幾個有名的數學問題(一)
Fermat問題(下)

康明昌

五、方程式$X^3+Y^3=Z^3$的第一種情況

我們先引入同餘（congruence）的概念。

若 n 是某個正整數，m_1 與 m_2 是整數，如果 n 可以整除 m_1-m_2，我們說：m_1 與 m_2 在模 n 之下同餘（m_1 is congruent to m_2 modulo n），記爲 $m_1\equiv m_2 \pmod n$。

我們不妨把兩個同餘的數 m_1 與 m_2 看成同一個「數」，因此在模 n 之下，我們得到一個只有 n 個「數」的數系，$\{0, 1, \cdots, n-1\}$。

例如，在模3之下，

$$2+2\equiv 1 \pmod 3$$
$$2\cdot 2\equiv 1 \pmod 3$$
$$1+2\equiv 0 \pmod 3$$

這個新數系的運算法則，加、減、乘，與整數系極相似。如果 p 是一個質數，數系 $\{0, 1, \cdots, p-1\}$ 甚至還有除法（除數不可爲零）；因此，這個數系可以像有理數一樣進行加、減、乘、除。理由何在，請讀者自已證明（註八）。

利用同餘的概念，我們計算 2^{32} 的個位數。你如果把 2^{32} 乘開來求其個位數，勇氣固然可嘉，方法卻不值得鼓勵。請注意，若

$$m_1\equiv m_2 \pmod n$$
$$k_1\equiv k_2 \pmod n$$

則
$$m_1+k_1\equiv m_2+k_2 \pmod n$$
$$m_1\cdot k_1\equiv m_2\cdot k_2 \pmod n$$

因此，在模 10 之下

$$2^{32}\equiv (2^4)^8\equiv (16)^8\equiv 6^8$$
$$\equiv (6^2)^4\equiv 36^4\equiv 6^4$$
$$\equiv 6 \pmod{10}$$

得：2^{32} 的個位數是 6。

現在我們介紹一個研究Fermat 問題的基本概念。

如果Fermat問題對於 n 是錯的，也就是，存在全異於零的整數 x，y，z，滿足 x^n

$+y^n=z^n$，考慮這個問題：n與xyz會不會互質？

如果在以上情形下，n與xyz必定不會互質，我們就說，Fermat方程式$x^n+y^n=z^n$的第一種情況成立。

法國女數學家Sophie Germain（1776～1831年）證明：若p與$2p+1$都是質數，則Fermat方程式$x^p+y^p=z^p$的第一種情況成立。Legendre推廣Germain的方法，證明：若p是質數，且$4p+1$，$8p+1$，$10p+1$，$14p+1$，$16p+1$至少有一個是質數，則Fermat方程式的第一種情況成立。

目前知道的是，若p是奇質數，且$p<3\times10^9$，則Fermat方程式$x^p+y^p=z^p$的第一種情況成立。（見本文第7節）

定理3 Fermat方程式$x^3+y^3=z^3$的第一種情況成立。換句話說，如果x_1，y_1，z_1是全異於零的整數並且滿足$x_1^3+y_1^3=z_1^3$，則$x_1y_1z_1\equiv0\pmod 3$。

討論：許多證據使人相信，Fermat的確能夠證明$x^3+y^3=z^3$沒有全異於零的整數解，Fermat把這個問題變成那些整數可以寫成x^2+3y^2的型式。Euler想要把這個定理的證明寫下來，但是Euler寫得並不完整。完整的證明請看G. H. Hardy and E. M. Wright, An introduction to the theory of numbers，第193～197頁。本文只解決Fermat方程式$x^3+y^3=z^3$的部份情形。有關Germain定理，請看H. M. Edwards, Fermaat's last theorem，第61～65頁。

以下要提出定理3的另一個證明。這個證明非常繁複，用這個方法來證明定理3簡直是愚蠢透頂。但是，從這個證明卻可以看出十九世紀研究Fermat問題的基本方法。事實上，把這個證明稍加修改，可以證明Kummer的一個定理：若p是一個規則質數，則Fermat方程式$x^p+y^p=z^p$的第一種情況成立（有關規則質數，請看本文第6節。）。

令x，y，z是互質且全異於零的整數，滿足$x^3+y^3=z^3$，我們要證明：$xyz\equiv0\pmod 3$。

不妨假設x與y是奇數，z是偶數（否則，重新命名，並且移項）。令$\omega=\dfrac{-1+\sqrt{-3}}{2}$。

請注意：

$$x^3=z^3-y^3$$
$$=(z-y)(z-\omega y)(z-\omega^2y)$$

一個異想天開的主意：如果$z-y$，$z-wy$，$z-\omega^2y$互質，則因

$$(z-y)(z-\omega y)(z-\omega^2y)$$

是完全立方數，$z-y$，$z-\omega y$，$z-\omega^2y$豈不也是完全立方數？

問題是，$z-\omega y$明明是個複數，怎麼可能變成整數的立方？

這個問題不難解決。我們可以把「整數」的概念推廣。先把$\boldsymbol{Q}(\omega)=\{\alpha+\beta\omega:\alpha與\beta是有理數\}$叫做三次分圓體（cyclotomic field），三次分元體的元素可以作加、減、乘、除（除數不爲零），三次分圓體是有理數的推廣。三次分圓體之內的「整數」就是$\boldsymbol{Z}[\omega]=\{\alpha+\beta\omega:\alpha與\beta是整數\}$，$\boldsymbol{Z}[\omega]$的元素叫做三次分圓整數（cyclotomic integers）。所以上述的問題只不過是，$z-\omega y$能不能寫成某一個三次分圓整數的立方？

