DOI:10.6851/MSHCM.201907_(16).0005

數

黎貝談費馬最後定理

作者：黎貝（Kenneth Ribet） 譯者：張哲睿

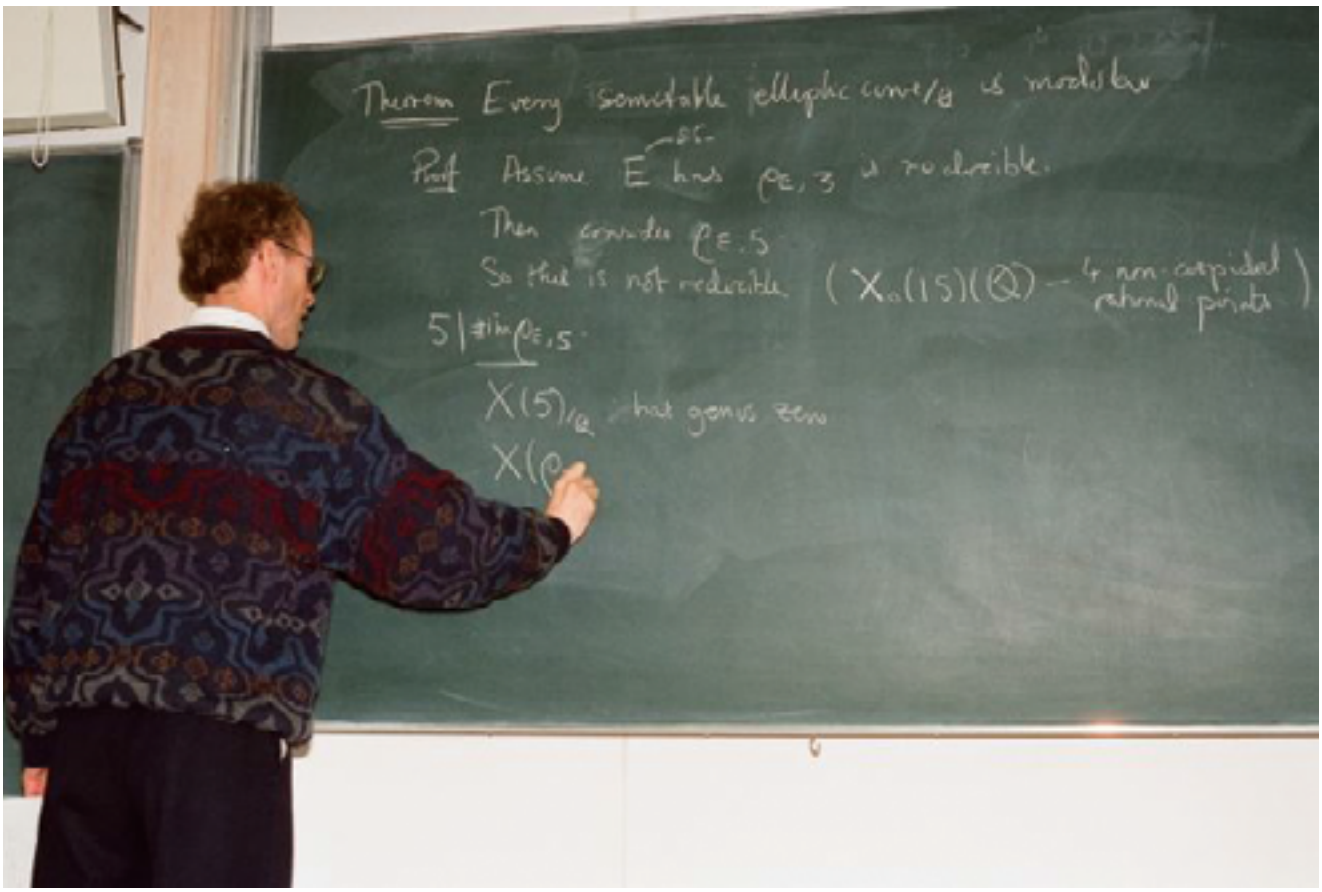
作者簡介：黎貝是加州柏克萊大學數學系教授，研究領域是代數數論與代數幾何。他也是在 2018 年底甫卸任的美國數學學會（American Mathematical Society，AMS）主席。他的許多研究成果為懷爾斯的費馬最後定理證明奠定了基礎。他經常參與各項關於費馬最後定理的教育推廣活動。

