§4. 同餘

1. 一般觀念

每當整數被除以一個固定的整數 d，因而出現整數之可（整）除性的問題時，出自高斯的「同餘」（congruence）觀念及其記號方法，便可用來使推理變得清晰明瞭和簡化。

為了使讀者熟悉「同餘」這一個觀念，讓我們把各整數用 5 去除，然後檢查各個餘數。我們可得下列各種情況：

$$
\begin{array}{lll}
0=0\cdot 5+0 & 7=1\cdot 5+2 & -1=-1\cdot 5+4 \\
1=0\cdot 5+1 & 8=1\cdot 5+3 & -2=-1\cdot 5+3 \\
2=0\cdot 5+2 & 9=1\cdot 5+4 & -3=-1\cdot 5+2 \\
3=0\cdot 5+3 & 10=2\cdot 5+0 & -4=-1\cdot 5+1 \\
4=0\cdot 5+4 & 11=2\cdot 5+1 & -5=-1\cdot 5+0 \\
5=1\cdot 5+0 & 12=2\cdot 5+2 & -6=-2\cdot 5+4 \\
6=1\cdot 5+1 & \cdots\cdots\cdots\cdots & \cdots\cdots\cdots\cdots
\end{array}
$$

我們察覺到當任何整數被除以 5 時，留下的餘數將是五個整數 $0,1,2,3,4$ 中之一個。當兩個整數 a 與 b 除以 5 而留下相同的餘數時，我們稱 a 與 b 這兩個整數為「同餘於模（congruence modulo） 5」。因此 $2,7,12,17,22,\cdots,-3,-8,-13,-18,\cdots$ 等對模數 5 皆同餘，因為它們留下相同的餘數 2。一般來說，如果 a 與 b 除以 d 之後留下相同的餘數，其中 d 為固定整數，也就是說，如果有那麼一個整數 n 使得 $a-b=nd$，那麼兩個整數 a 與 b 便可被稱為是同餘於模 d。譬如說，27 與 15 是同餘於模 4，因為

$$27=6\cdot 4+3,\quad 15=3\cdot 4+3,$$

由於同餘的觀念相當有用，因此值得為它取得一個簡潔的代表符號。我們用下列代號

$$a\equiv b \pmod{d}$$

以表示 a 與 b 是同餘於模 d。如果模數已屬確實無疑，那麼公式中的「$\bmod d$」便可省略。（如果 a 不與 b 同餘於模 d，我們便以 $a \not\equiv b \pmod{d}$ 來表示。）

同餘的例子常常出現於日常生活。譬如說，時鐘的指針表示小時的模數是 12，汽車的英里里程表指定了總里程的模數為 100,000。

對同餘問題進行細節討論之前，讀者們應該注意到下面的一些意義都是相同的表述：

1. a 與 b 同餘於模 d。

2. $a = b + nd$，其中 n 為某整數。

3. d 整除 $a - b$。

高斯創造的同餘概念之所以有用乃在於：就一個固定模數的同餘而言，它擁有許多在常見的相等關係上合乎邏輯形式的性質。下列就是 $a = b$ 的關係中最重要的形式性質：

1) 毫無例外 $a = a$。

2) 如果 $a = b$，那麼 $b = a$。

3) 如果 $a = b$ 且 $b = c$，那麼 $a = c$。

還有，如果 $a = a'$ 且 $b = b'$，那麼

4) $a + b = a' + b'$。

5) $a - b = a' - b'$。

6) $ab = a'b'$。

當 $a = b$ 的關係用同餘關係 $a \equiv b \pmod{d}$ 去取代時，各種形式性質仍舊正確合理。因此

1') 毫無例外 $a \equiv a \pmod{d}$。

2') 如果 $a \equiv b \pmod{d}$，那麼 $b \equiv a \pmod{d}$ 。

3') 如果 $a \equiv b \pmod{d}$ 且 $b \equiv c \pmod{d}$，那麼 $a \equiv c \pmod{d}$ 。

上面這些同餘等同性質的證明便留給讀者了。

此外，如果 $a \equiv a' \pmod{d}$ 且 $b \equiv b' \pmod{d}$，那麼

4') $a + b \equiv a' + b' \pmod{d}$ 。

5') $a - b \equiv a' - b' \pmod{d}$ 。

6') $ab \equiv a'b' \pmod{d}$ 。

因此，**就同一模數的諸同餘而言，它們是可以相加、相減和相乘**。要證明這些性質我們只須注意到，要是

$$a = a' + rd, \quad b = b' + sd ,$$

那麼

$$\begin{aligned} a + b &= a' + b' + (r + s)d \\ a - b &= a' - b' + (r - s)d \\ ab &= a'b' + (a's + b'r + rsd)d \end{aligned}$$

