1) 的各元素加 1，我們得到選法 1，1，1 (在列 1 及欄 2)。同樣的，選法 2，3，1 (在列 2 及欄 3) 來自選法 0，1，3 (在列 2 及欄 1) 的各元素加 2 且以 modulo 4 來簡化各個和。類似的計算提供欄 2，3，4 的其它 13 種選法。

表 14.10

和 0 (mod 4)	和 3 (mod 4)	和 2 (mod 4)	和 1 (mod 4)
0, 0, 0	1, 1, 1	2, 2, 2	3, 3, 3
0, 1, 3	1, 2, 0	2, 3, 1	3, 0, 2
0, 2, 2	1, 3, 3	2, 0, 0	3, 1, 1
1, 1, 2	2, 2, 3	3, 3, 0	0, 0, 1
2, 3, 3	3, 0, 0	0, 1, 1	1, 2, 2

欲一般化這個結果，我們計數由 {0, 1, 2, 3, ⋯, n} 選出 x_1，x_2，⋯，x_n 的方法數，其中允許重複且 $x_1+x_2+\cdots+x^n\equiv 0 \pmod{n+1}$。由 1.4 節，我們知道共有 $\binom{(n+1)+n-1}{n} = \binom{2n}{n}$ 種方法由 $n+1$ 個相異物體選出 n 個物體，且允許重複。令 Sel_n 表這 $\binom{2n}{n}$ 個選法所成的集合 (表 14.10 中的 20 種選法說明 Sel_3。) 定義在 Sel_n 上的關係 $\mathcal{R}$ 為 $s_1\,\mathcal{R}\,s_2$，若選法 s_1 上所有元素的和，模 $n+1$，和選法 s_2 上所有元素的和相同。則 κ 是一個等價關係，所以 Sel_n 可被分解成 $n+1$ 個等價類 (一個代表選法和為 0，1，2，⋯，n，取模 $n+1$ 中的一個)。[注意：我們得到所有 $n+1$ 個可能的選法和，

因為若 $0 \le k_1 \le n$，$0 \le k_2 \le n$，且 $nk_1 \equiv nk_2 \pmod{n+1}$，則 $k_1 \equiv k_2 \pmod{n+1}$。這是由於定理 14.14，因為 $\gcd(n, n+1)=1$。因 k_1，$k_2 \in \{0, 1, \cdots, n\}$，得 $k_1=k_2$。]

對 $0 \le s \le n$，令 Sel_n^s 表和 s，模 $n+1$ 的所有選法。當 $1 \le s \le n$，寫 $s=nk$ (因為 $k=n^{-1}s$)。定義 $f: Sel_n^0 \to Sel_n^s$ 如下。對 $\{x_1, x_2, \cdots, x_n\} \in Sel_n^0$，$f(\{x_1, x_2, \cdots, x_n\})=\{x_1+k, x_2+k, \cdots, x_n+k\}$，其中 x_i+k 被簡化模 $n+1$。現在考慮 $\{y_1, y_2, \cdots, y_n\} \in Sel_n^s$ 且定義 $g: Sel_n^s \to Sel_n^0$ 為 $g(\{y_1, y_2, \cdots, y_n\})=\{y_1+(n+1-k), y_2+(n+1-k), \cdots, y_n+(n+1-k)\}$。吾人發現 $g=f^{-1}$，所以 $|Sel_n^0|=|Sel_n^1|=\cdots=|Sel_n^n|$。因此，每個等價類有相同的大小，即 $\left(\frac{1}{n+1}\right)\binom{2n}{n}$，第 n 個 Catalan 數。

習題 14.3

1. a) 試決定下列各對整數是否同餘模 8。
   i) 62, 118　ii) −42, −237　iii) −90, 230
   b) 試決定下列各對整數是否同餘模 9。
   i) 76, 243　ii) −137, 700　iii) −56, −1199
2. 對下面各題，求整數 $n>1$ 的值以使所給的同餘為真。
   a) $28 \equiv 6 \pmod{n}$　b) $68 \equiv 37 \pmod{n}$
   c) $301 \equiv 233 \pmod{n}$　d) $49 \equiv 2 \pmod{n}$
3. 對下面各個等價類列出四個元素。
   (a) [1] 於 $\mathbf{Z}_7$　(b) [2] 於 $\mathbf{Z}_{11}$　(c) [10] 於 $\mathbf{Z}_{17}$。
4. 證明若 a，b，c，$n \in \mathbf{Z}$ 滿足 a，$n>0$，且 $b \equiv c \pmod{n}$，則 $ab \equiv ac \pmod{an}$。
5. 令 a，b，m，$n \in \mathbf{Z}$ 且 m，$n>0$。證明若 $a \equiv b \pmod{n}$ 且 $m|n$，則 $a \equiv b \pmod{m}$。
6. 令 m，$n \in \mathbf{Z}^+$ 滿足 $\gcd(m, n)=1$ 且令 a，$b \in \mathbf{Z}$。證明 $a \equiv b \pmod{m}$ 且 $a \equiv b \pmod{n}$ 若且唯若 $a \equiv b \pmod{mn}$。
7. 提供一個反例來證明前面習題的結果是錯的若 $\gcd(m, n)>1$。
8. 證明對所有整數 n，n，$2n-1$，和 $2n+1$ 中恰有一個可被 3 整除。
9. 若 $n \in \mathbf{Z}^+$ 且 $n>2$ 證明
$$\sum_{i=1}^{n-1} i \equiv \begin{cases} 0 \pmod{n}, & n \text{ 為奇數。} \\ \frac{n}{2} \pmod{n}, & n \text{ 為偶數。} \end{cases}$$
10. 完成定理 14.11 及 14.12 的證明。
11. 定義 $\mathbf{Z}^+$ 的關係 $\mathcal{R}$ 為 $a \mathcal{R} b$，若 $\tau(a)=\tau(b)$，其中 $\tau(a)=a$ 的正 (整數) 因子的個數。例如，$2 \mathcal{R} 3$ 且 $4 \mathcal{R} 25$ 但 $5 \not\mathcal{R} 9$。
    a) 證明 $\mathcal{R}$ 是 $\mathbf{Z}^+$ 上的一個等價關係。
    b) 對由 $\mathcal{R}$ 所導出的等價類 $[a]$ 和 $[b]$，定義加法和乘法的運算為 $[a]+[b]=[a+b]$ 且 $[a][b]=[ab]$。這些運算是良好定義的嗎？[亦即，$a \mathcal{R} c$，$b \mathcal{R} d$ 是否 $\Rightarrow (a+b) \mathcal{R} (c+d)$，$(ab) \mathcal{R} (cd)$？]。
12. 求 $\mathbf{Z}_{11}$，$\mathbf{Z}_{13}$ 及 $\mathbf{Z}_{17}$ 上各個元素的乘法反元素？
13. 求 $[a]^{-1}$ 於 $\mathbf{Z}_{1009}$ 上，對 (a) $a=17$, (b) a