費馬最後定理是最著名的數學問題之一，雖然早在 17 世紀就由費馬（Pierre de Fermat）所提出，卻一直到 1994 年才得到證明。在尚未解出費馬最後定理的 350 多年之間，人們為了要證明它而發展出了許多現代數學的重要分支，其中包括整個代數數論的領域。

1993 年 6 月 23 日，懷爾斯（Andrew Wiles）在英國劍橋的演講中發表了費馬最後定理的證明 ❶ 。雖然他當時給的證明有缺陷（或「不完整」），但懷爾斯和他的學生泰勒（Richard Taylor）在 15 個月後將原證明修正完成。由懷爾斯獨自撰寫的論文，以及他與泰勒合著的論文在 1995 年刊登在了同一期的《數學年刊》（*Annals of Mathematics*）。

要解釋費馬問題，自然而然要從完全平方數開始： $0, 1, 4, 9, 16, 25, \cdots\cdots$等等，任意挑選其中兩個數字相加，不太可能會得到另一個完全平方數；舉

❶ 編註：當天演講的題目是「模形式，橢圓曲線，與迦羅瓦表現」（Modular Forms, Elliptic Curves and Galois Representations）。懷爾斯也因證明費馬最後定理的貢獻，於 2016 年獲頒阿貝爾獎。



在劍橋演講的懷爾斯。

費馬。（維基）

例來說， $4+9=13$ 並不是一個完全平方數。但是「不太可能」並非意味著「不可能」；事實上，有些兩個完全平方數的和會是完全平方數，例如： $3^2+4^2=5^2$ ， $5^2+12^2=13^2$ ，……。畢氏三元數就是指滿足 $a^2+b^2=c^2$ 的三個整數 a,b,c ，因此由 $3^2+4^2=5^2$ 可以得知 $(3,4,5)$ 就是一組畢氏三元數。

挑戰：描述所有的畢氏三元數。

古希臘人想到的答案是這個：如果 n 和 m 是兩個滿足 $n>m$ 的正整數，則

$$(n^2-m^2)^2+(2nm)^2=(n^2+m^2)^2。$$

舉例來說，如果 $n=2$ ， $m=1$ ，則我們會得到三元數 $(3,4,5)$ ；同樣地，如果 $n=3$ ，$m=2$ ，則我們會得到三元數 $(5,12,13)$ 。希臘人同時也知道，將上述公式得到的三元數同時乘上一個整數或交換前兩個數字後，這個公式可以得到所有的畢氏三元數。要驗證這個事實，我們可以利用一個性質：如果兩個互質的正整數的乘積是完全平方數，則他們各自本來就是完全平方數。更精確來說，假使 $a^2+b^2=c^2$ ，則我們可以假定 a,b,c 兩兩互質。此外，我們也可以假定 a,c 是奇數而 b 是偶數，則 $\frac{c-a}{2}$ 和 $\frac{c+a}{2}$ 互質，由於他們的乘積 $\frac{b^2}{4}$ 是一個完全平方數，所以他們各自會是一個完全平方數：

$$\frac{c-a}{2}=m^2,\quad \frac{c+a}{2}=n^2。$$

所以我們得到 $a=n^2-m^2$ ， $c=n^2+m^2$ ，由此可知 $b^2=4n^2m^2$ ，因此 $b=2nm$ 。

費馬自問道：如果把平方改為立方、四次方、……等更高的次方，會發生什麼事呢？在費馬過世之後，他的兒子山姆爾（Samuel）發現他父親寫在書中頁邊的筆記，筆記中說道他已經證明如果 n 大於 2，則出兩個非零完全 n 次方數的話不會是一個完全 n 次方數。

若 n 是一個大於 2 的整數，

則方程式 $a^n+b^n=c^n$ 沒有正整數解。


Arithmeticorum Liber II. 61

QVÆSTIO VIII.

