費馬最後定理

黃文璋
國立高雄大學應用數學系

1 前言

歷史上, 可能沒有一個數學的問題, 其敘述是如此簡單, 但受到的重視卻又無與倫比, 這就是費馬最後定理(Fermat's Last Theorem), 或稱費馬大定理 (Fermat's Great Theorem), 此因爲了與另一費馬小定理(Fermat's Little Theorem)區別 。

費馬(Fermat, 1601-1665)出生於法國 Toulouse的一富裕家庭。小時候他雖然喜愛數學, 但他仍接受父親的建議於大學時讀法律。後來並成爲一名律師, 還當了議會的議員。他熱愛古典文藝,業餘時研究數學, 常與當時的一些著名數學家如笛卡兒(Descartes, 1596-1650) , Pascal (1623-1662)及Wallis (1616-1703)等通信, 交換心得。

費馬雖是一位業餘的數學愛好者, 但他在數學的許多領域均有開創性的工作。今日大部分的人只記得他在數論上的成就(他是現代數論的開創者), 其實他與笛卡兒並列爲解析幾何的創立者, 在機率論的早期發展也有不少貢獻。而微積分雖是牛頓 (Newton, 1642-1727) 及萊布尼茲(Leibnitz, 1646-1716)所發明, 但費馬爲他們做了奠基性的工作。他與笛卡兒被公認爲十七世紀上半期的兩位首要的數學家。不過費馬最著名的, 還是在數論方面的成就。數論上有許多重要的事項均與費馬有關。在近代數論中, 在一個世紀後的歐拉(Euler, 1707-1783)之前, 無人與之匹敵。

在十七、十八世紀, 由於數學期刊很少, 數學家往往藉互相通信來傳達他們的研究成果。費馬得到的結果也均發表於書信中, 沒有公開出版書籍。這樣的不公開出版研究成果,雖使其影響受到限制, 卻引發出一段連綿三百多年的歷史公案。

2 問題的由來

費馬花最多的功夫是在解整數方程式的問題, 這種問題又稱Diophantine, 此爲約西元前250年, 住在現今埃及亞歷山大里亞城 (Alexandria)的希臘數學家丟番圖 (Diophantus, 生平不詳)首先研究的。丟番圖被認爲是有史以來第一位研究數論的。他寫了一套13卷的論文, 稱爲算術學 (Arithmetica), 討論許多基本的數論問題。在算術學書第二卷的問題8爲: 將一平方數分成二數的平方和。丟番圖的解法如下: 設平方數爲16, 令x^2及$(2x-4)^2$分別表二數的平方。則由假設

$$x^2 + (2x-4)^2 = 16,$$

得$5x^2 = 16x$,因此$x = 16/5$。即

$$16 = (\frac{16}{5})^2 + (\frac{12}{5})^2 \text{。} \tag{1}$$

我們注意到兩件事情。第一件爲"解"假設爲有理數, 既不限制爲整數也不推廣至實數。第二件爲只要求出一解便滿意了, 而不在乎是否有其他解。

算術學有6卷流傳下來, 在西元1575年拉丁文的翻譯本出版。這是最後一批希臘的數學書籍被翻譯成拉丁文。費馬有一本西元1621年出版的翻譯本, 他在書的邊緣做了很多註解。在思考前面提到的問題(將一平方數分成二數的平方和)時, 費馬在算術學書該頁邊緣寫了底下一段著名的話: 另一方面, 將一立方數分成兩個立方數, 或將一四次方數分成兩個四次方數, 或一般地, 除了二次方外, 任意次方數皆不能分成兩個同次方的數。我已發現一絕妙無比的證明, 但此頁邊不夠大無法寫下。

由費馬與梅仙尼(Mersenne, 1588-1648)的通信, 推測此段話約寫於西元1637年。費馬的意思即方程式

$$x^n + y^n = z^n \tag{2}$$

當整數$n \geq 3$時, 無非零整數解。這就是費馬最後定理。讀者可很容易地看出無非零整數解與無正整數解是等價的。與丟番圖對方程式的解法明顯地不同的是, 費馬對解限制爲整數, 且是宣稱一組解都不存在, 斬釘截鐵地, 不若丟番圖對一方程式往往只是得到其中的幾組解。

前述丟番圖得到(1)式,由此即得$(4 \cdot 5)^2 = (4 \cdot 4)^2 + (4 \cdot 3)^2$。此式又等價於$5^2 = 4^2 + 3^2$。大家都學過畢氏定理 (Pythagorean Theorem, Pythagoras, 約西元前580-500年), 即若以x, y表一直角三角形的兩直角邊(或稱爲股)之邊長, z表斜邊(或稱爲勾)之邊長, 則

$$x^2 + y^2 = z^2 \text{。} \tag{3}$$

此定理在我國古代稱爲商高定理或勾股定理。丟番圖其實就是找(3)式之一些特別解。今日此問題已完全被解出, 即解爲

$$x = 2uv, y = u^2 - v^2, z = u^2 + v^2, \tag{4}$$

其中$u > v$爲二正整數。換句話說(3)式有無限組解。

讀者不妨試試(2)式當$n = 3$時的情況。依序列出正整數的立方: 1, 8, 27, 64, 125, 216, 343, $\cdots$。然後看有沒有那一數爲前面某二數之和, 你會發現一直找不到。但這個方法並無法證明$n = 3$時(2)式無解, 且當z值愈大時, 檢查也很困難。不像$n = 2$的情況, 由1, 4, 9, 16, 25, $\cdots$, 很快便發現$25 = 9 + 16$。

