費馬最後定理

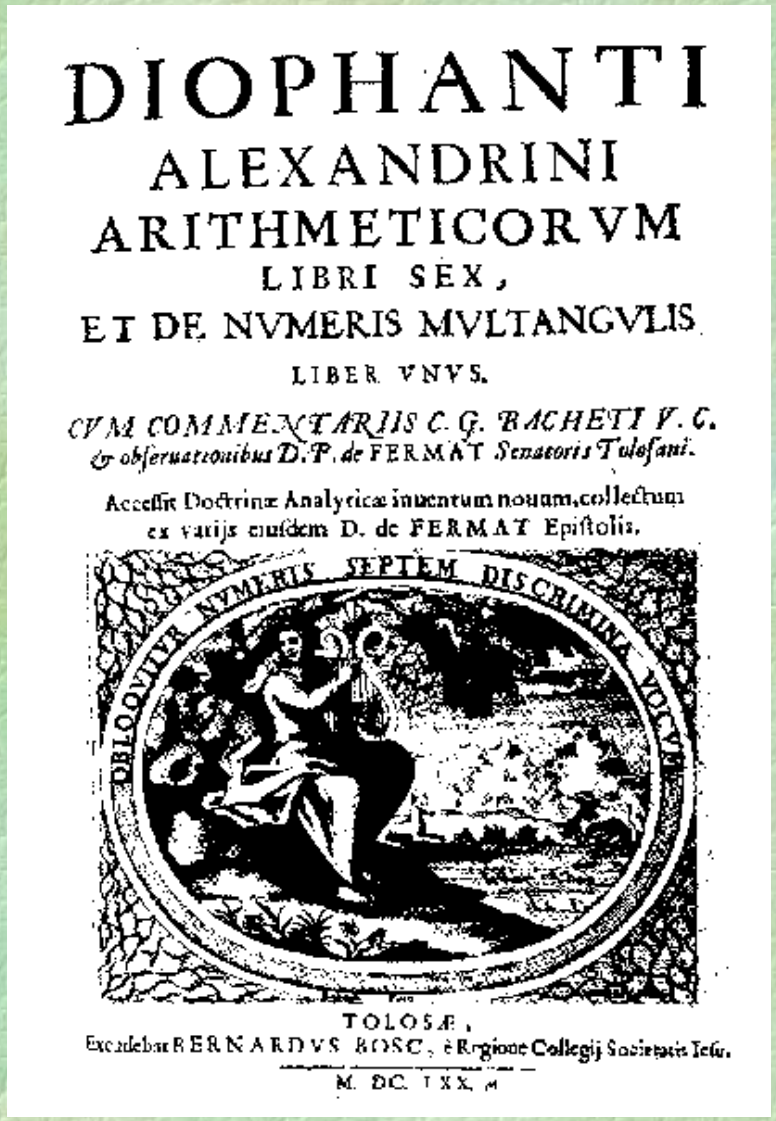
數學講座

費馬 Pierre de Fermat (1601 – 1665)

- 法國人
- 律師，1631年出任圖盧茲議院顧問。
- 業餘研究數學
- 他是幾何學、坐標幾何、概率論、微積分、數論等學問的先驅。
- 一生從未發表過數學論文，祇在書信和筆記中，紀錄了他的數學思想。

- 費馬曾經提出過的命題，大多數後來都被證實為正確，祇有一個命題，在他死後，數學家努力了幾個世紀都未能證實，直至三百五十多年後，1995年才有辦法証明 .....

費馬最後定理


DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX,
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
CVM COMMENTARIIS C. G. BACHETI V. C.
& obſeruationibus D. P. de FERMAT Senatoris Tolosani.
Accessit Doctrinæ Analyticæ inuentum nouum, collectum
ex variis eiusdem D. de FERMAT Epistolis.
DIOPHANTUS NUMERUS SEPTEM DISCRIMINA VOCAT
TOLOSÆ,
Excudebat BERNARDVS BOSC, è Regione Collegij Societatis Iesu.
M. DC. LXX.

大約 1637 年，費馬閱讀古希臘名著《算術》，讀到：

《算術》第 II 卷第八命題：

將一個平方數分為兩個平方數。

即求方程 $x^2 + y^2 = z^2$ 的正整數解。

勾股定理及勾股數組

- 勾股定理　在 ΔABC 中，若 $\angle C$ 為直角，則 $a^2 + b^2 = c^2$。
- 留意：$3^2 + 4^2 = 5^2$; $5^2 + 12^2 = 13^2$; $8^2 + 15^2 = 17^2$; $7^2 + 24^2 = 25^2$; ……等等
- 即 (3 , 4 , 5)、(5 , 12 , 13)…等等為方程 $x^2 + y^2 = z^2$ 的正整數解。
- 我們稱以上的整數解為「勾股數組」。

