幾個有名的數學問題(一)

Fermat問題(上)

康明昌

一、前　　言

二十世紀的今天仍然有人在解古希臘幾何三大問題，有人窮畢生之力研究方程式解的公式，也有人在搜集畢氏定理的各種證明，據說多達七、八十種。這些人多半是玩票性質的「數學家」，他們從小對數學很感興趣，並且往往頗有天分，可惜陰錯陽差，未能獲得完整的高等數學訓練，因此對於近世數學的內容與精神不甚清楚。他們可能在中學聽過數學老師講古希臘幾何三大問題、Fermat 問題、Goldbach 問題、四色問題，老師可能還鄭重其事的告訴他們：「如果能夠解決以上任何一個問題，你就可以一夜成名天下知。」從此他們就對這些問題一往情深的窮追不捨。

可是當他們把心血結晶公諸於世時，眞正數學家的反應卻是出奇冷淡。什麼原因呢？有人說是同行相忌，有人說是門戶之見，也有人說他們把精力用在丙個完全錯誤的地方。

十九世紀以來，數學的進步實在不是「一日千里」四個字所能形容的。如果有人告訴一個「業餘數學家」，他所認識的數學基本上不超出十八世紀Euler（1707～1783年）的範圍，「業餘數學家」一定不願意承認，並且以爲這種講法侮辱了他。有人可能認爲自己唸過「新數學」，應該跟得上時代潮流了吧。呵！我眞希望似商品出售的「新數學」能夠經久耐用，不要像泡泡糖一樣，咀嚼幾次就被吐掉了！

本系列文章準備討論幾個有名的數學問題，如Fermat 問題、古希臘幾何三大問題、方程式求解問題。這些問題都是初等的問題（elementary problems），也就是說只要具備高中程度的數學知識，就能夠了解與欣賞這些問題，也能夠自己動手研究這些問題。可是有多少人知道，幾個世紀以來數學家在研究這些問題的過程中已經走了多少路？開闢了多少新世界？發展了多少新工具？並且數學家對

於這些問題的基本看法也一直在變動中。例如,在傳統高中代數的課程裏,恆等式的證明(即式子的變換)是一項重要的訓練;但是二十世紀的數學並不強調這種訓練,而把重點放在運算律及其基本性質。因此,如果有人宣稱他求出一種簡便的三次方程式根的公式,對十六世紀的Francois Viète (1540～1603年)而言,可能是令人感興趣的成果,但是二十世紀的數學家或許只能很禮貌的說:「好極了,了不起的發見,就像有人想出某些口訣來幫助小學生更迅速的背誦九九乘法表。」

有天分的年輕人,如果對數學有興趣,不要把寶貴的時間浪費在沒有意義或已經解決的問題。在邁開脚步之前,能夠擡眼觀察一下,前人走過多少路、走過那些路,大概是不會有害的。

本文是本系列文章的第一篇,主題是Feamat 問題。Fermat 問題是整數論(Theory of numbers)的一個問題。

整數論的目的在研究整數的基本性質,例如:

- 那些整數可以寫成 x^2+3y^2 的形式,其中 x 與 y 都是整數?如,

$$7=2^2+3\cdot 1^2$$
$$11\neq x^2+3\cdot y^2$$

- 是不是所有的正整數都可寫成四個整數的平方和(如,$7=1^2+1^2+2^2$)?有幾種不同的寫法?

- 形式如 $4n+3$ 的質數,如 3, 7, 11, 19, …,是不是有無窮多個?

- 能否用已知的函數(如,多項式或對數函數)來描述質數的分布情形?

有歷史記載以來第一個研究整數論的,是亞歷山大城的Diophantus (約250～350年)。他的著作「Arithmetica」總共十三卷,但是希臘文本只有六卷流傳後世,直到最近才發現另有四卷尚存阿拉伯文譯本。這本書收集許多問題及其解法,假如,有一種問題是:求一組非零的有理數 x, y,滿足 $x^2-26y^2=1$。讀者願意做一做這個問題嗎?(註一)

Diophantus 的工作並沒有激發更進一步的研究,直到十七世紀Pierre de Fermat (1601～1665年)才突破了Diophantus 的局限,建立了近代整數論的基礎。此後由於Leonhard Euler、Joseph Louis Lagrange (1736～1813年)、Carl Friedrich Gauss (1777～1855年)、Adrien Marie Legender (1752～1833年)的苦心經營,整數論終於變成近代數學的一支主流。Gauss 曾經說:「數學是科學的女皇,而整數論是數學的女皇。」