而我們所希望的結論遂隨之可得。

同餘的觀念具有一個富於啟發性的幾何詮釋。通常假如我們想把整數用幾何圖形去表示的話，我們便選取一特定單位長的線段，然後在兩端增加其自身長度而作延伸。利用這種方式，我們便能夠在直線上找到相對應於每一個整數的每一點，如圖 6 所示。然而當我們處理以 d 為模數的一類整數時，任何兩個同餘於模 d 的整數——就它們被除以 d 之後所發生的變化來看——被視為相同，此乃由於兩者留下相同的餘數之故。為了用幾何圖形來表示，我們利用一個分為 d 個相同部分的圓周作為表示這種情況的幾何方式。當任何一個整數被除以 d 時，它所留下的餘數是 $0, 1, \cdots, d-1$ 諸數當中之一個，而這 d 個餘數就是位於圓周等分間隔上的區分點。每一個整數與 $0, 1, \cdots, d-1$ 其中之一個同餘於 d，因此它的幾何表示方式就是這些

在圓周上的等分點的其中一點；如果兩個整數由同一點來代表，那麼它們便是同餘。圖 7 是按模數 $d = 6$ 的情況而作。時鐘表面則是來自日常生活的另一個實例。

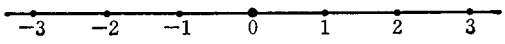

圖 6. 整數之幾何表示。

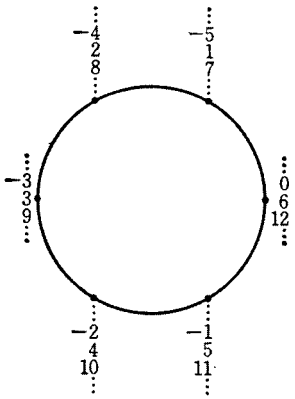

圖 7. 整數同餘於模 6 之幾何表示。

以同餘的乘法等同性質 6') 用來作為一個例子，當 10 的各個相繼乘方分別被除以某個相同的已知整數時，我們便可以把留下的諸餘數確定出來。譬如說，

$$10 \equiv -1 \pmod{11},$$

這是由於 $10 = 11 \cdot 1 + (-1)$。若把這個同餘連續自乘，所得結果為

$$\begin{aligned} 10^2 &\equiv (-1)(-1) = 1 && \pmod{11}, \\ 10^3 &\equiv -1 && \pmod{11}, \\ 10^4 &\equiv 1 && \pmod{11}, \end{aligned}$$ 等等。

據此我們便能夠證明任何一個用十進制來表示的整數

$$z = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + a_n \cdot 10,$$

以及整數 z 之各個位數值正負交替地相加起來之總和

$$t = a_0 - a_1 + a_2 - a_3 + \cdots,$$

分別被除以11之後各自得出之餘數是相同。這是因為，我們可以把 z 和 t 結合起來而有

$$z - t = a_1 \cdot 11 + a_2(10^2 - 1) + a_3(10^3 + 1) + a_4(10^4 - 1) + \cdots,$$

鑒於表示式中的各個整數 $11, 10^2 - 1, 10^3 + 1, \cdots$ 皆與0一致同餘於模11，可知 $z - t$ 的情況也是一樣，因此 z 被除以11之後，留下來的餘數與 t 被除以11所留下的餘數相同。隨之特別是一個可以被11整除的整數（就是說留下的餘數是0）乃是在而且只有在它的各個位數值正負交替之和為11所整除的情況下才行。舉例來說，由於 $3 - 1 + 6 - 2 + 8 - 1 + 9 = 22$，因此整數3162819能被11整除。若要找出能為3或9整除的規律則更為簡單，對任何整數 n 來說，由於 $10 \equiv 1 \pmod{3 \text{ 或 } 9}$，因此 $10^n \equiv 1 \pmod{3 \text{ 或 } 9}$。從而可見某一個數 z 之得以被3或9整除乃是在而且只有在其各個位數之和

$$s = a_0 + a_1 + a_2 + \cdots + a_n$$

同樣是分別為3或9所整除的情況下才行。

關於同餘於模數為7的情況，我們可看到

$$10 \equiv 3, \quad 10^2 \equiv 2, \quad 10^3 \equiv -1, \quad 10^4 \equiv -3, \quad 10^5 \equiv -2, \quad 10^6 \equiv 1。$$

相繼的各個10的乘方被除以7之後的各個餘數便再度重複出現。因此某數 z 之可被7整除乃是在而且只有在下面所示的一個數

$$r = a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + a_6 + 3a_7 + \cdots$$