OBSERVATIO DOMINI PETRI DE FERMAT.

QVÆSTIO IX.

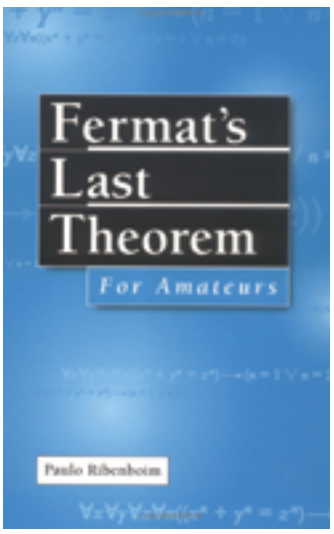
1670 年出版的丟番圖《算術》拉丁文譯本的第 16 頁，包含了費馬的評論「把立方分成兩個立方之和，或把四次方分成兩個四次方之和，或者更一般的將高於二的冪次分成兩個同冪次之和，都是不可能的。我發現了一個既正確又美妙的證法，但這裡頁邊太窄寫不下。」。（維基）

做為一個成熟的數學家，費馬寫下了「兩個非零完全四次方數的和不會是一個完全四次方數」的詳細證明；事實上，他證明的是更強的結果：$a^4+b^4=c^2$ 沒有非零整數解。他的證明用到的因式分解技巧就和我們先前遇到的一樣，再加上一個稱為「無窮遞降法」技巧，即現代數學家所認知的「數學歸納法」。

費馬之後的數學家們鑽研了費馬方程式 $a^n+b^n=c^n$ 於 $n=3$（歐拉）、$n=5$ 與其他 n 較「小」的情況。歐拉所考慮的情況 $a^3+b^3=c^3$，讓我想起了拉曼努真（Srinivasa Ramanujan）在 $a^3+b^3=c^3+d^3$ 的研究之一。一個很有名的故事是，當哈第（Godfrey Hardy）去醫院拜訪拉曼努真時，拉曼努真向哈第提到的一個巧合：

$$10^3+9^3=12^3+1^3$$ ❷

有一個強而有力的間接證據指出，事實上費馬想到的「證明」是錯的，其中一個線索就是費馬在四次方的情況中給的詳細證明。我們不確定費馬是否因意識到自己的錯誤，所以只能猜測原本的敘述是對的。因為理論上費馬還是可能有正確的證明，所以仍有許多業餘數學家持續的追求這座聖杯——找出費馬在費馬最後定理的原始證明。許多的數學期刊（特別是「數論」領域）幾乎每個月都會收到數十份自稱已經證明了費馬最後定理。



《給業餘者的費馬最後定理》的封面。

黎賓波因（Paulo Ribenboim）所著的《給業餘者的費馬最後定理》（*Fermat's Last Theorem For Amateurs*）是一本很精彩的書，推薦給想要以初等論述研究費馬最後定理的讀者。

文學作品中的費馬最後定理

在許多的書籍或電視上常常可以找到一些暗指費馬最後定理的橋段：

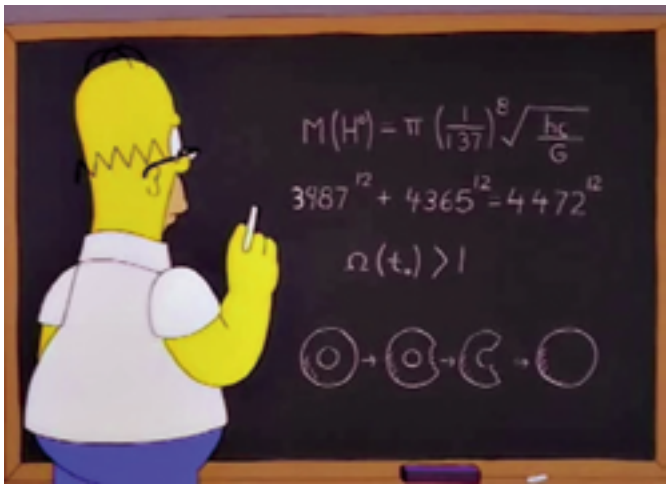
在已故的瑞典著名作家拉森（Stieg Larsen）的暢銷小說系列「千禧年三部曲」中的第三部《直搗蜂窩的女孩》中有段「……莉絲・莎蘭德（Lisbeth Salander）在加勒比海的最後一個冬天花了好幾週狂熱地研究費馬最後定理。當她回到瑞典時……。」