整數論有許多難題,到現在還無法解決。例如:

1. Fermat 問題:若 n 是任意大於 2 的整數,方程式 $x^n+y^n=z^n$ 沒有全異於零的整數解。

2. Goldbach 問題:任意大於 2 的偶數都可寫成兩個質數的和。

3. Catalan 問題:若 x, y, $m>1$, $n>1$ 都是正整數,則方程式 $x^m-y^n=1$ 的解只有 $x=3$, $y=2$, $m=2$, $n=3$。

以上三個問題不知耗費多少數學家的心力,卻始終得不到證明(註二)。正因爲這三個問題太淺顯易懂,有些「業餘數學家」不免見獵心喜,慨然以解決這些問題爲終身職志。如果他們知道專業數學家,曾經使用多少精妙艱

深的方法，試圖解決這些問題的話，大概會嚇一大跳。看來毫不起眼的問題，背後卻隱藏那麼多機關！

Fermat 問題是本文的中心題目。

二、什麼是Fermat問題？

法國數學家Pierre de Fermat（1601～1665 年）是一個有多方面才能的法官，他研究過希臘語言，也寫過詩，但是他在數學上的成就最大。Fermat 和René Descartes（笛卡爾，1596～1650 年）分別創建了解析幾何，他在微積分的創建與光學的研究上，卻曾有卓越的貢獻，他更是近世整數論的開山祖師。

Fermat 問題就是研究方程式 $x^n + y^n = z^n$ 的整數解。請注意幾個例子：

$$0^3 + 2^3 = 2^3$$
$$0^4 + 3^4 = (-3)^4$$
$$5^7 + (-5)^7 = 0$$

因此，在討論 Fermat 方程式 $x^n + y^n = z^n$ 時，我們眞正有興趣的是全異於零的整數解。先考慮 $n = 2$ 的情形，

$$3^2 + 4^2 = 5^2$$
$$5^2 + 12^2 = 13^2$$

因此，Fermat 方程式的確可能有全異於零的整數解。所謂Fermat 問題，就是想證明：

若 n 是任意大於 2 的整數，則方程式 $x^n + y^n = z^n$ 沒有全異於零的整數解。

在Fermat 的時代，除了 Fermat 之外，幾乎沒有人對整數論感到興趣。譬如 Blaise Pascal（1623～1662 年）是一個絕頂聰明的人，可惜他對整數論的問題興緻不高，更妙的是 Pascal 最後竟發現神學比數學還有趣。因此 Fermat 雖然發見了很多整數論的定理，卻只能孤芳自賞。這種情形或許可以說明，Fermat 爲什麼不愛把這些定理的證明寫下來。（註三）其實，Fermat 留下證明的整數論定理只有兩個，一個是：方程式 $x^4 + y^4 = z^4$ 沒有全異於零的整數解；另一個是：聯立方程式 $x = 2y^2 - 1$，$x^2 = 2z^2 - 1$ 只有當 $x = 1$ 或 7 時有整數解。

Fermat 在研究Diophantus 的著作「Arithmetica」時，曾在該書的空白處留下一段話。他說：

>「任何立方數（即，可以表示成 x^3 的數，其中 x 是整數）絕不能拆能兩個立方數的和。四方數亦然。更一般的，n 方數都如此，只要 $n \geqslant 3$。我發現一個精妙絕倫的證明。可惜在這兒寫不下。」

這就是Fermat 問題的來源。

Fermat 這本藏書現在早已失落了。Fermat 死後，他的兒子把他所有的數學文稿整理出版，數學家才知道，Fermat 已經開闢了一個新世界——整數論。

Fermat 自稱能夠證明的整數論定理，除了兩個例外，後代的數學家都能提出證明。這兩個例外，一個是錯的（見本文第 8 節），另一個就是 Fermat 問題，沒有人能夠證明或提出反例。正因爲Fermat 問題是 Fermat 留下的定理中最後一個還沒有解決的，所以有人把它叫做Fermat 最後定理（Fermat last theorem）；把它叫做定理，是有一點冒險，因爲到目前爲止並沒有人能夠證明它。

1816 年與1850 年巴黎科學院兩度提供3,000 法郎獎金，徵求Fermat 問題的答案，但是毫無結果。自Euler 算起，曾經和Fermat 問題打過交道的有名數學家不勝其數：例如，Gauss, Dirichlet, Legendre, Lamé, Kummer 分別做出幾個特殊情形；Euler, Germain, Abel 做出某些特殊情形的部分結果；而Cauchy 卻不幸從一開始就走錯了路。

