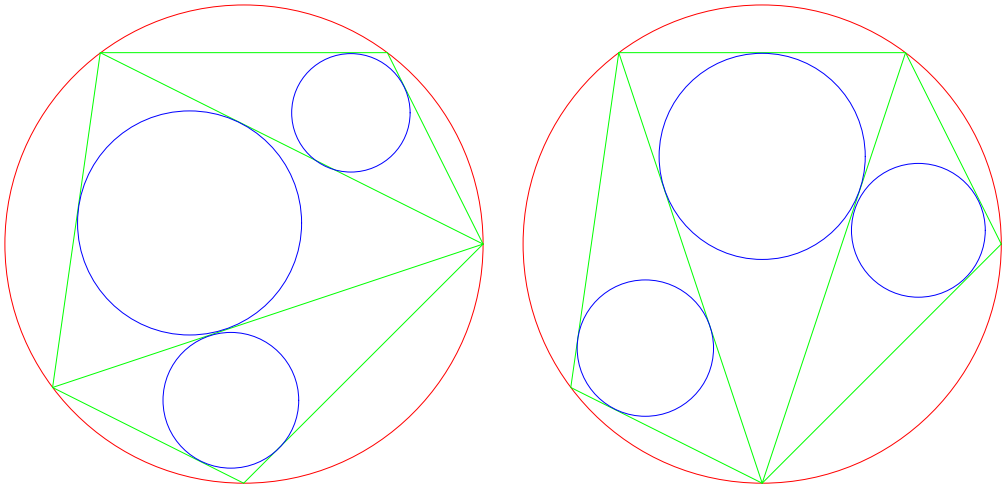
算術講義

許 志 農

國立台灣師範大學數學系

April 10, 2004



左圖三小圓半徑和＝右圖三小圓半徑和

目 錄

1　數學歸納法

當你研究一則數學問題時，常會發生的事情是：你可以猜想到問題的答案或者是公式（不等式），但是卻沒有辦法證明它。如果你的公式（或者是不等式）是與正整數相關的式子。那麼數學歸納法將提供你一個便捷的證明方法。這裡的目的就是要提出一些利用數學歸納法解決問題的範例，以供讀者參考。

數學歸納法是數學家皮阿諾把正整數的性質抽象而得的五個公理中的第五公設。數學歸納法的版本很多，最常用的方式是：先檢驗欲證的等式（或者不等式）在 $n=1$ 時成立。其次假設此等式（或者不等式）在 $n=k$ 時成立，然後利用假設的結果證明 $n=k+1$ 時亦成立。這是最常用的第一種形式的數學歸納法。事實上，我們也常用到第二種形式的數學歸納法。第二種形式的數學歸納法的證明模式也是先檢驗 $n=1$ 時成立。其次假設 $n=1,2,3,\cdots,k$ 時，欲證的結果也成立，然後利用這個假設結果證明 $n=k+1$ 時亦成立。

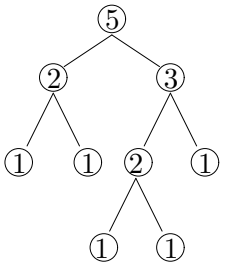
事實上，數學歸納法的證明方法就如同推骨牌一樣，只要你的版本能夠推倒所有的骨牌（這裡的骨牌是指所有的正整數），那它本身就是一種合法的證明方式，並非一定要墨守成規的使用上述所談的第一種形式或者是第二種形式的數學歸納法。最具代表性的例子就是證明算-幾不等式

$$\frac{a_1+a_2+\cdots+a_n}{n} \geq \sqrt[n]{a_1a_2\cdots a_n}$$

的歸納法形式，稱它為“以退為進”形的數學歸納法。其他還有所謂“分段”形、“迂迴”形、“曲線”形、“大誇度”形的數學歸納法。

1.1　用算術騙人的商店

月餅專賣店為了促銷，想出如下的花招：一盒月餅有 n 個，售價由顧客玩遊戲來決定，遊戲是這樣的，顧客須將 n 個月餅分成兩堆（每堆至少一個），並將兩堆的月餅個數相乘，得到第一個乘數。然後再將第一堆及第二堆各別再分成兩堆（每堆至少一個），又可得到兩個乘數。依此繼續下去，直到每一堆剩下一個月餅（不能再分）為止。這樣會產生很多乘數，n 個月餅的售價就是這些乘數的和。你知道如何將 n 個月餅分堆，才最省錢嗎？下圖是阿三在他的分堆方法之下，買五個月餅的錢數：



$2\times 3=\boxed{6}$

$1\times 1=\boxed{1}$　$2\times 1=\boxed{2}$

$1\times 1=\boxed{1}$

阿三這樣的分堆買五個月餅須付 $6+1+2+1=10$ 元美金。

【證明】當 $n=1$ 時，因為已經不可能再分了，所以不需要錢（0 美金）。當 $n=2$

時，只有一種分法，需要 1 美金。當 $n=3$ 時，不管是哪一種分法，都是 3 美金。因此猜想：n 個月餅時，無論你如何分，都需要

$$\frac{n(n-1)}{2}$$

美金。採用數學歸納法證明如下：

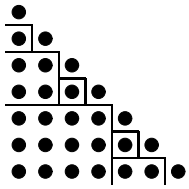
(1) 當 $n=1,2,3$ 時，與猜測的答案相同。

(2) 假設 $n=1,2,3,\cdots,k-1$ 時，無論哪一種分法，所需要的錢都是 $\frac{n(n-1)}{2}$ 美金。當 $n=k$ 時，設第一次將月餅分成 a 個與 $k-a$ $(1\le a\le k-1)$ 個兩堆。那麼所產生的第一個乘數為 $a\cdot(k-a)$。根據假設，a 個那堆繼續分下去所產生的乘數總和為 $\frac{a(a-1)}{2}$；而 $k-a$ 個那堆繼續分下去所產生的乘數總和為 $\frac{(k-a)(k-a-1)}{2}$。因此乘數總和為

$$a(k-a)+\frac{a(a-1)}{2}+\frac{(k-a)(k-a-1)}{2}=\frac{k(k-1)}{2}.$$

因此無論如何分，所需要的錢數都是 $\frac{n(n-1)}{2}$ 美金。 ⊠

【另解】不管你如何分堆，買七個月餅都是 21元美金。你可以從下圖觀察出來嗎？



⊠

1.2 埃及分數

像 $1/3, 1/11, 1/231$ 這樣分子為 1 的分數，我們稱之為埃及分數。萊茵紙草記載著“埃及人擅長將真分數寫成相異埃及分數的和”。例如

$$\begin{aligned}\frac{2}{3}&=\frac{1}{2}+\frac{1}{6},\\ \frac{3}{7}&=\frac{1}{3}+\frac{1}{11}+\frac{1}{231},\\ \frac{8}{11}&=\frac{1}{2}+\frac{1}{6}+\frac{1}{22}+\frac{1}{66}\end{aligned}$$

等。是否每個真分數 a/b（a,b 是滿足 $1<a<b$ 且互質的正整數）皆可表為若干個相異埃及分數的和一直困擾著埃及人及後來的數學家。在 1880 年時，西爾威斯特解決了這個問題，他僅用了數學歸納法而已。

