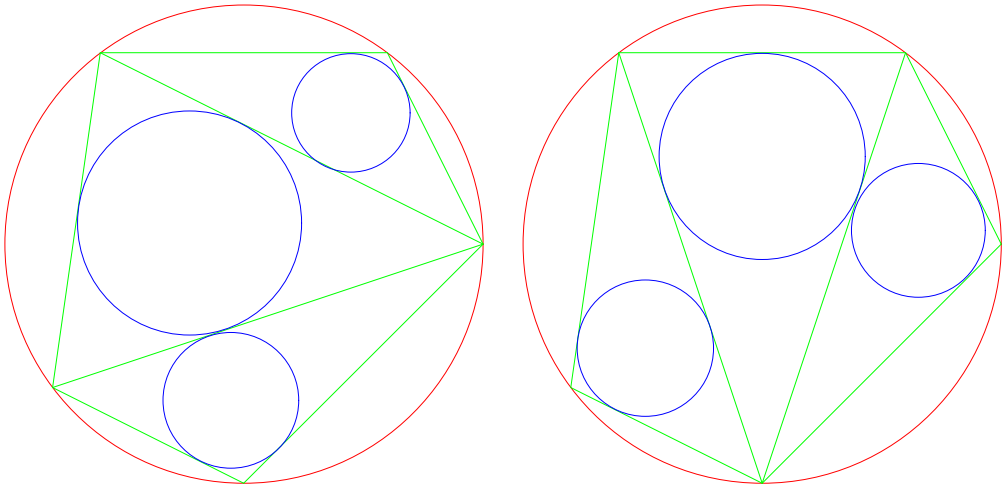
算術講義

許 志 農

國立台灣師範大學數學系

April 22, 2004



左圖三小圓半徑和＝右圖三小圓半徑和

目 錄

1 橢圓方程式（Elliptic Equation）

定理 **1.1** 證明：方程式

$$y^2 = x^3 + 23$$

無整數解 x 與 y。

【證明】假設整數 x 與 y 滿足原方程式，則我們有

$$\begin{cases} (\text{整數})^2 \equiv 0, 1 \pmod 4, \\ (\text{整數})^3 \equiv 0, 1, 3 \pmod 4, \\ y^2 \equiv x^3 + 23 \pmod 4. \end{cases} \Rightarrow \begin{cases} y^2 \equiv 0 \pmod 4, \\ x^3 \equiv 1 \pmod 4. \end{cases}$$

$$\Rightarrow \begin{cases} 2|y, \\ x \equiv 1 \pmod 4. \end{cases}$$

將原方程式改寫為

$$4(y/2)^2 + 4 = x^3 + 3^3 = (x+3)(x^2 - 3x + 9).$$

因為 $x \equiv 1 \pmod 4$, 所以 $x^2 - 3x + 9$ 被 4 除之，餘數為 3；即至少有一個被 4 除之，餘數為 3 的質數 p 整除 $x^2 - 3x + 9$。由此可推得

$$\begin{aligned} p \mid (y/2)^2 + 1 &\Rightarrow (y/2)^2 \equiv -1 \pmod p \\ &\Rightarrow (y/2)^4 \equiv 1 \pmod p. \end{aligned}$$

由費馬小定理知道

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

這與質數 p 先前的假設矛盾。 ☒

習題 **1.1** 證明：方程式 $y^2 = x^3 - 5$ 無整數解 x 與 y。

習題 **1.2** 證明：方程式 $y^2 = x^3 + 11$ 無整數解 x 與 y。 [1]

習題 **1.3** 證明：方程式 $y^2 = x^3 - 17$ 無整數解 x 與 y。

習題 **1.4** 考慮方程式 $y^2 = x^4 + x^3 + x^2 + x + 1$ 的整數解 x 與 y 如下：

(1) 當 $x < -1$ 或 $x > 3$ 時，證明：

$$(2x^2 + x)^2 < 4x^4 + 4x^3 + 4x^2 + 4x + 4 < (2x^2 + x + 1)^2.$$

(2) 利用 (1) 求方程式的整數解 x 與 y。

[1] 需要利用例題 ?? 的結果。

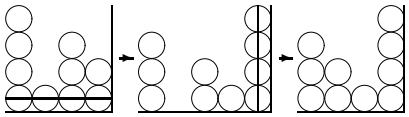
習題 **1.5** 數學家想要知道“是否有既可表為三個連續正整數乘積且亦可寫成兩個連續正整數乘積的正整數”。將此問題代數化，即是在解方程式

$$y^2 + y = x^3 - x$$

的正整數解 x 與 y。事實上，此方程式有顯然的整數解為 $(1,-1)$ 與 $(2,2)$。試求過此兩點的直線與方程式的另一個交點為何？ [2]

動手玩數學

如下圖：先將十個小皮球整齊地擺在一起（如第一圖所示），首先將最底下一列的小皮球（畫線的小皮球）拿掉，直擺到最右邊（如第二圖所示）；然後，如果有空白行出現，則將空白行左邊的小白球向右平移，讓它們緊靠在一起（如第三圖所示）。像這樣的過程，稱為操作一次。無論剛開始如何擺放小白球（不一定要擺四行，可擺任意行），在經過某些次的操作之後，是否都會產生同樣的結果。



挑戰題

考慮方程式 $y^2 = x^3 + 7$.