後來的數學家常會爭論費馬是否眞的會證明費馬最後定理, 許多專家對此是存疑的。一個理由是$x^n + y^n = z^n$並非一典型費馬所考慮的方程式。大部分費馬討論的方程式, 其次數均不超過4。並且在費馬與友人的通信中, 他只敘述$n = 3$時的情況。至於他所謂絕妙無比的證明, 很可能是用到無限下降法(infinite descent)的技巧。無限下降法主要是說, 先假設一方程式有一組正整數解, 然後證明可得到一組更小的正整數解。同理又得到一組更小的正整數解, 如此一直進行下去,得到的解愈來愈小。但既然所有解全爲正整數, 就不可能不斷地得到愈來愈小的解。此矛盾便導至原方程式不存在正整數的解。

費馬最後定理當$n = 4$時的證明給在費馬的頁邊註解中, 即使對此特別的情況, 費馬也是抱怨空間不夠無法給出所有證明的細節。費馬先證明一

直角三角形, 若其三邊長皆爲整數, 則其面積必不爲平方數。我們敘述其證明如下, 此爲無限下降法之一例。

設直角三角形兩股長爲a, b, 斜邊長爲c, 欲證其面積$ab/2$不爲一平方數。此問題即等價於證明

$$x^2 + y^2 = z^2, \frac{1}{2}xy = w^2 \tag{5}$$

無正整數解。不失一般性可設x與y互質。假設(5)式有正整數解x_0, y_0, z_0, w_0。則由(4)式知, 存在正整數$u > v$,使得

$$x_0 = 2uv, y_0 = u^2 - v^2, z_0 = u^2 + v^2 \text{。}$$

因u, v及$u^2 - v^2$兩兩互質(否則x與y不互質), 而其乘積

$$uv(u^2 - v^2) = \frac{1}{2}xy = w^2$$

爲一平方數,所以u, v及$u^2 - v^2$均爲平方數(爲什麼?), 即存在正整數l, m, 及n, 使得

$$u = l^2, v = m^2, u^2 - v^2 = n^2 \text{。}$$

由於x_0, y_0互質, 故u, v必爲一奇數及一偶數。又因$u^2 - v^2 = n^2$, 故n爲奇數。再由$u^2 = v^2 + n^2$知, 不可能u爲偶數而v爲奇數(爲什麼?)。所以u爲奇數, 且v爲偶數。因此仍由(4)式, 存在正整數$r > s$, 使得

$$v = 2rs, n = r^2 - s^2, u = r^2 + s^2 \text{。}$$

由上式得

$$r^2 + s^2 = u = l^2, \frac{1}{2}rs = \frac{1}{4}v = (\frac{m}{2})^2,$$

即$r, s, l, m/2$(因v爲偶數, 故m也是偶數)亦爲(5)式之一組正整數解。而此組解中的l比一開始那組解中的z_0爲小($l < u < z_0$)。即(5)式若有一組解,則可得第二組解, 且其z值要較第一組解中的z值小。同理由第二組解又可得到第三組解, 且有更小的z值。但z值都爲正整數, 不可能一直小下去。所以一開始假設(5) 式有解是錯的。即得證(5)式無正整數解。

由上述結果,立即可得$n = 4$時費馬最後定理之證明: 設$x^4 + y^4 = z^4$有正整數解, 則由$(x^2)^2 + (y^2)^2 = (z^2)^2$,可得存在正整數$u > v$, 使得

$$x^2 = 2uv, y^2 = u^2 - v^2, z^2 = u^2 + v^2 \text{。}$$

但由第一及第三式即得(5)式有解之矛盾的結果。

費馬最後定理當$n = 3$時之證明($n = 3$時的證明較$n = 4$時的證明困難)見余文卿(1994)。有許多證據顯示費馬能證明$n = 3$的情況。費馬很可能以爲他對$n = 3$及$n = 4$情況的證明, 可輕易地推廣到一般的n。無論如何, 我們對費馬還是蠻佩服的,因他只證了$n = 3$及$n = 4$的情況, 就敢大膽推斷對所有的n都成立, 並且還不容易推翻, 可見他對數學的現象之判斷相當敏銳。

丟番圖的工作在費馬之前並未引起注意, 因此未激發進一步的研究。即使在費馬的時代, 除了費馬之外的數學家對整數論的興致均不大。因此費馬雖得到很多整數論中的結果, 但卻不愛將其證明寫下。事實上費馬留下的整數論的證明只有兩個, 另一個爲聯立方程式$x = 2y^2 - 1, x^2 = 2z^2 - 1$, 只有當$x = 1$或7時才有整數解。

費馬去世後, 西元1670年, 他兒子將他的頁邊註解及文稿整理發表。他的一些往來信件也收錄在Wallis 的Opera Mathematica書中。數學家才知道他已開闢了一新領域, 即整數論。

西元1729年, 俄國數學家Goldbach (1690-1764)寫信給歐拉, 提到費馬的一些結果。因此引起時年22歲的歐拉開始探討數論。三年後,歐拉寫了他在數論上的第一篇論文, 推翻費馬在質數方面的一個猜想, 即對任一非負整數n, $2^{2^n} + 1$ 爲質數(見下節)。在其後的五十年, 歐拉證出了許多費馬的猜想, 也因此將數論從原來只是一些各種事實及結果之收集, 轉爲居數學很核心之一有組織的領域。

3 費馬數

大家都知道質數有無限多個, 但能否給出一函數, 使得若將每個正整數代入, 皆能產生質數呢?