定理 1.1 每個真分數 a/b 都可以表為若干個相異埃及分數的和。

【證明】我們對分子 a 進行數學歸納法的證明。

(1) 當 $a=1$ 時，$a/b=1/b$ 剛好是一個埃及分數。

(2) 設此定理對所有分子 $<a(a\geq 2)$ 的最簡真分數都成立。現在證明真分數 a/b 可以表為若干個相異埃及分數的和。因為 $1>a/b>0$ 及 $1>1/2>1/3>\cdots>0$，所以可以找到一個正整數 $q(q\geq 2)$ 滿足

$$\frac{1}{q}<\frac{a}{b}<\frac{1}{q-1}.$$

由此得到 $0<aq-b<a$,

$$\frac{a}{b}=\frac{1}{q}+\frac{aq-b}{bq} \quad 及 \quad \frac{aq-b}{bq}<\frac{1}{q}.$$

由歸納法得到：真分數

$$\frac{aq-b}{bq}$$

可以表成若干個相異埃及分數的和，且每一個都與 $1/q$ 相異。因此，a/b 可以表成若干個相異埃及分數的和

⊠

1.3 特納定理

定理 1.2 (特納定理) 空間中有 $2n$ $(n\geq 2)$ 個相異點且任三點不共線。若任意的以這些點為端點，連接出 n^2+1 條線段，則此 n^2+1 條線段至少可形成一個三角形（即有三個點互相連接）。

【證明】採用數學歸納法證明如下：

(1) 當 $n=2$ 時，共有 $4=2\cdot 2$ 個點，連結 $5=2^2+1$ 條線段。因為四個點共可決定六條線段，所以僅有一條線段未連結。因此可以連出兩個三角形。

(2) 設有 $2(n-1)$ 點，連結

$$(n-1)^2+1$$

條線段時，必存在至少一個三角形。當有 $2n$ 個點，連結

$$n^2+1$$

條線段時。因為 $n^2+1\geq 1$，所以至少有一條線段。不妨假設 P,Q 就是這 $2n$ 個點中的兩個，而且線段 PQ 就是此條線段。

(i) 如果其餘的 $2(n-1)$ 個點中，有一個點 R 同時與 P,Q 連結，則此時便形成三角形 PQR.

(ii) 如果其餘的 $2(n-1)$ 個點中，沒有任何點同時與 P, Q 連結，則這 $2(n-1)$ 個點與 P, Q 至多連結 $2(n-1)$ 條線段。由此知道：這 $2(n-1)$ 個點彼此所連結的線段數 $\geq n^2+1-1-2(n-1)=(n-1)^2+1$ 條。根據數學歸納法：這 $2(n-1)$ 個點至少構成一個三角形。

$\boxtimes$

1.4 拈的加法表

下圖是一個向右及向上無限延伸的棋盤。為了方便起見，例如將記號 $\star$ 所在的格子稱為 $(3,7)$ 格子。喜歡玩數學遊戲的數學家們，用一種很神奇的方法將每一個格子填入一個非負的整數。他們填入的方法是這樣的：由 (a,b) 格子垂直向下看及水平往左看，分別會看到 b 個及 a 個數字（有些數字可能相同）。將第一個不屬於這 $a+b$ 個數字的非負整數填入 (a,b) 格子內，並將此數字記為 $a \oplus b$。舉例來說：由 $(1,1)$ 格子垂直向下看及水平往左看，所看到的 $2=1+1$ 個數字都是 1，所以 $1 \oplus 1 = 0$（因為 0 是第一個不屬於 $\{1,1\}$ 的非負整數）。再舉例來說：由 $(2,1)$ 格子垂直向下看的數字為 2，水平往左看的數字為 $0,1$，不屬於 $\{0,1,2\}$ 的最小非負整數為 3。因此 $2 \oplus 1 = 3$。

$\vdots$

7			$\star$					
6								
5								
4								
3								
2								
1	0	3						
0	1	2	3	4	5	6	7	$\cdots$

(1) 根據上述的規則，試算出

$$3 \oplus 7, 7 \oplus 3, 4 \oplus 7, 7 \oplus 4$$

的值。

(2) 若 $x \oplus c = y \oplus c$，則 $x = y$。

(3) 試證明：$a \oplus a = 0$。

(4) 證明拈的加法具有交換律：

$$a \oplus b = b \oplus a.$$

(5) 證明拈的加法具有結合律：

$$(a \oplus b) \oplus c = a \oplus (b \oplus c).$$

(6) 如果 $0 \le a, b < 2^n$，則 $0 \le a \oplus b < 2^n$。

(7) 如果 $0 \le a < 2^n$，則 $a \oplus 2^n = a + 2^n$。

【解答】我們可以完成如下的表

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

關於 (2) 的證明，如果 $x \ne y$，不妨設 $x < y$。這時 $x \oplus c$ 出現在 (y, c) 的水平左方上。根據定義：$x \oplus c \ne y \oplus c$，跟已知矛盾，所以 $x = y$。

我們利用數學歸納法來證明 (3) 是成立的。當 $a = 0, 1$ 時顯然成立。假設 $a = 0, 1, 2, \cdots, n-1$ 時成立。當 $a = n$ 時，若 $n \oplus n \ne 0$，則由 (n, n) 垂直向下看或者是水平往左看時，會出現 0 的數字。不妨設 $b \oplus n = 0 (b < n)$，這與 $b \oplus b = 0 (b < n)$ 矛盾。因此 $n \oplus n = 0$。

現在來證明 (4)，對 $a + b$ 的值做數學歸納法。當 $a + b = 0, 1$ 時，$a \oplus b = b \oplus a$ 顯然成立。假設當 $a + b < n$ 時，此交換律都成立。當 $a + b = n$ 時，由定義知：$a \oplus b$ 是不屬於集合

$$\{x \oplus b, a \oplus y | 0 \le x < a, 0 \le y < b\}$$

的最小非負整數。因為 $x < a, y < b$，所以 $x + b < a + b = n, a + y < a + b = n$。由歸納假設知道：

$$x \oplus b = b \oplus x, \quad a \oplus y = y \oplus a.$$

因此，$a \oplus b$ 是不屬於集合

$$\{b \oplus x, y \oplus a | 0 \le x < a, 0 \le y < b\}$$

的最小非負整數。但是此數亦等於 $b \oplus a$。故 $a \oplus b = b \oplus a$。

我們利用數學歸納法來證明 (5) 是成立的。

(i) 當 $a + b + c = 0, 1$ 時，容易檢驗此結合律成立。

(ii) 假設 $a+b+c < n$ 時，結合律成立。當 $a+b+c = n$ 時，由定義知道：$(a \oplus b) \oplus c =$ 不屬於集合

$$\{x \oplus c, (a \oplus b) \oplus k \mid x < a \oplus b, k < c\}$$

的最小非負整數 $\leq$ 不屬於集合

$$\{(i \oplus b) \oplus c, (a \oplus j) \oplus c, (a \oplus b) \oplus k \mid i < a, j < b, k < c\}$$

的最小非負整數。因為

$$(a \oplus b) \oplus c \notin \{(i \oplus b) \oplus c, (a \oplus j) \oplus c, (a \oplus b) \oplus k \mid i < a, j < b, k < c\},$$

所以，$(a \oplus b) \oplus c$ 是不屬於集合

$$\{(i \oplus b) \oplus c, (a \oplus j) \oplus c, (a \oplus b) \oplus k \mid i < a, j < b, k < c\}$$

的最小非負整數。因為 $i + b + c < n, a + j + c < n, a + b + k < n$，所以

$$(i \oplus b) \oplus c = i \oplus (b \oplus c), (a \oplus j) \oplus c = a \oplus (j \oplus c), (a \oplus b) \oplus k = a \oplus (b \oplus k).$$

