# 費馬最後定理

余文卿

西元 1637 年左右, Fermat 在他的書的邊緣上這樣寫著: "$n$ 是大於 2 的正整數時, 不定方程式 $x^n + y^n = z^n$ 沒有非顯然的整數解。"

他並附加道: "我找到了一非常漂亮的證明, 但這裡沒有足夠的空間, 致無法將證明寫下"。到目前爲止, 這敍述並沒有得到證明, 但也舉不出反例, 而被稱爲費馬最後定理 (Fermat's Last Theorem)。

到底 Fermat 有沒有眞正證明了費馬最後定理? 以他那時的數學工具, 他可能證出 $n = 3, 4, 5$ 的特殊情形, 而據此推斷一般的 $n$ 都成立, 這也是當代不太成熟的數學歸納法, 三百多年來, 這問題雖未獲徹底解決, 但引發了一系列數論方面的主題, 使數論發展到另一新的境界。

顯然地, 若對某一冪次 $n$ 的費馬最後定理得證, 則對所有 $n$ 的倍數冪次, 定理也跟著成立。注意到任意大於 2 的正整數, 不是 4 的倍數, 就是奇質數的倍數, 故只需考慮 $n = 4$ 或 $n$ 是奇質數的情形。

我們將看到 $n = 4$ 時定理成立, 因而只需考慮 $n$ 是奇質數的情形。一般, 我們將奇質數冪次分成下面兩類。

(A)費馬最後定理第一種情形: 不定方程式

$$x^p + y^p = z^p, \quad (p, xyz) = 1$$

沒有整數解。

(B)費馬最後定理第二種情形: 不定方程式

$$x^p + y^p = z^p, \quad p|z, \quad (p, xy) = 1$$

沒有整數解。

在底下各節, 我們將分別探討 $n = 4, n = 3$ 以及 $p$ 是規則質數 (regular prime) 的特別情形。

## 一. $n = 4$的特別情形

在這一節, 我們將證明 $n = 4$ 時定理成立, 因而 $n$ 是 4 的倍數時, 定理也跟著成立。使用的手法通稱爲下降法 (method of decent)。即假設有一組整數解, 嘗試由這組解得出另一數據較小的整數解, 若原先出發的整數解已設定爲數據最小的, 則這與假設矛盾。故原先方程式不會有解, 這方法在 Fermat 的時代, 就有人用過。現我們從不定方程式 $x^2 + y^2 = z^2$ 的整數解談起。

**預備定理 1.** 在條件 $x>0,\ y>0,\ z>0,\ (x,y)=1,\ 2|x$ 限制下, 不定方程式

$$x^2+y^2=z^2$$

的一般解是

$$x=2ab,\quad y=a^2-b^2,\quad z=a^2+b^2,$$

其中 $a,b$ 是滿足 $(a,b)=1,\ a>b>1$ 的整數。

**證明**: 因 $2|x$ 且 $(x,y)=1$, 故 $y$ 與 $z$ 都是奇數且互質, 得出 $\frac{z-y}{2}$ 與 $\frac{z+y}{2}$ 是互質整數, 又

$$\left(\frac{x}{2}\right)^2=\left(\frac{z-y}{2}\right)\left(\frac{z+y}{2}\right)$$