勾股數組的通解

求方程 $x^2 + y^2 = z^2$ 的正整數解。

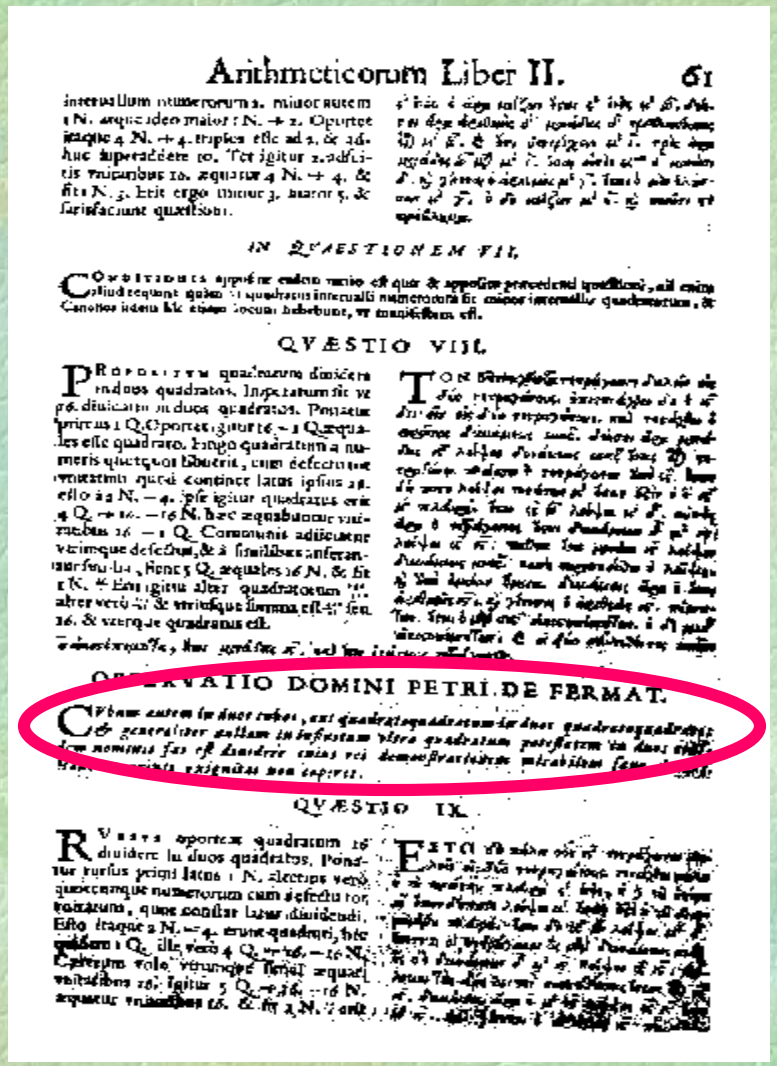
費馬利用他發明的方法來解此題，得到以下結果：

解　$x = u^2 - v^2 ; y = 2uv ; z = u^2 + v^2$，其中 $u > v > 0$。

v \ *u*	2	3	4	5	6
1	(3 , 4 , 5)	(8 , 6 , 10)	(15 , 8 , 17)	(24 , 10 , 26)	(35 , 12 , 37)
2	---	(5 , 12 , 13)	(12 , 16 , 20)	(21 , 20 , 28)	(32 , 24 , 40)
3	---	---	(7 , 24 , 25)	(16 , 30 , 34)	(27 , 36 , 45)
4	---	---	---	(9 , 40 , 41)	(20 , 48 , 56)
5	---	---	---	---	(11 , 60 , 61)

令人困惑的是，費馬在書邊的空白地方，他寫下了以下的一段說話：

- 那麼當 $n > 2$ 時，方程 $x^n + y^n = z^n$ 又有沒有整數解呢？
- 這是不可能的。我對這個命題有一個美妙的證明，這裏空白太小，寫不下。
- 到底費馬的說法是否正確呢？



Arithmeticorum Liber II. 61

IN QVÆSTIONEM VII.

QVÆSTIO VIII.

OBSERVATIO DOMINI PETRI DE FERMAT.

QVÆSTIO IX.

一個難解的謎！

◆**可不可能找到整數 x, y, z ，使**

$x^3 + y^3 = z^3$ 或 $x^4 + y^4 = z^4$ 或 $x^5 + y^5 = z^5$ 或 .....？

◆如果找到，費馬便是錯的。

◆如果找不到，也要証明永遠不可能找到，才可証明費馬是對。

費馬從未向其他人提及這個「美妙證明」，亦沒有任何紀錄提及這件事！

一點進展

- 費馬曾經提出過的命題，都已經被證實或否定，祇剩下這「最後」一題，未能獲證。
- 費馬在給朋友的信中，曾經提及他已證明了 $n = 4$ 的情況。但沒有寫出詳細的證明步驟。
- 1674 年，貝西給出這個情形的嚴格證明。
- 證明步驟主要使用了「無窮遞降法」。

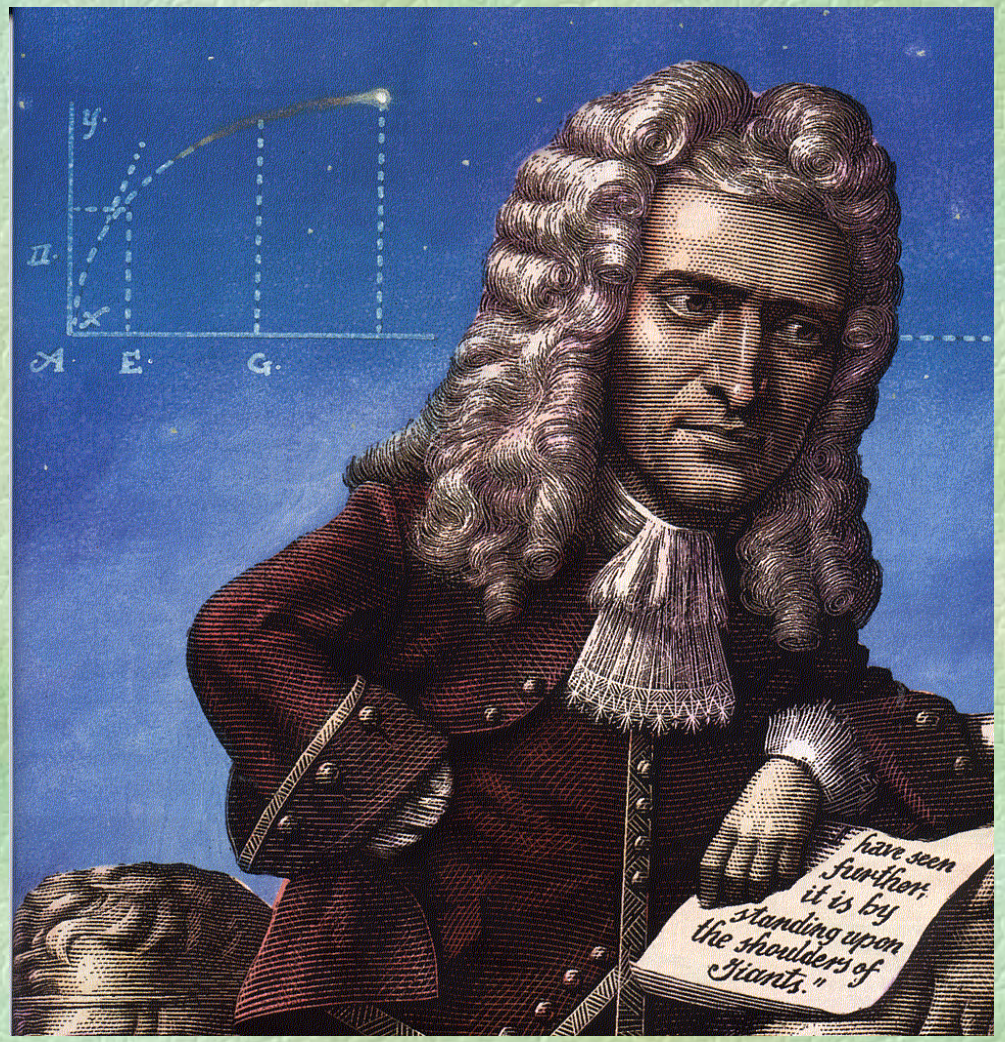
無窮遞降法

- 假設整數 (a,b,c) 是方程 $x^4 + y^4 = z^4$ 的正整數解， 因此 $a^4 + b^4 = c^4$ ；
- 則必定可以找到另一整數解 (d, e, f)，它們比 (a, b, c) 更小 ，同樣 $d^4 + e^4 = f^4$；
- 這個解不可能無窮遞降下去，因此這個解不存在。
- 因此對於 $x^4 + y^4 = z^4$ ，費馬是對的！