(1) 若整數數對 (x,y) 滿足此方程式，則 x 是奇數。

(2) 證明此方程式無整數解。（提示：利用 $y^2+1^2 = (x+2)((x-1)^2+3)$ 有一個被 4 除之，餘數為 3 的質因數。這個證明方法是由數學家勒貝格在 1869 年提出）。

獨立遊戲

這個遊戲是匈牙利的一位數學家圖沙在一個會議上所提出來的。現在就來介紹這個遊戲的玩法：一直線上有 n 個點（如下圖所示），甲、乙兩個人輪流每次只能選取一個點（甲先玩、乙後玩），而且每次所新選取的點，不能在之前已選的點的旁邊。最後當有人不能選取點的時候，那個人就輸了。

[2] 求出的解與 $(2,2)$ 是方程式的所有正整數解，參考 Quantum January/February 1997, pp. 5-10，像本問題的求點方法是有名的切線-割線法。

我們的目的是：當甲、乙兩人都玩得很有策略的時候，找出 n 等於多少的時候，誰會贏。例如：當 $n=3$ 時，甲選中間的點的時候，乙就不能再選了，那麼甲就贏定了。同時，我們也可以觀察到：當 n 是奇數的時候，甲有必贏的策略。因為甲選取中間點，就把這些點等分成兩個部份。而乙選取其中一個部份的某點時，那麼甲只要對稱中間點來選取另外一部份的那點即可。這樣下去，乙一定先遭遇到不能選取的情況（如下圖所示），那麼甲就贏定了。

如果 n 為偶數，很明顯地當 $n=2$ 時，甲贏。當 $n=4$ 時，乙會贏。而當 $n=6$ 時，只要甲選取最後一個點，那麼能夠選取的點就只剩下四個。因為 $n=4$ 是後玩的人贏，所以 $n=6$ 時，甲會贏。之後，我們可以檢驗出當 $n=8$ 時，乙贏； $n=10$ 時，是甲贏。繼續下去我們就可以知道當 $n=12,14,16,18$ 時，甲贏； $n=20,24,28$ 時，乙贏。

圖沙猜想：乙會贏的數字為 $n=0,14,34$ 或

$$n \equiv 4,8,20,24,28 \pmod{34}.$$

2 圓錐曲線上的格子點問題

本文的主要目的是要探討圓錐曲線上的格子點問題。底下是整數論常用有關因數，倍數的一個引理：若 d 為正整數，a,b 為整數且 $d \mid a, d \mid b$，則

$$d \mid am + bn,$$

其中 m,n 為整數。

例題 **2.1** 設分數 $\frac{x9}{9y}$ 與分數 $\frac{x}{y}$ 相等，其中 x,y 為阿拉伯數字。試求 x,y 的值？

【解】由題意知

$$\begin{aligned} \frac{10x+9}{90+y} = \frac{x}{y} &\Rightarrow 9xy - 90x + 9y = 0 \\ &\Rightarrow xy - 10x + y = 0 \\ &\Rightarrow (x+1)(y-10) = -10. \end{aligned}$$

因此

$x+1$	2	5	10
$y-10$	-5	-2	-1

$\Rightarrow (x,y) = (1,5), (4,8),$ 或 $(9,9).$

⊠

例題 **2.2** 設 m,n 為正整數且

$$\frac{n^3+1}{mn-1}$$

亦為正整數。試確定 m,n 的值。

【解】由 $(mn-1) \mid (n^3+1), (mn-1) \mid (mn-1)$ 得

$$\begin{cases} (mn-1) \mid (n^3+1)m - (mn-1)n^2 = n^2 + m, \\ (mn-1) \mid (n^3+1)m^3 - (mn-1)(m^2n^2 + mn + 1) = m^3 + 1. \end{cases}$$

故

$$\frac{n^3+1}{mn-1}, \frac{m^3+1}{mn-1}, \frac{n^2+m}{mn-1}$$

皆為正整數。由於 m,n 對稱的關係，我們假設 $m \geq n \geq 1$。又 m,n 不可能同時是 1，所以有 $m \leq 2(mn-1)$ 及 $n^2 \leq mn \leq 2(mn-1)$。故得