所以，$(a \oplus b) \oplus c$ 是不屬於集合

$$\{i \oplus (b \oplus c), a \oplus (j \oplus c), a \oplus (b \oplus k) \mid i < a, j < b, k < c\}$$

的最小非負整數。但由前面證明知道：此數亦等於 $a \oplus (b \oplus c)$。因此

$$(a \oplus b) \oplus c = a \oplus (b \oplus c).$$

關於 (6), (7) 的證明，我們對 n 作數學歸納法一起來證明。
(i) 當 $n = 0, 1$ 時，容易檢驗 (6), (7) 同時成立。
(ii) 假設 $n = k$ 時，(6), (7) 同時成立，即當 $0 \leq a, b < 2^k$ 時，

$$0 \leq a \oplus b < 2^k, \quad a \oplus 2^k = a + 2^k.$$

當 $n = k + 1$ 時，將 a 與 b 分如下四部分來考慮：

(a) 若 $0 \leq a, b < 2^k$ 時，則由數學歸納法知道成立。

(b) 若 $2^k \leq a < 2^{k+1}, 0 \leq b < 2^k$ 時，則令 $a = 2^k + a'$，其中 $0 \leq a' < 2^k$。由 $a' \oplus 2^k = a' + 2^k$ 及 $0 \leq a' \oplus b < 2^k$ 得到

$$\begin{aligned} a \oplus b &= (2^k + a') \oplus b \\ &= (2^k \oplus a') \oplus b \\ &= 2^k \oplus (a' \oplus b) \\ &= 2^k + (a' \oplus b) \\ &< 2^k + 2^k = 2^{k+1}. \end{aligned}$$

(c) 若 $0 \leq a < 2^k, 2^k \leq b < 2^{k+1}$ 時，則同理可以證明。

(d) 若 $2^k \le a < 2^{k+1}, 2^k \le b < 2^{k+1}$ 時，則令 $a = 2^k + a', b = 2^k + b'$，其中 $0 \le a', b' < 2^k$。由 $0 \le a' \oplus b' < 2^k$ 得到

$$\begin{aligned}
a \oplus b &= (2^k + a') \oplus (2^k + b') \\
&= (2^k \oplus a') \oplus (2^k \oplus b') \\
&= 2^k \oplus (a' \oplus (2^k \oplus b')) \\
&= 2^k \oplus (a' \oplus (b' \oplus 2^k)) \\
&= 2^k \oplus ((a' \oplus b') \oplus 2^k) \\
&= 2^k \oplus (2^k \oplus (a' \oplus b')) \\
&= (2^k \oplus 2^k) \oplus (a' \oplus b') \\
&= 0 \oplus (a' \oplus b') \\
&= a' \oplus b' \\
&< 2^k < 2^{k+1}.
\end{aligned}$$

現在證明：若 $0 \le a < 2^{k+1}$，則 $a \oplus 2^{k+1} = a + 2^{k+1}$。由定義知：$a \oplus 2^{k+1}$ 是不屬於集合

$$\left\{x \oplus 2^{k+1}, a \oplus y \middle| 0 \le x < a, 0 \le y < 2^{k+1}\right\}$$

的最小非負整數。因為 $0 \le a < 2^{k+1}, 0 \le y < 2^{k+1}$，所以由剛剛的歸納證明知道：$0 \le a \oplus y < 2^{k+1}$，而且由 (2) 知道：$a \oplus 0, a \oplus 1, \cdots, a \oplus (2^{k+1} - 1)$ 都不相同。因此

$$\left\{a \oplus y \middle| 0 \le y < 2^{k+1}\right\} = \left\{0, 1, \cdots, 2^{k+1} - 1\right\}. \tag{1.1}$$

根據 $a = 0, 1, 2, \cdots, 2^{k+1} - 1$ 的先後次序來計算 $a \oplus 2^{k+1}$。顯然有 $0 \oplus 2^{k+1} = 2^{k+1}$。現在考慮 $1 \oplus 2^{k+1}$，利用 (1.1) 的結果知道：由 $(1, 2^{k+1})$ 往下看的數字有 $0, 1, \cdots, 2^{k+1} - 1$；而由 $(1, 2^{k+1})$ 往左看的數字是 $0 \oplus 2^{k+1} = 2^{k+1}$。因此 $1 \oplus 2^{k+1} = 1 + 2^{k+1}$。其餘同理可逐步推得

$$1 \oplus 2^{k+1} = 1 + 2^{k+1}, 2 \oplus 2^{k+1} = 2 + 2^{k+1}, \cdots, a \oplus 2^{k+1} = a + 2^{k+1}.$$

⊠

例題 **1.1** 試求 $1057 \oplus 32$ 的值。

【解】善用 $\oplus$ 的性質可得到

$$\begin{aligned}
1057 \oplus 32 &= (2^{10} \oplus 33) \oplus 2^5 \\
&= (2^{10} \oplus 2^5 \oplus 1) \oplus 2^5 \\
&= 2^{10} \oplus 1 \oplus 2^5 \oplus 2^5 \\
&= 2^{10} \oplus 1 \\
&= 1025.
\end{aligned}$$

⊠

習題 1.1 試由下列的等式中歸納出一個結論，並用數學歸納法證明此結論。

$$\begin{aligned} 1^3+2^3+3^3 &= 9\times 4, \\ 2^3+3^3+4^3 &= 9\times 11, \\ 3^3+4^3+5^3 &= 9\times 24. \end{aligned}$$

習題 1.2 數列 $< a_n >$ 滿足：$a_1 = 3, a_{n+1} = a_n(a_n+2)\ (n \geq 1)$。

(1) 推測 a_n 的一般公式。

(2) 證明你的推測是正確的。

習題 1.3 設 n 是一個正整數。試將伽利略分數

$$\frac{1+3+5+\cdots+(2n-1)}{(2n+1)+(2n+3)+(2n+5)+\cdots+(4n-1)}$$

化簡成最簡分數。

習題 1.4 設 $\langle a_n \rangle$ 是一個正實數所構成的無窮數列，且滿足

$$\sum_{i=1}^{n} a_i^3 = \left(\sum_{i=1}^{n} a_i\right)^2, \quad n \geq 1.$$

是否此數列為 $a_n = n$。

習題 1.5 設數列 $\langle f_n \rangle$ 滿足

(a) f_n 都是正整數，且 $f_2 = 2$。

(b) 若 $a < b$，則 $f_a < f_b$。

(c) 對任意正整數 a 與 b，恆有 $f_{a\cdot b} = f_a \cdot f_b$。

證明：對任意正整數 n，恆有 $f_n = n$。

習題 1.6 有一副牌，有些牌朝上、有些牌朝下。小明任意的從這副牌中間抽出連續的一疊牌（此疊牌必須最上的一張是朝上的、最後一張也是朝上的）。然後把這疊牌上下翻轉後放回原來的位置。不斷地繼續上述動作，只要有牌朝上就必須要抽。試證：無論小明如何選取一疊牌，最後整副牌將全部朝下。（註：如果抽出的這“疊”牌只有一張牌，只需將這張牌翻面放回原來的位置即可）。

習題 1.7 試完成：

(1) 試利用西爾威斯特的方法將真分數 $\frac{4}{97}$ 表成若干個相異埃及分數的和。

(2) 設 n 為奇數。證明：$\frac{2}{n}$ 可以表為兩個相異埃及分數的和。

(3) 設正整數 n 滿足 $8|(n-5)$。證明：$\frac{4}{n}$ 可以表為三個相異埃及分數的和。

習題 **1.8** 設 n 為正整數，試判別命題

$$n^2+n+17 \text{ 都是質數。}$$

是否成立？成立，證明之；不成立，給反例。

動手玩數學

一條環形公路上有 n 個加油站，它們所儲的汽油總量足夠一輛汽車在整個環形公路上行駛一週。證明：帶著空油罐（容量很大）的汽車能夠從某個汽油站出發（帶上該站的汽油），完成環形公路上整個旅程。