同樣也可以為7所整除的情況下才行。

◆練習題：

試找出整數能被13整除之類似定律。

就一個固定模值——以5為例——的各個同餘在相加和相乘方面而言，我們始終可以用組合$0,1,2,3,4$中的一個數去取代任何一個有同餘關係的數a，以防止參與計算過程的各個數變得過大。因此為了估算同餘於模5的各整數之和及相乘積，我們只須利用下面的加法和乘法表便可。

$a+b$

$b \equiv$	0	1	2	3	4
$a \equiv 0$	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

$a \cdot b$

$b \equiv$	0	1	2	3	4
$a \equiv 0$	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

據乘法表所示，一個相乘積ab與0一致同餘於模5所需要的唯一條件是當$a \equiv 0$或$b \equiv 0 \pmod 5$。這便帶來了一條通則

7') $ab \equiv 0 \pmod d$所需要的唯一條件是當$a \equiv 0$或$b \equiv 0 \pmod d$，

這條同餘規律是一條相關的整數規律的延伸，即只有當$a=0$或$b=0$時，才能使整數a與b的相乘積為零，$ab=0$。**通則7') 只能在模數d是一個質數的情況下才適用**。因為同餘

$$ab \equiv 0 \pmod d$$

所指的是d可整除ab，而我們已曉得只有在質數d可整除a或b時，即只有在

$$a \equiv 0 \pmod d \quad 或 \quad b \equiv 0 \pmod d$$

其中之一種情況下，相乘積ab才可被d整除。

假如d不是一個質數，通則7') 便無法維持；因為我們可以把d表示如$d = r \cdot s$，其中r與s皆小於d，因此

$$r \not\equiv 0 \pmod{d}, \quad s \not\equiv 0 \pmod{d},$$

但是

$$r \cdot s = d \equiv 0 \pmod{d},$$

譬如說，$2 \not\equiv 0 \pmod{6}$、$3 \not\equiv 0 \pmod{6}$，然而$2 \cdot 3 = 6 \equiv 0 \pmod{6}$。

◆練習題：

試證明下面的消去法（law of cancellation）是適用於皆以同一個質數為模的各個同餘：如果$ab \equiv ac$、$a \not\equiv 0$，那麼 $b \equiv c$ 。

◆練習題：

1) 介於0與6之間（包括0與6）的哪一個數是與相乘積$11 \cdot 18 \cdot 2322 \cdot 13 \cdot 19$同餘於模7？

2) 介於0與12之間（包括0與12）的哪一個數是與相乘積$3 \cdot 7 \cdot 11 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 113$同餘於模13？

3) 介於0與4之間（包括0與4）的哪一個數是與幾何級數$1 + 2 + 2^2 + \cdots + 2^{19}$之和同餘於模5？

2. 費馬小定理

現代數論奠基者，法國大數學家費馬於十七世紀發現一個至為重要的定理：**如果任何一個質數 p 不能整除整數 a，那麼**

$$a^{p-1} \equiv 1 \pmod{p},$$

這就是說，a 的 $(p-1)$ 乘方除以 p 之後所得餘數是 1。

前面的一些計算其實已證實了這個定理；舉例來說，我們已碰上 $10^6 \equiv 1 \pmod{7}$，$10^2 \equiv 1 \pmod{3}$，和 $10^{10} \equiv 1 \pmod{11}$。我們亦可以證明 $2^{12} \equiv 1 \pmod{13}$，和 $5^{10} \equiv 1 \pmod{11}$。為了核對後者我們不必實際上從事高乘方的計算，因為我們可以利用同餘相乘性質所帶來的有利條件：

$$\begin{aligned}
&2^4 = 16 \equiv 3 && \pmod{13}, && 5^2 \equiv 3 && \pmod{11},\\
&2^8 = 9 \equiv -4 && \pmod{13}, && 5^4 \equiv 9 \equiv -2 && \pmod{11},\\
&2^{12} \equiv -4 \cdot 3 = -12 \equiv 1 && \pmod{13}, && 5^8 \equiv 4 && \pmod{11},\\
& && && 5^{10} \equiv 3 \cdot 4 = 12 \equiv 1 && \pmod{11}
\end{aligned}$$

為了證明費馬小定理，我們從 a 的倍數著手考量，

$$m_1 = a, \quad m_2 = 2a, \quad m_3 = 3a, \quad \cdots, \quad m_{p-1} = (p-1)a,$$