$=100$，及 (c) $a=777$。

14. a) 求 $\mathbf{Z}_{12}$，$\mathbf{Z}_{18}$，及 $\mathbf{Z}_{24}$ 的所有子環。
    b) 分別對這些子環集建構 Hasse 圖，其中偏序來自集合包含。比較 n ($n=12$；18；24) 的正因數集的 Hasse 圖，其中偏序來自整除關係。
    c) 找公式給 $\mathbf{Z}_n$ 的子環個數，$n>1$。
15. 有多少個可逆元素及多少個 (真) 零因子於 (a) $\mathbf{Z}_{17}$？(b) $\mathbf{Z}_{117}$？(c) $\mathbf{Z}_{1117}$？
16. 證明在任意 n 個連續整數列裡，其中有一個整數可被 n 整除。
17. 若由集合 {1, 2, 3, ⋯, 1000} 中隨機選出三個相異整數，它們的和可被 3 整除的機率是多少？
18. a) 對 c，d，n，$m \in \mathbf{Z}$，其中 $n>1$ 且 $m>0$，證明若 $c \equiv d \pmod n$，則 $mc \equiv md \pmod n$ 且 $c^m \equiv d^m \pmod n$。
    b) 若 $x_n x_{n-1} \cdots x_1 x_0 = x_n \cdot 10^n + \cdots + x_1 \cdot 10 + x_0$ 表一個 $(n+1)$ 位整數，則證明

$$x_n x_{n-1} \cdots x_1 x_0 = x_n + x_{n-1} + \cdots + x_1 + x_0 \pmod 9$$

19. a) 證明對所有 $n \in \mathbf{N}$，$10^n \equiv (-1)^n \pmod{11}$。
    b) 考慮習題 18(b) mod 9 的結果。敘述並證明一個類比結果給 mod 11。
20. 對質數 p，求所有元素 $a \in \mathbf{Z}_p$，其中 $a^2 = a$。
21. 對 a，b，$n \in \mathbf{Z}^+$ 且 $n>1$，證明 $a \equiv b \pmod n \Rightarrow \gcd(a, n) = \gcd(b, n)$。
22. a) 證明對所有 $[a] \in \mathbf{Z}_7$，若 $[a] \neq [0]$，則 $[a]^6 = [1]$。
    b) 令 $n \in \mathbf{Z}^+$ 滿足 $\gcd(n, 7) = 1$。證明 $7 \mid (n^6 - 1)$。
23. 使用 Caesar 密碼將明語： “All Gaul is divided into three parts.” 譯成密語。
24. 密語 *FTQIMKIQIQDQ* 是使用譯成密語函數 $E: \mathbf{Z}_{26} \to \mathbf{Z}_{26}$，其中 $E(\theta) = (\theta + \kappa) \bmod 26$ 譯成的。考慮密語中字母出現的頻率，求 (a) 這個密碼推移的鍵值。(b) 破解密碼函數 D；且 (c) 原始的 (明語) 訊息。
25. 求下面各字母集的仿射密碼的總個數：(a) 24 個字母；(b) 25 個字母；(c) 27 個字母；及 (d) 30 個字母。
26. 密語

RWJWQTOOMYHKUXGOEMYP

係以一個仿射密碼譯成的。已知明語字母 e，t 分別被譯成密語字母 W，X，求 (a) 譯成密碼函數 E；(b) 破解密碼函數 D；及 (c) 原始的 (明語) 訊息。
27. (a) 以 $a=5$，$c=3$，$m=19$，及 $x_0=10$ 的線性同餘生成器產生多少個相異項？(b) 所產生的擬隨機元素的數列？
28. 已知模 m 及兩個種子 x_0，x_1 滿足 $0 < x_0$，$x_1 < m$，一個擬隨機數列可由 $x_n = (x_{n-1} + x_{n-2}) \bmod m$，$m \geq 2$，遞迴產生。這個生成器被稱為 Fibonacci 生成器。求前十個生成的隨機數，當 $m=37$ 且 $x_0=1$，$x_1=28$。
29. 令 $x_{n+1} = (ax_n + c) \bmod m$，其中 $2 \leq a < m$，$0 \leq c < m$，$0 \leq x_0 < m$，$0 \leq x_{n+1} < m$，且 $n \geq 0$。證明

$$x_n = (a^n x_0 + c[(a^n - 1)/(a-1)]) \bmod m, \quad 0 \leq x_n < m$$

30. 以 $a=7$，$c=4$，及 $m=9$，考慮線性同餘生成器。若 $x_4=1$，求種子 x_0。
31. 證明三個連續整數的立方和可被 9 整除。

32. 求 3^{55} 的最後一個數字。
33. 對 m，n，$r \in \mathbf{Z}^+$，令 $p(m, n, r)$ 計數將 m 分割成至多 n 個 (正) 被加數的分割數，其中各個被加數不大於 r。計算 $\sum_{k=0}^{n-1} p(k(n+1), n, n), n \in \mathbf{Z}^+$。
34. 給一環 $(R, +, \cdot)$，元素 $r \in R$ 被稱是**冪等的** (idempotent) 當 $r^2 = r$。若 $n \in \mathbf{Z}^+$ 滿足 $n \geq 2$，證明若 $k \in \mathbf{Z}_n$ 且 k 是冪等的，則 $n-k+1$ 是冪等的。
35. 對例題 14.17 末的雜湊函數，求 (a) h (123-04-2275)；(b) 一個社會保險號碼 n 滿足 $h(n) = 413$，因此一個和該例中號碼 081-37-6495 的碰撞。
36. 寫一個電腦程式 (或開發一個演算法) 來執行習題 35 的雜湊函數。
37. 某餐館的停車場有 41 個停車格，由 0 到 40 連續編號。一旦開進這個停車場，由停車管理員指定一個停車格給顧客，管理員使用雜湊函數 $h(k) = k$ **mod** 41，其中 k 是整數，其由顧客駕照的最後三個數字得到。更而，欲避免碰撞 (其中已被佔用的停車格可能被指派)，當此一情況產生，顧客被引導去停下一個 (連續的) 可用的停車格，其中 0 被假設在 40 之後

    (a) 假設有八輛汽車到達當餐館營業時。若這八個顧客駕照最後三個數字 (依他們到達的順序) 分別為

    206, 807, 137, 444, 617, 330, 465, 905

    則停車管理員應指定那些停車格給這八輛汽車的駕駛？

    (b) 在 (a) 中八個顧客到達之後，及這八個中任何一個可能離開前，第九個顧客到達，其駕照的最後三個數字是 00x。若這個顧客被指定停車格 5，則 x 的可能值為何？
38. 解下面線性同餘給 x。

    a) $3x \equiv 7 \pmod{31}$　　b) $5x \equiv 8 \pmod{37}$

    c) $6x \equiv 97 \pmod{125}$

14.4　環同態變換及同構變換

本章最後一節，我們將檢視遵守特殊性質 (環間) 的函數，而這些性質依賴環上封閉的二元運算。

例題 14.19

考慮環 $(\mathbf{Z}, +, \cdot)$ 及 $(\mathbf{Z}_6, +, \cdot)$，其中 $\mathbf{Z}_6$ 上的加法和乘法被定義在 14.3 節。

定義 $f: \mathbf{Z} \to \mathbf{Z}_6$ 為 $f(x) = [x]$。例如，$f(1) = [1] = [7] = f(7)$ 且 $f(2) = f(8) = f(2+6k) = [2]$，對所有 $k \in \mathbf{Z}$。(所以 f 是映成，雖然其不是一對一。)

對 $2, 3 \in \mathbf{Z}$，$f(2) = [2]$，$f(3) = [3]$ 且我們有 $f(2+3) = f(5) = [5] = [2] + [3] = f(2) + f(3)$，及 $f(2 \cdot 3) = f(6) = [0] = [2][3] = f(2) \cdot f(3)$。

事實上，對所有 $x, y \in \mathbf{Z}$，

$$\begin{array}{ccccc} f(x+y) & = & [x+y] & = & [x]+[y] & = & f(x)+f(y), \\ \uparrow & & & & & & \uparrow \\ \mathbf{Z} \text{ 上的加法} & & & & & & \mathbf{Z}_6 \text{ 上的加法} \end{array}$$

且

$$\begin{array}{ccccc} f(x \cdot y) & = & [xy] & = & [x][y] & = & f(x) \cdot f(y). \\ \uparrow & & & & & & \uparrow \\ \mathbf{Z} \text{ 上的乘法} & & & & & & \mathbf{Z}_6 \text{ 上的乘法} \end{array}$$

定義 14.8

令 $(R, +, \cdot)$ 和 $(S, \oplus, \odot)$ 為環。函數 $f: R \to S$ 被稱是一個**環同態變換** (ring homomorphism) 若對所有 $a, b \in R$，

a) $f(a+b) = f(a) \oplus f(b)$，且
b) $f(a \cdot b) = f(a) \odot f(b)$.