挑戰題

數論上有許多問題是在探討相鄰整數相乘的性質，例如

$$\begin{aligned}1\cdot 2\cdot 3\cdot 4+1&=5^2,\\ 2\cdot 3\cdot 4\cdot 5+1&=11^2,\\ 3\cdot 4\cdot 5\cdot 6+1&=19^2.\end{aligned}$$

從上面的觀察容易猜測「四個相鄰正整數的乘積再加 1 必為完全平方數」，即

$$n(n+1)(n+2)(n+3)+1=\square^2.$$

讀者可以推得 $\square$ 的公式嗎（以 n 來表示）？

接下來考慮像 $n!+1$ 這樣的數。例如

$$\begin{aligned}n=4&\Rightarrow 4!+1=5^2,\\ n=5&\Rightarrow 5!+1=11^2,\\ n=7&\Rightarrow 7!+1=71^2.\end{aligned}$$

數論學家認為，除了這三個之外，$n!+1$ 都不會是完全平方數。這是一則尚未解決的問題。

皮阿諾與數學歸納法

十九世紀中葉，在數學公理化思想潮流影響下，義大利數學家皮阿諾在 1889 年把正整數的性質抽象而得到一組公設，後人稱它為皮阿諾公設。皮阿諾公設共有五條公理，數學歸納法就是其中的第五公理，這個公理與集合論裡的良序原理是等價的。所謂的「公設」或「公理」，指的是一些看起來很明顯，但卻無法證明的假設。既然無法證明，又那麼明顯，只好接受它，直接拿來使用吧！類似的情形，在兩千多年前也

發生過，歐幾里得的《幾何原本》裡面也同樣列舉了五個公設。其中第五個公設就是鼎鼎有名的「平行公設」。

清末數學家李善蘭曾提出過恆等式：若 $n \geq m \geq 1$，則

$$\sum_{j=0}^{m} \binom{m}{j}^2 \binom{n+2m-j}{2m} = \binom{n+m}{m}^2.$$

這則恆等式聲名遠播，流傳到海外。二十世紀五十年代初，匈牙利數學家吐朗（P. Turan）到中國的北京訪問，在一次演講中，用高深的數學知識加以證明李善蘭恆等式。華羅庚冥索苦思“中國人自己難道就不能證明他們的先輩提出的問題嗎？”終於在與吐朗告別時，華羅庚給了他一個數學歸納法的證明，並將這個證明寫入他的一本小冊子《數學歸納法》之中。這也算是皮阿諾創數學歸納法的一大功德吧！

2 費馬小定理

2.1 費馬小定理

費馬小定理是初等數論上一個基本而且重要的定理。現在敘述而且證明如下：

定理 2.1 (費馬小定理) 設 p 是質數，a 是與 p 互質的一個整數則

(1) $a^{p-1} \equiv 1 \pmod{p}$.

(2) 若 d 是使得 $a^d \equiv 1 \pmod{p}$ 成立的最小正整數，則

$$d \mid (p-1).$$

【証明】

(1) 因為 p 是質數， a 是與 p 互質的整數，所以模 p 之後的同餘數

$$1 \cdot a, 2 \cdot a, 3 \cdot a, \cdots, (p-1) \cdot a \pmod{p}$$

是同餘數

$$1, 2, 3, \cdots, (p-1) \pmod{p}$$

的某種排列。因此我們有

$$\begin{aligned}
&(1 \cdot a) \cdot (2 \cdot a) \cdots ((p-1) \cdot a) \equiv 1 \cdot 2 \cdots (p-1) \pmod{p} \\
&\Rightarrow a^{p-1} \cdot 1 \cdot 2 \cdots (p-1) \equiv 1 \cdot 2 \cdots (p-1) \pmod{p} \\
&\Rightarrow (a^{p-1} - 1)(1 \cdot 2 \cdots (p-1)) \equiv 0 \pmod{p}.
\end{aligned}$$

因為 p 與 $1 \cdot 2 \cdots (p-1)$ 互質，所以

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

(2) 設 $p-1$ 被 d 除之，所得的商及餘數分別為 q 與 r。可以表為

$$p - 1 = dq + r, \quad 0 \le r < d.$$

由

$$\begin{cases} a^{p-1} \equiv 1 \pmod{p}, \\ a^d \equiv 1 \pmod{p}, \end{cases}$$

得到

$$a^r = a^r \cdot 1^q \equiv a^r \cdot (a^d)^q = a^{dq+r} = a^{p-1} \equiv 1 \pmod{p}.$$

因為 d 是最小的，所以必須有 $r = 0$，即 $d \mid (p-1)$。 ⊠

（註）費馬小定理的 (2) 是習題 **??** 的特別情況，你注意到了嗎？

2.2 利用費馬小定理來因數分解大的正整數

費馬小定理的一個很重要的運用是利用它來因數分解很大的正整數。

例題 **2.1** 因數分解第四個費馬數

$$F_4 = 2^{2^4} + 1 = 65537.$$

【解】設質數 p 整除 F_4。我們有

$$\begin{aligned} p \mid 2^{16}+1 \quad &\Rightarrow 2^{16} \equiv -1 \pmod{p} \\ &\Rightarrow 2^{32} \equiv 1 \pmod{p}. \end{aligned}$$

利用習題 **??** 的結果，容易推得 32 是滿足上式的最小正整數。由費馬小定理得到

$$32 \mid (p-1) \Rightarrow p \equiv 1 \pmod{32}.$$

令 $p = 32n + 1$ 則

n	1	2	3	4	5	6	7	8
p	33	65	97	129	161	193	225	257

因為 $33, 65, 129, 161, 225$ 不是質數，又 $97, 193$ 不能整除 65537 且

$$\sqrt{65537} < 257,$$

所以 $F_4 = 2^{2^4} + 1 = 65537$ 是一個質數。 ⊠

例題 **2.2** 因數分解 $2^{13} - 1 = 8191$。

【解】設質數 p 整除 8191。我們有

$$p \mid 2^{13} - 1 \Rightarrow 2^{13} \equiv 1 \pmod{p}.$$

利用習題 **??** 的結果，容易推得 13 是滿足上式的最小正整數。由費馬小定理得到

$$\begin{cases} 13 \mid (p-1) \\ p \equiv 1 \pmod{2} \end{cases} \Rightarrow \begin{cases} p \equiv 1 \pmod{13} \\ p \equiv 1 \pmod{2} \end{cases} \Rightarrow p \equiv 1 \pmod{26}.$$

令 $p = 26n + 1$ 則

n	1	2	3
p	27	53	79

因為 27 不是質數，又 $53, 79$ 不能整除 8191 且 $\sqrt{8191} < 92$，所以 $2^{13} - 1 = 8191$ 是一個質數。 ⊠