如果ξ與η都是三次分圓整數且$\xi\neq0$，我們說ξ整除η，如果$\dfrac{\eta}{\xi}$也是三次分圓整數（$\dfrac{\eta}{\xi}$當然在$\boldsymbol{Q}(\omega)$之內。何故？）。因此在三次分圓整數之內也可討論同餘關係：因爲我們可以規定，$\eta_1\equiv\eta_2\pmod\xi$的充要條件是$\xi$整除$\eta_1-\eta_2$。

一個分圓整數ξ叫做可逆元素（invertible element），如果$1/\xi$也是分圓整數（

$\frac{1}{\xi}$當然在$Q(\omega)$之內；若$\xi=\alpha+\beta\omega$，則

$$\frac{1}{\xi}=\frac{\overline{\xi}}{\xi\cdot\overline{\xi}}$$

$$=\frac{\alpha+\beta\omega^2}{(\alpha+\beta\omega)(\alpha+\beta\omega^2)}$$

$$=\frac{\alpha+\beta(-1-\omega)}{\alpha^2-\alpha\beta+\beta^2}$$

$$=\frac{\alpha-\beta}{\alpha^2-\alpha\beta+\beta^2}$$

$$-\left(\frac{\beta}{\alpha^2-\alpha\beta+\beta^2}\omega\right)$$

$\boldsymbol{Z}[\omega]$內的可逆元素只有±1, $\pm\omega$, $\pm\omega^2$。（何故？）

一個非零的分圓整數ξ叫做不可約元素（irreducible element），如果ξ不是可逆元素，並且，如果η是分圓整數且$\eta\neq0$，η又能整除ξ，則η或$\frac{\xi}{\eta}$至少有一個是可逆元素。不可約元素是質數的推廣。

介紹了分圓整數、可逆元素、不可約元素之後，我們就可以討論$\boldsymbol{Z}[\omega]$的因數分解問題。我們把$\boldsymbol{Z}[\omega]$的幾個基本性質列舉如下：

(1)$\boldsymbol{Z}[\omega]$具有唯一分解性質。具體的說，(i) $\boldsymbol{Z}[\omega]$的任意元素ζ，若$\zeta\neq0$，ζ也不是可逆元素，則ζ可寫成$\xi_1\cdots\xi_n$的型式，ξ_i是不可約元素，(ii) 如果$\xi_1\xi_2\cdots\xi_n=\eta_1\cdots\eta_m$，其中$\xi_i$與$\eta_j$都是不可約元素，則$n=m$，並且（經過適當的重新排列之後）$\frac{\xi_i}{\eta_i}$都是可逆元素。

(2)若$\eta^3=\xi_1\cdots\xi_n$，其中$\xi_1,\cdots,\xi_n$，η都是非零的分圓整數，且$\xi_1,\cdots,\xi_n$兩兩互質，則$\xi_i=u_i\zeta_i^3$，u_i是可逆元素，ζ_i是某個分圓整數。

(3)設p是質數，α與β都是分圓整數且$\alpha\neq0$。若α能整除p與β，則p亦可整除β。

(4)設n與m是整數。若n與m在整數之內互質，則n與m在$\boldsymbol{Z}[\omega]$之內也互質。

(5)若α是任意分圓整數，則必可求得一個整數n，使得

$\alpha^3\equiv n\pmod 3$

說明：

第一個性質的敍述，我們不能寫成$\xi_i=\eta_i$，因爲要把類似

$6=2\cdot3=(-3)\cdot(-2)$

的情形包括在內。至於其證明，只要唸過抽象代數的人都很容易瞭解（先證明$\boldsymbol{Z}[\omega]$是歐氏環）。

第二個性質裏面，同樣的多出可逆元素u_i。例子，$3+6\omega$不是完全立方，但是

$$3+6\omega=\omega(1-\omega)^3$$

這個性質的證明倒是很容易。（利用性質(1)）

第三個性質的證明不容易，要利用到質數p在分圓整數環分解（ramified）的性質。

第四個性質的證明：$an+6m=1$；若α是整除n與m的分圓整數，則α整除1。故α是可逆元素。

要證明第五個性質，若α與β是分圓整數，在模3之下，

$$(\alpha+\beta)^3\equiv\alpha^3+3\alpha^2\beta+3\alpha\beta^2+\beta^3$$

$$\equiv\alpha^3+\beta^3\pmod 3$$

因此，在$\alpha=p+q\omega$時，

$$\alpha^3\equiv p^3+q^3\omega^3$$

$$\equiv p^3+q^3\pmod 3$$

即，取$n=p^3+q^3$即可。

現在可以證明定理3。已知$x^3+y^3=z^3$，z是偶數，x與y是奇數。考慮

$$x^3=z^3-y^3$$

$$=(z-y)(z-\omega y)(z-\omega^2y)$$

情況1：$z-y$與$z-\omega y$有公因數α，α是不可約。

則α整除

$$(z-\omega y)-\omega(z-y)=(1-\omega)z$$

同理，α整除$(1-\omega)y$。但y與z互質，故y與z在$\boldsymbol{Z}[\omega]$也互質（性質(4)）。得α整除$1-\omega$。但$1-\omega=\omega^2\sqrt{-3}$。故$\alpha$整除$\sqrt{-3}$，因此也整除3。今$\alpha$又整除$z-y$。故3整除$z-y$（性質(3)）。得證3整除$x^3$。得證。其他類似情況可仿此處理。