當函數 f 是映成時，我們稱 S 是 R 的一個**同態像** (homomorphic image)。

這個函數被稱**保留** (preserve) 環中的運算，因為有下面理由：考慮 $f(a+b) = f(a) \oplus f(b)$。首先將 a，b 加進 R 裡，接著求這個和在 S 的像 (在 f 之下)，我們得到相同結果，當我們先求 a，b 在 S 的像 (在 f 之下)，然後將 S 上的這兩個像**相加**。(因此，我們有函數運算和加法運算，可互相交換。) 類似的註解可被完成關於環的乘法運算。

對環 $\mathbf{Z}_4$ 和 $\mathbf{Z}_8$，定義函數 $f: \mathbf{Z}_4 \to \mathbf{Z}_8$ 為 $f([a]) = [a]^2 (= [a^2])$。則對所有 $[a], [b] \in \mathbf{Z}_4$，我們有

$$\begin{array}{ccccccccc} f([a][b]) & = & f([ab]) & = & [ab]^2 & = & ([a][b])^2 & = & [a]^2[b]^2 & = & f([a]) f([b]). \\ \uparrow & & & & & & & & & & \uparrow \\ \mathbf{Z}_4 \text{ 上的乘法} & & & & & & & & & & \mathbf{Z}_8 \text{ 上的乘法} \end{array}$$

因此，這個函數 f 保留環中的乘法運算。然而，對 $[1], [2] \in \mathbf{Z}_4$，我們發現 $f([1]+[2]) = f([3]) = [3]^2 = [1]$，而 $f([1]) + f([2]) = [1]^2 + [2]^2 = [1] + [4] = [5] (\neq [1]$ 於 $\mathbf{Z}_8$ 裡)。所以 f **無法**保留環中的加法運算——因此，f 不是一個環同態變換。

函數 $g: \mathbf{Z}_4 \to \mathbf{Z}_8$，被定義為 $g([a]) = 3[a]$，保留環中的加法運算，但不保留環中的乘法運算。

定義 14.9

令 $f: (R, +, \cdot) \to (S, \oplus, \odot)$ 是一個環同態變換。若 f 是一對一且映成，則 f 被稱是一個**環同構變換** (ring isomorphism) 且我們稱 R 和 S 為**同構環**(isomorphic rings)。

我們可認為同構環出現當“相同的”環被以兩種不同的語言處理。函數 f 提供一個字典或不含糊的翻譯由一個語言至另一個語言。

名詞“同態變換”(homomorphism) 和“同構變換”(isomorphism) 來自希臘文，其中 morphe 述及形狀或結構，homo 意指相似，且 iso 意指相等或相同。因此，同態環 (亦即，有兩個環，其中一個是另一個的同態像) 在結構上被認為是相似的，而同構環是 (抽象的) 相同結構的複製。

在定義 11.13，我們定義了圖同構的概念。在那裡，我們稱無向圖 $G_1 = (V_1, E_1)$ 和 $G_2 = (V_2, E_2)$ 同構當我們能找到一個函數 $f: V_1 \to V_2$ 滿足

a) f 是一對一且映成，及
b) $\{a, b\} \in E_1$ 若且唯若 $\{f(a), f(b)\} \in E_2$。

看看我們關於環同構變換，思考這裡的條件 (b) 的另一個方式是函數 f 保留無向圖 G_1 和 G_2 的結構。當 $|V_1| = |V_2|$，不難找到一個一對一且映成的函數 $f: V_1 \to V_2$。然而，對一個已知的頂點集 V，決定無向圖 $G = (V, E)$ 結構的是它的邊集 (其中頂點毗鄰被定義)。因此，一個一對一對應 $f: V_1 \to V_2$ 是一個圖同構變換，當它以保留這些頂點毗鄰來保留 G_1 和 G_2 的結構。

例題 14.20

對例題 14.5 的環 R 及環 $\mathbf{Z}_5$，函數 $f: R \to \mathbf{Z}_5$ 被給為

$$f(a) = [0], \quad f(b) = [1], \quad f(c) = [2], \quad f(d) = [3], \quad f(e) = [4]$$

提供我們一個環同構變換。

例如，$f(c + d) = f(a) = [0] = [2] + [3] = f(c) + f(d)$，而 $f(be) = f(e) = [4] = [1][4] = f(b)\, f(e)$。(因缺少其它方法和定理，所以為保留各個二元運算，共有 25 個此類等式必須被證明。)

由於共有 $5! = 120$ 個一對一函數 R 映至 $\mathbf{Z}_5$，是否有任何我們可使用的方法來決定這些函數中的某個何時是一個同構變換？由例題 14.20 的建議，下面定理提供一些方法，至少可開始決定何時兩環間的函數可為同態變換及同構變換。[這個定理的 (c) 和 (d) 依賴 14.2 節習題 20 和 21 的結果。]

定理 14.15 若 $f: (R, +, \cdot) \to (S, \oplus, \odot)$ 是一個環同態變換，則

a) $f(z_R) = z_S$，其中 z_R，z_S 分別是 R，S 的零元素；
b) $f(-a) = -f(a)$，對所有 $a \in R$；
c) $f(na) = nf(a)$，對所有 $a \in R$，$n \in \mathbf{Z}$；
d) $f(a^n) = [f(a)]^n$，對所有 $a \in R$，$n \in \mathbf{Z}^+$；且
e) 若 A 是 R 的一個子環，則 $f(A)$ 是 S 的一個子環。

證明：

a) $z_S \oplus f(z_R) = f(z_R) = f(z_R + z_R) = f(z_R) \oplus f(z_R)$。(為什麼？) 所以由 S 的加法消去律，我們有 $f(z_R) = z_S$。
b) $z_S = f(z_R) = f(a + (-a)) = f(a) \oplus f(-a)$。因為 S 上的加法反元素是唯一的且 $f(-a)$ 是 $f(a)$ 的一個加法反元素，得 $f(-a) = -f(a)$。
c) 若 $n = 0$，則 $f(na) = f(z_R) = z_S = nf(a)$。$n = 1$，結果亦為真，所以我們假設 $n = k$ (≥ 1) 時為真。以數學歸納法進行，我們檢視 $n = k + 1$ 的情形。由 14.2 節習題 20 的結果，我們得 $f((k+1)a) = f(ka + a) = f(ka) \oplus f(a) = kf(a) \oplus f(a)$ (為什麼？) $= (k+1)(f(a))$ (為什麼？)(注意：這裡有三種不同的加法。)

當 $n > 0$，$f(-na) = -nf(a)$。這個由我們前面的歸納法證明，本證明的 (b)，及定理 14.1 的 (b) 成立，因為 $f(-na) + f(na) = f(n(-a)) + f(na) = nf(-a) + nf(a) = n[f(-a) + f(a)] = n[-f(a) + f(a)] = nz_S = z_S$。因此，結果成立對所有的 $n \in \mathbf{Z}$。
d) 我們將這個結果留給讀者證明。
e) 因為 $A \neq \emptyset$，$f(A) \neq \emptyset$。若 $x, y \in f(A)$，則 $x = f(a)$，$y = f(b)$ 對某些 $a, b \in A$。則 $x \oplus y = f(a) \oplus f(b) = f(a + b)$，且 $x \odot y = f(a) \odot f(b) = f(ab)$，因為 $a + b$，$ab \in A$ (為什麼？)，所以 $x \oplus y$，$x \odot y \in f(A)$。而且，若 $x \in f(A)$ 則 $x = f(a)$ 對某些 $a \in A$。所以我們有 $f(-a) = -f(a) = -x$，且因為 $-a \in A$ (為什麼？)，我們有 $-x \in f(A)$。因此 $f(A)$ 是 S 的一個子環。