2.3 其它運用

例題 **2.3** 設 p 為奇質數，a,b 為互質的整數且 $p \mid a^2+b^2$。證明

(1) 存在整數 n 使得 $p \mid 1+n^2$。

(2) $p \equiv 1 \pmod 4$。

【解】

(1) 因為 a,b 為互質的整數，所以存在整數 x,y 使得 $ax-by=1$。利用恆等式

$$(a^2+b^2)(x^2+y^2)=(ax-by)^2+(ay+bx)^2,$$

我們得到

$$p \mid (x^2+y^2)(a^2+b^2)=1+n^2, \quad \text{其中} \quad n=ay+bx.$$

(2) 由 $p \mid 1+n^2$ 得到 $n^2 \equiv -1 \pmod p$，推得 $n^4 \equiv 1 \pmod p$。利用習題 **??** 的結果，容易推得 4 是滿足此式的最小正整數。根據費馬小定理知道：

$$4 \mid (p-1) \Rightarrow p \equiv 1 \pmod 4.$$

⊠

例題 **2.4** 設 m,n 為整數。證明

(1) $m^2-n^2, 2mn$ 兩數中至少有一個為 3 的倍數。

(2) $m^2-n^2, 2mn$ 兩數中至少有一個為 4 的倍數。

(3) $m^2-n^2, 2mn, m^2+n^2$ 三數中至少有一個為 5 的倍數。

【解】

(1) 若 m,n 有一為 3 的倍數，則 $3 \mid 2mn$，所以可假設 m,n 與 3 互質。根據費馬小定理知道：

$$\begin{aligned} m^2 \equiv 1 \pmod 3, n^2 \equiv 1 \pmod 3 &\Rightarrow m^2-n^2 \equiv 0 \pmod 3 \\ &\Rightarrow 3 \mid m^2-n^2. \end{aligned}$$

(2) 若 m,n 有一為 2 的倍數，則 $4 \mid 2mn$, 所以可假設 m,n 與 2 互質。因此知道：

$$\begin{aligned} m^2 \equiv 1 \pmod 4, n^2 \equiv 1 \pmod 4 &\Rightarrow m^2-n^2 \equiv 0 \pmod 4 \\ &\Rightarrow 4 \mid m^2-n^2. \end{aligned}$$

(3) 若 m,n 有一為 5 的倍數，則 $5 \mid 2mn$，所以可假設 m,n 與 5 互質。根據費馬小定理知道

$$\begin{aligned} m^4 \equiv 1 \pmod 5, n^4 \equiv 1 \pmod 5 &\Rightarrow m^4-n^4 \equiv 0 \pmod 5 \\ &\Rightarrow 5 \mid m^4-n^4 \\ &\Rightarrow 5 \mid m^2-n^2 \quad \text{或} \quad 5 \mid m^2+n^2. \end{aligned}$$

$\boxtimes$

習題 2.1 因數分解 $2^{11}-1=2047$。

習題 2.2 因數分解 $2^{17}-1=131071$。

習題 2.3 證明 $2^{37}-1=137438953471$ 不是質數。

習題 2.4 是否存在滿足下列條件的正整數 n：將集合

$$\{n, n+1, n+2, n+3, n+4, n+5\}$$

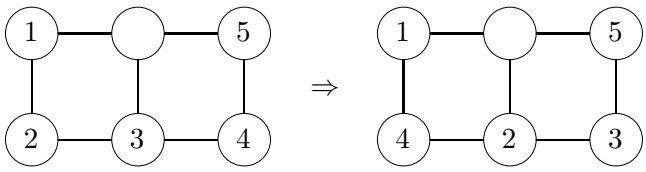
分成兩個不相交的非空子集合且第一個子集合的元素的乘積等於第二個子集合的元素的乘積。

習題 2.5 設 a, b, c 是三個整數，試證明

$$7 \mid abc(a^3-b^3)(b^3-c^3)(c^3-a^3).$$

動手玩數學

將寫有 $1, 2, 3, 4, 5$ 的五枚硬幣擺在左圖六格中的五格。規定每次移動僅能將空白格附近的硬幣沿著路徑滑動至空白格的位置。試問：是否可以將左圖經過有限次的滑動之後，變成右圖。



挑戰題

若 a 為整數，且 x^2-x+a 整除 $x^{13}+x+90$，則求 a 的值。

費馬

費馬是法國數學家，生於 1601 年，死於 1665 年。最有名的“費馬最後猜想”終於在 1994 年被英國數學家威爾斯證明是正確的定理。費馬最後猜想的敘述是這樣的：方程式

$$x^n+y^n=z^n,$$

當 $n>2$ 時沒有正整數解 x, y, z。

事實上，費馬僅證明了 $n=4$ 的情形，$n=4$ 的證明方法是很特殊的，今天我們稱此種方法為費馬無窮遞降法。關於 $n=4$ 的證明，可以看本書的定理 3.3。

除了費馬最後猜想之外，費馬小定理，平方和，四個平方和的問題都是費馬在數論上很有名的工作。費馬曾經認為所有的費馬數

$$F_n = 2^{2^n} + 1$$

都是質數。事實上這個猜想是錯誤的，例如

$$F_5 = 2^{2^5} + 1 = 4294967297 = 641 \times 6700417.$$

至於是否有無窮多個費馬數是質數是一個很難，而且至今仍未解的大難題。

3 畢氏數與費馬方程式

3.1 畢氏數

若正整數 a,b,c 互質且 a,b,c 剛好構成一個直角三角形的三邊邊長，即 $c^2=a^2+b^2$，則稱 (a,b,c) 是一組『畢氏數』。也就是說，邊長是正整數且互質之直角三角形的三邊邊長恰是一組畢氏數。有關畢氏數最有名的結果莫過於克羅內克在 1901 年證明的底下這個定理：

定理 3.1 (克羅內克定理) 方程式 $x^2+y^2=z^2$ 的互質正整數解（即 $(x,y,z)=1$ 的正整數解 x,y,z）或者說任何的畢氏數 (x,y,z) 均可表為

$$\begin{cases} x=m^2-n^2, \\ y=2mn, \\ z=m^2+n^2, \end{cases} \quad \text{或} \quad \begin{cases} x=2mn, \\ y=m^2-n^2, \\ z=m^2+n^2, \end{cases}$$

其中 m,n 為互質的正整數且一為奇數，一為偶數；而且 x 與 y 至少有一個為 3 的倍數，x 與 y 至少有一個為 4 的倍數，x,y 與 z 至少有一個為 5 的倍數。

【証明】首先令 x,y,z 是方程式 $x^2+y^2=z^2$ 的一組互質正整數解，由此方程式可以推得 x,y,z 其實是兩兩互質的。若 x,y 都是偶數，則 z 必為偶數，這與假設不符。如果 x,y 都是奇數，則 z 為偶數，此與 $z^2=x^2+y^2\equiv 2 \pmod 4$ 矛盾。所以 x,y 必須一個為奇數，一個為偶數。為了方便，不妨設 y 為偶數，x,z 為奇數（注意：x,y,z 兩兩互質）。

首先證明：$(z-x,z+x)=2$：
令 $(z-x,z+x)=d$ 則

$$d\mid z-x, d\mid z+x \Rightarrow d\mid 2x, d\mid 2z \Rightarrow d\mid 2 \Rightarrow d=1 \quad \text{或} \quad 2.$$

因為 $z-x,z+x$ 都是偶數，所以 $d=2$。現在由

$$\begin{aligned} y^2=(z+x)(z-x), &\quad \text{其中} \quad (z+x,z-x)=2 \\ \Rightarrow \begin{cases} z+x=2m^2, \\ z-x=2n^2, \\ y=2mn, \end{cases} &\quad \text{其中} \quad m,n \quad \text{互質} \\ \Rightarrow \begin{cases} x=m^2-n^2, \\ y=2mn, \\ z=m^2+n^2, \end{cases} &\quad \text{其中} \quad m,n \quad \text{互質且一奇，一偶.} \end{aligned}$$