情況2：$z-y$，$z-\omega y$，$z-\omega^2 y$兩兩互質。

$z-\omega y=u\cdot\alpha^3$，$u$是可逆元素，$\alpha$是分圓整數（性質(2)）。

故$z-\bar{\omega}y=\bar{u}\cdot\bar{\alpha}^3$。

但是可逆元素只有±1，$\pm\omega$，$\pm\omega^2$。

故$\frac{u}{\bar{u}}=\omega^k$，$k=0$，1，2。（註九）

在模3之下，$\alpha^3\equiv n\pmod 3$，因此$\bar{\alpha}^3\equiv n\pmod 3$。故$\alpha^3\equiv\bar{\alpha}^3\pmod 3$

得

$$\begin{aligned}z-\omega y&\equiv u\alpha^3\equiv\frac{u}{\bar{u}}\cdot\bar{u}\alpha^3\\&\equiv\omega^k\cdot\bar{u}\cdot\bar{\alpha}^3\\&\equiv\omega^k(z-\bar{\omega}y)\\&\equiv\omega^k z-\omega^{k-1}y\pmod 3\end{aligned}$$

就$k=0$，1，2，討論

$$z-\omega y\equiv\omega^k z-\omega^{k-1}y\pmod 3$$

可知 $xyz\equiv0\pmod 3$

$k=1$時較複雜，故只就此情況討論。由

$$z-\omega y\equiv\omega z-y\pmod 3$$

故 $y\equiv-z\pmod 3$

同理，由$y^3=z^3-x^3$可得

$$xyz\equiv0\pmod 3$$

或 $x\equiv-z\pmod 3$

若 $x\equiv y\equiv-z\pmod 3$

則 $x=-z+3s$，$y=-z+3t$

將此關係代入$x^3+y^3=z^3$。故

$$\begin{aligned}&3z^3-9z^2(s+t)+27z(s^2+t^2)\\&-27(s^3+t^3)\\&=0\end{aligned}$$

可知z是3的倍數。

類似以上的方法，Lagrange，Gauss，Jacobi，Kummer都曾使用過，其最大特點是把複數ω引入整數論的研究。讀者不妨想一下，如果把$\sqrt{-1}$引入方程式$x^2+y^2=z^2$的研究，結果如何？（註十）

當然，最大膽的嘗試還不只如此。Peter Gustav Lejeune Dirichlet（1805～1859年把分析的方法引入整數論的研究，結果是奠立了解析數論（analytic number theory）的基礎。Dirichlet一個有名的定理是，若a與n是互質整數，則型式爲$nl+a$的質數有無窮多個。

六、Kummer與代數數論

研究Fermat方程式$x^n+y^n=z^n$是否有全異於零的整數解，在1847年之前並沒有太大的進展。正如從本文第4節看得出來的，$n=4$的情況很簡單。至於$n=3$的情況，可以說Fermat與Euler都有能力解決。$n=5$的情況是Dirichlet與Legendre獨立的在1825年才解決的，Dirichlet在1832年又解決了$n=14$的情況，1839年Gabriel Lamé（1795～1871年）才解決了$n=7$的情況。眞正的突破是Ernst Eduard Kummer（1810～1893年）的研究成果，他在1857年證明：如果n是一個奇質數，$3\leqslant n\leqslant 61$且$n\neq 37$，59，則Fermat方程式$x^n+y^n=z^n$沒有全異於零的整數解。Kummer不僅在Fermat問題做出歷史性的貢獻，他還開闢一個新領域——代數數論（algebraic number theory）。

在介紹Kummer的工作之前，我們卻要把鏡頭轉到法國去。

1847 年三月一日Lamé在巴黎科學院發表一個演講，他宣布他可以解決Fermat 問題。方法如下，

若 p 是奇質數，x，y，z 是全異於零的整數且 $x^p + y^p = z^p$ 。

令 $$\zeta = e^{\frac{2\pi\sqrt{-1}}{p}}$$

考慮 $$x^p = z^p - y^p$$
$$= (z-y)(z-\zeta y)\cdots(z-\zeta^{p-1}y)$$

如果 $z-y$，$z-\zeta y$，$\cdots$，$z-\zeta^{p-1}y$ 兩兩互質，則其皆爲 p 次分圓整數環 $\boldsymbol{Z}[\zeta]=\{\alpha_0+\alpha_1\zeta+\cdots+\alpha_{p-2}\zeta^{p-2}$ ：α_i 都是整數$\}$ 之內的完全 p 方數。利用無窮遞減法，我們可以由此導出矛盾。在一般情形下，令 m 是 $z-y$，$z-\zeta y$，$\cdots$，$z-\zeta^{p-1}y$ 的最大公約數，則 $\frac{z-y}{m}$，$\frac{z-\zeta y}{m}$，$\cdots$，$\frac{z-\zeta^{p-1}y}{m}$ 兩兩互質（註十一），因此歸於以上的情況。