故得出 $\frac{z-y}{2}$ 與 $\frac{z+y}{2}$ 都是平方數, 定

$$\frac{z+y}{2}=a^2,\quad \frac{z-y}{2}=b^2$$

則 $z=a^2+b^2,\ y=a^2-b^2,\ x=2ab$。

更進一步

$$a>0,\ b>0,\ a>b,\ (a,b)=1。$$

反過來, 很容易驗證

$$z=a^2+b^2,\ y=a^2-b^2,\ x=2ab$$

確實是不定方程式 $x^2+y^2=z^2$ 的解, 這證明了預備定理。

底下我們利用下降法證明 $n=4$ 的情形。

**命題 1.** 不定方程式

$$x^4+y^4=z^4$$

沒有正整數解。

**證明**: 實際上, 我們是要證明不定方程式

$$x^4+y^4=u^2$$

沒有正整數解。設 $u$ 是滿足

$$u^2=x^4+y^4,\ x>0,\ y>0,\ u>0$$

的最小正整數, 則 $(x,y)=1$, 否則我們可找到一比 $u$ 更小的正整數滿足同一方程式。因此 $x$ 與 $y$ 中至少有一是奇數, 且

$$u^2\equiv 1 \text{ 或 } 2 \pmod 4。$$

但 $u^2\equiv 2 \pmod 4$ 不可能發生, 故 $x$ 與 $y$ 之中必有一是奇數與一偶數。

設 $x$ 是偶數, 則由預備定理 1 得出

$$x^2=2ab,\ y^2=a^2-b^2,\ u=a^2+b^2。$$

其中 $a>0,\ b>0,\ (a,b)=1$, 注意到

$$a^2+b^2\equiv a+b\equiv 1 \pmod 2。$$

故 $a$ 與 $b$ 之中剛好有一是偶數。若 $a$ 是偶數, $b$ 是奇數, 則

$$y^2\equiv -1 \pmod 4$$

這不可能, 故 $a$ 是奇數且 $b$ 是偶數, 定 $b=2c$, 則

$$(\frac{x}{2})^2=ac \text{ 且 } (\mathrm{a},c)=1$$

得出

$$\mathrm{a}=d^2,\ c=f^2,\ d>0,\ f>0,\ (d,f)=1$$

且 $d$ 是奇數。因此

$$y^2=a^2-b^2=d^4-4f^4$$

即

$$(2f^2)^2 + y^2 = (d^2)^2$$

但 $2f^2, y, d^2$ 兩兩互質, 再次利用預備定理 1, 得出

$$2f^2 = 2\ell m,\ d^2 = \ell^2 + m^2,\ \ell > 0, m > 0,\ (\ell, m) = 1$$

由 $f^2 = \ell m$ 且 $(\ell, m) = 1$, 可設

$$\ell = r^2,\ m = s^2$$

因此

$$r^4 + s^4 = d^2$$

且

$$d \le d^2 = a \le a^2 < a^2 + b^2 = u$$

與原先假設矛盾, 故得證這命題。

## 二. $n = 3$的特別情形

不定方程式

$$f(x_1, x_2, \ldots, x_n) = 0$$

有解的必要條件是對任意正整數 $m$, 同餘方程式

$$f(x_1, x_2, \ldots, x_n) \equiv 0 \pmod{m}$$

都有解。若能找到正整數 $m$, 使得上面的同餘方程式無解時, 則自然地, 原方程式就沒有整數解。現利用這方法證明 $n = 3$ 的特別情形。

**命題 2.** 不定方程式

$$x^3 + y^3 = z^3,\ (xyz, 3) = 1$$

沒有整數解。

**證明**: 我們將證明同餘方程式

$$x^3 + y^3 \equiv z^3 \pmod{9},\ (xyz, 3) = 1$$

沒有整數解。假設不然, 即同餘方程式有解, 由同餘式

$$x^3 + y^3 \equiv z^3 \pmod{3}$$

以及 Fermat 小定理:

$$(a, p) = 1 \ \Rightarrow\ a^p \equiv a \pmod{p}$$

得出

$$x + y \equiv z \pmod{3}$$

定 $z = x + y + 3\mu,\ \mu \in \mathbf{Z}$, 因此

$$\begin{aligned} x^3 + y^3 &\equiv (x + y + 3u)^3 \\ &\equiv x^3 + y^3 + 3x^2y + 3xy^2 \pmod{9} \end{aligned}$$

故

$$0 \equiv x^2y + xy^2 = xy(x+y) \equiv xyz \pmod{3}$$

與原來假設 $(xyz, 3) = 1$ 矛盾, 故得證。

**習題 1.** 證明下列的同餘方程式沒有整數解

$$x^5 + y^5 = z^5 \pmod{25},\ (xyz, 5) = 1。$$

**習題 2.** 證明不定方程式

$$x^3 + y^3 = 5z^3, \quad z \neq 0$$

沒有整數解。

## 三．分圓體

所謂的分圓體 (cyclotomic field) $k$, 是指多項式 $X^n-1$ $(n \geq 2)$ 在 $\mathbf{Q}$ 之上的分裂體 (splitting field)。因此 $k = \mathbf{Q}(e^{2\pi i/n})$, 而其 Galois 群 $Gal(k/\mathbf{Q})$ 是由自同構 $\sigma_a$ 所組成。$\sigma_a$ 定義爲

$$\sigma_a : e^{2\pi i/n} \longrightarrow e^{2\pi ia/n},\ (a,n)=1$$

故它的秩是 $\varphi(n)$。

爲簡化符號起見, 我們定 $\zeta_n = e^{2\pi i/n}$。在此我們只對 $n$ 是奇質數的情形比較感興趣。利用熟知的 Eisenstein 判定法, 我們知道多項式

$$\phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$$

是 $\mathbf{Z}[X]$中的不可約多項式。注意 $\zeta_p$ 是 $\phi_p$ 的一零位。因此

$$[\mathbf{Q}[\zeta_p] : \mathbf{Q}] = p-1$$

且 $\zeta_p^i$ $(i = 1, 2, \ldots, p-1)$ 是 $\zeta_p$ 的相異共軛數。

**預備定理 2.** 在環 $\mathbf{D} = \mathbf{Z}[\zeta_p]$ 中, $1-\zeta_p$ 是一質數, 且 $p$ 可分解成

$$p = \epsilon(1-\zeta_p)^{p-1}$$

其中 $\epsilon$ 是 $\mathbf{D}$ 中的單位 (unit)。

**證明**: 在等式

$$\begin{aligned} & X^{p-1} + X^{p-2} + \cdots + X + 1 \\ = \ & (X-\zeta_p)(X-\zeta_p^2)\cdots(X-\zeta_p^{p-1}) \end{aligned}$$

中, 令 $x = 1$ 則

$$p = (1-\zeta_p)(1-\zeta_p^2)\cdots(1-\zeta_p^{p-1})$$

設 $k = \mathbf{Q}[\zeta_p]$, 則

$$N_{k/\mathbf{Q}}\left(\frac{1-\zeta_p^j}{1-\zeta_p}\right) = 1, \quad 1 \leq j \leq p-1$$

故

$$1-\zeta_p^j = \epsilon_j(1-\zeta_p),$$

其中 $\epsilon_j$ 是一單位, 設 $\epsilon = \prod_{j=1}^{p-1}\epsilon_j$, 則

$$p = \epsilon(1-\zeta_p)^{p-1}。$$

**預備定理 3.** 若有理整數 $b$ 可被 $1-\zeta_p$ 整除, 則 $b$ 可被 $p$ 整除。

**證明**: 設 $b = (1-\zeta_p)\alpha$, 則

$$\begin{aligned} & N_{k/\mathbf{Q}}(b) = b^{p-1} \\ = \ & N_{k/\mathbf{Q}}(1-\zeta_p)N_{k/\mathbf{Q}}(\alpha) = p\ N_{k/\mathbf{Q}}(\alpha) \end{aligned}$$

其中$k = \mathbf{Q}[e^{2\pi i/p}]$, 因 $N_{k/\mathbf{Q}}(\alpha)$ 是整數且 $p$ 是質數, 故 $p$ 是 $b$ 的質因數。