我們看二型式簡單且類似的函數: $2^n - 1$及$2^n + 1$。之所以特別留意此二函數, 乃是因其分解因式上的特性。當$2^n - 1$爲質數, 則n必爲質數, 其逆則不眞。那些正整數n 會使得$2^n - 1$爲質數呢?也不太多, 由此並引申出完全數及梅仙尼質數的討論(見"完全數與梅仙尼質數"一文), 爲數學中一有趣的題材。至於$2^n + 1$何時爲質數呢? 見下定理。

定理1.若$2^n + 1$爲質數, 則n必爲2的次方。

[證明]:設2^n+1爲質數, 且將n寫成$2^k l$, 其中k,l爲整數,$k\geq 0, l\geq 1$, 且l爲奇數。若$l>1$, 則

$$2^n+1=(2^{2^k}+1)(2^{2^k(l-1)}-2^{2^k(l-2)}+\cdots-2^{2^k}+1)\text{。}$$

此與2^n+1爲質數的假設不合, 故$l=1$。即證得$n=2^k$。

現令

$$F_k=2^{2^k}+1, k=0,1,\cdots,$$

F_k被稱爲費馬數 (Fermat number)。我們給出一些F_k如下, 此數列增加極快速。

$$\begin{aligned}
F_0 &= 2^1+1=3,\\
F_1 &= 2^2+1=5,\\
F_2 &= 2^4+1=17,\\
F_3 &= 2^8+1=257,\\
F_4 &= 2^{16}+1=65{,}537,\\
F_5 &= 2^{32}+1=4{,}294{,}967{,}297\text{。}
\end{aligned}$$

費馬發現此數列是因他注意到只要n有一奇因數, 2^n+1便不爲質數(此即定理1)。所以費馬以爲所有的F_k皆爲質數(此即定理1 之逆)。費馬只檢驗F_0至F_4便做此推測, 可惜此推測並不正確, 底下我們將看歐拉如何推翻費馬的猜測。

歐拉在西元1732年證出F_5並非質數, 其證明要用到下述費馬小定理。在此"$\equiv$"表同餘記號。設a,b爲二整數, n爲一正整數, $a\equiv b \pmod n$表$n|(a-b)$, 其中$a|b$表b爲a之整數倍。

定理2.設p爲一質數, 則對每一正整數m,$m^p\equiv m \pmod p$。

系理1.設p爲一質數, m爲一正整數, 且$(m,p)=1$, 則

$$m^{p-1}\equiv 1 \pmod p\text{。} \tag{6}$$

歐拉又證明下述結果。

定理3.設$m>k$, 則

(i) $F_k \nmid F_m$;

(ii)若$d|F_k$, 且$d > 1$, 則$d \nmid F_m$。

[證明]:首先可將F_m寫成下式。

$$F_m = 2^{2^m} + 1 = 2^{2^{m-1}\cdot 2} - 1 + 2 = (2^{2^{m-1}} + 1)(2^{2^{m-1}} - 1) + 2。$$

故

$$F_m = F_{m-1}a_{m-1} + 2, \tag{7}$$

其中對$\forall n \geq 1$, 令

$$a_n = 2^{2^n} - 1。$$

由(7)又得

$$\begin{aligned} F_m &= F_{m-1}(2^{2^{m-2}} + 1)(2^{2^{m-2}} - 1) + 2 \\ &= F_{m-1}F_{m-2}a_{m-2} + 2。 \end{aligned}$$

餘此類推可得對$\forall 1 \leq k \leq m-1$,

$$F_m = F_{m-1}F_{m-2}\cdots F_k a_k + 2。 \tag{8}$$

因每一F_n皆爲奇數, 因此F_n之每一因數皆爲奇數, 故由(8)式即同時證出(i)及(ii)。

利用上述定理立即可得底下推論。

系理2. (i) $F_{n+1} \equiv 2 \pmod{F_n}, n \geq 0$;

(ii)若$d|F_n$, 則$F_{n+\ell} \equiv 2 \pmod{d}, \ell = 1, 2, \cdots$。

底下我們來看歐拉如何證明

$$641|F_5。 \tag{9}$$

首先由系理1知, 對一質數$p \neq 2$, 若$(a, p) = 1$且$(b, p) = 1$, 則因

$$p|(a^{p-1} - 1),\ p|(b^{p-1} - 1),$$

故

$$p|(a^{p-1} - b^{p-1})。 \tag{10}$$

由此又得

$$p \nmid (a^{p-1} + b^{p-1}) \tag{11}$$

(因若$p|(a^{p-1}+b^{p-1})$再加上有(10), 便得$p|2a^{p-1}$, 因此$p|a^{p-1}$ 不合) 。

若$p = 4n-1$,因$a^{p-1}+b^{p-1} = a^{2(2n-1)}+b^{2(2n-1)} = (a^2+b^2)m$, 故(11)導至

$$p \nmid (a^2 + b^2) \text{ 。} \tag{12}$$

前面提過奇質數有$4n+1$及$4n-1$兩種型式 。由(12)即知對一奇質數p, 除非$p|a$或$p|b$, 否則若$p|(a^2+b^2)$, 則p爲$4n+1$型之質數 。

現對此$4n+1$型的質數p, 又可分成$8k+1$ (若$n = 2k$)或$8k-3$ (若$n = 2k-1$)二型 。若p爲$8k-3$型, 則因此時$a^{p-1}+b^{p-1} = (a^4)^{2k-1}+(b^4)^{2k-1} = (a^4+b^4)\ell$,故由(11)知

$$p \nmid (a^4 + b^4) \text{ 。}$$

即對一奇質數p, 除非$p|a$或$p|b$, 否則若$p|(a^4+b^4)$, 則p爲$8k+1$型之質數(如17, 97, 113, 193等) 。

如此繼續討論下去, 可得下述一般的結果 。

定理4. 設a, b爲二整數, 則對一奇質數p, 除非$p|a$或$p|b$, 否則若$p|(a^{2^k}+b^{2^k})$,則p爲$2^{k+1}n+1$型的質數 。

