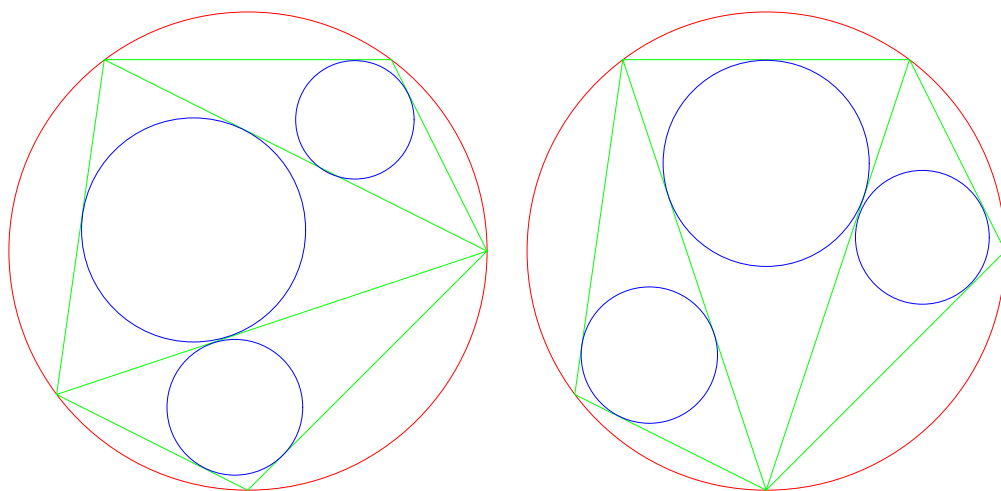


算術講義

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	平方和問題	1
1.1	威爾遜定理	1
1.2	圖埃定理	2
1.3	平方和問題	2

1 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

$$5, 13, 17, 29, 37, \dots$$

這類質數有如下的特性：

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

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。

1.1 威爾遜定理

定理 1.1 (威爾遜定理) 設 p 為一個質數則證明

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

【證明】如果正整數 m 滿足 $1 \leq m \leq p-1$ ，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' ($1 \leq m' \leq p-1$) 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

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

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

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

□

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。

1.2 圖埃定理

定理 1.2 (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

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

【證明】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

$$\begin{cases} au_1 - v_1 \equiv au_2 - v_2 \pmod{p}, \\ 0 \leq u_1, u_2, v_1, v_2 < \sqrt{p}. \end{cases} \Rightarrow \begin{cases} a(u_1 - u_2) \equiv (v_1 - v_2) \pmod{p}, \\ |u_1 - u_2| < \sqrt{p}, |v_1 - v_2| < \sqrt{p}. \end{cases} \quad (1.1)$$

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

$$|u_1 - u_2| = 0,$$

則由 (1.1) 知道

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

由 $|v_1 - v_2| < \sqrt{p}$ 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 $0 < |u_1 - u_2| < \sqrt{p}$, 再利用 (1.1) 及 $(a, p) = 1$ 亦可證得 $0 < |v_1 - v_2| < \sqrt{p}$ 。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。 □

1.3 平方和問題

引理 1.1 設 p 為一個質數且 $p \equiv 1 \pmod{4}$ 。證明: 可以找到整數 a 滿足 $a^2 \equiv -1 \pmod{p}$ 。

【證明】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

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

滿足引理的要求。 □

定理 1.3 (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。

【證明】在圖埃定理中取 $a = 1 \cdot 2 \cdots (\frac{p-1}{2})$ 及利用引理 1.1 知道：存在整數 x, y 滿足

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

□

習題 1.1 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 1.2 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 1.3 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 1.4 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 1.5 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 1.6 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？