**習題 3.** 敍述 $\mathbf{Z}[X]$ 中不可約多項式的 Eisenstein 判別法, 並證明之。

在底下, 我們決定 $\mathbf{Q}(\zeta_p)$ 的整數環, 首先我們定義基底的判別式。設 $k$ 是 $\mathbf{Q}$ 的 $n$ 次擴充體, 對任意 $k$ 的一組基底 $\alpha_1, \alpha_2, \ldots, \alpha_n$, 定義這組基底的判別式爲

$$\begin{aligned} & D(\alpha_1, \alpha_2, \ldots, \alpha_n) \\ = \ & \det[\mathrm{trace}(\alpha_i\alpha_j)]_{1\leq i,j\leq n} \end{aligned}$$

若 $\alpha_1, \alpha_2, \ldots, \alpha_n$ 也正好是模 (module) $M$ 的基底, 則稱 $D(\alpha_1, \alpha_2, \ldots, \alpha_n)$ 是模 $M$ 的

判別式, 以 $D(M)$ 表之。我們需要下面的一般性結果。

**命題 3.** 設 $M = \mathbf{Z}[\alpha_1, \alpha_2, \ldots, \alpha_n]$ 是 $\mathbf{O}_k$ 的任意子模, $\mathbf{O}_k$ 是代數擴充體的整數環。設 $\alpha_1, \alpha_2, \ldots, \alpha_n$ 是 $k$ 的一組基底且 $M$ 是 $\mathbf{O}_k$ 的眞子集, 則存在有質數 $p$ 滿足

(1) $p^2 \mid D(M)$

(2) $\alpha_t^* = (g_1\alpha_1 + g_2\alpha_2 + \cdots + g_{t-1}\alpha_{t-1} + \alpha_t)/p \in \mathbf{O}_k$, $0 \le g_i \le p-1$ 且 $1 \le t \le n$。若找到如此的 $\alpha_t^*$, 則

$$M \subset M^* = \mathbf{Z}[\alpha_1, \ldots, \alpha_{t-1}, \alpha_t^*, \ldots, \alpha_n]$$

且

$$D(M^*) = D(M)/p^2。$$

**證明**: 設 $\beta_1, \beta_2, \ldots, \beta_n$ 是 $\mathbf{O}_k$ 的一組基底且

$$\alpha_i = \sum_{j=1}^{n} m_{ij}\beta_j \quad (i = 1, 2, \ldots, n)$$

則

$$\begin{aligned} & D(\alpha_1, \alpha_2, \ldots, \alpha_n) \\ = \; & (\det[m_{ij}])^2 D(\beta_1, \beta_2, \ldots, \beta_n) \end{aligned}$$

若 $p|\det[m_{ij}]$, 利用 $\mathbf{Z}_p$ 中的 Cremer 法則, 則存在 $\mathrm{a}_i$, 不全滿足 $\mathrm{a}_i \equiv 0(\mathrm{mod}\ p)$, 使得

$$\sum_{i=1}^{n} \mathrm{a}_i m_{ij} \equiv 0 \ (\mathrm{mod}\ p)$$

若對 $1 \le i \le t$, $\mathrm{a}_i \not\equiv 0 \ (\mathrm{mod}\, p)$, 但 $\mathrm{a}_{t+1} \equiv \mathrm{a}_{t+2} \equiv \cdots \equiv \mathrm{a}_n \equiv 0(\mathrm{mod}\ p)$ 則

$$\gamma = \sum_{i=1}^{n} \mathrm{a}_1\alpha_1 \;=\; \sum_{i=1}^{n}\sum_{j=1}^{n} \mathrm{a}_i m_{ij}\beta_j = p\beta,$$

$$\beta \in \mathbf{O}_k$$

選擇 $\mathrm{a}^*$ 使得 $\mathrm{a}_t\mathrm{a}^* \equiv 1 \ (\mathrm{mod}\ p)$, 則

$$g_1\alpha_1 + g_2\alpha_2 + \cdots + g_{t-1}\alpha_{t-1} + \alpha_t = p\beta',$$
$$\beta' \in \mathbf{O}_k$$

其中

$$g_i \equiv \mathrm{a}_i\mathrm{a}^*(\mathrm{mod}\ p) \quad , \quad 0 \le g_i < p, \quad i = 1, \cdots, t-1$$

因此

$$\begin{aligned} \alpha_t^* &= (g_1\alpha_1 + g_2\alpha_2 + \cdots + g_{t-1}\alpha_{t-1} + \alpha_t)/p \\ &= \beta' \in \mathbf{O}_k \end{aligned}$$

很容易可驗證出 $D(M^*) = D(M)/p^2$。

注意到, $\mathbf{O}_k$ 的判別式是所有 $\mathbf{O}_k$ 中之子模的判別式中最小的, 且只有 $\mathbf{O}_k$ 的判別式會達到。故利用命題 3 的步驟有限多次, 即可找到 $k$ 的眞正整數環 $\mathbf{O}_k$。

**習題 4.** 決定 $\mathbf{Q}(\sqrt[3]{2})$ 的整數環。
[提示: 因 $D(1, \sqrt[3]{2}, \sqrt[3]{4}) = -108 = -2^2 3^3$, 故需檢驗 $p = 2$ 與 $p = 3$]

**習題 5.** 設 $k = \mathbf{Q}(\xi)$, $\xi$ 是方程式 $x^2 + x^2 - 2x + 8 = 0$ 的根。證明 $\mathbf{O}_k = \mathbf{Z}[1, \xi, (\xi + \xi^2)/2]$, 即證明 $(\xi + \xi^2)/2$ 的代數整數, 且 $D(1, \xi, (\xi + \xi^2)/2)$ 是質數。