至於剩下的部份由第 2 節的例題 2.4 馬上得證。 ⊠

例題 3.1 證明方程式

$$x^4-4y^4=z^2 \tag{3.1}$$

無正整數解 x,y,z。

【証明】設 x, y, z 是此方程式的一組正整數解。若有一個質數 p 同時整除 x 與 y，則由 (3.1) 得到：p^2 整除 z。此時可推得 $(x/p, y/p, z/p^2)$ 亦為 (3.1) 的一組正整數解。因此，我們不妨假設 x 與 y 互質，容易推得此時的 x, y, z 是兩兩互質的；甚至由

$$(2y^2)^2 + z^2 = (x^2)^2 \tag{3.2}$$

可進一步得到：$2y^2, z, x^2$ 是兩兩互質的。由 (3.2) 及定理 3.1 可得

$$\begin{cases} 2y^2 = 2mn, \\ z = m^2 - n^2, \\ x^2 = m^2 + n^2, \end{cases} \qquad m, n \quad \text{互質且一奇一偶.} \tag{3.3}$$

因為 m, n 互質且 $y^2 = mn$，所以必有 $m = a^2, n = b^2$。代入 (3.3) 得到：正整數 a, b, x 滿足

$$a^4 + b^4 = x^2. \tag{3.4}$$

在下一節的定理中，我們將證明方程式 $x^4 + y^4 = z^2$ 無正整數解 x, y, z。因此 (3.4) 是不可能的，所以本例題無正整數解。 ⊠

3.2 費馬方程式與費馬無窮遞降法

定理 3.2 證明方程式 $x^4 + y^4 = z^2$ 無正整數解 x, y, z。

【証明】假設 x, y, z 為 $x^4+y^4 = z^2$ 的正整數解中 z 值最小的一組解，則有 $(x, y, z) = 1$（自行檢驗）；同前定理的證明，不妨假設 y 為偶數， x, z 為奇數，則利用前定理得到

$$\begin{aligned}
&\begin{cases} x^2 = m^2 - n^2, \\ y^2 = 2mn, \\ z = m^2 + n^2, \end{cases} \qquad \text{其中正整數 } m, n \text{ 互質且一奇，一偶} \\
&\Rightarrow n \text{ 偶數， } m \text{ 奇數（由 } x^2 + n^2 = m^2 \text{ 得到）} \\
&\Rightarrow \begin{cases} x = c^2 - d^2, \\ n = 2cd, \\ m = c^2 + d^2, \end{cases} \qquad \text{其中正整數 } c, d \text{ 互質且一奇，一偶} \\
&\Rightarrow y^2 = 4cd(c^2 + d^2) \\
&\Rightarrow c = e^2, d = f^2, c^2 + d^2 = g^2 \text{（因為 } c, d, c^2 + d^2 \text{ 兩兩互質）} \\
&\Rightarrow e^4 + f^4 = g^2 \quad \text{其中 } e, f, g \text{ 為正整數。}
\end{aligned}$$

因為 $g \le g^2 = c^2 + d^2 = m < z$，所以我們找到另一組正整數解 (e, f, g)，其中 $g < z$，得到矛盾。 ⊠

這樣的證明方法稱為費馬無窮遞降法，是費馬首創的方法。

定理 3.3 費馬方程式 $x^4 + y^4 = z^4$ 無正整數解 x, y, z。

【解】因為 $x^4 + y^4 = (z^2)^2$, 定理 3.2 知道 $x^4 + y^4 = z^4$ 無正整數解 x, y, z。 ⊠

費馬方程式是泛指像“$x^n+y^n=z^n$”這樣的方程式。當 $n=3,4$ 時，費馬是第一位證明此方程式無正整數解的數學家；當 $n=5$ 時，勒讓德於 1823 年證明此方程式無正整數解；當 $n=7$ 時，狄利克雷於 1832 年證明此方程式無正整數解。事實上，當 $n\geq 3$ 時，費馬方程式皆無正整數解，這就是有名的費馬最後定理。這個定理在 1994 年時，被英國數學家威爾斯證明成立。

3.3 另一則方程式

定理 3.4 考慮方程式 $x^4-9y^4=z^2$。

(1) 若 x,y,z 為此方程式的一組正整數解，則證明：$2\mid y$。

(2) 證明：方程式 $x^4-9y^4=z^2$ 無正整數解 x,y,z。

【解】

(1) 為了方便起見，不妨假設 x,y,z 是方程式 $(x^2)^2=(3y^2)^2+z^2$ 的一組互質正整數解且 y 為奇數則

$$\begin{aligned}
&(x^2)^2=(3y^2)^2+z^2\\
&\Rightarrow\begin{cases}x^2=m^2+n^2,\\ 3y^2=m^2-n^2,\\ z=2mn,\end{cases}\qquad \text{其中正整數 } m,n \text{ 互質}\\
&\Rightarrow\begin{cases}3\mid m \text{ 或 } 3\mid n \quad (\text{由 } x^2=m^2+n^2 \text{ 得到}),\\ 3y^2=m^2-n^2,\end{cases}\\
&\Rightarrow 3\mid m \text{ 且 } 3\mid n,\ \text{這與 } m,n \text{ 互質矛盾。}
\end{aligned}$$

因此 y 必須是偶數。

(2) 設方程式 $x^4-9y^4=z^2$ 的正整數解中，x 值最小的一組是 x,y,z；因為 x 值最小，所以 x,y,z 必是互質的正整數解。現在考慮 $(x^2)^2=(3y^2)^2+z^2$。因為 $(x,y,z)=1$，所以容易推得 $(x^2,3y^2,z)=1,3$。當 $(x^2,3y^2,z)=3$ 時，我們有 $3|x,3|z$，但是 $3\nmid y$（這是因為 x,y,z 互質）。將式子 $(x^2/3)^2=(y^2)^2+(z/3)^2$ 模 3 得到 $0\equiv 1+(z/3)^2 \pmod 3$，這與 $(\text{整數})^2\equiv 0,1 \pmod 3$ 矛盾。若 $(x^2,3y^2,z)=1$，則由 (1) 及定理 3.1 可令

$$\begin{aligned}
&\begin{cases}x^2=m^2+n^2,\\ 3y^2=2mn,\\ z=m^2-n^2,\end{cases}\qquad \text{其中正整數 } m,n \text{ 互質}\\
&\qquad\Rightarrow\begin{cases}m=c^2-d^2,\\ n=2cd,\end{cases}\qquad \text{其中正整數 } c,d \text{ 互質且一奇，一偶}\\
&\qquad\Rightarrow 3\left(\tfrac{y}{2}\right)^2=cd(c^2-d^2),\ \text{其中正整數 } c,d,c^2-d^2 \text{ 兩兩互質。}
\end{aligned}$$

因為 c,d,c^2-d^2 為兩兩互質的正整數且 c,d 為一奇數、一偶數及

$$3\left(\frac{y}{2}\right)^2=cd(c^2-d^2).$$

現在分三種情形如下：

(a) 若 $3 \mid c$，則

$$\begin{aligned} c^2 - d^2 = e^2 \quad &\Rightarrow c^2 = d^2 + e^2 \\ &\Rightarrow 3 \mid d \text{ 或 } 3 \mid e \\ &\Rightarrow 3 \mid d \text{ （因為 } 3 \mid c\text{）。} \end{aligned}$$

此與 c, d 互質矛盾。

(b) 若 $3 \mid d$，則

$$\begin{cases} c = e^2, \\ d = 3f^2, \\ c^2 - d^2 = g^2, \end{cases} \quad \text{其中 } e, f, g \text{ 為正整數且 } e < c < n < x$$
$$\Rightarrow e^4 - 9f^4 = g^2.$$