$$\frac{n^2+m}{mn-1} = 1, 2, 3, \text{ 或 } 4.$$

(1) 若

$$\frac{n^2+m}{mn-1} = 1,$$

則 $(n-1)(m-n-1) = 2$，即 $(m,n) = (5,2), (5,3)$。

(2) 若

$$\frac{n^2+m}{mn-1} = 2,$$

則 $(2n-1)(4m-2n-1) = 9$，即 $(m,n) = (2,2), (3,1)$。

(3) 若

$$\frac{n^2+m}{mn-1}=3,$$

則 $(3n-1)(9m-3n-1)=28$，即 $(m,n)=(2,1)$。

(4) 若

$$\frac{n^2+m}{mn-1}=4,$$

則 (m,n) 無解。

由對稱的關係可得到另外四組解

$$(m,n)=(2,5),(3,5),(1,3),(1,2).$$

因此共有

$$(m,n)=(5,2),(2,5),(5,3),(3,5),(2,2),(3,1),(1,3),(2,1),(1,2)$$

九組正整數解。 ☒

習題 **2.1** 三角形 ABC 是邊長為 15 的正三角形，P 為 BC 邊上的點。若線段長 PA,PB,PC 均為正整數，試求線段 PA 的長度。

習題 **2.2** 若分數 $\frac{x6}{6y}$ 與分數 $\frac{x}{y}$ 相等，其中 x,y 為阿拉伯數字。試求 x,y 的值？

習題 **2.3** 若分數 $\frac{x99}{99y}$ 與分數 $\frac{x}{y}$ 相等，其中 x,y 為阿拉伯數字。試求 x,y 的值？

習題 **2.4** 試求

$$x^2-y^2=611$$

的正整數解 x,y。

習題 **2.5** 試求

$$(m^2+n)(m+n^2)=(m+n)^3$$

的正整數解 m,n。

動手玩數學

任意給定 7 個整數（可以相同），是否必有 4 個的和為 4 的倍數。

挑戰題

如果 p 是奇質數且滿足

$$\frac{2^{p-1}-1}{p}\text{（根據費馬小定理，此數為正整數）}$$

是一個完全平方數。試求 p 的值。

阿廷-邱拉猜想

如果 p 是一個被 4 除之餘數為 1 的質數且正整數 x, y 是滿足

$$x^2 - py^2 = 4$$

且離原點最近的正整數解，則 p 不能整除 y。這是有名的阿廷-邱拉猜想。

3 質多項式的問題

如果一個整係數多項式（以整數為係數的多項式）不能分解為兩個次數大於零次的整係數多項式的乘積則稱這個多項式為質多項式。本節的目的是要提出一些方法來判斷一個多項式是否為質多項式。

3.1 艾森斯坦判別法

定理 **3.1** 設 $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ 為整係數多項式且存在一個質數 p 使得

$$\begin{cases} p \mid a_i (0 \le i \le n-1), \\ p^2 \text{ 不能整除 } a_0. \end{cases}$$

證明 $f(x)$ 是一個質多項式。

【證明】利用反證法，假設 $f(x)$ 可以分解成兩個次數大於零次的整係數多項式的乘積，並令

$$\begin{cases} f(x) = (x^m+\cdots+b_lx^l+p(b_{l-1}x^{l-1}+\cdots+b_0))\times \\ \qquad\quad (x^{n-m}+\cdots+c_1x+c_0), \\ \text{但是 } p \text{ 不能整除 } b_l, c_0. \end{cases}$$

現在比較 x^l 項的係數，由已知得到 $p \mid a_l$；但是由乘式

$$(x^m+\cdots+b_lx^l+p(b_{l-1}x^{l-1}+\cdots+b_0))(x^{n-m}+\cdots+c_1x+c_0)$$

得到 x^l 項的係數不為 p 的倍數，這與假設矛盾。因此 $f(x)$ 就是一個質多項式。 ☒

例題 **3.1** 如果 p 是一個質數，證明多項式

$$f(x)=x^{p-1}+x^{p-2}+\cdots+x+1$$

是一個質多項式。

【證明】假設

$$f(x)=x^{p-1}+x^{p-2}+\cdots+x+1=\frac{x^p-1}{x-1}$$

可分解，則多項式

$$\begin{aligned} g(x) &= f(x+1)=\frac{(x+1)^p-1}{x} \\ &= x^{p-1}+\tbinom{p}{1}x^{p-2}+\tbinom{p}{2}x^{p-3}+\cdots+\tbinom{p}{p-2}x+p \end{aligned}$$

也是可分解的多項式，但這與艾森斯坦判別法相矛盾。 ☒

3.2 利用同餘多項式判別質多項式

如果 p 是一個質數，$f(x)$ 與 $g(x)$ 是兩個整係數的多項式則用符號 $f(x) \equiv g(x) \pmod{p}$ 代表多項式差 $f(x) - g(x)$ 的每一 x 次方冪的係數都是 p 的倍數。此時我們稱多項式 $f(x)$ 與多項式 $g(x)$ 模 p 同餘。例如

$$\begin{aligned} x+1 &\equiv x-1 \pmod{2}, \\ x^2+3x+1 &\equiv x^2+x+1 \pmod{2}, \\ x^2+5x+13 &\equiv x^2+2x+1 \pmod{3}. \end{aligned}$$

我們容易推得：每一個首項係數為 1 的一次多項式必與 x 或 $x+1$ 模 2 同餘；每一個首項係數為 1 的二次多項式必與 x^2, x^2+x, x^2+1 或 x^2+x+1 模 2 同餘；每一個首項係數為 1 的三次多項式必與 $x^3, x^3+1, x^3+x^2, x^3+x^2+1, x^3+x^2+x, x^3+x^2+x+1, x^3+x$ 或 x^3+x+1 模 2 同餘。又因為

$$\begin{aligned} x^2 &\equiv x \cdot x \pmod{2}, \\ x^2+x &\equiv x(x+1) \pmod{2}, \\ x^2+1 &\equiv (x+1)(x+1) \pmod{2}, \end{aligned}$$

所以 $x^2+x+1 \pmod{2}$ 是唯一的一個二次模 2 質多項式（也就是說：此多項式模 2 之後不能分解）；同樣由

$$\begin{aligned} x^3 &\equiv x \cdot x \cdot x \pmod{2}, \\ x^3+1 &\equiv (x+1)(x^2+x+1) \pmod{2}, \\ x^3+x^2 &\equiv x^2 \cdot (x+1) \pmod{2}, \\ x^3+x^2+x &\equiv x \cdot (x^2+x+1) \pmod{2}, \\ x^3+x^2+x+1 &\equiv (x+1)^3 \pmod{2}, \\ x^3+x &\equiv x(x+1)^2, \end{aligned}$$

知道 $x^3+x^2+1 \pmod{2}$ 及 $x^3+x+1 \pmod{2}$ 是僅有的兩個三次模 2 質多項式。讀者是否可以仿照上述的方法找出所有的二次及三次模 3 的質多項式（限定首項係數為 1）。

例題 **3.2** 證明 $f(x) = x^4+3x^3+3x^2-4x+1$ 是一個質多項式。

【證明】四次多項式 $f(x)$ 的分解狀況有

$$\begin{cases} \text{（一次）（一次）（一次）（一次），} \\ \text{（一次）（一次）（二次），} \\ \text{（一次）（三次），} \\ \text{（二次）（二次），} \\ \text{質多項式。} \end{cases}$$