現我們已做好決定 $k = \mathbf{Q}[\zeta_p]$ 之整數環的準備。

**命題 4.** 設 $p$ 是奇質數, 則 $\mathbf{Q}[\zeta_p]$ 的整數環是 $\mathbf{Z}[\zeta_p]$。

**證明**: 首先我們證明判別式 $D[1,\zeta_p,\ldots,\zeta_p^{p-1}]$ 是 $p$ 的冪次方乘上一單位。對任意 $1\le \mathrm{a}\le p_1$

$$\sigma_{\mathrm{a}}:\zeta_p\mapsto\zeta_p^{\mathrm{a}}$$

是 $Gal(\mathbf{Q}[\zeta_p]/\mathbf{Q})$ 的元素, 故

$$\begin{aligned} D[1,\zeta_p,\ldots,\zeta_p^{p-1}] &= \det[\zeta_p^{ij}]^2_{1\le i\le p-1,\ 0\le j\le p-2}\\ &= \prod_{0\le i\le j\le p-2}(\zeta_p^i-\zeta_p^j)^2 \end{aligned}$$

但由預備定理 2, 得

$$p=\epsilon(1-\zeta_p)^{(p-1)(p-2)}$$

$\epsilon$ 是單位, 故

$$D[1,\zeta_p,\ldots,\zeta_p^{p-1}]=\mu p^{p-2},\ \mu \text{ 是單位}$$

欲證 $\mathbf{Z}[\zeta_p]$ 是 $\mathbf{Q}[\zeta_p]$ 的整數環, 由命題 3, 只要證明

$$\begin{aligned} & p|(\mathrm{a}_0+\mathrm{a}_1\zeta_p+\cdots+\mathrm{a}_{p-2}\zeta_p^{p-2}),\\ & \mathrm{a}_0,\mathrm{a}_1,\ldots\mathrm{a}_{p-2}\in\mathbf{Z}\\ \Rightarrow\quad & p|\mathrm{a}_0, p|\mathrm{a}_1,\ldots,p|\mathrm{a}_{p-2}。 \end{aligned}$$

把 $\mathrm{a}_0+\mathrm{a}_1\zeta_p+\cdots+\mathrm{a}_{p-2}\zeta_p^{p-2}$ 改寫成

$$b_0+b_1(1-\zeta_p)+\ldots+b_{p-2}(1-\zeta_p)^{p-2},$$

則 $b_0,b_1,\ldots,b_{p-2}$ 還是有理整數。注意到 $1-\zeta_p$ 是 $p$ 的質因數, 故是 $b_0$ 的因數, 但由預備定理得 $p|b_0$, 經一步一步的過程得出 $p|b_1,\ldots,\ p|b_{p-2}$, 因 $\mathrm{a}_0,\mathrm{a}_1,\ldots,\mathrm{a}_{p-2}$ 可寫成 $b_0,b_1,\ldots,\ b_{p-2}$ 與整數的線性組合, 故得出

$$p|\mathrm{a}_0, p|\mathrm{a}_1,\ldots,p|\mathrm{a}_{p-2}$$

使用同樣的方法, 我們得出

**命題 5.** 設 $p$ 是奇質數, $r$ 是正整數且 $q=p^r$, 則 $\mathbf{Q}[\zeta_q]$ 的整數環是 $\mathbf{Z}[\zeta_q]$ 且 $\mathbf{Z}[\zeta_q]$ 的判別式是

$$\pm p^{p^{r-1}(pr-r-1)}$$

**習題 6.** 證明 Vondermonde 行列式

$$V=\det[\lambda_i^{j-1}]_{1\le i,j\le n}$$

的值是 $\pm\prod_{i<j}(\lambda_i-\lambda_j)$。

## 四. 分圓多項式

對任意正整數 $n$, 我們定義第 $n$ 個分圓多項式 ($n$-th cyclotomic polynomial) 爲

$$\Phi_n(X)=\prod_{(j,n)=1}(X-\zeta_n^j)。$$

因爲 $[\mathbf{Q}[\zeta_n]:\mathbf{Q}]=\varphi(n)=deg\Phi_n(X)$。故 $\Phi_n(X)$ 是 $\zeta_n$ 的首一不可約多項式, 而且 $\Phi_n(X)\in\mathbf{Z}[X]$, 因它的係數是代數整數且同時是有理數, 前面的幾個分圓多項式如下:

$$\begin{aligned} \Phi_1(X) &= X-1,\quad \Phi_2(X)=X+1,\\ \Phi_3(X) &= X^2+X+1,\quad \Phi_4(X)=X^2+1,\\ \Phi_5(X) &= X^4+X^3+X^2+X+1,\\ \Phi_6(X) &= X^2-X+1。 \end{aligned}$$

**習題 7.** 寫出 $\Phi_7(X),\Phi_9(X),\Phi_{15}(X)$ 與 $\Phi_{30}(X)$。

**習題 8.** 證明 $\mathbf{Z}[\zeta+\zeta^{-1}]$ 是 $\mathbf{Q}[\zeta+\zeta^{-1}]$ 的整數環, $\zeta=e^{2\pi i/3}$。

設 $E_n$ 是 $\mathbf{Q}[\zeta_n]$ 的單位群 (group of units), $V_n$ 是由

$$\{\pm\zeta_n,\ 1-\zeta_n^a \mid 0<a\le n-1\}$$

所生成的乘法群, 定義

$$C_n = V_n \cap E_n,$$

$C_n$ 稱爲 $Q[\zeta_n]$ 中的分圓單位群 (group of cyclotomic units)。

**命題 6.** 設 $p$ 是質數, $r$ 是正整數且 $q=p^r$, 則 $\mathbf{Q}[\zeta_q]$ 的分圓單位群的生成元素是 $\pm\zeta_q$ 與

$$\begin{aligned}\eta_a &= \zeta_q^{(1-\mathrm{a})/2}(1-\zeta_q^{\mathrm{a}})/(1-\zeta_q),\\ &\qquad 0<\mathrm{a}<q/2,\ (\mathrm{a},p)=1。\end{aligned}$$