這與 x 是最小的假設矛盾。

(c) 若 $3 \mid c^2 - d^2$，但 3 不整除 c 與 d，則

$$\begin{cases} c = e^2, \\ d = f^2, \end{cases} \quad \text{其中 } e, f \text{ 一奇，一偶且不是 3 的倍數}$$
$$\Rightarrow \begin{cases} (e^2 - f^2)(e^2 + f^2) = c^2 - d^2 = 3g^2, \\ 1 \equiv e^2 \equiv f^2 \pmod 3. \end{cases}$$

由 c, d 一奇、一偶且互質推得 $(e^2 - f^2, e^2 + f^2) = 1$；再利用 $3 \mid e^2 - f^2$ 得到

$$e^2 + f^2 = h^2 \Rightarrow e, f \text{ 至少有一個為 3 的倍數.}$$

這與 e, f 不是 3 的倍數矛盾。

綜合 (a)、(b)、(c) 得知：方程式 $x^4 - 9y^4 = z^2$ 無正整數解。 ⊠

3.4 費馬無窮遞降法的另一個應用

定理 3.5 利用費馬無窮遞降法證明：$\sqrt{2}$ 不是有理數。

【証明】設 $\sqrt{2}$ 是有理數，且將它表為

$$\sqrt{2} = \frac{q}{p}$$

的形式，其中 $p, q (p < q < 2p)$ 為正整數，且 q/p 是上述表示法中 p 值最小的一組。由

$$\begin{aligned} \sqrt{2} = \frac{q}{p} &\Rightarrow 2p^2 = q^2 \\ &\Rightarrow 2(q-p)^2 = (q-2p)^2 \\ &\Rightarrow \sqrt{2} = \frac{|q-2p|}{q-p} \end{aligned}$$

及分母 $(q-p) < p$ 知道：這與 q/p 是上述表示法中 p 值最小的一組矛盾。因此，$\sqrt{2}$ 不是有理數。 ⊠

習題 3.1 證明：邊長是正整數之直角三角形的內切圓半徑亦為正整數。

習題 3.2 試求 $x^4+1=z^2$ 的整數解 x,z。

習題 3.3 證明方程式 $x^4-y^4=z^2$ 無正整數解 x,y,z。

習題 3.4 證明方程式 $x^4-y^4=2z^2$ 無正整數解 x,y,z。

習題 3.5 證明方程式 $x^4+4y^4=z^2$ 無正整數解 x,y,z。

習題 3.6 證明：三邊皆為正整數的直角三角形的面積不可能是一個完全平方數。

習題 3.7 設 p 為質數，利用費馬無窮遞降法證明：$\sqrt{p}$ 不是有理數。

動手玩數學

希望之島西邊的居民都專說謊話，東邊的居民則有專說謊話的，也有專說實話的。一天一位數學家到這小島來觀光，一下飛機就有甲、乙、丙三位島上的居民爭著充當這位數學家的導遊。數學家分別叫甲去問乙、乙去問丙、丙去問甲住在島的哪一邊。結果回報是這樣的：

甲告訴數學家“乙說他住在島的東邊”

乙告訴數學家“丙說他住在島的西邊”

丙告訴數學家“甲說他住在島的東邊”

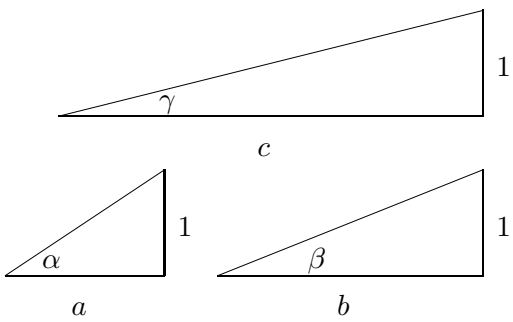
數學家猶豫一下之後，又叫丙去問乙住在島的哪一邊，回報是這樣的：

丙告訴數學家“乙說他住在島的西邊”

你能知道甲、乙、丙分別住在島的哪一邊，是老實人或者是說謊者嗎？

挑戰題

設正整數 a,b,c 是底下三個直角三角形的底邊之邊長。



如果

$$\alpha+\beta+\gamma=\frac{\pi}{4},$$

試求正整數 a,b,c 的值。

挑戰題

試求滿足

$$|3^m-2^n|=1$$

的正整數 m 與 n。

杰斯馬維奇猜想

杰斯馬維奇在 1956 年時，提出如下的猜想：如果正整數 a,b,c 滿足 $a^2+b^2=c^2$，則方程式

$$a^x+b^y=c^z$$

的正整數解僅有 $x=y=z=2$ 一組而已。中國數學家柯召在這方面有不錯的貢獻（大多發表在四川大學學報自然科學版）。例如在

$$\begin{cases} a=2n+1, \\ b=2n(n+1), \\ c=2n(n+1)+1, \end{cases} \qquad \text{其中 } n\equiv 1,4,5,9,10 \pmod{12}$$

時，杰斯馬維奇猜想是對的。

我國的數學奧林匹亞選訓營曾經考過如下的題目：若 $3^n+4^n=5^n$，則 $n=2$。有興趣的讀者，可以嘗試看看。

4 高斯引理

數學家高斯在數學上有許許多多有名的定理及猜想，高斯引理是大家最耳熟能詳及常用的一個。

4.1 高斯引理

定理 4.1 (高斯引理) 如果首項係數是 1 的多項式

$$x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0$$

整除另一個首項係數為 1 的多項式

$$x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0$$

其中 $a_{m-1}, \cdots, a_1, a_0$ 為有理數； $c_{n-1}, \cdots, c_1, c_0$ 為整數，則証明

$$a_{m-1}, \cdots, a_1, a_0$$

必須是整數。（註：這裡的整除是指所得的商是一個首項係數為 1，其它項係數為有理數的多項式）

【證明】假設多項式 $x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0$ 被多項式

$$x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0$$

除之，所得的商為

$$x^{n-m} + \frac{b_{n-m-1}}{b_{n-m}}x^{n-m-1} + \cdots + \frac{b_1}{b_{n-m}}x + \frac{b_0}{b_{n-m}},$$

其中

$$b_{n-m}, b_{n-m-1}, \cdots, b_1, b_0$$

是最大公因數為 1 的整數。將它整理成如下的橫式

$$\begin{array}{r} x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0 \\ \times)\ \ b_{n-m}x^{n-m} + b_{n-m-1}x^{n-m-1} + \cdots + b_1x + b_0 \\ \hline b_{n-m}(x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0) \end{array} \tag{4.1}$$

其次，將分數

$$a_{m-1}, \cdots, a_1, a_0$$

通分，可以令

$$a_i = \frac{a'_i}{a'_m}, \quad 0 \le i \le m-1,$$

其中 a'_m 為正整數且

$$a'_m, a'_{m-1}, \cdots, a'_1, a'_0$$

亦是最大公因數為 1 的整數。將乘式 (4.1) 乘以 a'_m 得到

$$\begin{array}{r} a'_m x^m + \cdots + a'_i x^i + \cdots + a'_0 \\ \times)\ \ b_{n-m}x^{n-m} + \cdots + b_j x^j + \cdots + b_0 \\ \hline a'_m b_{n-m}(x^n + \cdots + c_{i+j}x^{i+j} + \cdots + c_0) \end{array} \tag{4.2}$$