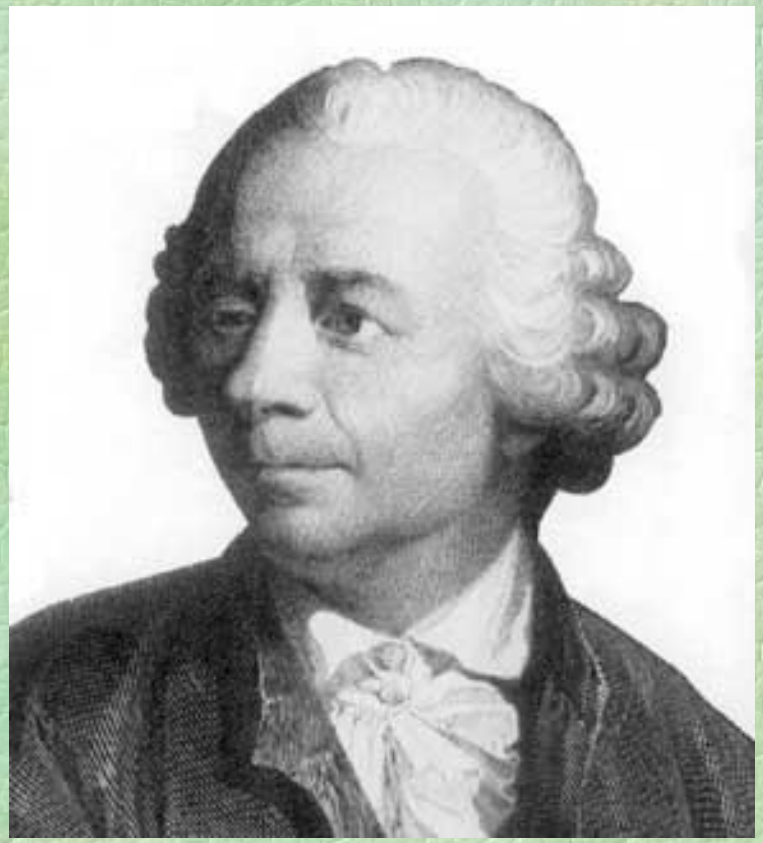
一個推論

- 可以斷言：對於任何正整數 k，方程 $x^{4k} + y^{4k} = z^{4k}$ 沒有正整數解。
- 如果方程有解，例如： $a^{4k} + b^{4k} = c^{4k}$，則 $(a^k)^4 + (b^k)^4 = (c^k)^4$，但這與費馬的結果矛盾！ ∴原方程沒有解。
- 同樣道理，以後祇需證明對於奇質數 p，方程 $x^p + y^p = z^p$ 沒有正整數解。

差不多過了一百年，仍沒有進展，但世界變了 ……



一切人的老師



歐拉 Leonhard Euler
(1707 – 1783)

- 瑞士人。
  18世紀最優秀的數學家。
- 世上最多產的數學家。
- 13歲入大學，17歲取得碩士學位，30歲右眼失明，60歲完全失明。
- 1770年提出 $n = 3$ 的證明，但其中有一點錯誤。

數學之王

高斯 Carl Friedrich Gauss
(1777 – 1855)

- 德國數學家。
- 數學神童。
- 歷史上三位最偉大的數學家之一。
- 發展複數理論。
- 完成歐拉的證明。

費馬之後，十八世紀兩位最偉大的數學家合力，才能第一次有所突破！！！

新的方向

熱爾曼 Sophie Germain (1776 – 1831)

- 法國人。少數研究數學的女性。
- 提出將「費馬定理」分成兩個情況：
  (I) n 能整除 x、y、z。
  (II) n 不能整除 x、y、z。
- 熱爾曼定理
  如果 p 是一個奇質數，並且 $2p + 1$ 亦是質數，那麼對於 $n = p$，「費馬定理」的第 I 情況成立。
- 熱爾曼初步完成了 $n = 5$ 的證明。

$n = 5$ 的證明

勒讓德 Legendre (1752 – 1833)

- 法國人
- 1823 年，證明了 $n = 5$。

狄利克雷 Dirichlet (1805 – 1859)

- 德國人
- 1828 年，獨立地證明了 $n = 5$。
- 1832 年，解決了 $n = 14$ 的情況。

尷尬的事件

1847年，兩位法國數學家分別表示他們証明了費馬最後定理

我証先！

我証先！

拉梅 Gabriel Lamé
(1795 – 1870)

柯西 Cauchy
(1789-1857)