將 $x = \pm 1$ 代入得到 $f(1) = 4, f(-1) = 6$，由一次因式檢驗法知 $f(x)$ 沒有一次因式。因此第一、二、三種情形都不可能。

將 $f(x)$ 對 $p=2$ 取同餘（模 2）：因為模 2 的一次因式僅有 $x \pmod 2, x+1 \pmod 2$ 兩個，經逐一檢查得到

$$f(x) \equiv (x+1)(x^3+x+1) \pmod 2,$$

其中 $x^3+x+1 \pmod 2$ 已不可再分解。這說明了 $f(x)$ 沒有二次因式（你會說明嗎），所以第四種情形亦不可能。

由上述討論知道：多項式

$$f(x) = x^4+3x^3+3x^2-4x+1$$

必是一個質多項式。 ☒

如果 $f(x)$ 是一個首項係數為 1 的整係數多項式，p 是一個質數。我們判別的基本原理是這樣的：

(0) 如果 $f(x)$ 是可分解的，則 $f(x) \pmod p$ 是模 p 可分解的。

(1) 命題 (0) 的否逆命題為“如果 $f(x) \pmod p$ 是模 p 質多項式（不可分解的），則 $f(x)$ 必定是一個質多項（不可分解的）。”這是我們最常用的原理。

(2) 如果 $f(x) \pmod p$ 是可分解的，則不代表 $f(x)$ 可以分解。例如 $f(x)=x^2+x+2$，當 $p=2$ 時，

$$f(x) \equiv x(x+1) \pmod 2.$$

但是 $f(x)$ 是一個質多項式。

利用同餘判別質多項式是一種很重要且有效的判別方法，它的困難之處在於取那一個質數來做模，一般而言都是從較小的質數模起。

3.3 質數與質多項式

定理 **3.2** 如果質數 p 的十進位表示數為 $a_n a_{n-1}\cdots a_1 a_0$，其中

$$a_n, a_{n-1}, \cdots, a_1, a_0 \in \{0,1,2,3,4,5,6,7,8,9\}.$$

證明

$$f(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0$$

是一個質多項式。

【證明】首先證明：若複數 z 滿足 $f(z)=0$，則 $\mathrm{Re}(z)<4$（$\mathrm{Re}(z)$ 表示複數 z 的實部）。若 $x=\mathrm{Re}(z)>1$（如果 $x=\mathrm{Re}(z)\le 1$，則自然有 $\mathrm{Re}(z)<4$），則得到

$$\mathrm{Re}\left(\frac{1}{z}\right) = \frac{\mathrm{Re}(z)}{|\ z\ |^2} > 0.$$

再利用三角不等式

$$|\,a\,|+|\,b\,|\geq|\,a+b\,|\geq|\,a\,|-|\,b\,|$$

得到

$$\begin{aligned}
0=\left|\frac{f(z)}{z^n}\right| &\geq \left|a_n+\frac{a_{n-1}}{z}\right|-\left|\frac{a_{n-2}}{z^2}+\cdots+\frac{a_0}{z^n}\right| \\
&\geq \left|a_n+\frac{a_{n-1}}{z}\right|-\left(\frac{a_{n-2}}{|\,z\,|^2}+\cdots+\frac{a_0}{|\,z\,|^n}\right) \\
&\geq \mathrm{Re}\left(a_n+\frac{a_{n-1}}{z}\right)-\frac{9}{x^2}-\cdots-\frac{9}{x^n} \\
&\geq 1-\frac{9}{x^2-x} \\
\Rightarrow \qquad & \mathrm{Re}(z)<4 \quad (\text{因為假設 } x=\mathrm{Re}(z)>1).
\end{aligned}$$

其次假設多項式 $f(z)=g(z)h(z)$，其中 $g(z)$ 與 $h(z)$ 至少一次以上。對方程式 $h(z)=0$ 的每一實根 α，利用 $\mathrm{Re}(z)<4$ 得到 $10-\alpha\geq 10-4=6$；對方程式 $h(z)=0$ 的每一對共軛複根 $\alpha,\bar{\alpha}$，同理得到

$$(10-\alpha)(10-\bar{\alpha})=10^2-20\mathrm{Re}(\alpha)+|\,\alpha\,|^2\geq 10^2-20\times 4>1.$$

綜合得到 $|\,h(10)\,|>1$，同理也有 $|g(10)|>1$。

因為 $f(10)=g(10)h(10)$ 與 $f(10)=a_na_{n-1}\cdots a_1a_0=p$ 是質數矛盾，所以

$$f(z)=a_nz^n+a_{n-1}z^{n-1}+\cdots+a_1z+a_0$$

必須是一個質多項式。 ☒

習題 **3.1** 證明 $f(x)=x^4-x+1$ 是一個質多項式。

習題 **3.2** 證明 $f(x)=x^5+3x^4+x^3+7x+1$ 是一個質多項式。

習題 **3.3** 判別 $f(x)=x^5-x^2+1$ 是否為質多項式？

習題 **3.4** 證明 $f(x)=x^5+x^4+8x^3+5x^2+8x+9$ 是一個質多項式。

習題 **3.5** 證明 $f(x)=x^6-x^3+1$ 是一個質多項式。

習題 **3.6** 將多項式 $f(x)=x^7+x^5+x^3+x^2-1$ 分解成質多項式的乘積。

習題 **3.7** 證明 $f(x)=x^6+3x^4+1$ 是一個質多項式。 [3]