在這些整數當中，任何兩個皆不可能同餘於模 a，因為要是這樣的話 a 便將會是 $m_r - m_s = (r-s)a$ 的一個因子，其中 r 與 s 是被界定於 $1 \le r < s \le (p-1)$ 範圍之內的某一對整數。但按定律 7')，這是不可能出現的；因為既然 $s-r$ 是小於 p，p 便不是 $s-r$ 的因子，而根據假設，p 不是 a 的一個因子。同理，沒有一個 a 的倍數與 0 是同餘於模 p。因此 $m_1, m_2, \cdots, m_{p-1}$ 必然在某種安排下分別與 $1, 2, 3, \cdots, p-1$ 一致同餘於模 p，從而可得

$$m_1 m_2 \cdots m_{p-1} = 1 \cdot 2 \cdot 3 \cdots (p-1) a^{p-1} \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p},$$

或者如果為簡單起見，我們用 K 去代表 $1 \cdot 2 \cdot 3 \cdots (p-1)$，

$$K(a^{p-1} - 1) \equiv 0 \pmod{p},$$

然而 K 不能為 p 所整除，因為在 K 的因子中，沒有一個能被 p 所整除；因此根據定律 7')，$(a^{p-1}-1)$ 必定可被 p 整除，也就是說

$$a^{p-1}-1 \equiv 0 \pmod{p},$$

這就是費馬小定理（Fermat's theorem）。

為了再一次證明費馬小定理無誤，讓我們以 $p=23$ 和 $a=5$ 為例。於是從所有以 23 為模的 5 的乘方中，

$$5^2 \equiv 2, \quad 5^4 \equiv 4, \quad 5^8 \equiv 16 \equiv -7,$$
$$5^{16} \equiv 49 \equiv 3, \quad 5^{20} \equiv 12, \quad 5^{22} \equiv 24 \equiv 1$$

若以 $a=4$ 取代 5，我們再一次得到以 23 為模的諸數為：

$$4^2 \equiv -7, \quad 4^3 \equiv -28 \equiv -5, \quad 4^4 \equiv -20 \equiv 3,$$
$$4^8 \equiv 9, \quad 4^{11} \equiv -45 \equiv 1, \quad 4^{22} \equiv 1$$

從上面 $a=4$、$p=23$ 的實例以及其它的例子中，我們察覺到不僅僅 a 的 $(p-1)$ 乘方與 1 是同餘於模 a，一個較低的 a 的乘方亦可能如此，而這類 a 的較低乘方中之最低值必然可把 $p-1$ 整除，在上述實例中 11 就是最低值（證明見下面之練習題 3）。

◆練習題：

1) 試沿用類似的計算，證明

$$2^8 \equiv 1 \pmod{17} \qquad 3^8 \equiv -1 \pmod{17} \qquad 3^{14} \equiv -1 \pmod{29}$$
$$2^{14} \equiv -1 \pmod{29} \qquad 4^{14} \equiv 1 \pmod{29} \qquad 5^{14} \equiv 1 \pmod{29}$$

2) 試用 $p=5,7,11,17,23$ 以及不同的 a 值以核對費馬小定理。

3) 證明下面的普遍定理：滿足 $a^e \equiv 1 \pmod{p}$ 的最小正整數 e 必須能整除 $p-1$。（提示：用 e 去除 $p-1$ 可得

$$p-1 = ke+r,$$

其中 $0 \le r < e$，並根據 $a^{p-1} \equiv a^e \equiv 1 \pmod{p}$ 這個事實加以利用。）

3. 二次剩餘

從引證費馬小定理的例題中，我們發現不僅僅 $a^{p-1} \equiv 1 \pmod{p}$ 始終成立，而且對一些不能為 p 所整除的 a 值來說（如果 p 是有別於 2 的一個質數，因此 p 是奇數，而且是以 $p = 2p' + 1$ 為形式）我們還可有 $a^{p'} = a^{(p-1)/2} \equiv 1 \pmod{p}$。這一個論據啟發了一連串有趣的研究。我們可以把費馬小定理用下面形式來表示：

$$a^{p-1} - 1 = a^{2p'} - 1 = (a^{p'} - 1)(a^{p'} + 1) \equiv 0 \pmod{p},$$

基於一個可被整除之相乘積僅僅只需其中一個因子能被整除便成，從上面的表示便馬上可知，$a^{p'} - 1$ 或 $a^{p'} + 1$ 其中之一必須可被 p 整除，因此對任何大於 2 的質數 p 以及不能被 p 整除的任何整數 a 而言，要麼 $a^{(p-1)/2} \equiv 1 \pmod{p}$，要麼 $a^{(p-1)/2} \equiv -1 \pmod{p}$，二者之中必然有一個會出現。