在辛（Simon Singh）所著的《辛普森家庭與他們的數學秘密》（*The Simpsons and Their Mathematical Secrets*）書中也有數個關於費馬最後定理的橋段。例如最引人注目的是：

下圖中的第二式是荷馬（Homer）的費馬最後定理解答，但考慮這些數除以 3 的餘數就可以發現驗證荷馬的方程式是錯的：3987 和 4365 都是三的倍數，但 4472 並不是。

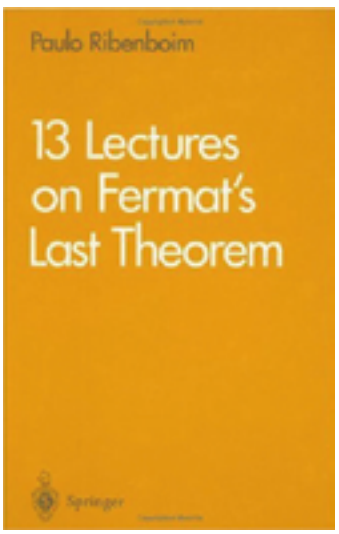
1980 年以前的研究

❷ 編註：此數 1729 亦稱為哈第 / 拉曼努真數，是能表示成兩種立方和的最小整數。



「辛普森家庭」第 10 季第 2 集的一幕。（YouTube 擷圖）

18 世紀時，歐拉（1707 ～ 1783）證明了任兩個非零的完全立方數之和不會是一個完全立方數。其他數學家繼續的將指數 3 改進到越來越大的指數，但也有很多人誤以為他們發現了完整的證明。直到 1979 年，這一路上成敗的故事可以在黎賓波因早期所著的《費馬最後定理的 13 堂課》（*13 Lectures on Fermat's Last Theorem*）找到。



《費馬最後定理的 13 堂課》的封面。

在懷爾斯的劍橋演講公布他的證明之前，布勒（Joe Buhler）、克蘭道爾（Richard Crandall）、艾恩瓦爾（Reijo Ernvall）與梅森克拉（Tuano Metsänkylä）已經用電腦計算證明出了費馬最後定定理於指數至多 $4,000,000$ 的情況。這代表著對於每個 $n \leq 4 \times 10^6$，不存在非零整數 a, b, c 滿足 $a^n + b^n = c^n$。

對於每個這樣的 n，(a, b, c) 的不存在性都是一個定理。而讓電腦可以證明這 $3,999,998$ 個定理是多虧了黎賓波因在他的兩本書所描述的一些技巧，而這些技巧則源自於 19 世紀庫默爾的貢獻。

當懷爾斯在 1993 年發表了完整定理的證明時，一個糟糕的新聞媒體問他：難道驗證了前四百萬個例子還「不夠好」嗎？如果一個論述對了四百萬次，難道還不能保證那個論述整體來說就是對的嗎？


庫默爾。（維基）

當然不能！舉例來說，費馬發現了 $x^2 - 109y^2 = 1$ 的第一個非零整數解是

$$(158070671986249, 15140424455100)。$$

而歐拉在 18 世紀猜想任何一個四次方數都不能寫成三個四次方數的和。他的猜想是錯的，但 $a^4 + b^4 + c^4 = d^4$ 的第一個非零整數解也一直拖到 1988 年才被發現，這是由哈佛的艾爾奇斯（Noam Elkies）找到：