習題 **3.8** 試

(1) 列出所有模 3 的二次質多項式（限定首項係數為 1 者）。

[3] 可以考慮模 2 及模 3。

(2) 將多項式 $f(x)=x^6-6x^4+6x^3+12x^2+36x+1$ 對模 3 作分解。

(3) 證明 $f(x)$ 是一個質多項式。

習題 **3.9** 試

(1) 判別 x^3-3x+1 是否為質多項式。

(2) 證明：使多項式

$$(x^3-3x+1)(ax+b)+12-3x^2$$

是一個整數係數多項式的完全平方之整數解 (a,b) 至多僅有一組。

動手玩數學

三個同心圓，半徑分別為 $1, r_1, r_2$ $(1<r_1<r_2)$。甚麼時候可以在此三圓上各取一點，使它們構成一個正三角形。

挑戰題

試證明

(1) 如果整數 a,b 滿足

$$(x^3-3x+1)(ax+b)-3x^2+12=f(x)^2$$

其中 $f(x)$ 是整係數多項式，試確定所有 a,b 及多項式 $f(x)$ 的值。

(2) 若 α 為 $x^3-3x+1=0$ 的一根，試證明此三次方程式的另兩個根均可表為 α 的整係數多項式，並求此兩根。

科拉茨猜想

如果 n 是一個正整數，我們定義：

$$T(n)=\begin{cases}\frac{n}{2} & n \text{ 是偶數},\\ \frac{3n+1}{2} & n \text{ 是奇數}.\end{cases}$$

如此，給定任一個正整數 n, 我們就產生了一個數列如下：

$$n, T(n), T(T(n)), T(T(T(n))), \cdots.$$

例如： $n=7$ 時，產生的數列為

$$7,11,17,26,13,20,10,5,8,4,2,1,2,1,\cdots.$$

科拉茨猜想是說：對任意的正整數 n, 我們所產生的數列

$$n, T(n), T(T(n)), T(T(T(n))), \cdots$$

至少有一項為 1（或者此數列最後一定是 1 與 2 交替出現）。

4 平方和問題

質數可以簡單的分成 2 及奇質數，其中奇質數又可分成被 4 除餘 1，被 4 除餘 3 兩大類。前幾個被 4 除餘 1 的質數為

$$5,\ 13,\ 17,\ 29,\ 37,\cdots.$$

這類質數有如下的特性：

$$5=1^2+2^2,\ \ 13=2^2+3^2,\ \ 17=1^2+4^2,\ \ 29=2^2+5^2,\ \ 37=1^2+6^2,\cdots.$$

這節的目的就是要證明“被 4 除之，餘數為 1 的質數均可表為兩個正整數的平方和”。在證明這定理之前，我們先證明威爾遜及圖埃定理，然後再利用它們來證明主要的定理。

4.1 威爾遜定理

定理 **4.1** (威爾遜定理) 設 p 為一個質數則證明

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

【証明】如果正整數 m 滿足 $1\le m\le p-1$，則因為 $(m,p)=1$，所以根據定理 **??**（二元一次不定方程式的整數解通解）：會有一組整數 m',p' $(1\le m'\le p-1)$ 使得 $mm'+pp'=1$，即

$$mm'\equiv 1 \pmod{p}.$$

如果 $m=m'$，則

$$\begin{aligned} m^2\equiv 1 \pmod{p} &\Rightarrow \ (m+1)(m-1)\equiv 0 \pmod{p}\\ &\Rightarrow \ m=1 \ \text{ 或 } \ p-1. \end{aligned}$$

在繼續證明之前，我們舉例計算 $p=7$ 的情形。因為

$$2\cdot 4\equiv 1 \pmod{7}, 3\cdot 5\equiv 1 \pmod{7},$$

所以 $2'=4, 3'=5$。因此

$$\begin{aligned} 1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6 &\equiv 1\cdot 6\cdot\{2\cdot 2'\cdot 3\cdot 3'\} \pmod{7}\\ &\equiv 6\cdot\{1\cdot 1\} \pmod{7}\\ &\equiv -1 \pmod{7}. \end{aligned}$$

模仿這個例子，我們得到

$$\begin{aligned} 1\cdot 2\cdots(p-1) &\equiv 1\cdot(p-1)\cdot\{2\cdot\cdots\cdot(p-2)\} \pmod{p}\\ &\equiv -1\cdot\{2\cdot 2'\cdot 3\cdot 3'\cdots\} \pmod{p}\\ &\equiv -1\cdot\{1\cdot 1\cdots 1\} \pmod{p}\\ &\equiv -1 \pmod{p}. \end{aligned}$$

⊠

威爾遜定理是由華林於 1770 年時首先發表。這裡的方法是高斯的證明方法。

4.2 圖埃定理

定理 4.2 (圖埃定理) 設 $p \geq 2$ 為一個質數，a 是與 p 互質的整數。那麼可以找到整數 x, y 滿足

$$\begin{cases} ax \equiv y \pmod{p}, \\ 0 < |x|, |y| < \sqrt{p}. \end{cases}$$

【証明】當整數 u, v 滿足 $0 \leq u, v < \sqrt{p}$ 時（即 u 與 v 在這個範圍變動時），$au - v$ 一共產生了 $([\sqrt{p}] + 1)^2$ 個數字（相同的數字需重複計算）。因為超過 p 個整數，所以至少有兩個數字被 p 除之，餘數一樣，並令此兩組不同的數對為 $(u_1, v_1), (u_2, v_2)$。所以我們有

$$\begin{cases} au_1 - v_1 \equiv au_2 - v_2 \pmod{p}, \\ 0 \leq u_1, u_2, v_1, v_2 < \sqrt{p}. \end{cases} \Rightarrow \begin{cases} a(u_1 - u_2) \equiv (v_1 - v_2) \pmod{p}, \\ \mid u_1 - u_2 \mid < \sqrt{p}, \mid v_1 - v_2 \mid < \sqrt{p}. \end{cases} \tag{4.1}$$