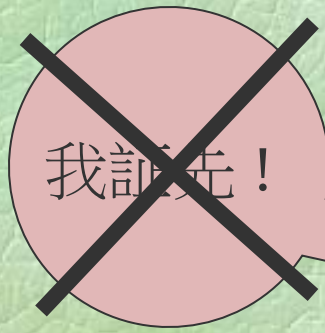
1847 年發生的事件

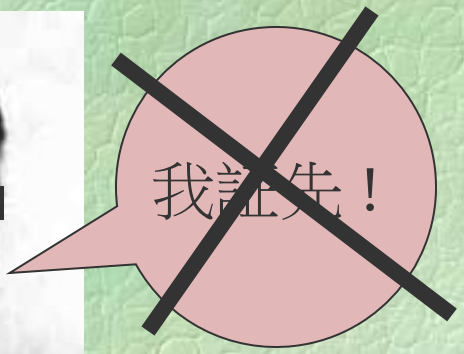
巴黎科學院為費馬最後定理提供了金獎章及3000法郎獎金。

3 月 22 日，兩人同時向巴黎科學院提出自己的證明。

不過，對於「唯一分解定理」的問題，二人都未能成功地解決。

5 月 24 日，德國數學家庫麥爾發表了一封信，指出「唯一分解定理」的必要性，亦清楚地顯示，拉梅和柯西的方法是行不通的，從而平息了二人的爭論。

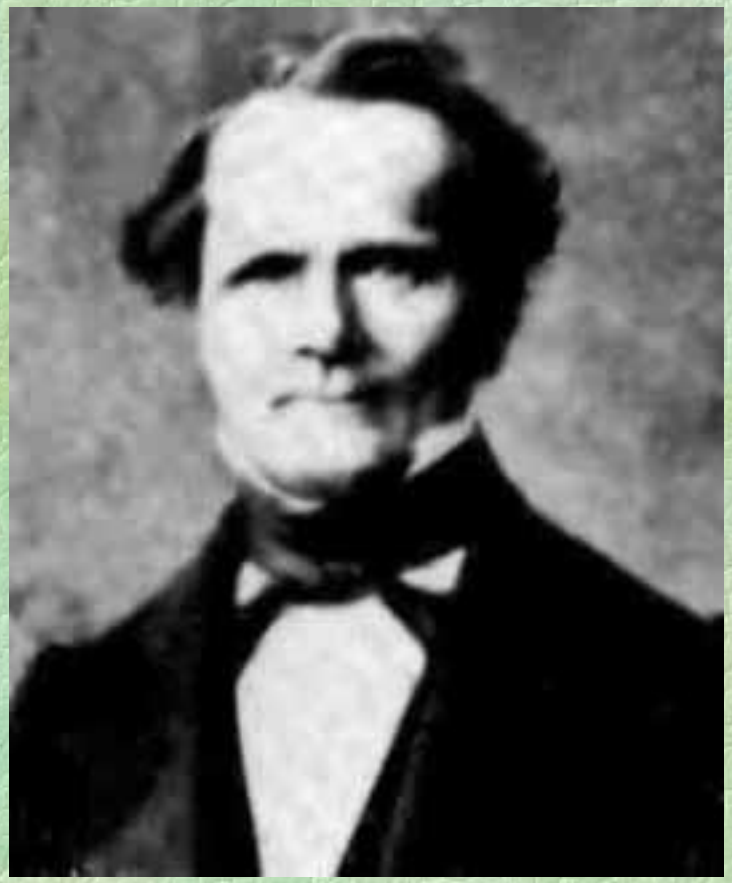




拉梅 Gabriel Lamé
(1795 – 1870)

柯西 Cauchy
(1789-1857)

邁進一大步



庫麥爾 Ernst Edward Kummer (1810 – 1893)

- 德國人
- 提出「正規質數」的概念，並證明當 n 為正規質數時，「費馬最後定理」成立。
- 庫麥爾證明當 $n < 100$ 時，「費馬最後定理」成立。
- 1857 年，庫麥爾獲巴黎科學院頒發獎金三千法郎。

懸紅十萬馬克

沃爾夫斯凱爾 Paul Friedrich Wolfskehl (1856 – 1908)

- 德國商人。
- 曾學習醫學。1883 年跟庫麥爾學習。
- 訂立遺囑，懸紅十萬馬克，獎賞在他死後一百年內能證明「費馬最後定理」的人。

- 1909 至 1934 年間，收到無數的「證明」，但無一成立。
- 經過兩次大戰後，該筆獎金已大幅貶值，以 1977 年的價值計算，祇約值一萬馬克或四千美元。

無數英雄盡折腰

- 1941年，雷麥證明當 $n < 253747887$ 時 ，「費馬最後定理」第 I 情況成立。
- 1977 年，瓦格斯塔夫證明當 $n < 125000$ 時，「費馬最後定理」成立。
- 1983 年，德國數學家伐爾廷斯證明了「莫德爾猜想」，從而推出方程 $x^n + y^n = z^n$ 最多祇有有限多個整數解。
- 1988 年，日本數學家宮岡洋一宣布以微分幾何的角度，證明了「費馬最後定理」！
- 不過，該證明後來被發現有重大而無法補救的缺陷，證明不成立！

兩個疑問

費馬到底有沒有那個「美妙證明」？

☺ 相信沒有。可能費馬後來發現自己的證明有錯，所以沒有將它紀錄下來，但是，他修改了自己的方法，最後得到 $n = 4$ 的證明。

研究「費馬最後定理」有甚麼好處？

☺ 滿足人類的求知慾。

☺ 刺激數論的研究，從而發展出各種的數學工具和理論。

☺ 到今天，由研究「費馬最後定理」而發展出來的技術，已廣泛地應用到各種科學技術之上，特是編碼理論和各種電腦計算技巧。

谷山—志村猜想

谷山豊 (1927 – 1958)

志村五郎（生於1926）

谷山—志村猜想

- 1954 年，志村五郎於東京大學結識谷山豐。
- 之後，就開始了二人對「模形式」的研究。
- 1955 年，谷山開始提出他的驚人猜想。
- 1958 年，谷山突然自殺身亡。
- 其後，志村繼續谷山的研究，並提出以下的猜想：
- 谷山—志村猜想
  每一條橢圓曲線，都可以對應一個模形式。