這麼多的一流數學家竟然會比不上一個 Fermat 嗎？因此，有人開始懷疑是不是 Fermat 自己的證明也不完全？這個定理會不會根本就是錯的呢？有趣的是，到目前爲止，我們知道至少在 $3 \leqslant n \leqslant 125{,}000$ 時，方程式 $x^n + y^n = z^n$ 的確沒有全異於零的整數解（見本文第 7 節）。

從另一個角度來看，Fermat 問題究竟有什麼重要性呢？

Gauss 在給朋友的一封信說道：「Fermat 問題是一個孤立的問題，對我沒有特別的吸引。我很容易列舉一大堆這類型的問題，你既不能證明也提不出反例。」整數論的確有許多這種問題，例如，奇完全數的存在問題，Mersenne 數問題（註四）。研究這些問題的人，有時過度渲染它們，結果常把初學者引入牛角尖去，並且極易造成非數學家對數學價值的疑問。

但是偉大的 Gauss 這一次完全看走了眼。Fermat 問題並不是孤立的問題。Fermat 問題的探討很自然的引起代數整數（algebraic integers）的研究，因而創立了理想數（ideal numbers）的概念與代數數論（algebraic number theory）的基礎。從另一方面來看，Gauss 在同一封信說：「如果能夠進行二次、三次、四次互逆定律（reciprocity low）的推廣，則 Fermat 問題只不過是這種高次互逆定律所能推演出來的結果之一而已。」歷史證明 Gauss 只看到事物發展的一個方向，沒有看到另一個方向：Fermat 問題與高次互逆定律的研究其實是相互影響的。德國數學家 David Hilbert（1862～1943 年）在1900 年的巴黎國際數學會，提出 23 個尙未解決的數學問題，他預測這些問題的研究將構成二十世紀數學的主流。Hilbert 的第九個問題就是高次互逆定律的研究。

Fermat 問題的敍述是這樣的淺顯，不免使某些人想憑從高中數學學來的粗淺整數性質解決 Fermat 問題。我不能說這種戰術一定不能解決 Fermat 問題，我只想指出一點，嘗試解決 Fermat 問題過程中，所耗費的智力與精力遠非一般人所能想像。1982 年在美國西雅圖開了一次有關 Fermat 問題的會議，會議記錄「Number theory related to Fermat's last theorem」由 Birkhäuser 公司出版。只要翻一翻這本書的目錄，馬上能夠感覺出來 Fermat 問題對數論的影響是多麼深廣。

1908 年 Fermat 問題的研究再度掀起高潮。一個德國人 Paul Wolfskehl 捐了100,000 馬克，懸賞 Fermat 問題的完整解答，他委託 Göttingen 大學負責評審工作。應徵的論文必須刋登在數學期刋或自行印成專門著作的形式，然後向 Göttingen 大學提出申請。

這份獎金反而造成某些數學家的災難。1907 到 1908 一年之中，有 621 件應徵函件，不過全部是錯誤的。負責在這些滿紙荒唐言的論文中找出錯誤的數學家，一定是前世沒有積夠功德，今生才受此業報。

第一次世界大戰之後，馬克大幅貶值，這份獎金幾乎變成毫無價值。可是由於第二次世界大戰後西德的經濟復興，這份獎金在 1958 年還值 7,600 馬克，到1974年已積累至10,000 馬克左右（1 馬克滙率約爲 14.7 元新台幣）。

近年來 Fermat 問題每年的應徵函件，堆積起來仍有三呎高。評審的人員極感困擾。他們只好把應徵函件分成兩類，一類是完全胡說八道的，立即退回；另一類看來還有幾分像數學的，交給 Göttingen大學數學系研究生找出錯誤。

一位在評審小組工作的人說：「目前每個月大約總要收到三、四封信。

有些應徵者這麼說：『我現在只寄來答案的前半部，如果評審人員先寄 1,000 馬克過來，們才會把後半部寄出去。』也有人告訴我們，只要我們支持他的解答，他願意分給我們十分之一的獎金；否則，他寧可把解答投寄給蘇