$$2682440^4 + 15365639^4 + 18796760^4 = 20615673^4$$

順道一提，要找到以下類似方程的非零整數解也不是太難：

$$a^4 + b^4 = c^4 + d^4，$$

這個方程式是歐拉在 18 世紀所研究的，該方程的其中一個解是

$$59^4 + 158^4 = 133^4 + 134^4;$$

等號兩邊都等於 635318657 ❸

谷山 / 志村 / 威伊猜想

1993 年所發表的費馬最後定理證明是源於當時在德國薩爾布魯根（Saarbrücken）的數學家弗瑞（Gerhard Frey）的某項發現，他現在在德國埃森（Essen）。弗瑞大膽的猜測費馬最後定理其實可以和數論的一個重要猜想有關：橢圓曲線的模猜想（modularity conjecture for elliptic curves）。這個猜想（現在是定理！）說的是，每個橢圓曲線都可以用模形式表達。後面我會試著解釋這是什麼意思。

當我還是研究生時，模猜想是被稱為威伊猜想 (Weil's conjecture) 的。這是因為威伊在他的一篇著名文章中，解釋了如何可以由一個大家預期是正確的關於橢圓曲線的敘述中，推導得這個猜想的一個嚴謹版本論述。一個小問題是，威伊從未真正的敘述過這個猜想，甚至有傳聞指出他根本不覺得那是

❸ 編註：也是能表示成兩種四次方和的最小整數。

弗瑞（左）與作者（右）

對的。當時，谷山豐（Yutaka Taniyama）和志村五郎（Goro Shimura）❹ 也討論了與這猜想有關的問題，所以也有人把這個猜想稱為「谷山 / 志村 / 威伊猜想」。到了 1999 年，這猜想變為**模定理**（modularity Theorem，又稱谷山 / 志村定理）。

志村五郎與作者，1973 年。

從猜想到定理的時間軸線

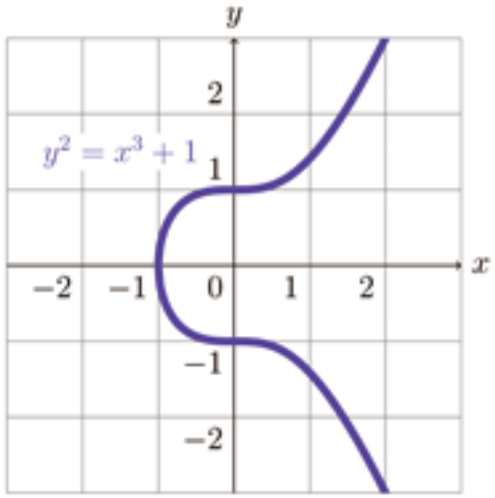
- 1980 年代早期：弗瑞建議了一個推導性證明

  模猜想 ⟶ 費馬最後定理

- 1985 年：塞爾（Jean-Pierre Serre）指出要有人可以證明一個模形式的困難問題，也就是 ϵ 猜想，那弗瑞的推論才有道理。
- 1986 年：我證明了塞爾的問題，因此弗瑞的推論是合理的。❺
- 1993 年：懷爾斯發表了關於模猜想的幾個重要特例證明，而那些特例就足以推得費馬最後定理。
- 1994 年：懷爾斯與泰勒將懷爾斯的證明修正完畢。
- 1995 ～ 1999 年：所有模猜想剩下的情況都被布勒伊（Christophe Breuil）、康拉德（Brian Conrad）、戴蒙德（Fred Diamond）與泰勒證明完成。

橢圓曲線

橢圓曲線是一個方程式如 $y^2 = x^3 + 1$ 或 $y^2 = x^3 - 17x - 3$ 等等的解集合，一般的方程式形式是 $y^2 = x^3 + ax + b$ 。