利用定理4得, 若$F_5(= 2^{2^5}+1)$有一質因數p(此時p當然爲奇數, 爲什麼?), 則p 必爲$2^6n+1 = 64n+1$的型式, 此數列的質數爲193, 257, 449, 577, 641,$\cdots$ 。依序去試除F_5, 我們發現$641|F_5$ 。

事實上, 若利用同餘的概念及641可寫成

$$641 = 2^4 + 5^4 = 2^7 \cdot 5 + 1$$

的型式, 則經由下述步驟可證出$641|F_5$ 。首先因

$$2^7 \cdot 5 \equiv -1 \pmod{641},$$

故由"同餘數及質數在密碼學上應用"一文的例1,

$$(2^7 \cdot 5)^4 \equiv (-1)^4 \pmod{641},$$

即

$$2^{28} \cdot 5^4 \equiv 1 \pmod{641}。$$

又

$$2^4 \equiv -5^4 \pmod{641},$$

由上二式得

$$2^{32} \cdot 5^4 \equiv -5^4 \pmod{641},$$

因$(5^4, 641) = 1$, 故上式導至

$$2^{2^5} = 2^{32} \equiv -1 \pmod{641},$$

即證出$641|F_5$, 故F_5非爲質數。

自歐拉後, 在西元1880年, Landry(時年82歲)證明F_6可寫成274,177與67,280,421,310,721 二數之積。而F_7於西元1905年被證明出爲一合成數, 但此39位數的質因數, 卻直到西元1970年才由Morrison與Brillhart兩人以IBM 360/91 電子計算機花了1.5小時才找出。F_8 則在西元1981年, 由Brent與Pollard 所分解。另兩個完全被分解的爲F_9 及F_{11}。至於$k \geq 12$, F_k就都沒有完全被分解(有些只是找出一些因數)。Ribenboim (1996)一書, 列出目前已知非質數及被分解出之費馬數的名單。事實上, 至今所知爲質數的費馬數只有前面5個。

至西元1996年止, 所知之最大的非質數的費馬數爲$F_{23,471}$, 其位數超過$10^{7,000}$ 位, 且有一因數$5 \cdot 2^{23,473} + 1$。許多費馬數F_k皆有一呈$a \cdot 2^{k+2} + 1$型式的因數。最小的兩個仍不知是否爲質數的費馬數爲F_{24}及F_{28}(F_{22}爲合成數是西元1993年才確定的)。有人猜測當$k \geq 5$, 所有費馬數F_k皆非質數。如果此猜測爲正確, 那就使費馬的猜測當$k \geq 5$時, 恰好是相反的, 也是一件趣事。

費馬數有什麼用途呢? 爲何我們會關心它是否爲質數呢?

費馬數與正多邊形的作圖有關。在高斯 (Gauss, 1777-1855) 十九歲的時候(西元1796 年),以直尺與圓規作出正17邊形。他高興萬分, 原先他是對哲學 與數學皆感興趣的, 但自此他便決心致力於數學。高斯雖在天文及物理上亦皆有卓越的貢獻,但最大的成就仍是在數學上的研究。數學中

大部分的領域都會用到他的一些研究成果。德國對產生如此一位大數學家也很自豪, 現今德國的10馬克(Mark)便是以高斯爲人像。

高斯發現正n多邊形可作圖的充分且必要條件是n可寫成

$$n = 2^m p_1 \cdots p_r, \tag{13}$$

其中$p_1, \cdots, p_r$爲相異的費馬質數(費馬數若爲質數便稱費馬質數), $m \geq 0$爲一整數。這是一件有趣的事, 雖然費馬數未能達到表示出一數列質數的目的, 但卻與正多邊形的作圖有關係。我們已指出首五個費馬質數爲3、5、17、257及65,537 (這也是至今所知的所有費馬質數)。由於正3及正5邊形早就知道可作, 因此由高斯的結果知正4、6、8、10、12、15、16邊形皆可作圖, 而正7、9、11、13、14邊形皆不可作圖。因下一個費馬質數就是17, 這更顯出正17邊形能作圖的歷史意義。之後在西元1832年Richelot作出正257邊形。在西元1894年Hermes經過十年時光, 完成正65,537邊形的作圖。其作法及證明的原稿放滿一大箱子, 現置於德國哥丁根大學 (University of Göttingen)。由於我們只知道五個費馬質數, 由(13)式知, 目前所能做出的奇數正多邊形共有31個(見習題第2題), 且最大的邊數爲$3 \cdot 5 \cdot 17 \cdot 65{,}537 = 4{,}294{,}967{,}295$。高斯一生都對他在數學上的第一個成就感到自豪。他告訴他的友人說, 要在他的墓碑上刻一個正十七邊形。可惜他的願望並沒達成。不過, 在高斯的故鄉Braunschweig 的高斯紀念碑上, 刻著一顆十七個角的星。至於爲什麼是十七個角的星而不是十七邊形呢?原來負責紀念碑的雕刻家認爲十七邊形和圓太像了, 不容易分辨。

對二如此簡單型式的數$2^n - 1$及$2^n + 1$是否爲質數的討論, 居然一引出最大質數及完全數的尋找, 一引出正多邊形的作圖, 這可能是費馬始料未及的。

4 費馬最後定理之解決

不難看出費馬最後定理要成立, 只要證出$n = 4$及n爲奇質數時的情況即可。此因任意大於或等於3的正整數必爲4的倍數或奇質數的倍數, 又若n爲m的整數倍, 且$x^m + y^m = z^m$沒有正整數解,則$x^n + y^n = z^n$也沒有正整數解。例如, 若$x^{15} + y^{15} = z^{15}$, 則$(x^5)^3 + (y^5)^3 = (z^5)^3$。即