當同態變換是映成時，我們得到下面定理。

定理 14.16 若 $f: (R, +, \cdot) \to (S, \oplus, \odot)$ 是一個由 R 映成 S 的環同態變換，其中 $|S| > 1$，則

a) 若 R 有么元 u_R，則 $f(u_R)$ 是 S 的么元；

b) 若 R 有么元 u_R 且 a 是 R 的一個可逆元素，則 $f(a)$ 是 S 上的一個可逆元素，且 $f(a^{-1})=[f(a)]^{-1}$；

c) 若 R 是可交換的，則 S 是可交換的；且

d) 若 I 是 R 的一個理想，則 $f(I)$ 是 S 的一個理想。

證明：我們將證明 (d) 而將其它部份留給讀者。因為 I 是 R 的一個子環，由定理 14.15(e) 得 $f(I)$ 是 S 的一個子環。欲證明 $f(I)$ 是一個理想，令 $x \in f(I)$ 且 $s \in S$。則 $x=f(a)$ 及 $s=f(r)$，對某些 $a \in I$，$r \in R$。所以 $s \odot x = f(r) \odot f(a) = f(ra)$，因 $ra \in I$，且我們有 $s \odot x \in f(I)$。同理，$x \odot s \in f(I)$，所以 $f(I)$ 是 S 的一個理想。

這些定理增強同態變換及同構變換保留結構的方法。但我們可否發現對這些函數的任何使用，及使用它們來證明更多的定理嗎？欲幫助回答這個問題，我們以考慮下面例題開始。

例題 14.21

擴大 14.2 節習題 18 所發展的概念，令 R 為環 $\mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_5$，則 $|R| = |\mathbf{Z}_2| \cdot |\mathbf{Z}_3| \cdot |\mathbf{Z}_5| = 30$，且定義 R 上的加法和乘法運算如下：

對所有 $(a_1, a_2, a_3), (b_1, b_2, b_3) \in R$ 其中 $a_1, b_1 \in \mathbf{Z}_2, a_2, b_2 \in \mathbf{Z}_3$, 且 $a_3, b_3 \in \mathbf{Z}_5$,

$$\underset{\substack{\uparrow \\ \mathbf{R}\text{ 上的} \\ \text{加法}}}{(a_1, a_2, a_3) + (b_1, b_2, b_3)} = \underset{\substack{\uparrow \quad \uparrow \quad \uparrow \\ \mathbf{Z}_2\text{ 上的} \quad \mathbf{Z}_3\text{ 上的} \quad \mathbf{Z}_5\text{ 上的} \\ \text{加法} \quad \text{加法} \quad \text{加法}}}{(a_1 + b_1, a_2 + b_2, a_3 + b_3)}$$

且

$$\underset{\substack{\uparrow \quad \uparrow \quad \uparrow \quad \uparrow \\ R\text{ 上的} \quad \mathbf{Z}_2\text{ 上的} \quad \mathbf{Z}_3\text{ 上的} \quad \mathbf{Z}_5\text{ 上的} \\ \text{乘法} \quad \text{乘法} \quad \text{乘法} \quad \text{乘法}}}{(a_1, a_2, a_3) \cdot (b_1, b_2, b_3) = (a_1 \cdot b_1, a_2 \cdot b_2, a_3 \cdot b_3).}$$

定義函數 $f: \mathbf{Z}_{30} \to R$ 為 $f(x) = (x_1, x_2, x_3)$，其中

$$x_1 = x \bmod 2$$
$$x_2 = x \bmod 3$$
$$x_3 = x \bmod 5.$$

換句話說，x_1，x_2，和 x_3 分別是 x 被 2，3，和 5 除所得的餘數。

表 14.11 的結果證明 f 是一個函數，其為一對一且映成。

表 14.11

x (在$\mathbf{Z}_{30}$)	$f(x)$ (在R)	x (在$\mathbf{Z}_{30}$)	$f(x)$ (在R)	x (在$\mathbf{Z}_{30}$)	$f(x)$ (在R)
0	(0, 0, 0)	10	(0, 1, 0)	20	(0, 2, 0)
1	(1, 1, 1)	11	(1, 2, 1)	21	(1, 0, 1)
2	(0, 2, 2)	12	(0, 0, 2)	22	(0, 1, 2)
3	(1, 0, 3)	13	(1, 1, 3)	23	(1, 2, 3)
4	(0, 1, 4)	14	(0, 2, 4)	24	(0, 0, 4)
5	(1, 2, 0)	15	(1, 0, 0)	25	(1, 1, 0)
6	(0, 0, 1)	16	(0, 1, 1)	26	(0, 2, 1)
7	(1, 1, 2)	17	(1, 2, 2)	27	(1, 0, 2)
8	(0, 2, 3)	18	(0, 0, 3)	28	(0, 1, 3)
9	(1, 0, 4)	19	(1, 1, 4)	29	(1, 2, 4)

欲註明f是一個同構變換，令x，$y \in \mathbf{Z}_{30}$，則

$$\begin{aligned} f(x+y) &= ((x+y) \bmod 2, (x+y) \bmod 3, (x+y) \bmod 5) \\ &= (x \bmod 2, x \bmod 3, x \bmod 5) + (y \bmod 2, y \bmod 3, y \bmod 5) \\ &= f(x) + f(y), \end{aligned}$$

且

$$\begin{aligned} f(xy) &= (xy \bmod 2, xy \bmod 3, xy \bmod 5) \\ &= (x \bmod 2, x \bmod 3, x \bmod 5) \cdot (y \bmod 2, y \bmod 3, y \bmod 5) \\ &= f(x)f(y), \end{aligned}$$

所以f是一個同構變換。

在檢視表 14.11 時，我們發現，例如，

1) $f(0)=(0, 0, 0)$，其中 0 是 $\mathbf{Z}_{30}$ 的零元素且 (0, 0, 0) 是 $\mathbf{Z}_2\times\mathbf{Z}_3\times\mathbf{Z}_5$ 的零元素。
2) $f(2+4)=f(6)=(0, 0, 1)=(0, 2, 2)+(0, 1, 4)=f(2)+f(4)$。
3) 元素 21 是 9 在 $\mathbf{Z}_{30}$ 上的加法反元素，而 $f(21)=(1, 0, 1)$ 是 $f(9)=(1, 0, 4)$ 在 $\mathbf{Z}_2\times\mathbf{Z}_3\times\mathbf{Z}_5$ 上的加法反元素。
4) {0, 5, 10, 15, 20, 25} 是 $\mathbf{Z}_{30}$ 的一個子環，因 {(0, 0, 0) ($=f(0)$), (1, 2, 0) ($=f(5)$), (0, 1, 0) ($=f(10)$), (1, 0, 0) ($=f(15)$), (0, 2, 0) ($=f(20)$), (1, 1, 0) ($=f(25)$)} 為 $\mathbf{Z}_2\times\mathbf{Z}_3\times\mathbf{Z}_5$ 上相對應的子環。

但對這個介於 $\mathbf{Z}_{30}$ 和 $\mathbf{Z}_2\times\mathbf{Z}_3\times\mathbf{Z}_5$ 間的同構變換，我們還能做什麼其它的嗎？假設，例如，我們需計算 28・17 於 $\mathbf{Z}_{30}$ 上。我們可將這個問題轉至 $\mathbf{Z}_2\times\mathbf{Z}_3\times\mathbf{Z}_5$ 上且計算 $f(28)\cdot f(17)=(0, 1, 3)\cdot(1, 2, 2)$，其中模數

2，3，和 5 均小於 30 且較易於工作。因為 (0, 1, 3)・(1, 2, 2)＝(0・1, 1・2, 3・2)＝(0, 2, 1) 且 $f^{-1}(0, 2, 1)=26$，得 28・17 (在 $\mathbf{Z}_{30}$ 上) 是 26。

在例題 14.21，我們看到若我們被給 $\mathbf{Z}_2\times\mathbf{Z}_3\times\mathbf{Z}_5$ 上的一個元素 (x_1, x_2, x_3)，則我們可使用表 14.11 來求 $\mathbf{Z}_{30}$ 上的唯一元素使得 $f(x)=(x_1, x_2, x_3)$。但假若我們沒有這樣的表，我們將怎麼做呢？尤其，若我們發現我們在處理較大的環，例如 $\mathbf{Z}_{32736}$ 和 $\mathbf{Z}_{31}\times\mathbf{Z}_{32}\times\mathbf{Z}_{33}$，及同構變換 $g:\mathbf{Z}_{32736}\to\mathbf{Z}_{31}\times\mathbf{Z}_{32}\times\mathbf{Z}_{33}$，其中 $g(x)=(x \bmod 31, x \bmod 32, x \bmod 33)$ 對 $x\in\mathbf{Z}_{32736}$。下面結果提供一個技巧來決定像這樣的同構變換 g 的對應域上一個已知元素的唯一前像。