Lamé 的演講其實有許多漏洞。第一，他把整數的因數分解的所有性質全部搬到 p 次分圓整數環 $\boldsymbol{Z}[\zeta]$；事實上 $\boldsymbol{Z}[\zeta]$ 是否具有唯一分解性質都有疑問。第二，他忽略了 $\boldsymbol{Z}[\zeta]$ 的可逆元素比整數的情況增加了很多（見上節基本性質 2）。第三，如何用無窮遞減法來導出矛盾，也令人非常懷疑。

Lamé 的演講內容眞正有創意的部分是把複數 ζ 引入整數論的研究，這個想法其實 Lagrange、Gauss、Jacobi 都使用過，只是沒有像Lamé這麼興奮罷了。Lamé的演講卻激起Cauchy 的熱情。他們爲了修改這些漏洞足足瘋狂了兩、三個月。

1847 年五月二十四日，Liouville 在巴黎科學院宣讀一封來自德國的信，這個德國人Kummer告訴他們，在三年前他已經證明，一般的 p 次分圓整數環 $\boldsymbol{Z}[\zeta]$ 沒有唯一分解的性質（註十二），他的學生Kronecker 在其博士論文把 $\boldsymbol{Z}[\zeta]$ 的可逆元素研究得清清楚楚。Kummer 還告訴他們，他在一年前創立了理想數（ ideal numbers ） 的概念，可以挽救 $\boldsymbol{Z}[\zeta]$ 沒有唯一分解性質所造成的困難。

以二次整數環 $\boldsymbol{Z}[\sqrt{-5}]=\{\alpha+\beta\sqrt{-5}$ ：α 與 β 是整數$\}$ 爲例。請注意，

$$2\cdot 3=(1+\sqrt{-5})(1-\sqrt{-5})$$

並且 2，3，$1+\sqrt{-5}$，$1-\sqrt{-5}$ 都是不可約元素（註十三）。因此唯一分解性質在 $\boldsymbol{Z}[\sqrt{-5}]$ 是不對的。

Kummer 的解決辦法是，假想有一些「數」α，β，γ，δ 滿足

$$2=\alpha\cdot\beta,\quad 3=\gamma\cdot\delta$$
$$1+\sqrt{-5}=\alpha\cdot\gamma,\quad 1-\sqrt{-5}=\beta\cdot\delta$$

那麼 $\boldsymbol{Z}[\sqrt{-5}]$ 沒有唯一分解的性質這個事實就沒有那麼可怕。它缺乏這些理想的數 α，β，γ，δ，所以沒有唯一分解的性質。如果把這些理想數加進 $\boldsymbol{Z}[\sqrt{-5}]$，它就有唯一分解的性質。

這些理想數並不是在 $\boldsymbol{Z}[\sqrt{-5}]$ 或 $\boldsymbol{Q}[\sqrt{-5}]=\{a+b\sqrt{-5}$ ：a 與 b 是有理數$\}$ 找得到的。事實上，令

$$\alpha=1+\sqrt{-1},\quad \beta=1-\sqrt{-1}$$
$$\gamma=\frac{1+\sqrt{-5}}{1+\sqrt{-1}}=-2+\frac{\sqrt{-5}-\sqrt{-1}}{2}$$
$$\delta=\frac{1-\sqrt{-5}}{1-\sqrt{-1}}=-2-\frac{\sqrt{-5}-\sqrt{-1}}{2}$$

原來 α，β，γ，δ，可以躲在

$$\boldsymbol{Q}[\sqrt{-5},\sqrt{-1}]$$
$$=\{a+b\sqrt{-5}+c\sqrt{-1}+d\sqrt{5}$$
$$:a,b,c,d\text{是有理數}\}$$

用近世的代數數論的眼光來看，$\boldsymbol{Q}[\sqrt{-5},\sqrt{-1}]$ 是 $\boldsymbol{Q}[\sqrt{-5}]$（或 $\boldsymbol{Z}[\sqrt{-5}]$）的類體（ class field ），$\boldsymbol{Z}[\sqrt{-5}]$ 的理想數全部躲在其類體裏面。

Kummer憑空造出理想數卻有一段因緣。在十九世紀初期，人類已經知道很多氯化物，卻不能把氯氣分離出來。Kummer認爲，理想數就像不能分離的氯氣，在 $\boldsymbol{Q}[\sqrt{-5}]$ 不一

定找尋得到。因此Kummer認爲，$Z[\sqrt{-5}]$的因數分解不應以$Z[\sqrt{-5}]$的數爲限，還應該把理想數也包括進去。Kummer的方法用現代的語言來講就是除子理論（divisor theory）。可是Kummer這套方法對十九世紀的人未免太玄奧了，因因此Richard Dedekind（1831～1916年）與Leopold Kroneker（1823～1891年）各提出一套修正的理論。以下就介紹Dedekind的理論。

Dedekind的辦法是用「集合」來代替「數」。例如，在整數之內，質數5可以用集合$(5)=\{5n : n$ 是任意整數$\}$來「表示」。（注意，集合(5)與集合(-5)是相同的集合。這不奇怪，質數5與-5有什麼不一樣？）同樣的，在$Z[\sqrt{-5}]$之內，3就用集合$(3)=\{3u : u\in Z[\sqrt{-5}]\}$表示，理想數$\alpha$就用$Z[-5]\cap\{\alpha v : v$ 是$Q[\sqrt{-5}, \sqrt{-1}]$之內的代數整數$\}$表示。（註十四）這些集合，姑且叫做I，有一些共同的特性：