現在證明 $0 < \mid u_1 - u_2 \mid, 0 < \mid v_1 - v_2 \mid$。利用反證明法，如果

$$\mid u_1 - u_2 \mid = 0,$$

則由 (4.1) 知道

$$0 \equiv v_1 - v_2 \pmod{p} \Rightarrow p \mid (v_1 - v_2).$$

由 $\mid v_1 - v_2 \mid < \sqrt{p}$ 推得 $v_1 - v_2 = 0$，即 $v_1 = v_2$。因此得到 $u_1 = u_2, v_1 = v_2$。這與此兩序對是不同的序對矛盾。因此 $0 < \mid u_1 - u_2 \mid < \sqrt{p}$，再利用 (4.1) 及 $(a, p) = 1$ 亦可證得 $0 < \mid v_1 - v_2 \mid < \sqrt{p}$。現在取

$$\begin{cases} x = u_1 - u_2 \neq 0, \\ y = v_1 - v_2 \neq 0, \end{cases}$$

則滿足定理所要的條件。 ☒

4.3 平方和問題

引理 4.1 設 p 為一個質數且 $p \equiv 1 \pmod{4}$。證明：可以找到整數 a 滿足 $a^2 \equiv -1 \pmod{p}$。

【証明】令 $p = 4n + 1$，則由威爾遜定理得到

$$\begin{aligned} (1 \cdot 2 \cdots (2n))^2 &\equiv \{1 \cdot 2 \cdots (2n)\}\{(-2n-1) \cdot (-2n-2) \cdots (-4n)\} \pmod{p} \\ &\equiv \{1 \cdot 2 \cdots (2n)\}\{(2n+1) \cdot (2n+2) \cdots (4n)\} \pmod{p} \\ &\equiv -1 \pmod{p}. \end{aligned}$$

取

$$a = 1 \cdot 2 \cdot \cdots \cdot \left(\frac{p-1}{2}\right)$$

滿足引理的要求。 ☒

定理 **4.3** (平方和問題) 證明：被 4 除之餘數為 1 的質數均可表為兩個正整數的平方和。

【証明】在圖埃定理中取 $a = 1 \cdot 2 \cdots (\frac{p-1}{2})$ 及利用引理 4.1 知道：存在整數 x, y 滿足

$$\begin{cases} ax \equiv y \pmod{p} \\ a^2 \equiv -1 \pmod{p} \\ 0 < |x|, |y| < \sqrt{p} \end{cases} \Rightarrow \begin{cases} a^2x^2 \equiv y^2 \pmod{p} \\ a^2 \equiv -1 \pmod{p} \\ 0 < x^2 + y^2 < 2p \end{cases}$$
$$\Rightarrow \begin{cases} x^2 + y^2 \equiv 0 \pmod{p} \\ 0 < x^2 + y^2 < 2p \end{cases}$$
$$\Rightarrow \quad x^2 + y^2 = p.$$

⊠

習題 **4.1** 若 p 是一個奇質數，則證明

(1) p 可表為兩個整數的平方和的充要條件為

$$p \equiv 1 \pmod{4}.$$

(2) 若質數 $p \equiv 1 \pmod{4}$，則 p 可表為 $5x^2 + 6xy + 2y^2$ 的形式，其中 x, y 為整數。

習題 **4.2** 證明

(1) 證明恆等式

$$\begin{aligned} (a^2 + b^2)(c^2 + d^2) &= (ac + bd)^2 + (ad - bc)^2 \\ &= (ac - bd)^2 + (ad + bc)^2 \end{aligned}$$

(2) 如果正整數 m, n 均可表為 2 個整數的平方和，則證明 mn 亦可表為 2 個整數的平方和。

習題 **4.3** 解

(1) 將 8177 因數分解。

(2) 將 8177 表為 2 個正整數的平方和（寫出一組即可）。

習題 **4.4** 設正整數 $p \geq 2$。

(1) 試猜測

$$((p-1)! + 1, p!) = ?$$

(2) 證明你的猜測是正確的。

習題 **4.5** 若 p 為質數，m, n 為互質的整數且 $p \mid 2m^2 + n^2$，則證明：

(1) 可以找到整數 a 使得 $a^2 \equiv -2 \pmod{p}$。

(2) 質數 p 可表為 $2x^2 + y^2$ 的形式，其中 x, y 為整數。（提示：使用圖埃定理）。

習題 **4.6** 若正整數 m, n 可表為 $3x^2 + y^2$ 的形式，其中 x, y 為整數，則證明 mn 亦可表為 $3x^2 + y^2$ 的形式。

動手玩數學

是否能將 $0, 1, 2, 3, 4, 5, 6, 7$ 八個數字填在正立方體的八個頂點上，使得任意一邊的兩個數字和都是質數？

挑戰題

若 p 為奇質數，m, n 為互質的整數且 $p \mid 3m^2 + n^2$，則證明：

(1) 可以找到整數 a 使得 $a^2 \equiv -3 \pmod{p}$。

(2) 奇質數 p 可表為 $3x^2 + y^2$ 的形式，其中 x, y 為整數。

愛爾特希猜想

是否存在相異的正整數數對 (a, b) 及 (c, d)（其中 $a < b$ 且 $c < d$）使得

$$a^5 + b^5 = c^5 + d^5.$$

一般猜想這樣的正整數序對是不存在的。也就是說：當正整數序對 (a, b) 不同時，所產生的值 $a^5 + b^5$ 也是不相同的。

如果將冪數 5 改成 3，這個猜想是不對的。例如：印度數學家拉馬努金發現數對 $(9, 10)$ 與 $(1, 12)$ 同時滿足

$$1729 = 9^3 + 10^3 = 1^3 + 12^3.$$

其它的結果還有

$$\begin{aligned} 87539319 &= 167^3 + 436^3 \\ &= 228^3 + 423^3 \\ &= 255^3 + 414^3. \end{aligned}$$