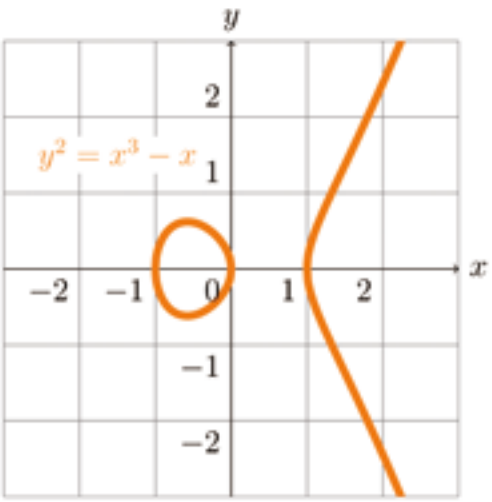


它在密碼學上有很廣泛的應用，你可以在網路上搜尋「橢圓曲線密碼學」來查證看看，事實上，橢圓曲線被用在很多純數學、應用數學甚至物理領域。

橢圓曲線和費馬方程式的連結其實非常簡單：如果 $a^n + b^n = c^n$ 的話，我們就寫下橢圓曲線

❹ 志村五郎於 2019 年 5 月 3 日在紐澤西的家中過世，享壽 89 歲。
❺ 編註：現在稱為黎貝定理（Ribet's theorem）。

$y^2 = x(x-a^n)(x+b^n)$ 。弗瑞直覺認為這個曲線不符合模猜想，而這就是我在 1986 年所證明的。



模猜想

我們用這個特別的橢圓曲線 $E : y^2 = x^3 - x$ 來解釋模猜想。考慮質數 $p = 3, 5, 7, \cdots\cdots$，對於每個質數 p ，我們考慮 E 在模 p 同餘之後定義的方程式。同餘是一個了解餘數的簡潔方式，當我們模 m 時，我們會去掉所有 m 的倍數。就如我同事所說的，模 5 就好像是留住 1 塊錢，並把所有的 5 元、10 元、50 元或以上的都丟掉。我們也會用模 12 的同餘來表示時間：24 小時制的 1400 代表的是 2 點（但我們通常會記得加「下午」）。

我們需要考慮的是質數模 4。質數們有 $2, 3, 5, 7, 11, \cdots\cdots$。除了 2 之外，其他的質數都是奇數，在模 4 之後，他們不是 1 就是 3（或可以說是 -1 ）。 $1 \bmod 4$ 的質數有 $5, 13, 17, \cdots\cdots$。$3 \bmod 4$ 的質數有 $3, 7, 11, 19, \cdots\cdots$。可以精確的說，大概有一半的質數是 $1 \bmod 4$ ，另一半是 $3 \bmod 4$ 。舉例來說如果去算所有小於 10^9 的質數中 $1 \bmod 4$ 的質數個數，並將他除以小於 10^9 的質數個數，則得到的比值會非常靠近 $1/2$ 。而隨著 $10^9 \to \infty$ ，該比值也會越來越靠近 $1/2$ 。這個事實是由狄利克雷在 19 世紀前半葉所證明。


狄利克雷。（維基）

回到 $y^2 = x^3 - x$ ：我們挑一個質數 p 並開始考慮模 p。我們整個世界就這樣變成了有限個數字：$0\ 1, \ldots, p-1$ ，這是因為我們不管所有 p 的倍數。因為現在這個世界只有 p 個數字的關係，我們會有 p^2 個模 p 數對 (x, y)。在這些數對中，只有相對少數會滿足 y^2 和 $x^3 - x$ 模 p 同餘。我們把這些符合的數對個數記錄下來，稱為 $N(p)$ 。舉例來說，令 $p = 5$ 。那滿足同餘的解有 $(x, 0)$ ，$x = 0, 1, 4$（三個數對）還有 $(2, 1)$ 、 $(2, 4)$ 、 $(3, 2)$ 以及 $(3, 3)$ 。全部總共有七個數對，所以 $N(5) = 7$ 。

以下是在比較小的 p 中 $N(p)$ 的樣子：

P	3	5	7	$\cdots$	17	19	23	29	31	37	41
$N(P)$	3	7	7	$\cdots$	15	19	23	39	31	37	41

以下的兩個敘述是由以上表格而來，而他們一般來說也是正確的。

- $N(p)$ 這個數字可以比 p 大，也可以比 p 小，但並不會誇張的遠離 p。事實上它們的差距最多只有 $2\sqrt{p}$（由哈塞證明的）。
- 那些滿足 $N(p) = p$ 的質數會是 4 的倍數少 1（也就是說，這些質數是 $3 \bmod 4$）。