橢圓曲線

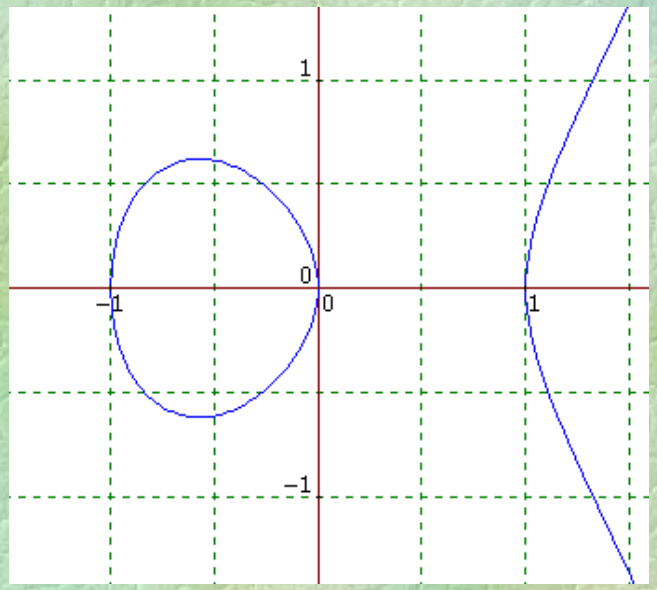
- 簡單來說，就是由滿足方程

$$y^2 = x^3 + ax + b$$

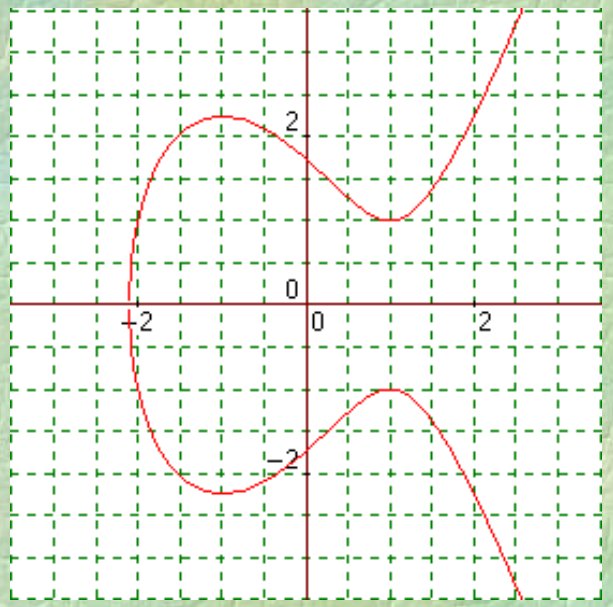
的點所組成的曲線，其中 a、b 為任意的有理數。

- 「橢圓曲線」原本用來研究「橢圓函數」，而「橢圓函數」則用於計算橢圓的周長。事實上，「橢圓曲線」的形狀和橢圓形完全不同，到了現在，「橢圓曲線」已被獨立地研究。

橢圓曲線



$y^2 = x^3 - x$



$y^2 = x^3 - 3x + 3$

甚麼是「模形式」？

「模形式」f 是一個定義於半複平面上（即對於複數 z，$\mathrm{Im}\, z > 0$ 的集合）並滿足下列條件的複變解析函數：

★ $f((az + b) / (cz + d)) = (cz + d)^k f(z)$，其中 k 為正整數，a、b、c、d 為整數並且 $ad - bc = 1$。

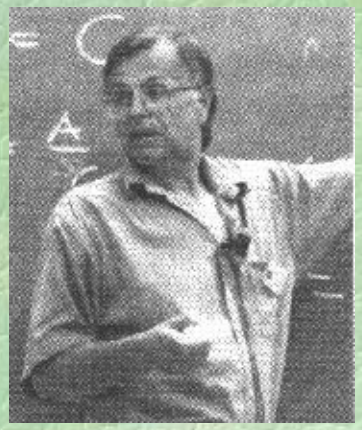
✸ $f(z) = \sum a_n e^{2\pi inz}$，其中 a_n 為複數，n 為由 0 至無限大的整數。

有關「谷山志村猜想」

- 起初，大多數的數學家都不相信「谷山志村猜想」。
- 60 年代後期，眾多數學家反覆地檢驗該猜想，既未能證實，亦未能否定它。
- 到了 70 年代，相信「谷山志村猜想」的人越來越多，甚至以假定「谷山志村猜想」成立的前提下進行論證。
- 一些人稱之為『谷山 - 威爾』猜想，但其實美國數學家威爾本來根本不相信它。

「谷山志村猜想」
與
「費馬最後定理」
有甚麼關係？

弗賴曲線（ε猜想）



⑦1984年秋，德國數學家弗賴（Gerhand Frey），在一次數學會議上，提出以下的觀點：

⑦首先，假設「費馬最後定理」不成立。即發現 A、B、C 和 N，使得 $A^N + B^N = C^N$。

⑦從此得出「橢圓曲線」（後來稱這線為「弗賴曲線」）：$y^2 = x^3 + (A^N - B^N)x^2 - A^N B^N x$。

⑦弗賴發現這曲線非常特別，特別到不可能對應任何一個「模形式」！

⑦換句話說，弗賴認為：如果「費馬最後定理」不成立，那麼「谷山志村猜想」也是錯的！

假如

費馬最後定理 錯

⇓

弗賴曲線

⇓

谷山志村猜想 錯

費馬最後定理 對

⇑

弗賴曲線 錯

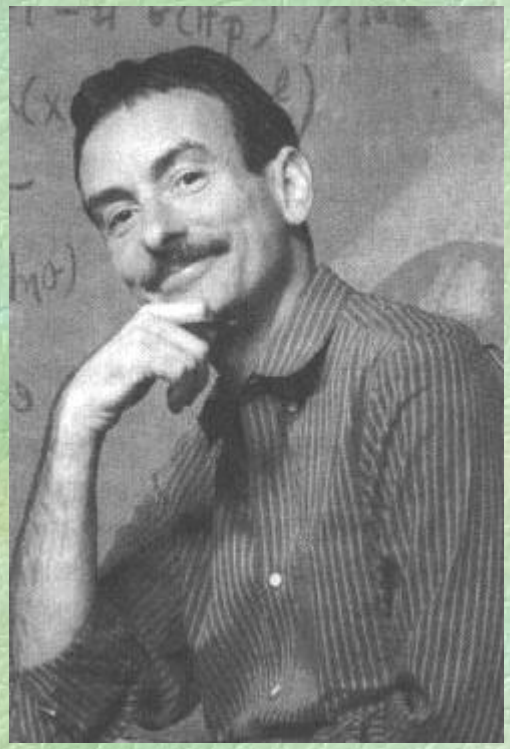
⇑

假如 谷山志村猜想 對

⑦再換句話說，如果「谷山志村猜想」正確，那麼「費馬最後定理」就必定成立！

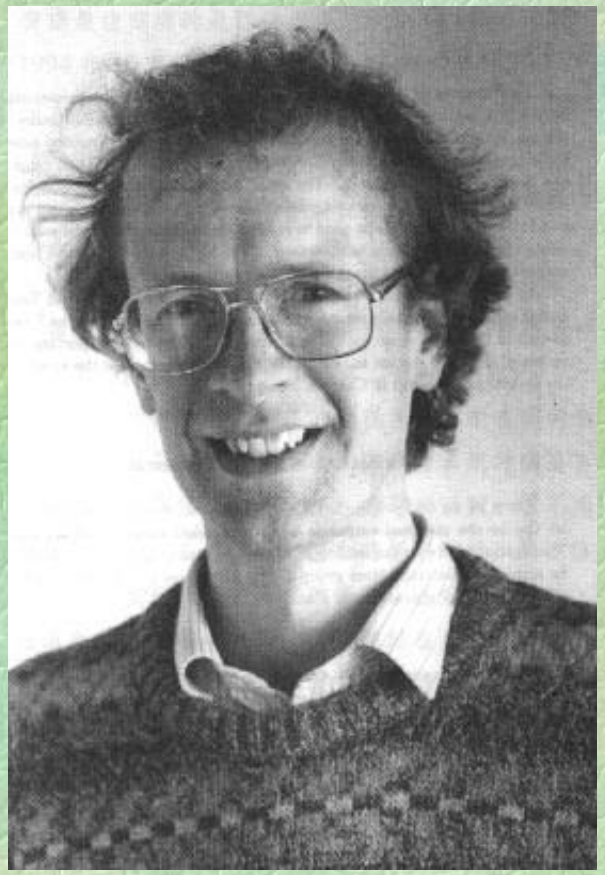
⑦可惜的是弗賴在 1984 年的證明犯錯，他的結果未獲承認。故此，它祇可稱為「猜想」。