**證明**: 若 $k<r$ 且 $(b,p)=1$, 則由關係式

$$1-X^{p^k}=\prod_{j=0}^{p^k-1}(1-\zeta_q^{jp^{r-k}}X)$$

得出

$$1-\zeta_q^{bp^k}=\prod_{j=0}^{p^k-1}(1-\zeta_q^{b+jp^{r-k}})$$

因 $(p,b+jp^k)=1$, 故我們只需考慮 $(a,p)=1$ 的情形, 又 $1-\zeta_q^{\mathrm{a}}$ 與 $1-\zeta_q^{-\mathrm{a}}$ 只差 $-\zeta_q$ 的冪次方, 故只要考慮 $1\le \mathrm{a}<q/2$。

假設

$$\begin{aligned}\xi &= \pm\zeta_q^d\prod_{\mathrm{a}}(1-\zeta_q^{\mathrm{a}})^{\alpha(a)},\\ &\qquad 1\le\mathrm{a}<q/2,\ (\mathrm{a},q)=1。\end{aligned}$$

是 $\mathbf{Q}[\zeta_q]$ 中的分圓單位, 因 $N_{k|\mathbf{Q}}(1-\zeta_q^{\mathrm{a}})$, $k=\mathbf{Q}[\zeta_q]$ 都相等, 故 $\Sigma\alpha(a)=0$, 因此

$$\begin{aligned}\xi &= \pm\zeta_q^d\prod_{\mathrm{a}}(1-\zeta_q^{\mathrm{a}})^{\alpha(a)}(1-\zeta_q)^{-\alpha(a)}\\ &= \pm\zeta_q^{d'}\prod_{\mathrm{a}}\eta_{\mathrm{a}}\end{aligned}$$

**習題 9.** 證明在 $\mathbf{Q}[\zeta_n]$, $n=2,3$ 中, 每一單位都是分圓單位。

## 五. 規則質數的第一種情形

質數 $p$ 若不能整除 $\mathbf{Q}[e^{2\pi i/p}]$ 的類數 (class number), 則稱 $p$ 是規則質數 (regular prime), 否則稱爲不規則質數, 在這一節中, 我們將證明 $p$ 是規則質數時, 不定方程式

$$x^p+y^p=z^p,\quad (xyz,p)=1$$

沒有整數解。

**預備定理 4.** 若 $\alpha$ 是一代數整數且 $\alpha$ 的所有共軛數的絕對值都是 1, 則 $\alpha$ 是 1 的方根。

**證明**: 只要證明 $\alpha$ 的所有冪次所成的集合是一有限集合, 設 $\alpha=\alpha_1,\ldots,\alpha_n$ 是 $\alpha$ 的所有共軛數, 且

$$P(X)=\prod_{j=1}^{n}(X-\alpha_j^m)$$

則 $P(X)\in\mathbf{Z}[X]$ 且其係數都被一與 $m$ 無關的常數界定住, 故只有有限多個多項式以 $\alpha$ 的冪次方爲根。因此, $\alpha$ 只有有限個相異冪次。

**命題 7.** 設 $\epsilon$ 是 $\mathbf{Z}[\zeta_p]$ 中的單位, 則存在有 $\mu\in\mathbf{Q}[\zeta_p+\zeta_p^{-1}]$ 與 $r\in\mathbf{Z}$, 使得 $\epsilon=\mu\cdot\zeta_p^r$。

**證明**: 設 $\alpha=\epsilon/\bar{\epsilon}$, 則由預備定理 4, $\alpha$ 是 1 的方根, 因此

$$\frac{\epsilon}{\bar{\epsilon}}=\pm\zeta_p^{\mathrm{a}},\quad \mathrm{a}\in\mathbf{Z}。$$

設 $\epsilon/\bar{\epsilon} = -\zeta_p^{\mathrm{a}}$ 且

$$\epsilon = b_0 + b_1\zeta_p + \cdots + b_{p-2}\zeta_p^{p-2},$$

則

$$\epsilon \equiv b_0 + b_1 + \cdots + b_{p-2} \pmod{(1-\zeta_p)}$$

且

$$\begin{aligned}\bar{\epsilon} &= b_0 + b_1\zeta_p^{-1} + \cdots + b_{p-2}\zeta_p^{-p+2} \\ &\equiv b_0 + b_1 + \cdots + b_{p-2} \pmod{(1-\zeta_p)} \\ &\equiv \epsilon \pmod{(1-\zeta_p)} \\ &\equiv -\zeta_p^{\mathrm{a}}\bar{\epsilon} \pmod{(1-\zeta_p)} \\ &\equiv -\bar{\epsilon} \pmod{(1-\zeta_p)}。\end{aligned}$$

因此 $2\bar{\epsilon} \equiv 0 \pmod{(1-\zeta_p)}$, 因 $1-\zeta_p$ 是質因數且 2 不能被 $1-\zeta_p$ 整除, 故 $\bar{\epsilon}$ 可被 $1-\zeta_p$ 整除, 與 $\epsilon$ 是單位的事實矛盾。

因此 $\epsilon/\bar{\epsilon} = \zeta_p^a$, 設 $2r \equiv \mathrm{a} \pmod{p}$, 則 $\epsilon = \zeta_p^r\epsilon_1$ 且 $\bar{\epsilon}_1 = \epsilon_1 \in \mathbf{Q}[\zeta_p + \zeta_p^{-1}]$。