定理 14.17

中國餘數定理 (The Chinese Remainder Theorem)。令 $m_1, m_2, \cdots, m_k\in\mathbf{Z}^+-\{1\}$，其中 $k\geq 2$，且 $\gcd(m_i, m_j)=1$ 對所有 $1\leq i<j\leq k$，則 k 個同餘方程組

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}\\ x &\equiv a_2 \pmod{m_2}\\ &\vdots\\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

有一個聯立解。更而，方程組的任兩個此類解為同餘模 $m_1m_2\cdots m_k$。

證明：我們以證明如何建構 k 個同餘方程組的一個聯立解開始。

令 $m=m_1m_2\cdots m_k$，且對 $1\leq j\leq k$，令 $M_j=m/m_j$。[所以，例如 $M_1=m_2m_3m_4\cdots m_k$ 且 $M_2=m_1m_3m_4\cdots m_k$。] 我們發現對所有 $1\leq j\leq k$，$\gcd(m_j, M_j)=1$。若否，則對某些 (固定) j，其中 $1\leq j\leq k$，存在一個質數 p 滿足 $p|m_j$ 及 $p|M_j$。但由引理 4.3 得若 $p|M_j$ 則 $p|m_j$ 對某些 $1\leq j\leq k$，其 $i\neq j$。因此，我們發現 $p|m_j$ 且 $p|m_i$ 對 $i\neq j$，且這個和 $\gcd(m_i, m_j)=1$ 矛盾。

對每個 $1\leq j\leq k$，$\gcd(m_j, M_j)=1$。因此，由定理 14.14，我們知道 M_j 是 $\mathbf{Z}_{mj}$ 上的一個可逆元素。所以存在 $x_j\in\mathbf{Z}_{mj}$ 使得 $M_jx_j\equiv 1 \pmod{m_j}$。現在考慮和

$$x=a_1M_1x_1+a_2M_2x_2+\cdots+a_kM_kx_k.$$

我們要求 x 是 k 個同餘方程組的一個聯立解。注意對 $1\leq j\leq k$ 且 $1\leq i\leq k$，若 $i\neq j$，則 $M_i\equiv 0 \pmod{m_j}$，因為 $m_j|M_i$。因此，$M_ix_i\equiv 0 \pmod{m_j}$。因為 $M_jx_j\equiv 1 \pmod{m_j}$，我們發現

$$x\equiv a_jM_jx_j\equiv a_j \pmod{m_j},$$

對每個 $1 \le j \le k$。

現在假設 x，y 同時為 k 個同餘方程組的聯立解，則 $x \equiv y \pmod{m_j}$ 對所有 $1 \le j \le k$。考慮 $m = m_1 m_2 \cdots m_k$ 的質因數分解。令 p 為一質數滿足 $p^t | m$ 但 $p^{t+1} \nmid m$，對某些 $t \in \mathbf{Z}^+$。因為 $\gcd(m_i, m_j) = 1$ 對所有 $1 \le i < j \le k$，得 $p^t | m_j$ 對一個 (且僅有一個) 模 m_j。因此，我們看到 $p^t | (x - y)$，且所以由算術基本定理得 $m | (x - y)$，或 $x \equiv y \pmod{m}$。

現在讓我們看看我們可如何應用中國餘數定理。

例題 14.22

在 Marjorie 的四年級算術課上有三位學生——名叫 Megan，Avery，和 Elizabeth ——正在做長除法問題 (不使用計算器)。Marjorie 選一個正整數 n 且要求分別除以三個不同的除數後之餘數。Megan 除以 31 後得餘數 14。Avery 將 n 除以 32 且得餘數 16。同時，Elizabeth 得餘數 18，當她將 n 除以 33。則 Marjorie 能選的 n 最小值是多少？

這裡我們找三個同餘方程組

$$x \equiv 14 \pmod{31}, \quad x \equiv 16 \pmod{32}, \quad x \equiv 18 \pmod{33}.$$

的一個聯立解。所以 $a_1 = 14$，$a_2 = 16$，$a_3 = 18$，$m_1 = 31$，$m_2 = 32$，$m_3 = 33$，且 $m = m_1 m_2 m_3 = 32736$。更而，$M_1 = m/m_1 = 1056$，$M_2 = m/m_2 = 1023$，且 $M_3 = m/m_3 = 992$。使用歐幾里得演算法 (需要時)，例如題 14.13，我們得到

$$[x_1] = [M_1]^{-1} = [1056]^{-1} = [34(31) + 2]^{-1} = [2]^{-1} = [16] \text{ 於 } \mathbf{Z}_{m_1} = \mathbf{Z}_{31},$$
$$[x_2] = [M_2]^{-1} = [1023]^{-1} = [31(32) + 31]^{-1} = [31]^{-1} = [31] \text{ 於 } \mathbf{Z}_{m_2} = \mathbf{Z}_{32}, \text{ 且}$$
$$[x_3] = [M_3]^{-1} = [992]^{-1} = [30(33) + 2]^{-1} = [2]^{-1} = [17] \text{ 於 } \mathbf{Z}_{m_3} = \mathbf{Z}_{33}.$$

因此，

$$\begin{aligned} x &\equiv (14)(1056)(16) + (16)(1023)(31) + (18)(992)(17) \pmod{32736} \\ &\equiv 1047504 \pmod{32736} \\ &\equiv 31(32736) + 32688 \pmod{32736} \\ &\equiv 32688 \pmod{32736}. \end{aligned}$$

所以，Marjorie 能選的 (最小的) 正整數 n 是 32688。

(做一驗算，我們發現 $32688 = 1054(31) + 14 = 1021(32) + 16 = 990(33) + 18$，所以 x 滿足所給的三個同餘方程組且是滿足的最小正整數。)

現在若我們回看同構變換 $g : \mathbf{Z}_{32736} \to \mathbf{Z}_{31} \times \mathbf{Z}_{32} \times \mathbf{Z}_{33}$ (我們在敘述中國

餘數定理之前所提的) 我們看到對應域 $\mathbf{Z}_{31}\times\mathbf{Z}_{32}\times\mathbf{Z}_{33}$ 上的元素 (14, 16, 18)，定義域 $\mathbf{Z}_{32736}$ 上的元素 32688 是其 (唯一的) 前像。亦即，$g(32688)=(14, 16, 18)$ 且對任一其它整數 y，若 $g(y)=(14, 16, 18)$，則 $y\equiv 32688 \pmod{32636}$，所以 32688 是在 {0, 1, 2, 3, …, 32735} 中的唯一解。

例題 14.21 的同構變換 f 及例題 14.22 的 g 是我們現在將敘述的一個更一般的結果†之特殊情形。若 $n=n_{12}\cdots n_k$，其中 $n_i>1$ 對所有 $1\le i\le k$ 且 $\gcd(n_i, n_j)=1$ 對所有 $1\le i<j\le k$，則環 $\mathbf{Z}_n$ 和 $\mathbf{Z}_{n_1}\times\mathbf{Z}_{n_2}\times\cdots\times\mathbf{Z}_{n_k}$ 同構。特別地，由算術基本定理，我們知道對每個 $n\in\mathbf{Z}^+-\{1\}$，我們可將 n 分解為 $p_1^{e_1}p_2^{e_2}\cdots p_t^{e_t}$，其中 p_1，p_2，…，p_t 為 t 個相異質數，$t\ge 1$，且 e_1，e_2，…，$e_t\in\mathbf{Z}^+$。則得環 $\mathbf{Z}_n$ 和 $\mathbf{Z}_{m1}\times\mathbf{Z}_{m2}\times\cdots\times\mathbf{Z}_{m_t}$ 同構，其中 $m_1=p_1^{e_1}$, $m_2=p_2^{e_2}, \ldots, m_t=p_t^{e_t}$。