⑦美國數學家里貝特（Kenneth Ribet）經過多番嘗試後，終於在 1986 年的夏天成功地證得以下結果：



⑦如果「谷山志村猜想」對每一個半穩定橢圓曲線都成立，則「費馬最後定理」成立。

懷爾斯 *Andrew Wiles*



- 英國人，出生於 1953 年。
- 10 歲已立志要證明「費馬最後定理」。
- 1975 年，開始在劍橋大學進行研究，專攻「橢圓曲線」及「岩澤理論」。
- 在取得博士學位後，就轉到美國的普林斯頓大學繼續研究工作。

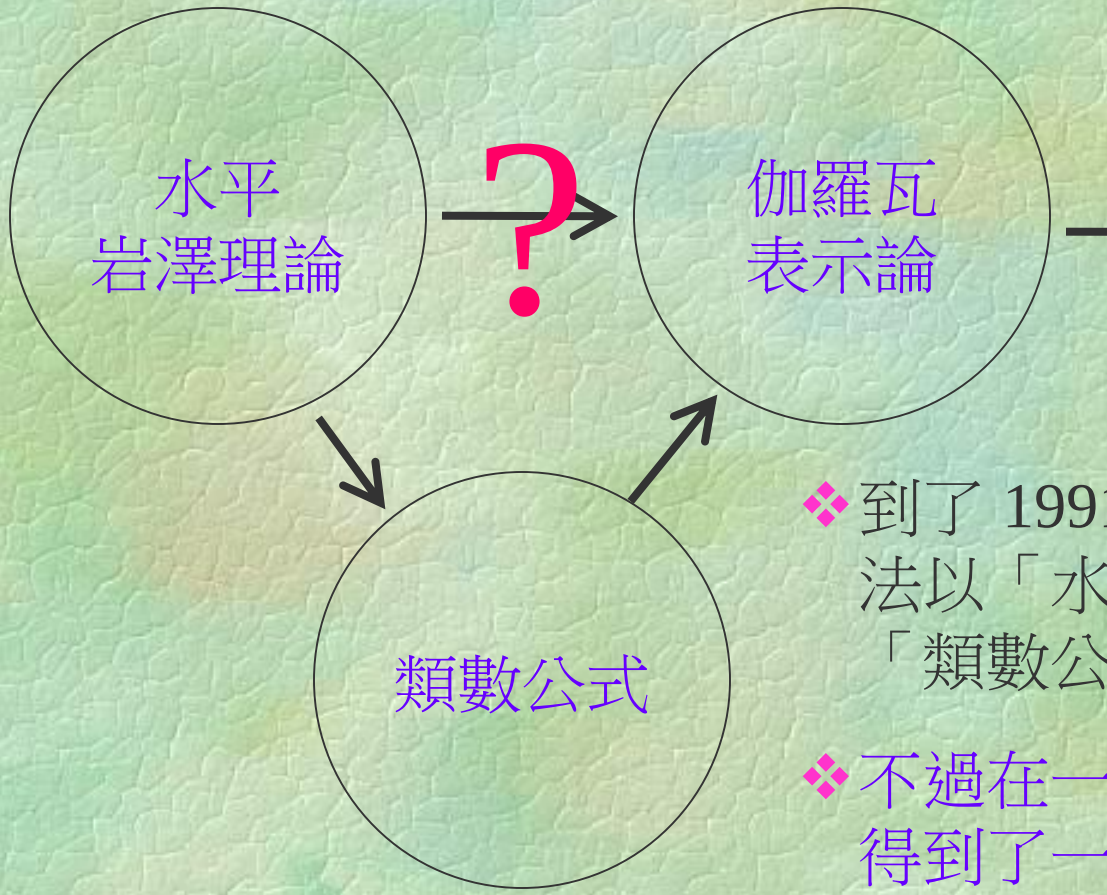
秘密計算

- 1986 年，當里貝特證得「ε 猜想」後，懷爾斯就決心要證明「谷山志村猜想」。
- 由於不想被別人騷擾，懷爾斯決定秘密地進行此證明。
- 經過三年的努力，他開始引入「伽羅瓦表示論」來處理將「橢圓曲線」的分類問題。