數學家從現代數論一開始成形，就已經對找出 a 是什麼樣的數，才會出現第一個情況和第二個情況而深感興趣。假定 a 與某一個數 x 的平方一致同餘於模 p，

$$a \equiv x^2 \pmod{p},$$

那麼 $a^{(p-1)/2} \equiv x^{p-1}$，而根據費馬小定理，$a^{(p-1)/2}$ 與 1 是同餘於模 p。若整數 a 與某整數之平方同餘於模 p 而同時 a 不是 p 的倍數，a 遂被稱為 p 的一個**二次剩餘**（quadratic residue），同理，不是 p 的倍數但不與任何一個整數之平方同餘於 p 的整數 b，則被稱為 p **之非二次剩餘**（quadratic non-residue）。我們剛才已獲知，作為 p 的二次剩餘，每一個整數 a 滿足同餘關係 $a^{(p-1)/2} \equiv 1 \pmod{p}$。在沒有多大困難的情況下便可證實每一個 p 的非二次剩餘的整數 b 之同餘關係為 $b^{(p-1)/2} \equiv -1 \pmod{p}$。接著下來我們現在要指出，在諸數 $1, 2, 3, \cdots, p-1$ 當中，恰恰有 $(p-1)/2$ 個整數是二次剩餘，而另一半的 $(p-1)/2$ 個整數則是非二次剩餘。

雖然從直接計算中可收集大量的實際數據，但是要從頭開始發掘出一條統攝二次剩餘和非二次剩餘的普遍律公諸於世則並非易事。有關二次剩餘與非二次剩餘的第一個潛藏性質是勒讓德所發現，這就是後來由高斯命名的**二次互反律**（Law of Quadratic Reciprocity）。該定律關係到兩個不同質數 p 與 q 在特定情況下出現的

變化，指出 q 之成為 p 的二次剩餘是要在而且只有在 p 是 q 的二次**剩餘**而同時以相乘積 $\left(\frac{p-1}{2}\right)\cdot\left(\frac{q-1}{2}\right)$ 等於偶數作為條件，當這個相乘積是奇數時，情況便顛倒過來，即要在而且只有在 q 是 p 的**非二次剩餘**的條件下，p 才成為 q 的二次剩餘。為這一條定律提出第一個精確縝密的證明是青年高斯的一項成就，在他之前，這個證明曾長時期被視為數學上的一項挑戰。高斯率先提出的證明絕不簡單，即使在今天對於二次互反律之證明仍非易事，雖然許多不同的證明方法已發表，但其真正的內涵只有到最近與現代代數數論的進展產生關係之後才見其端倪。

讓我們選擇 $p=7$ 作為說明二次剩餘之分佈的一個實例。於是，由於

$$0^2\equiv 0,\quad 1^2\equiv 1,\quad 2^2\equiv 4,\quad 3^2\equiv 2,\quad 4^2\equiv 2,\quad 5^2\equiv 4,\quad 6^2\equiv 1$$

皆同餘於模 7，同時由於接著下來的各個整數的平方是按上面次序重複出現，故模 7 之二次剩餘乃是分別與 $1,2,4$ 同餘的諸數，而非二次剩餘則是與 $3,5,6$ 同餘的諸數。一般說來，模 p 之二次剩餘包含了那些與 $1^2,2^2,\cdots,(p-1)^2$ 同餘的數。但它們是成雙成對的同餘（例如，$2^2\equiv 5^2 \pmod 7$），由於

$$(p-x)^2=p^2-2px+x^2\equiv x^2 \pmod p,$$

故有

$$x^2\equiv (p-x)^2 \pmod p。$$

因此在 $1,2,3,\cdots,p-1$ 諸數當中，有一半是模 p 的二次剩餘，而其它一半則是非二次剩餘。

讓我們挑選 $p=5$，$q=11$ 作為說明二次互反律的例子。由於 $11\equiv 1^2 \pmod 5$，因此 11 是一個二次剩餘 $(\bmod 5)$；由於相乘積 $[(5-1)/2]\cdot[(11-1)/2]$ 是一個偶數，二次互反律告訴我們 5 是一個二次剩餘 $(\bmod 11)$，為了證實這一點，我們可看到 $5\equiv 4^2 \pmod{11}$。在另一方面，如果 $p=7$，$q=11$，那麼相乘積 $[(7-1)/2]\cdot[(11-1)/2]$ 是一個奇數，而 11 的確是一個二次剩餘 $(\bmod 7)$（因為 $11\equiv 2^2 \pmod 7$），故 7 是一個非二次剩餘 $(\bmod 11)$。