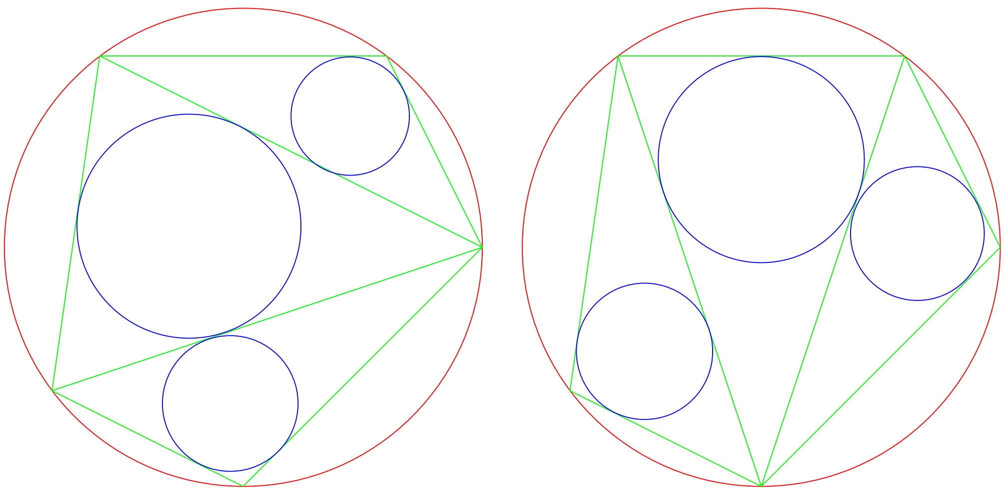
# 算術講義

許　志　農

國立台灣師範大學數學系

December 26, 2004



左圖三小圓半徑和＝右圖三小圓半徑和

# 目 錄

# 1 同餘數與斐波那契問題

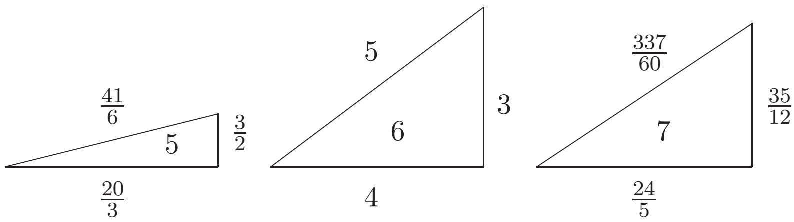
## 1.1 同餘數與例子

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。

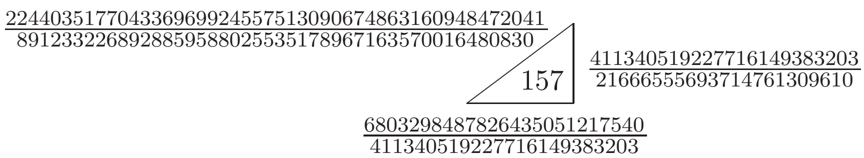
(3) 勾，股分別為 $\frac{24}{5},\frac{35}{12}$；而弦為 $\frac{337}{60}$ 的直角三角形的面積為 7。因此 $N=7$ 為同餘數。




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）




## 1.2 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 **1.1** 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

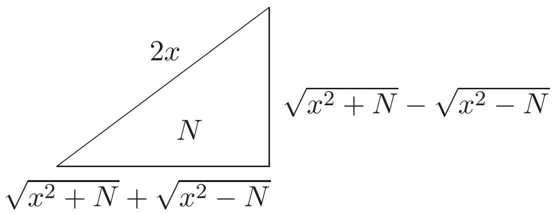
$$\begin{cases}\left(\frac{p+q}{2}\right)^2-N=\left(\frac{r}{2}\right)^2,\\ \left(\frac{p-q}{2}\right)^2+N=\left(\frac{r}{2}\right)^2.\end{cases}$$

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。




$\boxtimes$

### 1.3 $N=3$ 不是同餘數

定理 **1.2** $N=3$ 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

$$\begin{cases} m=a^2, n=b^2, \quad \text{正整數 } a,b \text{ 互質，一奇一偶且 } 3 \nmid ab, \\ (a^2+b^2)(a^2-b^2)=a^4-b^4=3q_2^2, \quad q_2 \text{ 為正整數}. \end{cases} \tag{1.1}$$

因為正整數 $a,b$ 互質，一奇一偶且不被 3 整除，所以有

$$\begin{cases} (a^2-b^2, a^2+b^2)=1, \\ 3 \mid a^2-b^2. \end{cases} \tag{1.2}$$

由式子 (1.1) 與 (1.2) 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 **1.1** 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 **1.2** 證明 $N=2$ 不是同餘數。

習題 **1.3** 證明 $N=14$ 是同餘數。

習題 **1.4** 證明 $N=15$ 是同餘數。

習題 **1.5** 證明 $N=41$ 是同餘數。

習題 **1.6** $(5/2, 1/2, 7/2)$ 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-洼田忠彥 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 $E_N : y^2 = x^3 - N^2 x$，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笈多發現的：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。