費馬最後定理 ⇐ 谷山志村猜想

=

橢圓曲線可模形化

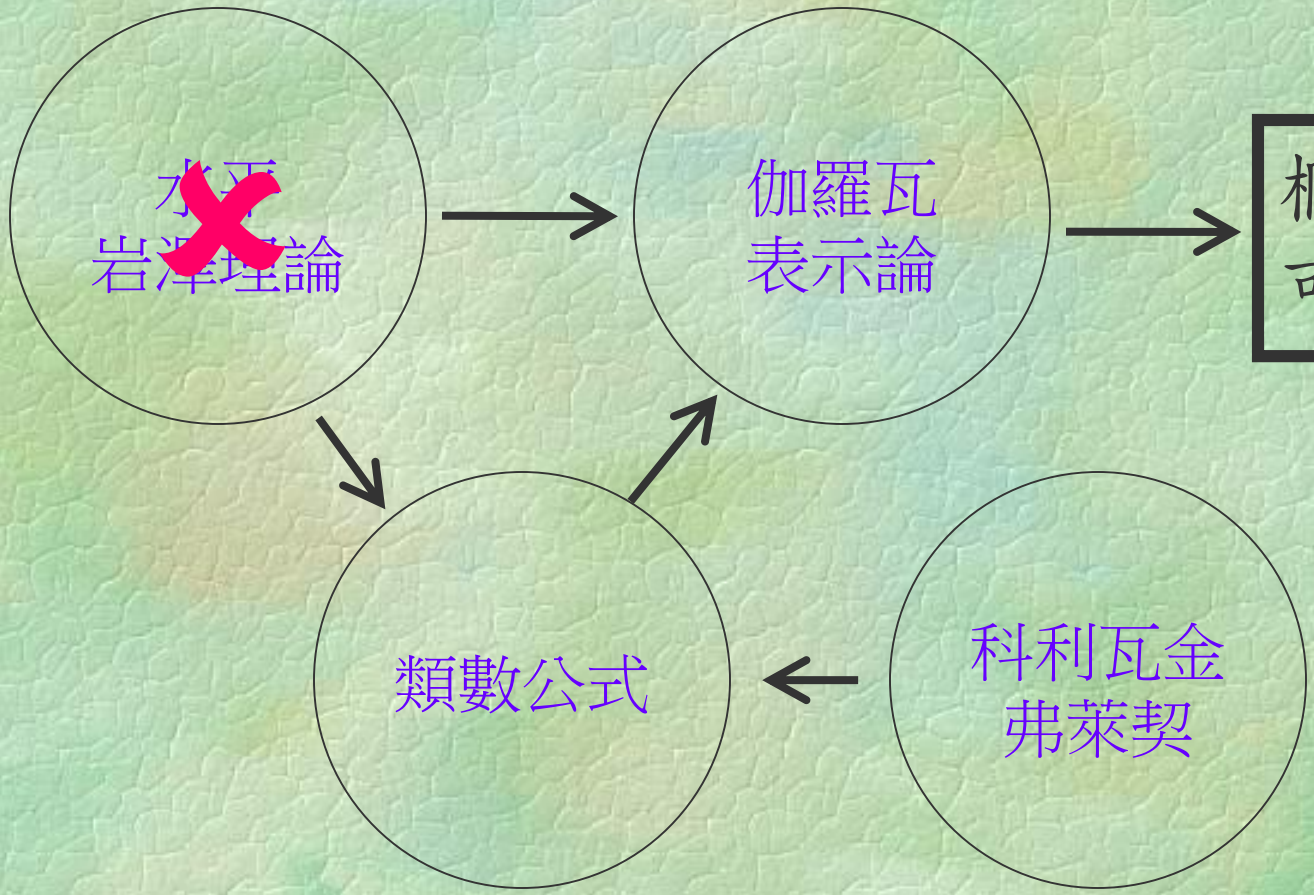


- 到了 1991 年，懷爾斯發覺無法以「水平岩澤理論」完成「類數公式」的計算。
- 不過在一個數學會議中，他得到了一個新的計算方法。

費馬最後定理 ⇐ 谷山志村猜想

=

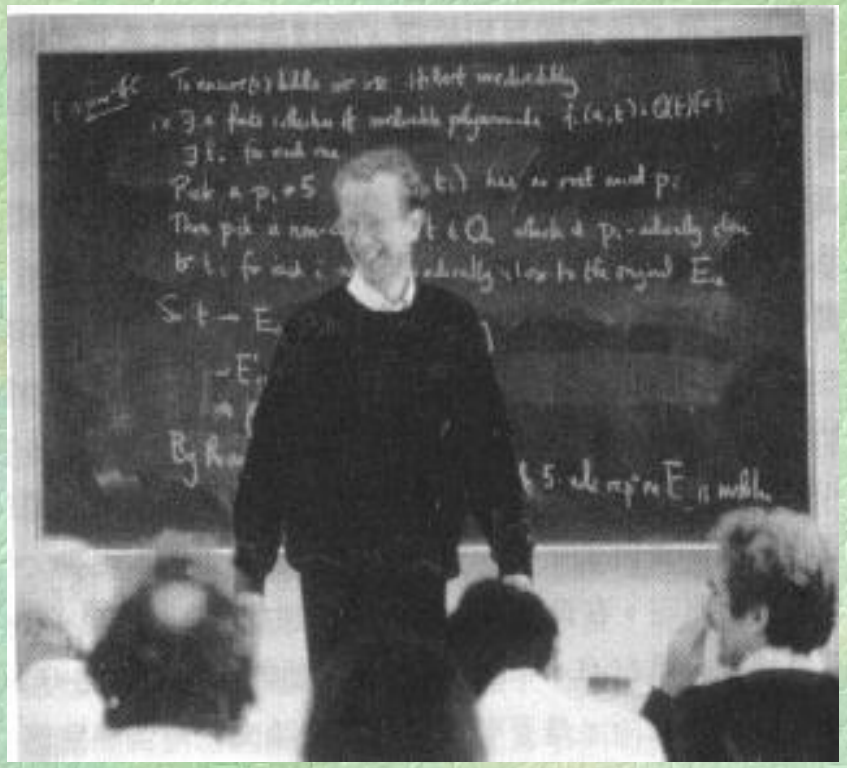
橢圓曲線
可模形化



❖懷爾斯將此方法改造後，成功地解決了有關問題。

劍橋演講

- 1993 年 6 月 23 日，在劍橋大學的牛頓研究所，懷爾斯以「模形式、橢圓曲線、伽羅瓦表示論」為題，發表了他對「谷山志村猜想」（即「費馬最後定理」）的證明。



- 演講非常成功，「費馬最後定理」經已被證實的消息，很快便傳遍世界。

噩夢開始！

- 演講會過後，懷爾斯將長達二百多頁的證明送給數論專家審閱。
- 起初，祇發現稿件中的有些微的打印錯誤。
- 但，同年 9 月，證明被發現出現了問題，尤其是「科利瓦金—弗萊契方法」，並未能對所有情況生效！
- 懷爾斯以為此問題很快便可以修正過來，但結果都失敗！
- 懷爾斯已失敗的傳聞，不脛而走。同年 12 月，懷爾斯發出了以下的一份電子郵件：