(i) 若$u, v\in I$，則$u+v\in I$；

(ii) 若$u\in I$，$v\in Z[\sqrt{-5}]$，則$uv\in I$。

最幸運的是，具有以上兩個性質的集合剛好可以捕捉Kummer的理想數。因此，若p是一個奇質數，

$$\zeta = e^{\frac{2\pi\sqrt{-1}}{p}}$$

$$Z[\zeta]=\{a_0+a_1\zeta+\cdots+a_{p-2}\zeta^{p-2} : a_i\in Z\}$$

是p次分圓整數環，I是$Z[\zeta]$的非空集合的子集合，Dedekind把滿足以下兩個性質的I叫做理想集合（ideal）：

(i) 若$u, v\in I$，則$u+v\in I$

(ii) 若$u\in I$，$v\in Z[\zeta]$，則$uv\in I$

$Z[\zeta]$本身也是一個理想集合。只包括零元素的集合也是理想集合，我們把它記爲0。兩個理想集合I與J可以「相乘」，定義爲

$$I\cdot J=\{u_1v_1+\cdots+u_nv_n : u_i\in I, v_i\in J, n\text{任意正整數}\}$$

一個理想集合I叫做質理想集合（prime ideal），如果I滿足

(i) $I\neq 0$，$Z[\zeta]$

(ii) 若$xy\in I$，且$x, y\in Z[\zeta]$，則$x\in I$或$y\in I$。

質理想集合是「質數」概念的推廣，第(i)個性質就像是規定0，± 1都不是質數，第(ii)個性質就像是通稱的Euclid性質：若p是質數，且p整除$x\cdot y$，則p必整除x或y。

運用理想集合的概念，可以把Kummer第一個主要定理敘述如下：

第一定理：

若p是奇質數，I是p次分圓整數環$Z[\zeta]$的理想集合，若$I\neq 0$，$Z[\zeta]$，則I可寫成$p_1\cdots p_n$的型式，其中p_i是質理想集合；如果I另外也可寫成$Q_1\cdots Q_m$的型式，其中Q_j是質理想集合，則$n=m$並且（經過適當的重新排列之後）$p_i=Q_i$。

在p次分圓整數環$Z[\zeta]$之內，不爲零的理想集合，雖然有無窮無盡之多，我們卻可以做個分類：把兩個理想集合I與J歸在同一類，如果$I=xJ$，其中x是$Q[\zeta]$的某個元素，xJ代表集合$\{xu : u\in J\}$。用這個分類法，$Z[\zeta]$內不爲零的理想集合的種類只不過是個有限數，這個數目叫做p次分圓整數環的類數（class number）。類數會隨p的變化而改變。類數爲1的充要條件是這個分圓整數環具有唯一分解的性質。（這並不是顯而易見的定理。）

如果奇質數p不能整除p次分圓整數環的類數，那麼p就叫做規則質數（regular prime）。

1847年十月，約在Lamé演講之後半年，Kummer證明他的第二個主要定理，

第二定理：

(1)若p是規則質數，則Fermat方程式$x^p+y^p=z^p$沒有全異於零的整數解。

(2) p 是規則質數的充要條件是 p 不整除 $B_2 \cdot B_4 \cdots B_{p-3}$，其中 B_i 是有名的Bernoulli 數，可以定義如下：

$$1 + B_1 t + \frac{B_2}{2!} t^2 + \frac{B_3}{3!} t^3 + \cdots\cdots$$

$$+ \frac{B_k}{k_1} t^k + \cdots\cdots$$

$$= \frac{t}{e^t - 1}$$

Kummer 檢查一些Bernoulli 數，發現：從 3 到 61 之間的質數，只有 37 與 59 是不規則質數（其實，在 100 之內的不規則質數只有 37, 59, 67。）。因此他就把Fermat 問題的研究大大的往前推動了。1850 年巴黎科學院懸賞Fermat 問題，由於所有的應徵信件都毫無新的突破，七年之後這個獎只好頒給 Kummer，雖然Kummer 沒有去應徵。

可惜的是，規則質數究竟有多少，我們到現在都不知道。我們甚至不知道規則質數是不是無窮多個。不規則質數是無窮多個，這倒是能夠證明。統計的數字使我們相信，規則質數可能比不規則質數還要多出一些。

Kummer 生於普魯士一個貧困的家庭。1831 年，21 歲的時候得到Halle 大學的博士學位。此後在中學教了十年書，並且還參加過志願軍。服役期間，他寄了一篇論文給C. G. J. Jacobi（1804～1851 年），Jacobi 吃了一驚說：「如果普魯士的小兵都能夠做出這麼好的數學，他們的軍官的表現倒是有的瞧囉！」

1842 年他到Breslau 大學教書，1853 年轉到 Berlin 大學。自從Dirichlet、Riemann 在十九世紀六十年代相繼去世，Kummer，Kronecker，Weierstrass 任教的 Berlin 大學隱然成爲德國數學的重鎮。1886 年Felix Klein 到Göttingen 大學之後，情況才有所改變。

Kummer不僅在Fermat 問題的研究做出劃時代的貢獻，他還打開代數數論的第一道大門。分圓整數環只是一種特殊的代數整數環（the rings of algebraic integers）。研究各種代數整數環的類數、可逆元素、質數分解情形，是近世的代數數論的開宗明義第一章。