如同這個同構變換的一個結果，包含大整數 (超過所給電腦的字大小) 的算術可使用較小的相異模來執行。更而對這些較小模的計算可以平行電腦來執行——因此，可減少計算時間。[欲知更多有關中國餘數定理併用於電腦剩餘算術的應用，我們引導有興趣的讀者至 K. H. Rosen [12] 所著的教科書的第 146-149 頁，J. P. Tremblay 和 R. Manohar [14] 所著之教科書的第 344-359 頁，及 D. E. Knuth [8] 的教科書。

習題 14.4

1. 若 R 是例題 14.6 的環，試建構一個同構變換 $f: R\to\mathbf{Z}_6$。
2. 完成定理 14.15 及 14.16 的證明。
3. 若 R，S，及 T 為環且 $f: R\to S$，$g: S\to T$ 是環同態變換，證明合成函數 $g\circ f: R\to T$ 是一個環同態變換。
4. 若 $S=\left\{\begin{bmatrix} a & 0\\ 0 & a\end{bmatrix}\middle| a\in\mathbf{R}\right\}$，則 S 在矩陣加法和乘法之下是一個環。證明 $\mathbf{R}$ 和 S 同構。
5. a) 令 $(R, +, \cdot)$ 及 $(S, \oplus, \odot)$ 為分別具有零元素 z_R 及 z_S 的環。若 $f: R\to S$ 是一個環同態變換，令 $K=\{a\in R | f(a)=z_S\}$。證明 K 是 R 的一個理想。(K 被稱是同態變換 f 的**核集** (Kernel)。)
   b) 求例題 14.19 的同態變換之核集。
   c) 令 f，$(R, +, \cdot)$，和 $(S, \oplus, \odot)$ 如 (a) 所示。證明 f 是一對一若且唯若 f 的核集是 $\{z_R\}$。
6. 使用表 14.11 的資訊計算下面各個小題

† 在某些教科書，這個結果被述為中國餘數定理。

於 $\mathbf{Z}_{30}$ 裡。

a) (13)(23)＋18　b) (11)(21)－20

c) (13＋19)(27)　d) (13)(29)＋(24)(8)

7. a) 建構一個表 (如例題 14.21) 給同構變換 $f: \mathbf{Z}_{20} \to \mathbf{Z}_4 \times \mathbf{Z}_5$。

   b) 使用 (a) 的表來計算下面各小題於 $\mathbf{Z}_{20}$ 裡。

   (i) (17)(19)＋(12)(14)

   (ii) (18)(11)－(9)(15)

8. 令 n，r，$s \in \mathbf{Z}^+$，其中 n，r，$s \geq 2$，$n = rs$，且 $\gcd(r, s) = 1$。若 $f: \mathbf{Z}_n \to \mathbf{Z}_r \times \mathbf{Z}_s$ 是一個環同構變換滿足 $f(a) = (1, 0)$ 且 $f(b) = (0, 1)$，證明若 $(m, t) \in \mathbf{Z}_r \times \mathbf{Z}_s$，則 $f^{-1}(m, t) = ma + tb \pmod{n}$。

9. a) 環 $\mathbf{Z}_8$ 中有多少個可逆元素？

   b) 環 $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$ 中有多少個可逆元素？

   c) $\mathbf{Z}_8$ 和 $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$ 是同構環嗎？

10. a) $\mathbf{Z}_{15}$ 中有多少個可逆元素？$\mathbf{Z}_3 \times \mathbf{Z}_5$ 中有多少個可逆元素？

    b) $\mathbf{Z}_{15}$ 和 $\mathbf{Z}_3 \times \mathbf{Z}_5$ 同構嗎？

11. $\mathbf{Z}_4$ 和例題 14.4 的環同構嗎？

12. 若 $f: R \to S$ 是一個環同態變換且 J 是 S 的一個理想，證明 $f^{-1}(J) = \{a \in R | f(a) \in J\}$ 是 R 的一個理想。

13. 求兩個同餘方程組

$$x \equiv 5 \pmod 8$$
$$x \equiv 73 \pmod{81}.$$

的一聯立解。

14. 一群 17 個海盜擄掠一個充滿 (相同) 金幣的寶箱。當金幣被等數目來分時，剩 3 個金幣。有個海盜控訴分配者誤數且在決鬥中把他殺了。第二次，金幣以等數且重新分配，分給 16 位存活的海盜，剩 10 個金幣。爆發爭論且導致槍戰，因而致另一位海盜死亡。現在金幣被分成 15 個等堆，沒有金幣剩下。寶箱中可能有的金幣最小數是多少？

15. 求四個同餘方程組

$$x \equiv 1 \pmod 2$$
$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 5 \pmod 7.$$

14.5　總結及歷史回顧

強調由兩個封閉的二元運算所導出的結構，本章為我們介紹稱為環的數學系統。在整個數學發展裡，整數環扮演一個關鍵角色。在數論這個數學分支，我們檢視 $(\mathbf{Z}, +, \cdot)$ 的基本性質，並檢視有限環 $(\mathbf{Z}_n, +, \cdot)$。矩陣環提供熟悉的不可交換環的例子。

本章包含一個抽象理論的發展。基於環定義，我們建立基本代數原理，自從我們早先遇到的算術、符號數，及未知數的巧妙處理，我們已使

Pierre de Fermat (1601-1665)

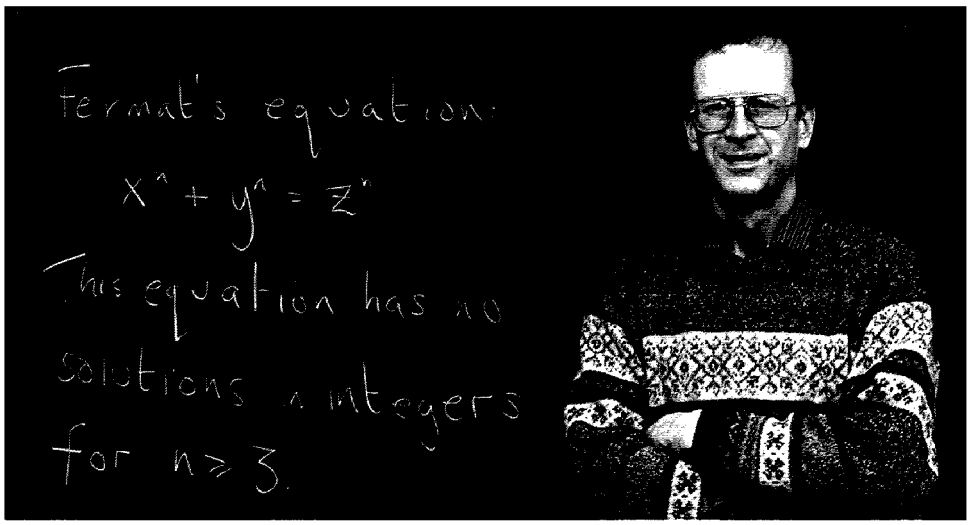
Sophie Germain (1776-1831)

用過這個原理。讀者可能已發現某些證明是令人生厭的，當我們在導演過程中驗證所有步驟時。面對試著證明抽象數學結果的挑戰時，吾人應追隨羅馬雄辯家 Marcus Fabius Quintilianu (西元第一世紀) 所給的忠告，他說：“吾人不應集中目標在可能瞭解 (或跟隨)，而應集中目標在不可能誤解”。