事實上，還有另外一個四位數正整數可以有兩種不同的立方和表示法。你知道是哪一個嗎？

5 同餘數與斐波那契問題

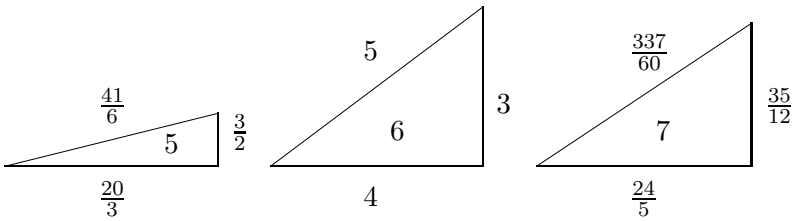
5.1 同餘數與例子

一個正整數 N 稱為同餘數是指“存在一個三邊都是有理數的直角三角形且此直角三角形的面積恰為 N”。例如 $N=5,6,7$ 都是同餘數，它們所對應的直角三角形如下（註：很多有理數邊長的直角三角形之面積為同一個同餘數 N 是可能發生的）：

(1) 勾，股分別為 $\frac{20}{3},\frac{3}{2}$；而弦為 $\frac{41}{6}$ 的直角三角形的面積為 5。因此 $N=5$ 為同餘數。

(2) 勾，股分別為 $3,4$；而弦為 5 的直角三角形的面積為 6。因此 $N=6$ 為同餘數。

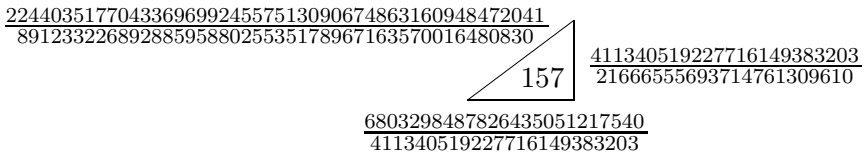
(3) 勾，股分別為 $\frac{24}{5},\frac{35}{12}$；而弦為 $\frac{337}{60}$ 的直角三角形的面積為 7。因此 $N=7$ 為同餘數。



事實上，$N=157$ 也是一個同餘數，它所對應的有理數邊長直角三角形如下：

$$\begin{aligned}
\text{勾} &= \frac{6803298487826435051217540}{411340519227716149383203}\\
\text{股} &= \frac{411340519227716149383203}{21666555693714761309610}\\
\text{弦} &= \frac{224403517704336969924557513090674863160948472041}{8912332268928859588025535178967163570016480830}
\end{aligned}$$

（由 D. Zagier 計算得到）



5.2 斐波那契問題

斐波那契在 1225 年參加羅馬皇帝腓特烈二世所舉行的數學競賽，他解出了所有的數

學問題，輕易的拿到冠軍。其中有一題與同餘數相關，斐波那契算出底下的式子：

$$\begin{cases} \left(\frac{41}{12}\right)^2 - 5 = \left(\frac{31}{12}\right)^2, \\ \left(\frac{41}{12}\right)^2 + 5 = \left(\frac{49}{12}\right)^2. \end{cases}$$

這個式子後來出現在斐波那契獻給熱中學術活動的腓特烈二世的書《平方數之書》上。事實上，第九世紀以前，阿拉伯的紙草上就有這樣的一則問題：給定一個正整數 N，是否可以找到三個正有理數 x, y, z 使得

$$\begin{cases} x^2 - N = y^2, \\ x^2 + N = z^2. \end{cases}$$

現在我們都稱這樣的問題為斐波那契問題。斐波那契問題與同餘數問題是緊密不可分的，這可由底下的定理看出來。

定理 **5.1** 設 N 是一個正整數，則底下兩則敘述是一樣的。

(1) N 是一個同餘數。

(2) 斐波那契問題對正整數 N 有解。

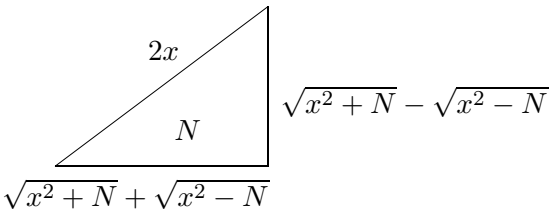
【證明】 (1) $\Rightarrow$ (2)：設有理數 p, q, r 滿足：$p^2 + q^2 = r^2, pq = 2N$，則

$$\begin{cases} \left(\frac{p+q}{2}\right)^2 - N = \left(\frac{r}{2}\right)^2, \\ \left(\frac{p-q}{2}\right)^2 + N = \left(\frac{r}{2}\right)^2. \end{cases}$$