得$x^3+y^3=z^3$ 之一組解。歐拉在西元1822年他死後才出版的一本代數書上提供$n=3$時的證明, 其證明雖不完整但基本上是對的(歐拉對他未能證出費馬最後定理, 感到很沮喪, 曾託友人至費馬故居搜尋, 看是否可找到遺留下來的重要文稿)。後來高斯給了一正確的證明。

費馬在數論方面提出許多重要的定理, 這其中除了兩個之外, 後來的數學家均能一一證明。此二例外, 一個是錯的, 即前面所提費馬數皆爲質數, 另一個即費馬最後定理。因這是費馬留下的定理中最後一個還沒解決的, 由此而得名。由於此定理的敘述是如此簡單, 令人以爲光憑中學數學的工具便可解決, 費馬又是這麼輕描淡寫地說他可以證明, 使數學家們忍不住也要試試。

十九世紀與費馬最後定理有關的一些重要事件如下。

1.西元1816年法國科學院提供獎金徵求費馬最後定理的解答。

2.西元1820年代, 著名的女數學家Sophie Germain證出, 若p 與$2p+1$皆爲質數, 則當$p\nmid xyz$時, $x^p+y^p=z^p$無解(即無非零整數解)。此稱爲費馬最後定理的第一情況。當$p|xyz$ 稱爲第二情況, 一般視爲難多了的情況。

3.西元1825年, Dirichlet (1805-1859)及Legendre (1752-1833) 分別獨立地證出$n=5$ 的情況。

4.西元1832年, 在試圖證明$n=7$的情況時, Dirichlet證出$n=14$的情況。

5.西元1839年Lamé (1795-1871)證出$n=7$的情況。

6.西元1847年,Lamé與歌西(Cauchy, 1789-1857)對一般的n給出證明, 只是他們的證明是錯的。

7.西元1847年, 德國數學家Kummer (1810-1893)定義所謂正則質數(regular primes)。他利用他所提出的理想數理論(theory of ideals), 可以證明$n<100$ 的正則質數的情況, 除了$n=37,59$及67等三個非正則質數(irregular primes)。

8.西元1850年, 法國科學院再度提供獎金, 此第二次懸賞吸引了不少人來應徵, 包括一些未受過數學訓練的冒險家。

9.西元1856年, 在歌西之建議下, 法國科學院撤消獎金, 並頒給Kummer一獎牌。

10.西元1857年, Kummer證明發展出複雜的方法來證明非正則質數的

情況。其證明中有些漏洞, 但在西元1920年代, 被Yandiver補起來。因此費馬最後定理對$n < 100$便皆成立。

自歐拉起, 與費馬最後定理打交道的著名數學家很多, 但都無法證出。難道這麼多一流的數學家的才智都比不上費馬嗎? 不少人懷疑費馬到底會不會證? 或此結果根本是錯的? 因費馬的確也犯過錯, 就是他推斷所有費馬數皆爲質數。如前所述, 對於費馬數, 他只檢驗至F_4就做了推斷, 結果卻是錯的。而對於$x^n + y^n = z^n$, 他也只證出$n = 3$及$n = 4$時無正整數解,會不會又是做了一錯誤的判斷? 只是費馬的信用卻是很好(只犯過一個錯), 令數學家們不敢小覷。要推翻費馬的推斷, 只要找到一大於4的質數n, 及一組最大公因數爲1的正整數x, y, z, 滿足$x^n + y^n = z^n$(因若$x^n + y^n = z^n$, 則$(ax)^n + (ay)^n = (az)^n$, 故只要找最大公因數爲1的解即可。若找不到,$x^n + y^n = z^n$便無解了)。只是反例也一直找不到, 以前計算工具固然不發達, 近年來在快速計算機的幫助下, 仍找不到反例。至西元1992年, 確知在$n \leq 4{,}000{,}000$時, 費馬最後定理成立。可見反例並不容易找, 只是要以這樣的方式證出費馬最後定理成立, 自然是緣木求魚。

高斯曾在一封給朋友的信中提到, 他認爲費馬最後定理只是一孤立的問題, 對他並無特別的吸引力, 他可輕易地列出許多這類型的問題, 既無法證明也舉不出反例。高斯的判斷後來證實並不正確, 費馬最後定理並非一孤立的問題。例如, Kummer雖未能解決費馬最後定理, 但他引進了理想數(ideal number)的概念, 並引起了代數整數 (algebraic integers) 的研究, 並奠定代數數論(algebraic number theory)的基礎。所以對數學家而言, 費馬究竟會不會證費馬最後定理已不是很重要,但若能將它證出, 將是一件很大的成就。

西元1908年, 一愛好數學的德國富豪Wolfskehl捐出了十萬馬克設立Wolfskehl獎(Wolfskehl Prize), 做爲費馬最後定理之解答的懸賞(根據一些歷史學家的說法, Wolfskehl 有一度因厭世而很想自殺,後因投入費馬最後定理的證明, 而打消了自殺的念頭。於是他重寫遺囑,此獎金便是用來做爲酬謝此救他一命的難題), 條件是必須在西元2007年前給出正確解法。他並委託哥丁根大學負責評審。此獎的設立, 又引起了成千上萬的人投入, 單單在西元1908年至1911年間便有1,000封應徵的信。也造成數學家的災難, 經常要讀一大堆荒唐無比的證明。第一次世界大戰後, 馬克

大幅度地貶值,但並未減少各種古怪的解答之投入。有一位數學教授他標準回覆信的開頭爲"Your first mistake is on page ⋯ "。當然大家也逐漸發現, 如果想發財, 做任何事都比解費馬最後定理還容易。