數論上一個著名問題，即著名的 *Fermat* 最後定理，其要求方程式 $x^n+y^n=z^n$，$n \in \mathbf{Z}^+$，$n>1$，在 $\mathbf{Z}^+$ 上無解當 $n>2$ 時。在 1637 年，法國數學家 Pierre de Fermat (1601-1665) 記載他已證明這個結果，但其證明太長，無法包含在他手稿的邊緣內。許多 18 世紀及 19 世紀出名的數學家試著證明這個結果——他們之中有 Leonhard Euler (1707-1783)，Peter Gustav Lejeune Dirichl (1805-1859)，Carl Friedrich Gauss (1777-1855)，Sophie Germain (1776-1831)，Adriel Marie Legendre (1752-1833)，Niels Henrik Abel (1802-1829)，Gabriel Lamé (1795-1870) 和 Leopold Kronecker (1823-1891)。雖然沒有成功，但努力再解 Fermat 要求，確實得到新的數學概念和理論。20 世紀亦有許多學者，他們付出驚人的努力在這個問題上面。其中有位學者於 1953 年出生在英國劍橋。在十歲那一年，他進去他住的小城的公立圖書館且查閱一本數學書。當他讀到 Fermat 最後定理時，它似乎是如此的簡單——且他想證明這個定理。1970 年代，Andrew Wiles 進入劍橋大學，且在他完成學位後，他成為劍橋的研究生專攻於數論方面——一個叫做 Iwasawa 理論的領域。因為在那時刻 Fermat 最後定理並不流行。當 Wiles完成他的博士學位後，他轉到美國，在普林斯頓大學任職。在 1980 年代，他對他小時候夢想的狂熱再被點起，且他花將近七年

的時間單獨工作——鎖在他的閣樓辦公室。他最後透露給他的同事 Nick Katz ——於 1993 年 1 月。1993 年 6 月，Wiles 教授回到劍橋，在一個數論的研討會上，他發表一序列的三個演講。最後一個演講是在熱烈的讚賞聲中結束，伴著鎂光燈的照像機及報告者的問題，似乎他已解了 Fermat 最後定理。不幸的，當他 200 頁的手稿由諸如 Nick Katz 的專家們仔細地檢閱時，問題開始出現，且證明上的漏洞導致每件事像紙牌屋的倒塌一樣。1993 年秋天，Wiles 回到普林斯頓——現在的他是氣餒的、生氣的，且是羞辱的。但在補強的努力後，於 1994 年 9 月 19 日，他看他的大綱證明最後一次。隔天早上他寫出一個新的證明，仿如每件事均進入其位置。這次沒人能發現任何瑕疵。1995 年 5 月出刊的 *Annals of Mathematics* 學報包含有 Andrew Wiles 原先的劍橋論文及 Wiles 和他的朋友也是他先前的學生 Richard Taylor 的修正論文。最後，Fermat 最後定理平息了。(雖然 Wiles 得到許多稱讚，其它許多數學家也應受推崇——他們之中有 Kenneth Ribet，Barry Mazur，Goro Shimura，Yutaka Taniyama，Gerhard Frey，Matthias Flach，和 Richard Taylor。) 欲知更多有關這個著名定理證明的歷史和發展，讀者被引導至由 A. D. Aczel [1] 所給的易讀的報告。

在試著證明 Fermat 最後定理，德國數學家 Ernst Kummer (1810-1893) 發展了理想 (ideal) 概念的基礎。這個概念稍後被他同鄉 Richard Dedekind (1831-1916) 明確的陳述、命名，且使用於他的研究裡。現在被命名為 Dedekind 域。然而，使用“環”這個名詞，似乎應歸功於德國數學家 David Mibert (1862-1943)。



Andrew John Wiles (1953-)

環同態變換及它和理想間的互相作用被德國數學家 Emmy Noether (1882-1935) 廣闊的發展。因為那時候大學普及的性別偏見，這個偉大的英才由她的祖國政府得到少許的薪水、財務或其它。雖然如此，Emmy Noether 的能力受到她同事的承認，且她被 Albert Einstein (1879-1955) 讚揚在 1935 年 5 月 3 日的紐約時報上，Einstein 感謝她的研究對相對論發展的影響和重要。除了忍受性別偏見之外，做為一個猶太人，她被迫於 1933 年逃離她的家鄉，當納粹掌權時。她將人生的最後兩年付出照顧美國的年輕數學家。欲多瞭解這個迷人的人物之一生，可檢視 A. Dick 所著的傳記及 C. Kimberling [7] 的文章。

Emmy Noether (1882-1935)

稱之為體 (field) 的特殊環出現在有理數系、實數系，及複數系。但我們亦看到一些有趣的有限體。這些結構將再被檢視於第 17 章和組合設計連結。體理論是法國天才 Evariste Galois (1811-1832) 在回答次數 > 4 的多項式方程之解時所發展出來的。這些問題令數學家挫折了好幾世紀，且他的概念，著名的 Galois 理論，仍然是至今所發展的最優雅的數學理論之一。欲知更多的 Galois 理論可參閱 O. Zariski 和 P. Samuel [16] 的書。

欲多讀導引層次的環論，有興趣的讀者應檢視 J. A. Gallian [5] 的第 12- 18 章，V. H. Larney [9] 的第 6 章，及 N. H. McCoy 和 T. R. Berger [10] 的第 6，7，及 12 章。一個稍為進階的教材可被發現於 E. A. Walker [15] 的第 4 章。

模同餘的發展，及許多相關概念，我們應歸功於 Carl Friedrich Gauss。包含同餘方程組的問題可追朔到第一世紀末，這些問題出現在 Gerasa 的希臘數學家 Nicomachus 方程式的作品上。兩個同餘方程組亦可

被發現於第 7 世紀數學家 Brahmagupta (於 598 年出生於印度西北部) 的作品裡。然而，直到 1247 年，我們才發現線性同餘方程組的一般解法之出版。在他的 *Shushu jiuzhang* (含九節的數學論文)，這個方法現在被稱為中國餘數定理，由中國數學家秦九韶 (西年 1202-1261) 所提出的。出生在成吉思汗時代的四川省，這位卓越的數學天才也是一位有才華的建築師、音樂家，及詩人，他也是一位完全的運動家——在弓術、劍術，及馬術等方面。更多的同餘之解及中國餘式定理可被發現於 I. Niven，H. S. Zuckerman，及 H. L. Montgomery [11] 及 K. H. Rosen [12] 的書裡。

如稍早所提的 (在例題 14.16 的註腳裡)，更多的密碼學歷史、發展，及應用可被發現於 T. H. Barr [3]，P. Garrett [6]，及 W. Trappe 和 L. C. Washington [13] 書裡。

最後，雜湊或分散的主題，可被進一步探討於 J. P. Tremblay 和 R. Manhar [14] 的第 2 章。A. V. Aho，J. E. Hopcroft，及 J. D. Ullman [2] 的第 4 章含有一個雜湊函數效率性的討論及由雜湊函數所產生的碰撞問題的一個蓋然性之探討。

參考資料

1. Aczel, Amir D. *Fermat's Last Theorem: Unlocking the Secret of an Ancient Mathematical Problem.* New York: Four Walls Eight Windows, 1996.
2. Aho, Alfred V., Hopcroft, John E., and Ullman, Jeffrey D. *Data Structures and Algorithms.* Reading, Mass.: Addison-Wesley, 1983.
3. Barr, Thomas H. *Invitation to Cryptology*. Upper Saddle River, N.J.: Prentice-Hall, 2002.
4. Dick, Auguste. *Emmy Noether (1882–1935)*, trans. Heidi Blocher. Boston: Birkhäuser-Boston, 1981.
5. Gallian, Joseph A. *Contemporary Abstract Algebra*, 5th ed. Boston: Houghton Mifflin, 2002.
6. Garrett, Paul. *Making, Breaking Codes: An Introduction to Cryptology*. Upper Saddle River, N.J.: Prentice-Hall, 2001.
7. Kimberling, Clark. "Emmy Noether, Greatest Woman Mathematician." *Mathematics Teacher* (March 1982): pp. 246–249.
8. Knuth, Donald Ervin. *The Art of Computer Programming*, 3rd ed., Volume 2, *Semi-Numerical Algorithms*. Reading, Mass.: Addison-Wesley, 1997.
9. Larney, Violet Hachmeister. *Abstract Algebra: A First Course*. Boston: Prindle, Weber & Schmidt, 1975.
10. McCoy, Neal H., and Berger, Thomas R. *Algebra: Groups, Rings and Other Topics*. Boston: Allyn and Bacon, 1977.
11. Niven, Ivan, Zuckerman, Herbert S., and Montgomery, Hugh L. *An Introduction to the Theory of Numbers*, 5th ed. New York: Wiley, 1991.
12. Rosen, Kenneth H. *Elementary Number Theory*, 4th ed. Reading, Mass.: Addison-Wesley, 1999.
13. Trappe, Wade, and Washington, Lawrence C. *Introduction to Cryptography with Coding Theory*. Upper Saddle River, N.J.: Prentice-Hall, 2002.
14. Tremblay, Jean-Paul, and Manohar, R. *Discrete Mathematical Structures with Applications to Computer Science*. New York: McGraw-Hill, 1975.