因此，斐波那契問題對正整數 N 有解。
(1) $\Leftarrow$ (2)：設斐波那契問題對正整數 N 有解，則可以找到正有理數 x, y, z 滿足

$$\begin{cases} x^2 - N = y^2, \\ x^2 + N = z^2. \end{cases}$$

考慮底下的直角三角形，得到：N 是一個同餘數。



$\boxtimes$

5.3 $N = 3$ 不是同餘數

定理 **5.2** $N = 3$ 不是同餘數。

【証明】假設 $N=3$ 是一個同餘數且

$$\frac{x}{q},\frac{y}{q},\frac{z}{q}$$

構成一個面積為 3 的直角三角形的（勾，股，弦）三有理數邊，其中 x,y,z,q 為正整數且可令 x,y,z 兩兩互質。因為 $z^2=x^2+y^2$，所以存在互質的正整數 m,n 使得

$$\begin{cases} x=m^2-n^2, \\ y=2mn, \\ z=m^2+n^2, \\ mn(m^2-n^2)=3q^2 \text{（因為面積為 3 的關係）}, \end{cases}$$

其中正整數 m,n,m^2-n^2 兩兩互質且正整數 m,n 為一奇一偶。由式子 $mn(m^2-n^2)=3q^2$ 可分成下列三種來討論：

(1) 若 $3\mid m$ 則由式子 $mn(m^2-n^2)=3q^2$ 可得 m^2-n^2 必是一個完全平方數，且令 $m^2-n^2=q_1^2$，即 $n^2+q_1^2=m^2$。因此 $3\mid n$ 或 $3\mid q_1$，即 $3\mid(m,n)$（由 $3\mid m, n^2+q_1^2=m^2$ 得到），這與 m,n 互質不合。

(2) 若 $3\mid n$ 則由式子 $mn(m^2-n^2)=3q^2$ 的分解可得 $m=a^2,n=3b^2,m^2-n^2=c^2$，其中 a,b,c 為正整數；因此 $a^4-9b^4=c^2$；此與定理 ?? 矛盾。

(3) 若 $3\mid m^2-n^2$ 且 m,n 不為 3 的倍數，則由式子 $mn(m^2-n^2)=3q^2$ 的分解可得

$$\begin{cases} m=a^2,n=b^2, \quad \text{正整數 } a,b \text{ 互質，一奇一偶且 } 3\nmid ab, \\ (a^2+b^2)(a^2-b^2)=a^4-b^4=3q_2^2, \quad q_2 \text{ 為正整數.} \end{cases} \tag{5.1}$$

因為正整數 a,b 互質，一奇一偶且不被 3 整除，所以有

$$\begin{cases} (a^2-b^2,a^2+b^2)=1, \\ 3\mid a^2-b^2. \end{cases} \tag{5.2}$$

由式子 (5.1) 與 (5.2) 得到

$$a^2+b^2=q_3^2 \Rightarrow a,b \text{ 至少有一個為 3 的倍數.}$$

這與 a,b 不為 3 的倍數不合。

綜合得知：$N=3$ 不是同餘數。 ☒

習題 **5.1** 證明

(1) 若 $N=1$ 是同餘數則證明方程式

$$x^4-y^4=z^2$$

有正整數解 x,y,z.

(2) 證明 $N=1$ 不是同餘數。

習題 **5.2** 證明 $N=2$ 不是同餘數。

習題 **5.3** 證明 $N=14$ 是同餘數。

習題 **5.4** 證明 $N=15$ 是同餘數。

習題 **5.5** 證明 $N=41$ 是同餘數。

習題 **5.6** $(5/2,1/2,7/2)$ 是斐波那契問題對正整數 $N=6$ 的一組解，是否可以找到其它的解。

動手玩數學

平面上由上而下依序劃三條相異的平行線，其中第一條與第二條、第二條與第三條的距離分別為 d_1,d_2。試問：可以在三條直線上各取一點，使它們構成一個正三角形嗎？又此正三角形的邊長為何？

挑戰題

在一個邊長為 $3a$ 的正方形上放著一支長度為 $5a$ 寬度為 a 的直尺。試問此直尺應該如何擺設才能使蓋住的面積為最大？此蓋住的最大面積又是多少呢？

同餘數

$N=7$ 是同餘數為大數學家尤拉發現的。事實上，古代就可以證明：$N=1,2,3,4$ 都不是同餘數，另外 $N=13,14,15$ 亦知是同餘數。

同餘數問題是相當古老的問題，它的判別也很不容易。數學家一直到最近才有比較多的進展，不過距離解決此問題也許仍有一大段距離。如果 P 是一個被 8 除之，餘數為 3 的質數則數學家可以證明：P 不是同餘數，但是 $2P$ 是同餘數。著名的歐特-庫爾第-注田忠彥 猜想是說：如果正整數 N 滿足 $N\equiv 5,6,7 \pmod 8$ 則 N 是同餘數。

從較深的橢圓曲線的知識，我們可以得到判斷同餘數較好的方法如下：假設橢圓曲線 $E_N: y^2=x^3-N^2x$，則 N 是同餘數的充分必要條件為橢圓曲線 E_N 有無窮多組有理數解 (x,y)。

同餘數問題是歷史上的難題，有關它的研究有很多。當 n 為正整數時，$N=6(1^2+2^2+3^2+\cdots+n^2)$ 及 $N=8n^3-2n$ 都是同餘數。讀者可以用斐波那契方法試試看。

與同餘數相關的另一個問題是由印度數學家婆羅摩芨多發現的：設以有理數 a,b,c 為邊長的三角形面積亦為有理數。那麼一定可以找到正有理數 u,x,y 使得

$$\begin{cases} a=\frac{u^2+x^2}{x}, \\ b=\frac{u^2+y^2}{y}, \\ c=\frac{u^2-x^2}{x}+\frac{u^2-y^2}{y}. \end{cases}$$

有興趣的讀者，可以試試看這則第六世紀的問題。