**預備定理 5.** 設 $x$ 與 $y$ 是互質整數, 若 $x+y$ 不能被 $p$ 整除, 則所有主理想 $(x+\zeta_p^i y)$ $i = 0, 1, \ldots, p-1$ 兩兩互質。

**證明**: 設 $\mathcal{P}$ 是一質理想滿足

$$\mathbf{P}|(x+\zeta_p^i y) \text{ 且 } \mathbf{P}|(x+\zeta_p^i y),\ i \neq j。$$

則

$$\mathbf{P}|(\zeta_p^i y - \zeta_p^j y) = (\text{單位})\ (1-\zeta_p)y$$

所以 $\mathbf{P} = 1-\zeta_p$ 或 $\mathbf{P}|y$。

同理證明 $\mathbf{P} = 1-\zeta_p$ 或 $\mathbf{P}|x$。若 $\mathbf{P} \neq (1-\zeta_p)$, 則 $\mathbf{P}|x$ 且 $\mathbf{P}|y$, 這不可能, 原因是 $(x, y) = 1$。因此 $\mathbf{P} = (1-\zeta_p)$, 故

$$x + y \equiv x + \zeta_p^i y \equiv 0 \pmod{\mathbf{P}}$$

因而

$$x + y \equiv 0 \pmod{p}$$

這與假設不合, 故得所欲證。

現我們考慮 $p$ 是規則質數的情形。

**命題 8.** 設 $p$ 是規則質數, 則不定方程式

$$x^p + y^p = z^p, \qquad (xyz, p) = 1$$

沒有整數解。

**證明**: $p = 3$的情形已得證, 現設 $p \geq 5$, 設方程式有一組整數解 $x, y$ 與 $z$, 則

$$x^p + y^p \equiv x + y \equiv z^p \equiv z \pmod{p}$$

因此 $p$ 不是 $x+y$ 的質因數, 把等式

$$\prod_{i=0}^{p-1}(x+\zeta_p^i y) = (z)^p$$

視爲主理想間的關係式, 由預備定理 4, 我們知理想

$$(x+\zeta_p^i y), \qquad 0 \leq i \leq p-1$$

兩兩互質, 故每一個必是理想的 $p$ 次方

$$(x+\zeta_p^i y) = A_i^p, \qquad 0 \leq i \leq p-1$$

但 $Q[\zeta_p]$ 的類數不能被 $p$ 整除, 故 $A_i$ 也是主理想。設

$$A_i = (\alpha_i), \qquad 0 \leq i \leq p-1$$

則

$$(x+\zeta_p^i y) = (\alpha_i^p)$$

故

$$x + \zeta_p^i y = (\text{單位}) \quad \alpha_i^p$$

考慮 $i=1$, 並把上標略去, 則

$$x+\zeta_p y=\epsilon\alpha^p$$

其中 $\epsilon$ 是 $\mathbf{Q}[\zeta_p]$ 的單位, 把 $\epsilon$ 表爲 $\zeta_p^r\epsilon_1$, $\bar{\epsilon}_1=\epsilon_1$, 令

$$\alpha=a_0+a_1\zeta_p+\cdots+a_{p-2}\zeta_p^{p-2}$$

且

$$\mathrm{a}=a_0^p+a_1^p+\cdots+a_{p-2}^p$$

則

$$\alpha^p\equiv a\ (\mathrm{mod}\ p)$$

且

$$x+\zeta_p y=\zeta_p^r\epsilon_1\alpha^p\equiv\zeta_p^r\epsilon_1 a\ (\mathrm{mod}\ p)$$

而且有

$$x+\zeta_p^{-1}y\equiv\zeta_p^{-r}\epsilon_1 a\ (\mathrm{mod}\ p)$$

結合兩式得出

$$\zeta_p^{-r}(x+\zeta_p y)\equiv\zeta_p^r(x+\zeta_p^{-1}y)\ (\mathrm{mod}\ p)$$

或

$$x+\zeta_p y-\zeta_p^{2r}x-\zeta_p^{2r-1}y\equiv 0\ (\mathrm{mod}\ p)$$

若 $1,\zeta_p,\zeta_p^{2r},\zeta_p^{2r-1}$ 兩兩相異, 則 $p$ 可整除 $x$ 與 $y$, 與原假設矛盾。但 $\zeta_p\neq 1$ 且 $\zeta_p^{2r}\neq\zeta_p^{2r-1}$, 故剩下底下三種情形。

(1) $1=\zeta_p^{2r}$, 則 $\zeta y-\zeta^{-1}y\equiv 0\ (\mathrm{mod}\ p)$, 故 $y\equiv 0\ (\mathrm{mod}\ p)$ 這不可能, 原因是 $(xyz,p)=1$。

(2) $1=\zeta_p^{2r-1}$, 則 $(x-y)-(x-y)\zeta\equiv 0\ (\mathrm{mod}\, p)$, 這表示 $x-y\equiv 0\ (\mathrm{mod}\, p)$, 同樣手法, 由 $x-\zeta_p z=\epsilon_1\alpha_1^p$ 得出

$$x+z\equiv 0\ (\mathrm{mod}\ p)$$

故 $x^p+y^p-z^p\equiv x+y-z\equiv 3x\ (\mathrm{mod}\ p)$ 因 $p\neq 3$, 故 $x\equiv 0\ (\mathrm{mod}\ p)$, 再次得出矛盾。

(3) $\zeta_p=\zeta_p^{2r-1}$, 則 $x-\zeta_p^2 x\equiv 0\ (\mathrm{mod}\ p)$, 則 $x\equiv 0\ (\mathrm{mod}\ p)$ 也不可能。