七、Fermat問題的主要結果

Fermat 問題的研究到目前爲止，有何進展？現分述如下（註十五）：

(1) S.S. Wagstaff（1976 年）證明：若 p 是一個奇質數，且 $p < 125{,}000$，則Fermat方程式 $x^p + y^p = z^p$ 沒有全異於零的整數解。

Wagstaff 的計算主要是依賴Vandiver 在Fermat 問題的成果。判斷 p 是不是一個規則質數，Vandiver 有一個關於Bernoulli 數的恆等式。這個恆等式很容易利用計算機檢查。當 p 是一個不規則質數，如果某些 Bernoulli 數滿足特定條件，仍然可以證明Fermat 問題。這些條件也可用計算機檢查。

(2) J. Brillhart J. Tonascia 與 P. Weinberger（1971 年）證明：如果 p 是奇質數，且 $p < 3 \times 10^9$，則Fermat 方程式 $x^p + y^p = z^p$ 的第一種情況成立。G. Terjanian（1977年）證明：如果 n 是任意偶數，則Fermat方程式 $x^n + y^n = z^n$ 的第一種情況成立。

Brillhart, Tonascia 與Weinberger 的計算也是根據理論結果推演而來的。在二十世紀初期，數學家知道：如果Fermat 方程式 $x^p + y^p = z^p$ 的第一種情況不成立，則

$$2^{p-1} \equiv 1 \pmod{p^2}$$

且

$$3^{p-1} \equiv 1 \pmod{p^2}$$

二十世紀初期的理論在七十年代終於迸發出一朵鮮花，高速計算機的問世使得檢驗以上的式子非常容易。

(3)C.L. Siegel（1929年）證明：若 $n \geqslant 3$，Fermat 方程式 $x^n + y^n = z^n$ 頂多有有限個互質整數解。

K. Inkeri 與S. Hyyrö（1964年）證明：對於任意奇質數 p 與任意正數 M，只有有限組正整數 x，y，z 滿足 $x^p + y^p = z^p$ 且 $0 < y - x$，$z - y < M$。他們又證明：對於任意奇質數 p，只有有限組正整數 x，y，z 滿足 $x^p + y^p = z^p$，其中 $0 < x < y < z$，並且 x 是某個質數的次方。

專門討論 Fermat 問題的書並不多。比較新的有兩本，

P. Ribenboim, 13 lectures on Fermat's last theorem, Springer, 1979。

H. M. Edwards, Fermat's last theorem, 1977,「凡異出版社」翻印本。

Edwards 的書只討論到 Kummer 爲止。Ribenboim 書的涵蓋面非常廣濶，他討論到最新的結果，他幾乎觸及每一個層次、每一種角度的方法與結果。

Ribenboim 的書並沒有對於各種結果給出完整的證明，但是他雄辯的把數學的精神與近代數學一部份的面貌描繪出來。只要具備大學數學系訓練的人應該看得懂這本書，說不定還會因此而喜歡數學。

Edwards 的書寫得比較慢，比較悠閒。前面六章做爲大學部初等數論或抽象代數的補充教材倒是相當合適，其實這本書（共九章）做爲大學部四年級代數數論的教科書也極合適。

八、幾個重要的Fermat定理

Fermat 在整數論提出許多重要的定理，我們僅列出幾個比較爲人熟知的。

(1)若 p 是質數，a 是任意整數，則

$$a^p \equiv a \pmod{p}$$

(2)正整數 n 可以寫成兩個平方數的和之充分必要條件是，如果 $n = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ 是 n 的質因數分解乘積，$p_i \neq p_j$ 若 $i \neq j$，且

$$p_1 \equiv p_2 \equiv \cdots \equiv p_r \equiv 3 \pmod{4}$$

$p_{r+1} \not\equiv 3 \pmod{4}$，$\cdots p_m \not\equiv 3 \pmod{4}$ 則 α_1，$\cdots \alpha_r$ 都是偶數。

(3)任意正整數 n 都可以寫成四個平方數的和。

(4)Fermat 是第一個求出 $x^2 - Ay^2 = \pm 1$ 的所有整數解的人，其中 A 是一個不含平方項的數。Fermat 曾提出以下幾個問題，向英國數學家挑戰，如，求

$$x^2 - 61y^2 = 1$$
$$x^2 - 109y^2 = 1$$
$$x^2 - 149y^2 = 1$$

所有的整數解。結果被W. Brouncker 求出答案。Brouncker 的名字被Euler誤會成Pell，從此這種方程式被叫做 Pell 方程式。其實叫做Fermat 方程式還比較適當。

(5)Fermat 曾經聲稱，形式如 $F_n = 2^{2^n} + 1$ 的數都是質數。的確，在 $n = 1$，2，3，4 時都如此。但是Euler發現641 能夠整除 F_5。這幾乎是Fermat 在整數論犯過的唯一錯誤。

以下我們將證明第(1)與(2)的結果。

若 p 是一個質數，我們先列出在 p 之下同餘的幾個基本性質：

(i) 若 $ab \equiv 0 \pmod{p}$
則 $a \equiv 0 \pmod{p}$
或 $b \equiv 0 \pmod{p}$

(ii) 若 a，b 是任意數且
$a \not\equiv 0 \pmod{p}$
則方程式
$ax \equiv b \pmod{p}$
必有唯一的解（在模 p 之下）。