因為 $N(p)$ 和 p 很靠近，傳統上我們會專注在他們兩個的差。我們令

$$a(p) := p - N(p)。$$

挑戰

為什麼當 $p = 3 \bmod 4$ 時，$a(p) = 0$ ？

為什麼當 $p = 1 \bmod 4$ 時，$a(p)$ 是偶數？

對於 $y^2 = x^3 - x$，模定理對於計算 $a(p)$ 來說是一個方法，或是公式。這個公式源自於高斯而且是相當明確的。對於 $p = 2$ ，我們可以直接考慮四種可能的 (x, y) 並直接計算 $N(p)$；當 p 是 4 的倍數少 1 時，我們可以得到 $a(p) = 0$，換句話說，就是 $N(p) = p$ ，這個的證明蠻基礎的；比較有趣的是剩下的情況：當 p 是 4 的倍數多 1 時。

讓我們重新做一個表格，並只列出那些 p ：

P	5	13	17	29	37	41	53	61
$\frac{1}{2}a(p)$	-1	3	1	-5	-1	5	7	-5

因為 $a(p)$ 的值都是偶數，所以我擅自把他們都除以 2 了。我們可以從表格猜測 $\frac{1}{2}a(p)$ 會是一個奇數 —— 但是哪個奇數呢？

可以注意到在表格中， $p - \left(\frac{1}{2}(a(p))\right)^2$ 會是一個完全平方數：

$$\ldots, 17 - 1^2 = 16, 29 - (-5)^2 = 4, 37 - (-1)^2 = 36, \ldots$$

這可是天大的新聞！因為費馬證明過：

定理：如果質數 p 是 4 的倍數多 1，則存在著一個正奇數 r 和正偶數 s 使得 $p = r^2 + s^2$ 。此外，的 r 和 s 還是唯一的。

作業

找找看一些以費馬最後定理推得「一個奇質數會是兩個完全平方數的和若且唯若該質數是 $1 \bmod 4$ 」的證明。一個很有名證明是扎吉爾 (Don Zagier) 在《*Proofs from the book*》一書中所給的「一行」證明。

回到橢圓曲線

高斯的方法證明出 $\frac{1}{2}a(p) = \pm r$ 。（請記得 $p = r^2 + s^2$ 而 r 是奇數且 s 是偶數。）

挑戰：你能想出這個公式

$$\frac{1}{2}a(p) = \pm r$$

的正負號該如何決定嗎？

一個高斯公式的精確版本：當 $r+s\equiv 1 \bmod 4$ 時，$\frac{1}{2}a(p)=r$ ；當 $r+s\equiv 3 \bmod 4$ 時，$\frac{1}{2}a(p)=-r$。舉例來說，當 $p=61$ 時，$r=5$ 且 $s=6$，由於 $11\equiv 3 \bmod 4$，符號是負的。

對於一般的橢圓曲線來說，模猜想給了一個 $a(p)=p-N(p)$ 的「公式」，該公式用到了傅立葉係數的模形式；那是一個特別的函數，類似於高中學到的三角函數 sin 和 cos。在舊金山的費馬慶典（Fermatfest，1993 年 7 月）上，魯賓（Karl Rubin）建議以一般形的高斯公式來描述模猜想。

到目前為止，我在提到模形式時只說它像三角函數，而沒有真正地刻畫它。你可以記得它和 sin 函數一樣有週期性就好，也就是對於所有的 x，都有

$$\sin(x+2\pi)=\sin(x)。$$

模形式是一個複變數函數，並具有兩個相互獨立的週期性。它可以寫成一個複指數 $q=e^{2\pi iz}$ 的無窮級數和，像是

$$q-2q^2-3q^3+2q^4-2q^5+6q^6-q^7+6q^9+4q^{10}-5q^{11}-6q^{12}-\cdots。$$

這個級數的係數們被稱為模形式的傅立葉係數。例如 -6 就是這個形式的第 12 項傅立葉係數。

模猜想 ➡ 費馬最後定理

從什麼角度來看才會讓弗瑞曲線（Frey's curve）$y^2=x(x-a^n)(x+b^n)$ 在模猜想中顯得格格不入呢？從模猜想可以推得，這個曲線的 $a(p)$ 會是模形式 f 的傅立葉係數。利用 a^n+b^n 會是完全 n 次方數的假設，我可以建構出一個模形式的鏈

$$f=f_1\rightsquigarrow f_2\rightsquigarrow f_3\rightsquigarrow\cdots\rightsquigarrow f_t$$