這證明了命題 8。

## 六. 規則質數的第二種情形

現考慮規則質數的第二種情形, 即 $p$ 是規則質數時不定方程式

$$x^p+y^p=z^p,\quad p|z,\quad (xy,p)=1$$

沒有異於零的整數解。定理證明過程中, 我們需用到更深入的關於單位的同餘理論。

**定理 1.** (Kummer 預備定理) 設 $p$ 是規則質數, $u$ 是 $\mathbf{Q}(\zeta_p)$ 的單位, $a$ 是有理整數, 且

$$u\equiv a\ (\mathrm{mod}\, p)$$

則 $u$ 是另一單位 $v$ 的 $p$ 次方。

顯然地, 任一單位的 $p$ 次方在 $\mathrm{mod}\, p$ 之下是一有理整數, 事實上, 若

$$v=a_0+a_1\zeta_p+\cdots+a_{p-2}\zeta_{p-2}^{p-2},$$

則

$$v^p\equiv a_0^p+a_1^p+\cdots+a_{p-2}^p\ (\mathrm{mod}\ p)。$$

而反過來, 證明並不容易, 有興趣的讀者可參考 [1] 中的 377 頁, 現我們利用這預備定理證明規則質數的第二種情形也成立。

**命題 9.** 設 $p$ 是規則質數, 則不定方程式

$$x^p + y^p = z^p, \quad p|z, \quad (x, y, p) = 1$$

沒有非零的整數解。

**證明**: 設 $x, y, z$ 是方程式的一組整數。令 $z = z_0 p^k, (z_0, p) = 1$, 因 $p = (1-\zeta_p)^{p-1}\mathcal{E}$, $\mathcal{E}$ 是一單位, 故方程式可改寫成

$$\text{(A)} \qquad x^p + y^p = \mathcal{E}(1-\zeta_p)^{pm} z_0^p,$$
$$m = k(p-1) > 0。$$

想證明原命題成立, 只需證明 (A) 沒有代數整數解即可。

設 (A) 有一組代數整數解 $x, y, z_0$ 且 $x, y$, $z_0$ 與 $1-\zeta_p$ 互質, 在所有可能的解中, 選定一組, 使對應的指數 $m$ 最小。設 $\mathbf{P}$ 是由 $1-\zeta_p$ 生成的主理想, 則有

$$\prod_{k=0}^{p-1}(x + \zeta_p^k y) = \mathbf{P}^{pm}(z_0)。$$

因 $pm \geq p > 0$, 故 $(x + \zeta_p^k y)$ $(k = 0, \ldots, p-1)$ 中至少有一可被 $\mathbf{P}$ 整除。又

$$x + \zeta_p^i y = x + \zeta_p^k y - \zeta_p^k(1 - \zeta_p^{i-k})y。$$

只要有一可被 $\mathbf{P}$ 整除, 則每一個都可被 $\mathbf{P}$ 整除。故 $x + \zeta_p^k y$ $(0 \leq k \leq p-1)$ 均可被 $\mathbf{P}$ 整除。

另一方面, 若

$$x + \zeta_p^k y \equiv x + \zeta_p^i y \pmod{(1-\zeta_p)^2}$$

則 $\zeta_p^k y(1 - \zeta_p^{i-k}) \equiv 0 \pmod{(1-\zeta_p)^2}$, 得出 $y$ 可被 $1-\zeta_p$ 整除, 而這與假設矛盾, 這表明

$$\frac{x + \zeta_p^k y}{1-\zeta_p} \quad (k = 0, 1, \ldots, p-1)$$

除以 $1-\zeta_p$ 後的餘數相異, 但

$$N_{\mathbf{Q}(\zeta_p)/\mathbf{Q}}(1-\zeta_p) = p,$$

故其中剛好有一可被 $1-\zeta_p$ 整除, 可設定是 $x+y$, 設 m 是 $(x)$ 與 $(y)$ 的最大公因數, 因 $x$ 與 $y$ 不能被 $1-\zeta_p$ 整除, 故 m 與 $p$ 互質, 故可定

$$\begin{aligned} (x+y) &= \mathbf{P}^{p(m-1)+1}\mathrm{m}\mathbf{C}_0 \\ (x+\zeta_p^k y) &= \mathbf{P}\mathrm{m}\mathbf{C}_k \quad (k = 1, \ldots, p-1) \end{aligned}$$

現 $\mathbf{C}_0, \mathbf{C}_1, \ldots, \mathbf{C}_{p-1}$ 是兩兩互質的理想, 又

$$\mathrm{m}^p\mathbf{P}^{pm}\mathbf{C}_0\mathbf{C}_1\cdots\mathbf{C}_{p-1} = \mathbf{P}^{pm}(z_0)^p,$$

故每一理想都是 $p$ 平方, 設

$$\mathbf{C}_k = \mathrm{a}_k^p \qquad (0 \leq k \leq p-1)$$

如此

$$\begin{aligned} (x+y) &= \mathbf{P}^{p(m-1)+1}\mathrm{m}\mathrm{a}_0 \\ (x+\zeta_p^k y) &= \mathbf{P}\mathrm{m}\mathrm{a}_k \qquad (1 \leq k \leq p-1) \end{aligned}$$

上面式子消去 m 得出

$$(x + \zeta_p^k y)\mathbf{P}^{p(m-1)} = (x+y)(\mathrm{a}_k\mathrm{a}_o^{-1})^p$$

故 $(\mathrm{a}_k\mathrm{a}_o^{-1})^p$ 是主理想, 但 $p$ 是規則質數, 因而 $(\mathrm{a}_k\mathrm{a}_o^{-1})$ 也是主理想, 定爲

$$\mathrm{a}_k\mathrm{a}_o^{-1} = (\frac{\alpha_k}{\beta_k}) \qquad (1 \leq k \leq p-1)。$$

其中 $\alpha_k$ 與 $\beta_k$ 是代數整數, 又 $\mathrm{a}_k$ $(0 \le k \le p-1)$ 與 $\mathbf{P}$ 互質, 故可選定 $\alpha_k, \beta_k$ 不能被 $1-\zeta_p$ 整除, 如此

(B)

$$(x+\zeta_p^k y)(1-\zeta_p)^{p(m-1)} = (x+y)(\tfrac{\alpha_k}{\beta_k})^p \mathcal{E}_k \qquad (1 \le k \le p-1)$$

其中 $\mathcal{E}_k$ 是 $\mathbf{Q}[\zeta_p]$ 中的單位, 利用方程式

$$\begin{aligned} & (x+\zeta_p y)(1+\zeta_p) - (x+\zeta_p^2 y) \\ = \;& \zeta_p(x+y) \end{aligned}$$