(iii) 若 $n \leqslant p - 1$，方程式
$x^n + a_1 x^{n-1} + \cdots + a_n$
$\equiv 0 \pmod{p}$

至多有 n 個不同餘的解。

說明：

(i) 只是「若 p 整除 ab ，則 p 整除 a 或 b 」的變形。

(ii) 因爲 a ， p 互質，故可找到 u ， v ，滿足 $au+pv=1$ ，兩邊再乘上 b 。

(iii) 常見的因子定理仍可使用。再配合 (i) 。

定理4 若 $a \not\equiv 0 \pmod{p}$

則 $$a^{p-1} \equiv 1 \pmod{p}$$

證明 根據

$$(a+b)^p$$

$$=a^p+\binom{p}{1}a^{p-1}b+\binom{p}{2}a^{p-2}b^2$$

$$+\cdots\cdots+\binom{p}{p-1}ab^{p-1}+b^p$$

$$\equiv a^p+b^p \pmod{p}$$

因爲 $\binom{p}{k}=\dfrac{p\cdot(p-1)\cdots(p-k+1)}{1\cdot 2\cdots\cdots k}$

是整數，且其分母部分與 p 互質，故 p 整除 $\binom{p}{k}$ 。

令 $b=1$

得 $(a+1)^p=a^p+1 \pmod{p}$

故 $(a+1)^p-(a+1)\equiv a^p-a$

以 $a=0$ ， 1 ， 2 ，… ， $p-2$ 代入，得

$$0\equiv 0^p-0\equiv 1^p-1\equiv 2^p-2\equiv\cdots$$

$$\equiv(p-1)^p-(p-1)$$

故 $$a^p\equiv a \pmod{p}$$

若 $$a \not\equiv 0 \pmod{p}$$

利用性質 (i)，得

$$a^{p-1}\equiv 1 \pmod{p}$$

引1 $(p-1)!\equiv -1 \pmod{p}$

證明 1 ， 2 ，… ， $p-1$ 是方程式

$$x^{p-1}-1\equiv 0 \pmod{p}$$

的 $p-1$ 個不同餘的根。故

$$x^{p-1}-1$$

$$\equiv(x-1)(x-2)\cdots\{x-(p-1)\}$$

利用根與係數的關係（必須有性質 (iii)），得

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

p 是奇數，故 $(-1)^{p-1}=1$ 。（若 $p=2$ ，這個敍述根本就不值得證明。）

引2 若 p 是奇質數，則

$$x^2+1\equiv 0 \pmod{p}$$

有解的充分必要條件是 $p\equiv 1 \pmod{4}$

證明 若 $x^2+1\equiv 0 \pmod{p}$

則 $$(-1)^{\frac{p-1}{2}}\equiv(x^2)^{\frac{p-1}{2}}\equiv x^{p-1}$$

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

故 $\dfrac{p-1}{2}$ 必須是偶數。

若 $$x^2+1\equiv 0 \pmod{p}$$

無解。對於 $a \not\equiv 0 \pmod{p}$ ，找 b ，滿足

$$ab\equiv -1 \pmod{p}$$

（利用性質 (ii)）很明顯的 $a \not\equiv b \pmod{p}$ 。把 1 ， 2 ，… ， $p-1$ 這樣配對起來，再全部乘起來，得

$$(p-1)!\equiv(-1)^{\frac{p-1}{2}} \pmod{p}$$

由引1，得

$$-1\equiv(-1)^{\frac{p-1}{2}} \pmod{p}$$

故 $\dfrac{p-1}{2}$ 是奇數。

定理5 若 $n = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ 是 n 的質因數乘積，$p_i \neq p_j$ 若 $i \neq j$，且

$$p_1 \equiv \cdots \equiv p_r \equiv 3 \pmod 4$$

$p_{r+1} \not\equiv 3 \pmod 4$，$\cdots$，$p_m \not\equiv 3 \pmod 4$

則 $n = x^2 + y^2$ 有整數解的充分必要條件是 $\alpha_1, \cdots, \alpha_r$ 是偶數。

証明 第一步驟，若 $p \equiv 1 \pmod 4$ 是質數，則 $p = x^2 + y^2$ 有解。

假設以上敍述不成立，取這樣最小的 p，使 $p = x^2 + y^2$ 無解。

因爲 $x^2 + 1 \equiv 0 \pmod p$ 有解，我們可取出互質整數 a，b，$0 < a$，$b < \frac{p}{2}$，使得 $np = a^2 + b^2$，且 n 是最小。顯然 $1 < n < p$。

n 不是偶數，否則 a 與 b 必須是奇數。得

$$\frac{n}{2} p = \left(\frac{a+b}{2}\right)^2 + \left(\frac{a-b}{2}\right)^2$$

，矛盾。

若 q 是奇質數，且 q 整除 n，則

$$q \equiv 1 \pmod 4$$

否則 $a^2 + b^2 \equiv 0 \pmod q$

因 a，b 互質，故至少 a 或 b 不是 q 的倍數，得

$$\left(\frac{a}{b}\right)^2 + 1 \equiv 0 \pmod q$$

或 $$\left(\frac{b}{a}\right)^2 + 1 \equiv 0 \pmod q$$

由引2得 $q \equiv 1 \pmod 4$

因 $q \leqslant n < p$，故 $q = u^2 + v^2$，得

$$\frac{n}{q} p = \left(\frac{ua \pm vb}{u^2+v^2}\right)^2 + \left(\frac{ub \mp va}{u^2+v^2}\right)^2$$