其中這個鏈的最後一個鏈結 f_t 是一個有許多限制條件的模形式，它會在最後得出一個矛盾的性質。而因為這個鏈的存在性是建立於「a^n+b^n 會是完全 n 次方數」上，所以這樣的 a 和 b 就一定不存在。

模猜想是怎麼被建立起來的？

模猜想是一個公式：

$a(p)$ 模形式的第 p 項傅立葉係數。

懷爾斯挑了一個小質數 —— 比方說 3 —— 來證明一個一般性的結果，把一個看起來較弱的模 3 同餘公式：

$$a(p)\equiv p \text{ 模形式的第 } p \text{ 項傅立葉係數}$$

$$(\text{對於所有的 } p)$$

提升成為一個成熟的公式。事實上，那個看起來較弱的公式是一個 1970 年代由朗蘭茲（Robert Langlands）證明的主要定理。順帶一提，朗蘭茲贏得該年的阿貝爾獎。

把同餘提升為公式的技巧現在被稱為模提升（modularity lifting），這個由懷爾斯與泰勒 / 懷爾斯創始的技巧在近幾年來被哈佛的齊辛（Mark Kisin）大大地改善。

證明了費馬最後定理有什麼好處呢？

馬上可以回答你，即使是在不遠的將來，費馬最後定理可能也不太能對生活有什麼幫助。但是歷史上數學也有許多例子是乍看之下非常理論，但後來卻變成現實中非常重要的一環。複數以前也被認為

寇茨（John Coates）、懷爾斯、黎貝、魯賓。

是「虛構」的，一點也沒用。但現在工程領域卻天天都會碰到。當我還是學生的時候，橢圓曲線也還沒有任何應用，結果現在每個密碼學家都要學習這個理論。

下一步是？

懷爾斯、泰勒 / 懷爾斯與齊辛等人對現代數論有巨大的貢獻。盤根錯節的猜想把代數結構（如橢圓曲線）連結到模形式一般化的**自同構表現**（automorphic representations）。這些猜想被放在一個「綱領」（即藍圖）裡，我們稱之為**朗蘭茲綱領**（Langlands program）。最近幾年有許多其中的猜想都變成了定理，若想學更多的話可以搜尋：

- 模 p 的模形式中的塞爾猜想（Serre's conjectures on mod p modular forms），
- 方丹 / 馬佐猜想（The Fontaine-Mazur conjecture），
- 佐藤 / 泰特猜想（The Sato-Tate conjecture）……。

這個領域目前還是很活躍。懷爾斯在 1990 初期的工作仍持續催生許多新的發展。

本文出處

本文是由作者在 2018 年 6 月 4 日南京大學思廉講座的講稿。本刊感謝黎貝教授同意翻譯刊登。

譯者簡介

張哲睿為國立交通大學應用數學系學生。

延伸閱讀

- 在《數學傳播》中有多篇關於費馬最後定理的文章，如第 17 卷第 3 期的李文卿與余文卿〈威伊猜想〉；第 18 卷第 2 期的李文卿與余文卿〈費馬最後定理：懷爾斯的解決方案〉和余文卿〈費馬最後定理〉；以及第 23 卷第 3 期余文卿〈關於懷爾斯解決費馬最後定理的一些補充說明〉等文章。有興趣的讀者可由 https://w3.math.sinica.edu.tw/mathmedia/archive18.jsp 網站搜尋閱讀。
- Michael Harris，〈為何不必再改進費馬最後定理的證明〉，Quanta 雜誌，2019/6/3：https://www.quantamagazine.org/why-the-proof-of-fermats-last-theorem-doesnt-need-to-be-enhanced-20190603/