我們的目標是證明：$a'_m = 1$。利用反證法，假設正整數 $a'_m \neq 1$，因此至少有一個質因數 p 整除 a'_m。由

$$(a'_m, a'_{m-1}, \cdots, a'_1, a'_0) = 1$$

及

$$(b_{n-m}, b_{n-m-1}, \cdots, b_1, b_0) = 1$$

知道：可以找到整數

$$i, j(0 \leq i \leq m-1; 0 \leq j \leq n-m)$$

使得

$$\begin{cases} p \mid a'_0, p \mid a'_1, \cdots, p \mid a'_{i-1}; p \mid b_0, p \mid b_1, \cdots, p \mid b_{j-1}, \\ \text{但是 } p \text{ 不能整除 } a'_i \text{ 及 } b_j. \end{cases} \tag{4.3}$$

現在比較乘式 (4.2) 中 x^{i+j} 項的係數：因為 $p \mid a'_m$，所以乘式 (4.2) 下方的 x^{i+j} 項的係數為 p 的倍數；而乘式 (4.2) 上方的 x^{i+j} 項的係數為

$$\cdots + a'_{i-1}b_{j+1} + a'_i b_j + a'_{i+1}b_{j-1} + \cdots.$$

利用式子 (4.3)，可以將它整理為

$$\cdots + a'_{i-1}b_{j+1} + a'_i b_j + a'_{i+1}b_{j-1} + \cdots = a'_i b_j + p \text{ 的倍數。}$$

再由式子 (4.3) 知道此數不是 p 的倍數。互相矛盾，即 $a'_m = 1$，所以

$$a_{m-1}, \cdots, a_1, a_0$$

為整數。 ⊠

4.2 高斯引理的應用

一個角如果可以表為 $\frac{n}{m}\pi$（其中 m 為正整數，n 為整數）則我們稱這種角為有理角。

定理 4.2 如果 m, n 為正整數且 $\cos\frac{n}{m}\pi$ 為有理數則

$$\cos\frac{n}{m}\pi = 0, \pm\frac{1}{2}, \pm 1.$$

【証明】根據隸美佛定理知道

$$\cos\frac{n}{m}\pi + i\sin\frac{n}{m}\pi, \cos\frac{n}{m}\pi - i\sin\frac{n}{m}\pi$$

為方程式 $x^{2m}-1=0$ 的兩個根，所以

$$\begin{aligned}&x^2-2\cos\tfrac{n}{m}\pi x+1\\&=(x-\cos\tfrac{n}{m}\pi+i\sin\tfrac{n}{m}\pi)(x-\cos\tfrac{n}{m}\pi-i\sin\tfrac{n}{m}\pi)\mid x^{2m}-1.\end{aligned}$$

因為 $2\cos\frac{n}{m}\pi$為有理數，所以由高斯引理知道 $2\cos\frac{n}{m}\pi$ 為整數。所以我們得到

$$2\cos\frac{n}{m}\pi=-2,-1,0,1,2\Rightarrow\cos\frac{n}{m}\pi=0,\pm\frac{1}{2},\pm1.$$

又因為取特別角時，我們有

$$\cos 0\pi=1,\cos\frac{\pi}{3}=\frac{1}{2},\cos\frac{\pi}{2}=0,\cos\frac{2\pi}{3}=-\frac{1}{2},\cos\pi=-1.$$

所以這五個值都可能發生。 ⊠

這個定理是說：在 x 為有理數時（除了幾組特別值之外），函數 $f(x)=\cos(x\cdot\pi)$ 的值都是無理數。這是三角函數一個很重要而且奇怪的現象。

定理 4.3 三邊長為有理數且三內角為有理角的三角形必為正三角形。

【証明】設三角形 $\triangle ABC$ 的三邊長及三內角分別為 a,b,c 及 $\angle A,\angle B,\angle C$；由餘弦定理知道 $a^2=b^2+c^2-2bc\cos\angle A$；因為 a,b,c 為有理數，所以 $\cos\angle A$ 亦為有理數。根據定理 4.2 得

$$\cos\angle A=0,\pm\frac{1}{2},\pm1\Rightarrow\angle A=60^\circ,90^\circ,120^\circ.$$

同理有

$$\begin{cases}\angle A=60^\circ,90^\circ,120^\circ\\\angle B=60^\circ,90^\circ,120^\circ\\\angle C=60^\circ,90^\circ,120^\circ\end{cases}\Rightarrow\angle A=\angle B=\angle C=60^\circ.$$

因此三角形 $\triangle ABC$ 為正三角形。 ⊠

三角形最重要的兩個量為三邊的邊長及三個內角的角度。當三邊的邊長給定時，三內角的角度可以經由餘弦定理確定；而三內角的角度知道時，三邊的邊長比也可以經由正弦定理算出。這告訴我們，這兩個量是互相牽制的。有些人比較喜歡三邊邊長是正整數的三角形；但是也有些人比較欣賞三內角是有理角的三角形。定理 4.3 告訴我們，這兩種人共同中意的三角形就只有正三角形而已。也就是說，魚（好的邊長）與熊掌（好的內角）是不能兼得的。

習題 4.1 如果 m,n 為正整數且 $\sin\frac{n}{m}\pi$ 為有理數，則求 $\sin\frac{n}{m}\pi$ 的可能值。

習題 4.2 如果 m,n 為正整數且 $\tan\frac{n}{m}\pi$ 為有理數，則求 $\tan\frac{n}{m}\pi$ 的可能值。

習題 4.3 設 a,b 是互質的整數，且一次因式 $ax-b$ 整除整係數多項式

$$a_nx^n+\cdots+a_1x+a_0.$$

證明：整除所得的商式也是一個整係數多項式。

習題 **4.4** 設 m, n 為正整數，且令 $\theta = \frac{n}{m}\pi$。

(1) 如果 $\sin\theta + \cos\theta$ 為有理數，則求 $\sin\theta + \cos\theta$ 的可能值。

(2) 是否有這樣的 θ 滿足 $0 < n/m < 1/2$ 及 $\sin\theta - \cos 2\theta$ 為有理數。

動手玩數學

下圖是一張寫有八個數字的紙張。現在沿著格子線摺數次之後，變成看起來是一個正方格大小，但是厚度卻有八張紙張厚。如果依照次序將數字寫下來會產生一個八位數的正整數。你是否可以找到好的摺疊方式，讓產生的八位數恰為 12345678。

1	8	7	4
2	3	6	5

如果要變成 12364587，可辦到嗎？

挑戰題

試確定所有滿足底下條件的正整數 m 與正整數 n：

$$\sin\frac{2\pi}{m} = \left(\frac{1}{\sqrt{2}}\right)^n.$$

高斯

德國大數學家，生於 1777 年，死於 1855 年。高斯是一位天才數學家，被稱為數學王子。終其一生做了很多數學上偉大的貢獻，即使是今天的數學，仍然受高斯的影響非常深遠。高斯證明了古代有名的作圖題“正十七邊形可尺規作圖”，另外他也證明了“被八除之餘數不為七的正整數皆可表為三個整數的平方和”。事實上，在數論上，高斯有很多偉大的貢獻。

高斯提過很多有名的問題；例如是否有無窮多個質數 p 使得 $\frac{1}{p}$ 的循環節為 $p-1$ 位。$p = 7$ 即是一個

$$\frac{1}{7} = 0.\overline{142857}.$$

事實上，如果“黎曼猜想”成立的話，我們可以證明這樣的質數有無窮多個。

代數上有名的代數基本定理是高斯首先給予證明的。所謂的代數基本定理是指：任意以複數為係數的多項式（次數大於零次）必有複數根存在。