以及 (B) 中 $k = 1, 2$ 代入, 則得出

$$\begin{aligned} & (x+y)(\frac{\alpha_1}{\beta_1})^p \mathcal{E}_1(1+\zeta_p) - (x+y)(\frac{\alpha_2}{\beta_2})^p \mathcal{E}_2 \\ = \;& (x+y)\zeta_p(1-\zeta_p)^{p(m-1)}。 \end{aligned}$$

故

$$\begin{aligned} & (\alpha_1\beta_2)^p - \frac{\mathcal{E}_2}{\mathcal{E}_1(1+\zeta_p)}(\alpha_2\beta_1)^p \\ = \;& \frac{\zeta_p}{\mathcal{E}_1(1+\zeta_p)}(1-\zeta_p)^{p(m-1)}(\beta_1\beta_2)^p \end{aligned}$$

即找到方程式

$$\alpha^p + \mathcal{E}_0\beta^p = \mathcal{E}'(1-\zeta_p)^{p(m-1)}\gamma^p$$

的一組解, $\mathcal{E}_0, \mathcal{E}'$ 是單位, 而其 $1-\zeta_p$ 的冪次則降爲 $p(m-1)$, 又 $m > 1$, 故 $m-1 > 0$, 且 $p(m-1) \ge p$, 這表示

$$\begin{aligned} \alpha^p + \mathcal{E}_0\beta^p &\equiv 0 \pmod{(1-\zeta_p)^p} \\ \mathcal{E}_0 &\equiv -(\beta^{-1}\alpha)^p \pmod{p} \end{aligned}$$

$\mathcal{E}_1$ 與一有理整數對 $p$ 同餘, 由 Kummer 預備定理, $\mathcal{E}_0$ 是另一單位 $\eta$ 的 $p$ 次方。因而

$$\alpha^p + (\eta\beta)^p = \mathcal{E}'(1-\zeta_p)^{p(m-1)}\gamma^p。$$

這與原先假設 $m$ 是最小指數矛盾, 故得證原命題。

綜合命題 8 與命題 9, 則得證底下的 Fermat 最後定理的特殊情形。

**定理 2.** 設 $p$ 是規則質數, 則不定方程式

$$x^p + y^p = z^p$$

沒有非顯然的整數解。

現我們面對了一實際問題: 如何決定一質數是規則質數或不規則質數。Kummer 提出了一個利用 Bernoulli 數來判定的法則。

**定理 3.** $p$ 是規則質數的充要條件是 $p$ 不能整除 Bernoulli 數 $B_2, B_4, \ldots, B_{p-3}$ 的分子。

**討論**: Bernoulli 數 $B_m$ $(m \ge 0)$ 是由底下冪級數所定義:

$$\frac{t}{e^t - 1} = \sum_{m=0}^{\infty} \frac{1}{m!} B_m t^m, \quad |t| < 2\pi$$

奇數下標的 Bernoulli 數除 $B_1 = -1/2$ 外都是零, 即

$$B_{2k+1} = 0, \quad (k = 1, 2, 3, \ldots)$$

這可由 $\frac{t}{e^t-1} + \frac{t}{2}$ 是偶函數得證出來。$B_m (m \ge 0)$ 滿足遞迴定義式

$$\begin{aligned} & B_0 + 2B_1 = 0 \\ & B_0 + 3B_1 + 3B_2 = 0 \\ & B_0 + 4B_1 + 6B_2 + 4B_3 = 0 \\ & \cdots\cdots\cdots \end{aligned}$$

$$B_0+\binom{n}{1}B_1+\binom{n}{2}B_2+\cdots+\binom{n}{n-1}B_n = 0,\ (n\geq 2)$$

底下是一些偶數下標的 Bernoulli 數

$$B_2=\frac{1}{6}, B_4=-\frac{1}{30}, B_6=\frac{1}{42},$$
$$B_8=-\frac{1}{30}, B_{10}=-\frac{5}{66}, B_{12}=-\frac{691}{2730},$$
$$B_{14}=\frac{7}{6}, B_{16}=-\frac{3617}{510}, B_{18}=\frac{43867}{792}。$$

**習題 10.** 設 $S_k(n)=1^k+2^k+\ldots+(n-1)^k$, 試證

$$(m+1)S_m(n) = \sum_{k=0}^{m} C(m+1,k)B_k n^{m+1-k},\quad m\geq 1,$$

其中 $C(m,n)$ 是二項係數 $m!/n!(n-m)!$。

**習題 11.** 證明 Riemann zeta 函數 $\zeta(s)$ 在 $S=2m$ 的取值是

$$\zeta(2m)=(-1)^{m-1}\frac{(2\pi)^{2m}}{2(2m)!}B_{2m}。$$

在此我們要提一下 Fermat 最後定理的最新發展。到目前爲止，這斷言已證到冪次 $n\leq 125000$。又第一種情形已證到 $p\leq 6\times 10^9$。然而最引人注目的相關性定理要算 Faltings 在 1983 年提出的下面定理。方程式 $x^n+y^n=z^n$ 的一組解 $x,y,z$ 若滿足

$$xyz\neq 0 \quad 且 \quad (x,y,z)=1$$

則稱爲方程式的*原始解* (primitive solution)。因此任一非顯然的解都可化成一組原始解。

**定理 4.** (Faltings) 對每一冪次 $n\geq 3$, 不定方程式 $x^n+y^n=z^n$ 至多有有限個原始解。

## 參考書目


1. Z. I. Borevich and I. R. Shafarevich, Number Theory, Academic Press, New York and London, 1966.
2. G. H. Hardy and E. M. Wright, An introduction to the theory of numbers, Oxford sicence publications, 1979.


—本文作者任教於國立中正大學應數所—