就在Wolfskehl獎鼓舞許多業餘數學與費馬最後定理奮戰的那段時期, 職業數學家卻多半做壁上觀。曾有人問著名的德國數學家Hilbert (1862-1943),爲何他從未去嘗試?他答"在著手嘗試前, 我必須先花三整年的預備工作, 但我沒有那麼多時間來浪費在一很可能失敗的嘗試"。那時期的數學家, 雖認爲費馬最後定理爲數論中的一核心問題, 但視此問題卻有如化學家之看待煉丹術(alchemy)。

第二次世界大戰後, 陸續有一些數學家專研費馬最後定理, 也逐漸有了一些進展。眞正吸引數學家致力於費馬最後定理的研究之原動力, 絕對不是金錢, 而是那份好奇心, 那種對揭開大自然之奧祕的渴望。

費馬最後定理的探討, 不但激發許多數學領域的發展, 也成爲數學中許多猜想 (conjecture)的試金石: 如果某猜想是正確的話,則費馬最後定理成立。這些猜想或有可能找到其他的驗證方式, 但費馬最後定理卻是最有意思的一個。

西元1993年6月23日, 出生於英國劍橋(Cambridge)並於1977年獲劍橋大學 (Cambridge University) 博士學位, 自1982年起任教於美國普林斯頓大學 (Princeton University) 的Andrew J. Wiles, 在母校劍橋大學宣佈他證出了費馬最後定理。Wiles 在那爲期一週有關主題爲"p-adic Galois representations, Iwasawa theory and the Tamagawa number of motives"的研討會上發表一篇論文,題目爲"Modular forms, elliptic curves and Galois representations"(橢圓曲線模式與Galois 表現), 費馬最後定理爲其結果之一推論。由研討會的主題及Wiles 的演講題目, 可看出費馬最後定理的證明並不易爲一般人所能了解。

此消息立即傳遍全世界, 各傳播媒體也立即報導此消息。許多數學家也以爲終於可喘一口氣,因他們過去常會收到宣稱證出費馬最後定理的來信, 而那些證明當然是錯的。

Wiles的整個證明非常複雜, 不僅用到過去幾十年裡代數數論與算術幾何學家所發展出來的龐大理論, 也包含不少新的想法。即使是這一行的專家, 也無法在短時間內完全了解其整個證明。香港中文大學還在西

元1993年12月18日至21日舉行一"橢圓曲線與模式研討會", 邀請一些專家就Wiles的工作做系統性的介紹。又Wiles的證明寫成一200頁的論文, 顯然不是費馬書上的頁邊容納的下的。

Wiles小時候便曾試圖去證明費馬最後定理。西元1963年, 10歲的他從當地圖書館讀到此問題, 便下定決心要證出來。學校的老師勸他不要浪費時間在此不可能的問題。升大學後, 老師亦勸阻他。直到進入劍橋大學的研究所, 指導教授Coates帶領他跨進屬於數學主流的橢圓曲線(elliptic curves), 開拓了他的視野, 終於有了日後的突破。當Wiles成爲一職業數學家後,起初他認爲費馬最後定理只是一孤立的難題, 能證出固然很好, 但並非眞很重要, 除了它很有名外。但當他讀了Ribet在西元1986年的工作後, 他決定致力於費馬最後定理的證明。經過七年的時光, 終於完成此兩百頁的論文。當然其他數學家的努力, 爲Wiles所鋪下的路, 其功勞也是不容忽視的。幸好在學術裡一向重視每個人的貢獻, 不會有一將功成萬骨枯的情況。

有趣的是, 此事仍有餘波, 稍後Coates 教授宣稱Wiles 之證明中有一小漏洞。他說要補上此漏洞並非易事, 可能要花數個月至數年的時間。Wiles 在1993 年12 月4 日承認他先前描述的結果有漏洞, 但他相信他仍可在短期內加以修正。在西元1994 年10 月7日, Wiles 完成了兩篇論文稿, 後來均發表於西元1995年的Annals of Mathematics, 這是數學中最好的期刊, 其一爲Modular elliptic curves and Fermat's last theorem, 有109頁, 以及他與學生R. Taylor合著的Ring-theoretic properties of certain Hecke algebras, 有20頁。第一篇論文證明了半穩定情形的Taniyama-Shimura-Weil猜想, 此結果可導出費馬最後定理。第一篇論文中關鍵步驟之一要用到第二篇論文。

經由電子郵件(e-mail), Wiles的論文迅速地傳到世界各地的專家手上, 讀過此二論文的數學家均認爲Wiles這回的證明是正確的。此一三百餘年來的懸案,終於告一段落。對費馬最後定理有興趣的讀者可參考康明昌(1985)、姚玉強(1993)、余文卿 (1994)、李文卿 、余文卿 (1994)、于靖(1994)、余文卿(1995)、Cook (1994)及Cox (1994)。Stewart (1993)是一篇較通俗的文章, 藉一教授與坐時光隧道機回來的費馬之對話, 介紹過去三百多年來費馬最後定理之探討的演變, 有趣且易讀。Cipra (1993)一

文發表於通俗性的科學刊物Science, 並列出近年來在該刊物發表之關於費馬最後定理的一些文章。Singh and Ribet (1997) 一文也頗值得一讀,淺顯有趣, 且將問題的來龍去脈, 交待得很清楚。Aczel (1996)則是一本很好的回顧性的專書, 林瑞雲譯(1998) 爲其譯本。通俗的中文書籍中, Singh原著, 薛密譯(1998), 一書包含不少相關文件, 想了解此問題之解決過程的讀者不妨一讀。