聯的期刊，讓德國數學界分享不到這份榮譽，而大丟其臉。

這些所謂的解答，只不過動用了非常初等的數學知識，然而還是要花費極大的心神才看得懂在說什麼，才找得出錯誤何在。應徵者有不少受過專科教育，因爲在自己工作崗位上不受重視，希望藉解決 Fermat 問題成名。我拿過幾封應徵信給醫生看，醫生認爲寫信的人有嚴重的精神分裂症。」（註五）

三、方程式 $x^2+y^2=z^2$

我們先討論 $x^n+y^n=z^n$ 的整數解的基本性質。

性質1 如果 x，y，z 是滿足 $x^n+y^n=z^n$ 的整數，且 x，y，z 三數的最大公約是 1，則 x，y，z 兩兩互質。理由：若 e 是 x 與 y 的最大公約數，且 $e>1$，則 e 整除 $x^n+y^n=z^n$，故 e 與 z 不會互質。矛盾。

性質2 若 x，y，z 是滿足 $x^n+y^n=z^n$ 的整數，則必可找到另一組整數 u，v，w，使得 $u^n+v^n=w^n$，且 u，v，w 兩兩互質。理由：令 d 是 x，y，z 的最大公約數，$u=\dfrac{x}{d}$，$v=\dfrac{y}{d}$，$w=\dfrac{z}{d}$。

性質3 若 p 與 m 是正整數，且 $x^p+y^p=z^p$ 沒有全異於零的整數解，則 $x^{pm}+y^{pm}=z^{pm}$ 也沒有全異於零的整數解。

性質4 要解決 Fermat 問題只需證明：$x^n+y^n=z^n$ 沒有全異於零的整數解，其中 $n=4$ 或奇質數（不爲 2 的質數）。理由：任何一個大於 2 的整數必有一個因數是 4 或奇質數。

現在我們要找出 $x^2+y^2=z^2$ 的所有整數解。

定理1 $x^2+y^2=z^2$ 的互質整數解爲 $x=2uv$，$y=u^2-v^2$，$z=\pm(u^2+v^2)$，其中 u，v 是任意互質整數，且 u，v 不同時爲奇數。

証明1 令 x，y，z 是互質正整數，且 $x^2+y^2=z^2$。

若 x 與 y 都是奇數，則 z 是偶數。故 x^2+y^2 是 $4l+2$ 的型式，z^2 是 $4l'$ 的型式（l 與 l' 是整數）。矛盾。

因此，不妨假定 x 是偶數，y 與 z 是奇數。

由 $x^2=z^2-y^2=(z-y)(z+y)$，令 $x=2r$，$z-y=2s$，$z+y=2t$。得 $r^2=st$。

s 與 t 互質，因 y 與 z 互質。但 st 是完全平方。故 $s=u^2$，$t=v^2$。得證。

証明2 $x^2+y^2=z^2$ 的正整數解對應於 $A^2+B^2=1$ 的正有理數解。$A^2+B^2=1$ 的參數方程式是 $A=\dfrac{2T}{1+T^2}$，$B=\dfrac{1-T^2}{1+T^2}$。把 T 用 $\dfrac{v}{u}$ 代入，得 $x=2uv$，$y=u^2-v^2$，$z=u^2+v^2$。利用以上的想法，讀者請自己寫出一個完整的證明（註六）。

討論： 證明 2 其實是把 $x^2+y^2=z^2$ 的整數解看成代數曲線上的有理點。在本文第 5 節還會介紹第三種證明方法。這個定理雖然很簡單，我們卻不厭其煩的提出三個證明，原因是，第一個證明是算術的方法，第二個證明是從代數曲線的角度來進行的，第三個證明是從代數數論的角度來進行。

四、方程式 $x^4+y^4=z^4$

我們要證明方程式 $x^4+y^4=z^4$ 沒有全

異於零的整數解。事實上我們甚至可以證明

定理2 方程式 $x^4+y^4=z^2$ 沒有全異於零的整數解。

証明 令 x_1，y_1，z_1 是互質正整數，且 $x_1^4+y_1^4=z_1^2$。

由定理1，可設 y_1 是奇數，且 $x_1^2=2uv$，$y_1^2=u^2-v^2$，$z_1=u^2+v^2$，其中 u 與 v 是互質正整數。

因 $v^2+y_1^2=u^2$，y_1 是奇數，且 v，y_1，u 互質，故 v 是偶數（定理1），令 $v=2u$

代入 $x_1^2=2uv$，得 $(\frac{x}{2})^2=uw$。因 u 與 w 互質，且 uw 是完全平方。故 $u=r^2$，$w=s^2$，$v=2w=2s^2$。很顯然的，$r<r^2=u<u^2+v^2=z_1$（$u\neq 1$，因爲 $u>v$）。