今 $$\left(\frac{u}{v}\right)^2 \equiv -1 \pmod q$$

$$\left(\frac{a}{b}\right)^2 \equiv -1 \pmod q$$

故 $$\left(\frac{u}{v}\right)^2 \equiv \left(\frac{a}{b}\right)^2 \pmod q$$

得 $$\frac{u}{v} \equiv \pm \frac{a}{b} \pmod q$$

故 $$ub \mp va \equiv 0 \pmod q$$

因此 $\frac{ub \mp va}{u^2+v^2}$ 至少有一個可能是整數，可得 $\frac{ua \pm vb}{u^2+v^2}$ 也是整數。

因此 n 不是滿足 $np = a^2 + b^2$ 的最小數。矛盾。

第二步驟，利用

$$(u^2+v^2)(a^2+b^2) = (ua+vb)^2 + (ub-va)^2$$

可證明，若 α_1，$\cdots$，α_r 是偶數，則 $n = x^2 + y^2$ 有解。

第三步驟，若 $n = x^2 + y^2$ 有解，則 $\alpha_1, \cdots, \alpha_r$ 是偶數。

令 d 是 x 與 y 的最大公約數，且 $\alpha_1, \cdots, \alpha_r$ 有一個不是偶數。設 α_1 是奇數。

因 $\frac{n}{d^2} = \left(\frac{x}{d}\right)^2 + \left(\frac{y}{d}\right)^2$，且 p_1 整除 $\frac{n}{d^2}$，得

$$\left(\frac{x}{d}\right)^2 + \left(\frac{y}{d}\right)^2 \equiv 0 \pmod{p_1}$$

今 $\frac{x}{d}$ 與 $\frac{y}{d}$ 互質，故

$$\left(\frac{x}{y}\right)^2 \equiv -1 \pmod{p_1}$$

或 $$\left(\frac{y}{x}\right)^2 \equiv -1 \pmod{p_1}$$

與引2矛盾。

—本文作者任敏於台大數學系—

註 釋

註八 若p是質數，且$n \not\equiv 0 \pmod p$，利用輾轉相除法可找到m與l滿足

$$n \cdot m + pl = 1$$

故 $n \cdot m \equiv 1 \pmod p$

因此不妨把m看成是模p之下的$\frac{1}{n}$。

註九 在p次分圓整數環，這個敍述就是有名的 Kummer 預備定理（Kummer's lemma）。

註十 $z^2 = x^2 + y^2$

$= (x + \sqrt{-1}\, y)(x - \sqrt{-1}\, y)$

因z是奇數，且x與y互質，故

$x + \sqrt{-1}\, y$ 與 $x - \sqrt{-1}\, y$

互質。得

$x + \sqrt{-1}\, y = \alpha \cdot (u + \sqrt{-1}\, v)^2$

α是可逆元素。但是可逆元素只有± 1與$\pm\sqrt{-1}$。故

$\alpha (u + \sqrt{-1} v)^2$

$= \pm (u^2 - v^2) \pm 2uv\sqrt{-1}$

或 $2uv \pm (u^2 - v^2)\sqrt{-1}$

得證 $x = \pm (u^2 - v^2)$

或 $\pm 2uv$

註十一 若m整除$z - \zeta^i y$與

$z - \zeta^{i+k} y$（$k \not\equiv 0 \pmod p$）

則m整除$\zeta^i y - \zeta^{i+k} y$。故$m$整除

$(z - \zeta^{i+k} y) + \zeta^k (\zeta^i y - \zeta^{i+k} y)$

$= z - \zeta^{i+2k} y$

以此類推，m整除 $z - \zeta^{i+jk} y$，

$j = 0, 1, \cdots, p-1$。

註十二 p次分圓整數環$\boldsymbol{Z}[\zeta]$具有唯一分解的性質的充要條件是$p = 3, 5, 7, 9, 11, 13, 17, 19$。這是一個困難的定理，幾年前才證明出來的。以$p = 23$爲例，令

$\alpha = 1 + \zeta^2 + \zeta^4 + \zeta^5 + \zeta^6 + \zeta^{10} + \zeta^{11}$

$\beta = 1 + \zeta + \zeta^5 + \zeta^6 + \zeta^7 + \zeta^{11}$

讀者自己證明一下：2不整除α或β，但是2整除$\alpha\beta$。

註十三 定義一個函數

$N(\alpha + \beta\sqrt{-5}) = \alpha^2 + 5\beta^2$

注意，如果

$\alpha + \beta\sqrt{-5}$

整除 $\gamma + \delta\sqrt{-5}$

則 $N(\alpha + \beta\sqrt{-5})$

整除 $N(\gamma + \delta\sqrt{-5})$

利用這個性質，讀者自己證明2, 3, $1 \pm \sqrt{-5}$都是不可約元素。

註十四 很抱歉，我們沒有定義代數整數（algebraic integers）。讀者可以不必追究。簡單的說，$\boldsymbol{Z}[\sqrt{-5}]$是$\boldsymbol{Q}[\sqrt{-5}]$之內所有的代數整數，$\boldsymbol{Z}[\zeta]$是$\boldsymbol{Q}[\zeta]$之內所有的代數整數。

註十五 這一節的材料完全取自 P. Ribenboim, 13 lectures on Fermat's last theorem, Springer, 1979, New York。