附帶一提, 西元1974年,出生於英國, 37歲的哈佛大學 (Harvard University)的Mumford (1937-), 他以代數幾何的工具證明了當$n \geq 3$, 如果$x^n+y^n=z^n$有正整數解, 則解一定"非常的少",因而獲得每4年頒發一次的數學界的極高榮譽費爾茲獎 (Fields Medal)。另一位因研究費馬最後定理而獲費爾茲獎(西元1986年)的爲出生於德國, 普林斯頓大學的Faltings (1954-)。他證明對一固定的$n \geq 3$,(2)式只可能有有限多組最大公因數爲1的解。費爾茲獎一向只頒給四十歲以下的數學家(見"數學與諾貝爾獎"一文)。Wiles出生於西元1953 年4 月11 日,由於解決費馬最後定理時超過40歲(如果他1993年的結果沒有漏洞就好了), 所以無緣獲費爾茲獎, 殊爲可惜(但在西元1998年, 於柏林舉行的國際數學家會議 (International Congress of Mathematicians), 他獲得首度頒發的一個特別獎)。在西元1996 年3 月24 日, 他與設在普林斯頓大學內的高等研究所(Institute for Advanced Study)的Robert P. Langlands教授,同獲當年的Wolf獎(Wolf Prize, 見"數學與諾貝爾獎"一文)。由以色列總統Weizmen在耶路撒冷 (Jerusalem) 的國會大廈頒獎, 兩人均分10萬美金。Langlands於西元1936年出生於加拿大 的英屬哥倫比亞(British Columbia), 1960年獲美國耶魯大學 (Yale University) 的博士學位。Wolf獎爲當今學術界極爲重要的一大獎。Wiles以他在數論和相關領域的傑出貢獻, 在某些基本猜想上所做的重大推進, 及解決費馬最後定理(for spectacular contributions to number theory and related fields, for major advances on fundemental conjectures, and for settling Fermat's Last Theorem)的成就得到此殊榮, 成就獲得肯定。他們二位得獎的相關資料見1996年2月號的Notices of the American Mathematical Society , pp.221-222: Langlands and Wiles Share Wolf Prize 一文。

在費馬最後定理的成就, 使Wiles在得Wolf獎之後, 又於同年得美

國 國家科學院數學獎 (National Academy of Sciences Award in Mathematics)。此獎是美國數學學會爲紀念該學會成立100周年,而於西元1988年設立。每四年頒發一次, 獎勵過去十年內發表的傑出數學研究成果。與Wiles合得Wolf獎的Langlands (1988)爲首位得獎者, Robert D. MacPherson (1992) 爲第二位得獎者。西元1997年, Wolfskehl 獎也在哥丁根大學頒給Wiles。這筆在當年頗高的獎金(依今日的幣值約爲二百萬美元), 經過90年的通貨膨脹及馬克 的貶值, 只餘5萬美元。Wiles尚得過不少獎, 包括獲1997年Frank Nelson Cole Prize in Number Theory (關於此獎見"完全數與梅仙尼質數"一文), 及1998 King Faisal International Prize for Science, 獎金20 萬美元。這是爲紀念沙烏地阿拉伯(Saudi Arabian) 已去世的國王Faisal(費瑟)而設的。Wiles的指導教授Coates, 還在西元1996年7 月號的Notices of the American Mathematical Society, pp.760-763, 描述Wiles的研究工作。

5 結語

你對費馬是否產生景仰之心呢? 一位專業的律師居然可對數學界產生如此大的影響。是否更鼓勵你學習題數學呢? 二十世紀以來費馬最後定理的進展以及Wiles的論文, 由於都牽涉到複雜及深奧的理論, 我們自然無法在這篇通俗性的文章中多加著墨。

今日數論的研究與複變函數論及橢圓曲線等均有密切的關係, 此現象是有些令人驚訝, 因整數是離散的(discrete), 但複數及曲線皆爲連續的。另外, 歐拉曾對費馬最後定理猜測可有下述推廣: $x_1^n+x_2^n+\cdots+x_m^n = y^n$, 其中$1 < m < n$,$n \geq 3$, 無非零整數解。約兩百年後, 在西元1967年, Lander與Parkin 給了一反例:

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5 \text{ 。}$$

後來對$n = 4$, Elkies亦給了一反例:

$$2{,}682{,}440^4 + 15{,}365{,}639^4 + 18{,}796{,}760^4 = 20{,}615{,}673^4 \text{ 。}$$

不過$n = 3$時此猜測(含在費馬的猜測中)卻是正確的(見Siu (1995))。

近年來, 美國德州(Texas) Dallas當地最大銀行的總裁Beal, 他一向喜歡解腦力遊戲及數學謎題, 也提出費馬最後定理的另一版本, 並懸賞給第一位證出的人。Beal是在Wiles宣佈其證法後才第一次聽到費馬最後定理。在試圖給一較簡單的證明時, Beal想到若允許次方可以不同, 即考慮

$$a^x + b^y = c^z, \tag{14}$$

則此式之解會是如何?這種式子有無限組整數解, 如

$$17^4 + 34^4 = 17^5, \quad 33^5 + 66^5 = 33^6$$

等(你是否看出這些解的共同性質?)。但若a, b互質, 且$1/x+1/y+1/z < 1$, 則目前僅知10組解:

$$\begin{aligned}
1^n + 2^3 &= 3^2 (n \geq 3), \\
2^5 + 7^2 &= 3^4, \\
7^3 + 13^2 &= 2^9, \\
2^7 + 17^3 &= 71^2, \\
3^5 + 11^4 &= 122^2, \\
17^7 + 76{,}271^3 &= 21{,}063{,}928^2, \\
1{,}414^3 + 2{,}213{,}459^2 &= 65^7, \\
43^8 + 96{,}222^3 &= 30{,}042{,}907^2, \\
33^8 + 1{,}549{,}034^2 &= 15{,}613^3, \\
9{,}262^3 + 15{,}312{,}283^2 &= 113^7 \text{。}
\end{aligned}$$