將 u 與 v 的值代入 $y_1^2=u^2-v^2$。得

$$(2s^2)^2+y_1^2=(r^2)^2$$

故

$$2s^2=2ab$$
$$y_1=a^2-b^2$$
$$r^2=a^2+b^2$$

其中 a 與 b 互質。

由 $s^2=ab$ 得 $a=x_2^2$，$b=y_2^2$，其中 x_2 與 y_2 互質。將 a 與 b 之值代入 $r^2=a^2+b^2$，並令 $z_2=r$，得

$$x_2^4+y_2^4=z_2^2\text{，且 } z_2<z_1$$

以上步驟其實證明一件事：若（x_1，y_1，z_1）是方程式 $x^4+y^4=z^2$ 的一組互質正整數解，則必存在另一組互質正整數解，則必存在另一組互質正整數解（x_2，y_2，z_2），且 $z_2<z_1$。以次類推，必得到一個矛盾，因爲正整數數列 $z_1>z_2>z_3>\cdots\cdots$ 不可能是無限的。

討論：以上的方法，其實是「無窮遞減法」（method of infinite descent）的一個應用。這個方法是Fermat 最得意的發明。詳細的說，如果想證明有關正整數的性質 $p(n)$ 對於所有正整數 n 都成立（例如，$p(n)$ 代表 n 可以寫成四個平方數的和），我們只需證明：如果對於某一個正整數 n_1，$p(n_1)$ 是錯的，則必存在另一個正整數 n_2，$n_2<n_1$ 且 $p(n_2)$ 也是錯的。由此就可導出矛盾。

換另一種講法，「無窮遞減法」的原理是，如果 n_1 是 $p(n)$ 的最小反例（the minimal counterexample），我們只要找出 $n_2<n_1$，使得 $p(n_2)$ 也是一個反例，就得到一個矛盾。由此看來，「無窮遞減法」、「最小反例法」、「數學歸納法」，三者其實是同一種方法（註七）。

註　釋

註一 這個問題與求雙曲線 $x^2-26y^2=1$ 的參數方程式有關。令 $x=1+ty$，得

$$y=\frac{2t}{26-t^2}\text{，}\quad x=\frac{26+t^2}{26-t^2}$$

令 t 爲任意異於零之有理數，得一組異於零的有理數解。讀者如果求出

$$x=\sec\theta\text{，}\quad y=\frac{1}{\sqrt{26}}\tan\theta$$

的參數方程式，對這個問題的求解有沒有幫助？

註二 關於Goldbach 問題，陳景潤在 1973 年證明：任意足夠大的偶數都可寫成質數與至多兩個質數乘積的和。關於 Catalan 問題的背景，請參考 A. Baker, Some historical remarks on number theory, Historia Mathematika 2（1975）549～553。

註三 見 A. Weil, Two lectures on number theory : past and present, Enseign. Math. 20（1974）215～222。

註四 這些問題的價值有待商榷，因此作者不願介紹其內容。好奇心特別強烈的讀者

可參考Hua Loo Keng, Introduction to number theory, Springer, 1982, New York.

註五 見P. Ribenboim, 13 lectures on Fermat's last theorem, Springer, 1979, New York.

註六 令x，y，z是互質正整數，且$x^2+y^2=z^2$。仿證明1，可令x是偶數。

令$r=\frac{x}{z}$，$s=\frac{y}{z}$。得$r^2+s^2=1$。

$\frac{r}{1-s}=\frac{1+s}{r}$，令其比值爲$t$，$t$是有理數。解$r=(1-s)t$，$1+s=rt$；得$r=\frac{2t}{1+t^2}$，$s=\frac{1-t^2}{1+t^2}$。

令$t=\frac{v}{u}$，u與v互質，得

$$\frac{x}{z}=r=\frac{2t}{1+t^2}=\frac{2uv}{u^2+v^2}$$

因x與z互質，且$2uv$與u^2+v^2互質，得$x=2uv$，$z=u^2+v^2$。（若$2uv$與u^2+v^2不是互質，則其公約數爲2，且u與v都是奇數，故$x=uv$，$z=\frac{u^2+v^2}{2}$，與x是偶數的假設違反。）

註七 請參考，康明昌，「數的極念」（上），「數學傳播季刊」 1982 年第四期。