15. Walker, Elbert A. *Introduction to Abstract Algebra*. New York: Random House/Birkhäuser, 1987.
16. Zariski, Oscar, and Samuel, Pierre. *Commutative Algebra*, Vol. I. Princeton, N.J.: Van Nostrand, 1958.

補充習題

1. 判斷下面各敘述的真假。若敘述為假，請給一個反例。
   a) 若 $(R,+,\cdot)$ 是一個環，且 $\emptyset \neq S \subseteq R$ 滿足 S 在 $+$ 和 $\cdot$ 之下是封閉的，則 S 是 R 的一個子環。
   b) 若 $(R,+,\cdot)$ 是一個具有么元的環，且 S 是 R 的子環，則 S 有一個么元。
   c) 若 $(R,+,\cdot)$ 是一個具有么元 u_R 的環，且 S 是 R 的一個具有么元 u_S 的子環，則 $u_R = u_S$。
   d) 每個體是一個整環。
   e) 體的每個子環是一個體。
   f) 有個體可僅有兩個子環。
   g) 每個有限體有質數個元素。
   h) 體 $(\mathbf{Q},+,\cdot)$ 有無限多個子環。
2. 證明環 R 是可交換的若且唯若 $(a+b)^2 = a^2+2ab+b^2$，對所有 $a, b \in R$。
3. 環 R 被稱是布林 (Boolean) 環若 $a^2 = a$ 對所有 $a \in R$。若 R 是布林環，證明 (a) $a+a = 2a = z$，對所有 $a \in R$；且 (b) R 是可交換的。
4. 以複數體 $\mathbf{C}$，及型如 $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ 的 2×2 實矩陣所成的環 S，定義 $f: \mathbf{C} \to S$ 為 $f(a+bi) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$，對 $a+bi \in \mathbf{C}$。證明 f 是一個環同構變換。
5. 若 $(R,+,\cdot)$ 是一個環，證明 $C = \{r \in R | ar = ra,$ 對所有 $a \in R\}$ 是 R 的一個子環。(子環 C 被稱是 R 的中心(center))。
6. 給一個有限體 F，令 $M_2(F)$ 為元素來自 F 的所有 2×2 矩陣所成的集合。如在例題 14.2，$(M_2(F), +, \cdot)$ 是一個具有么元的不可交換環。
   a) 分別求 $M_2(F)$ 裡的元素個數，若 F 是
   i) $\mathbf{Z}_2$　ii) $\mathbf{Z}_3$　iii) $\mathbf{Z}_p$，p 是質數。
   b) 如 14.1 節的習題 13，$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbf{Z}_p)$ 是一個可逆元素若且唯若 $ad - bc \neq z$。這個將發生若 A 的第一列不全為 0 (亦即，z 的 0) 且第二列不是第一列的倍數 (此倍數為 $\mathbf{Z}_p$ 的某元素)。使用這個觀察，決定下面各題的可逆元素個數：
   i) $M_2(\mathbf{Z}_2)$　ii) $M_2(\mathbf{Z}_3)$　iii) $M_2(\mathbf{Z}_p)$，p 為質數。
7. 給一個具有零元素 z 的整環 $(D,+,\cdot)$，令 $a, b \in D$ 滿足 $ab \neq z$。(a) 若 $a^3 = b^3$ 且 $a^5 = b^5$，證明 $a = b$。(b) 令 $m, n \in \mathbf{Z}^+$ 滿足 $\gcd(m, n) = 1$。若 $a^n = b^m$ 且 $a^m = b^n$，證明 $a = b$。
8. 令 $A = \mathbf{R}^+$。定義 $\oplus$ 和 $\odot$ 在 A 上為 $a \oplus b = ab$，即 a, b 的尋常積；及 $a \odot b = a^{\log_2 b}$。
   a) 證明 $(A, \oplus, \odot)$ 是一個具有么元的可

交換環。

b) 這個環是一個整環或是一個體嗎？

9. 令 R 是一個具有理想 A 和 B 的環。定義 $A+B=\{a+b|a\in A, b\in B\}$。證明 $A+B$ 是 R 的一個理想。(對任意環 R，R 的理想在集合包含下形成一個偏序集。若 A 和 B 是 R 的理想，滿足 $\text{glb}\{A, B\}=A\cap B$ 且 $\text{lub}\{A, B\}=A+B$，則這個偏序集是一個格點。)

10. a) 若 p 是一個質數，證明 p 整除 $\binom{p}{k}$，對所有 $0<k<p$。

b) 若 a，$b\in\mathbf{Z}$，證明 $(a+b)p\equiv a^p+b^p \pmod p$。

11. 給 n 個正整數 x_1，x_2，…，x_n，未必相異，證明不是 $n|(x_1+x_2+\cdots+x_i)$，對某些 $1\le i\le n$，就是存在 $1\le i<j\le n$ 滿足 $n|(x_{i+1}+\cdots+x_{j-1}+x_j)$。

12. 考慮環 $(\mathbf{Z}^3, \oplus, \odot)$，其中加法和乘法被定義為 $(a, b, c)\oplus(d, e, f)=(a+d, b+e, c+f)$ 及 $(a, b, c)\odot(d, e, f)=(ad, be, cf)$。(此處，例如，$a+d$ 和 ad 係使用 $\mathbf{Z}$ 上標準的加法及乘法的二元運算來計算。) 令 S 為 $\mathbf{Z}^3$ 的子集合，其中 $S=\{(a, b, c)|a=b+c\}$。證明 S 不是 $(\mathbf{Z}^3, \oplus, \odot)$ 的子環。

13. a) 有多少種方法，吾人可選兩個正整數 m，n，未必相異，使得 $1\le m\le 100$，$1\le n\le 100$，且 7^m+3^n 的最後數字是 8？

b) 若 $1\le m\le 125$，$1\le n\le 125$，回答 (a)。

c) 若吾人隨機選 m，n [如 (a)]，則 7^m+3^n 的最後數字是 2 的機率為何？

14. 令 $n\in\mathbf{Z}^+$ 滿足 $n>1$。

a) 若 $n=2k$，其中 k 是奇數，證明
$$k^3\equiv k \pmod n。$$

b) 若 $n=4k$，對某些 $k\in\mathbf{Z}^+$，證明
$$(2k)^2\equiv 0 \pmod n。$$

c) 證明
$$\sum_{i=1}^{n-1} i^3 \equiv \begin{cases} \frac{n}{2} \pmod n, & \text{對 } n \text{ 為偶數且} \frac{n}{2} \text{ 為奇數} \\ 0 \pmod n, & \text{其它。} \end{cases}$$

15. 假設 a，b，$c\in\mathbf{Z}$ 且 $5|(a^2+b^2+c^2)$。證明 $5|a$ 或 $5|b$ 或 $5|c$。

16. 寫一個電腦程式 (或開發一個演算法) 來顛倒一個已知正整數的數字順序。例如，輸入 1374 應得輸出 4731。

17. 假設 a，b，$k\in\mathbf{Z}^+$ 滿足 $a-b=p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$，其中 p_1，p_2，…，p_k 為質數且 e_1，e_2，…，$e_k\in\mathbf{Z}^+$，有多少個 n 值可使 $a\equiv b \pmod n$ 為真？

18. 身為回家遊行委員會的副主席 Jerina 和 Noor 必須組織新生來一個預演。當他們安排這些學生成 8 位一列時，尚餘 3 位學生。當試著 11 位為一列時，尚餘 4 位學生。最後，以 15 位為一列時，尚餘 5 位學生。所以兩位副主席使用 15 位為一列的排法且將剩餘的 5 位學生排在第一列的中央 (即位置 6-10)。Jerina 和 Noor 試著安排的新生之最小數是多少？