Beal懸賞5,000美元給第一位證出"當a, b, c爲互質正整數, 且正整數$x, y, z \geq 3$, 則(14)式無解"的人。此獎金每年增加5,000美元, 直到五萬美元的上限。各位可看出費馬最後定理爲Beal定理之一特例。你要不要試一試?若欲對本問題進一步了解, 可參考Mackenzie (1997), 及Mauldin (1997)。

最後, 數論中仍有許多敘述極簡單的猜測尚未解決。例如, Goldbach在西元1742 年, 寫了一封信給歐拉, 問他能否證明每一大於2之偶數都可

寫成二質數之和? Goldbach 在數學上並無特殊的成就, 卻因這封信而留名, 此尚未能解決的命題就被稱爲Goldbach猜測。如果你依序檢驗可得$4=2+2, 6=3+3, 8=5+3, 10=5+5=3+7, 12=5+7, 14=7+7=3+11, \cdots$, 有些數且有不只一種的表示法。Goldbach 猜測至今仍未爲被證實, 其困難的主要原因爲, 質數是屬於"乘性", 而Goldbach 的猜測則屬"加性"。一般而言, 我們對整數的乘法及加法之間的關連仍不十分清楚。不過此問題亦已有一些部分的結果, 可參考波蘭數學家Sierpinski著之"A Selection of Problems in the Theory of Numbers",此爲一本淺顯易讀的數論方面的入門書(林聰源譯(1976))爲該書之中譯本; 或陳景潤、邵品琮 (1987), 該書指出著名數學家華羅庚 (1910-1985) 及陳景潤等人, 在此問題上也有傑出的貢獻。另外, Niven and Zuckerman (1969) 也是一本很好的數論的入門書。

習　題

1. 試證若s, t爲二互質正整數,且設正s邊及正t邊形皆可作圖,則正st邊形亦可作圖。

2. 試證目前所能作出的奇數正多邊形共有31個。

3. 設書一本80元,筆一枝50元,現有810元,可買書及筆各若干?

4. 試證$x^2-3y^2=17$沒有整數解。

5. 試證$x^2+5=y^3$沒有整數解。

6. 試證$x^3+y^3=2z^3$只有一組最大公因數爲1的正整數解,並給出此組解。

7. 費馬曾宣稱$x^3=y^2+2$只有二組整數解,歐拉並給了一(並不完整的)證明。試找出此二組解。

8. 費馬數成長極快。有人曾這樣形容:若將F_{73}這個數印出來並裝訂成冊, 則全世界沒有一個圖書館容納的下。請加以解釋。

9. 試說明爲何(14)式有無限組整數解。

參考文獻

1. 于靖(1994). 費瑪最後定理的解決。數學傳播季刊,第18卷第4期, 46 。

2. 余文卿(1994). 費瑪最後定理 。數學傳播季刊,第18卷第2期, 32-41 。

3. 余文卿(1995). 費瑪最後定理的過去、現在與未來。自然科學簡訊,第7卷第1期, 19-21 。

4. 李文卿、余文卿(1994).費馬最後定理:A Wiles 的解決方法。數學傳播季刊,第18卷第2期, 42-47 。

5. 林瑞雲譯(1998). 費馬最後定理 。時報文化出版企業股份有限公司, 台北 。

6. 林聰源譯(1976). 整數論的問題 。楓城出版社, 新竹 。

7. 姚玉強(1993). 費瑪猜想 。九章出版社, 台北 。

8. 陳景潤、邵品琮(1987). 哥德巴赫猜想 。九章出版社, 台北 。

9. 康明昌(1985). 幾個有名的數學問題。中央研究院數學研究所, 台北 。

10. 薛密譯(1998). 費瑪最後定理 。台灣商務印書館, 台北 。

11. Aczel, A. D. (1996). *Fermat's Last Theorem, Unlocking the Secret of an Ancient Mathematical Problem.* Four Walls Eight Windows, New York.

12. Cipra, B. (1993). Fermat's last theorem finally yields. *Science* 261, 32-33; July 2.

13. Cook, R. (1994). Fermat's last theorem —a theorem at last. *Mathematical Spectrum* 26, 65-73.

14. Cox, D. A. (1994). Introduction to Fermat's last theorem. *The American Mathematical Monthly* 101, 3-14.

15. Mackenzie, D. (1997). Number theorists embark on a new treasure hunt. *Science* 278, 1396.

16. Mauldin, R. D. (1997). A generalization of Fermat's Last Theorem: the Beal conjecture and prize problem. *Notices of the American Mathematical Society* 44, 1436-1437.

17. Niven, I. and Zuckerman, H. S. (1969). *An Introduction to the Theory of Numbers*, 2nd ed. John Wiley and Sons, New York.

18. Ribenboim, P. (1996). *The New Book of Prime Number Records,* 3rd ed. Springer-Varlag, New York.

19. Singh, S. and Ribet, K. A. (1997). Fermat's last stand. *Scientific American* 277, No.5, 68-73.

20. Siu, M. -K. (1995). Euler and heuristic reasoning. In *Learn From the Masters* (Edited by F. Swetz, J. Fauvel, O. Bekken, B. Johansson and V. Katz). The Mathematical Association of America, Washington, D. C.

21. Stewart, I. (1993). Fermat's last time-trip. *Scientific American* 269, No.5, 112-115.