噩夢開始！

標題：費馬狀況

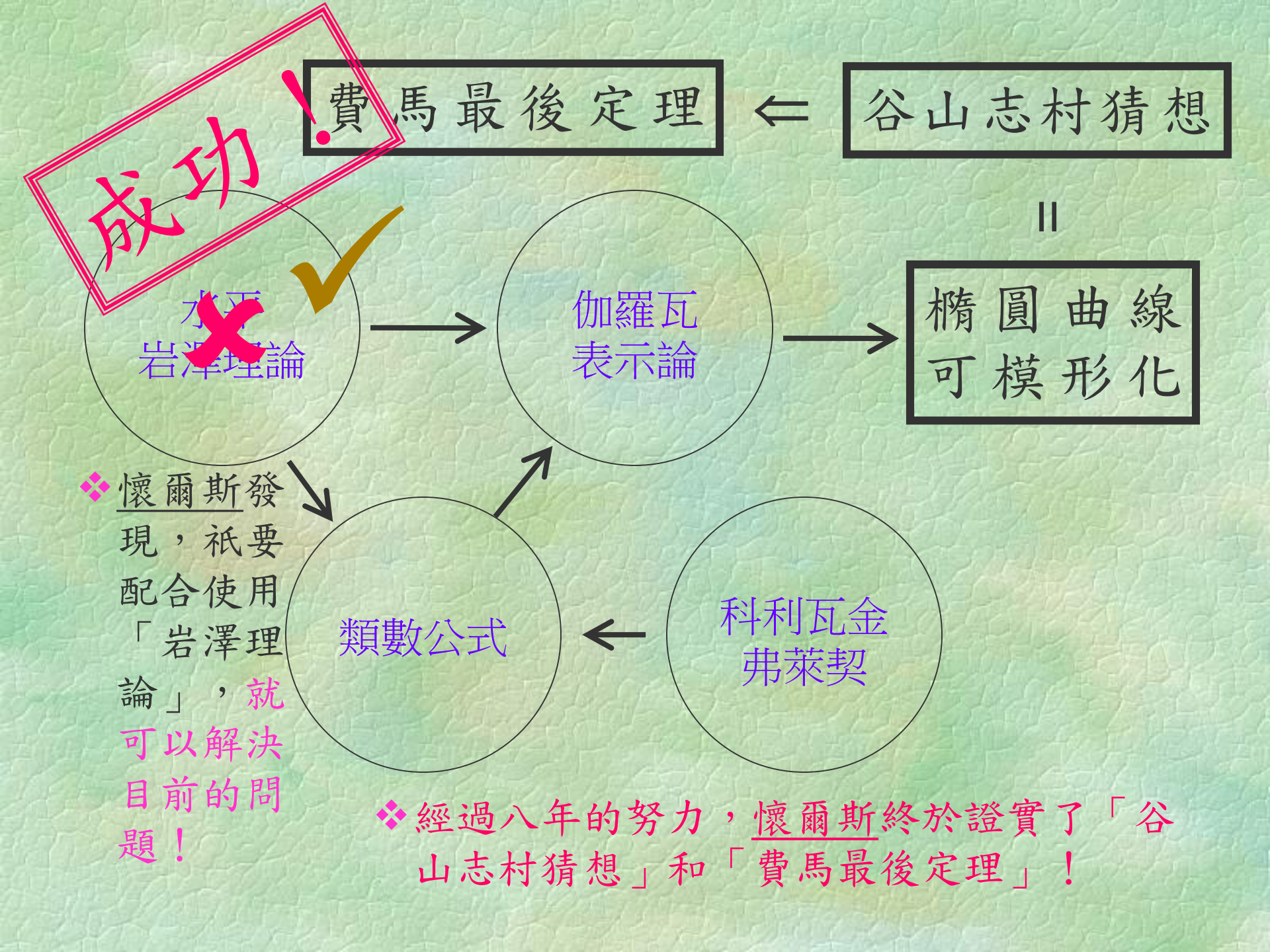
日期：1993 年 12 月 4 日

對於我在谷山志村猜想和費馬最後定理方面的種種推測，我要作一個簡短的說明。在審查過程中，我們發現了許多問題，其中大部分已經解決，祇剩一個問題仍然存在……。我相信不久後，我就能用在劍橋演講中說明的概念解決它。基於尚有許多工作未能完成，所以目前不適宜發送預印本。……我將對這工作給出一個詳細的說明。

安德魯　懷爾斯

再次閉關

- 1994 年 1 月，懷爾斯重新研究他的證明。但，到了同年 9 月，依然沒有任何進展。
- 其間，不斷有數學家要求懷爾斯公開他的計算方法。
- 更有人懷疑：既然過去都無法證明「費馬最後定理」，到底現在又能否證實「谷山志村猜想」呢？
- 但在 9 月 19 日的早上，當懷爾斯打算放棄並作最後一次檢視「科利瓦金—弗萊契方法」時，……

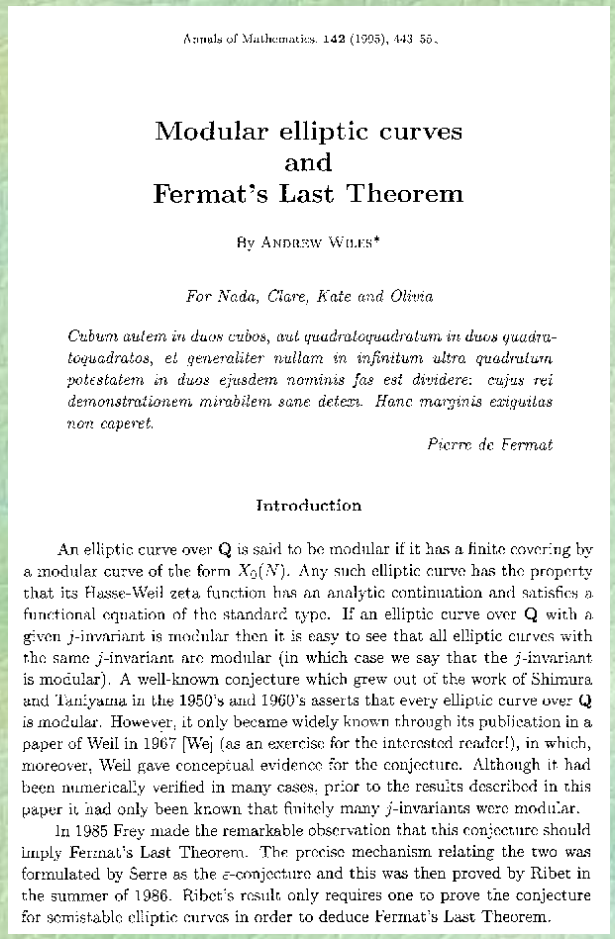


❖懷爾斯發現，祇要配合使用「岩澤理論」，就可以解決目前的問題！

❖經過八年的努力，懷爾斯終於證實了「谷山志村猜想」和「費馬最後定理」！

最後勝利

- 1995 年 5 月，懷爾斯長一百頁的證明，在雜誌《數學年鑑》中發表。



Annals of Mathematics, 142 (1995), 443–551

Modular elliptic curves and Fermat's Last Theorem

By Andrew Wiles*

For Nada, Clare, Kate and Olivia

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos ejusdem nominis fas est dividere: cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

Pierre de Fermat

Introduction

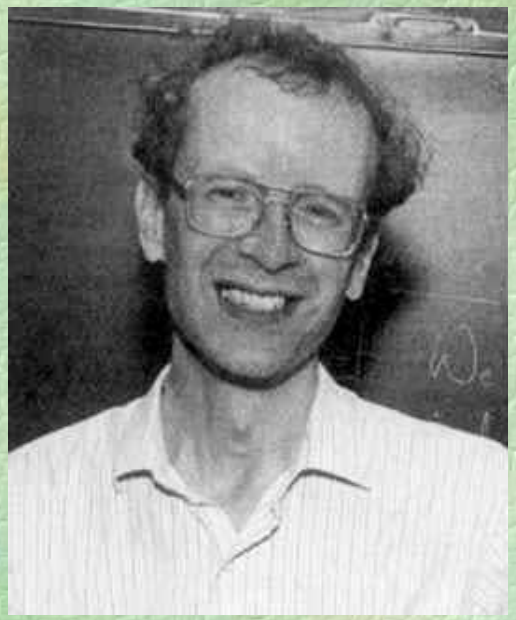
An elliptic curve over $\mathbf{Q}$ is said to be modular if it has a finite covering by a modular curve of the form $X_0(N)$. Any such elliptic curve has the property that its Hasse-Weil zeta function has an analytic continuation and satisfies a functional equation of the standard type. If an elliptic curve over $\mathbf{Q}$ with a given j-invariant is modular then it is easy to see that all elliptic curves with the same j-invariant are modular (in which case we say that the j-invariant is modular). A well-known conjecture which grew out of the work of Shimura and Taniyama in the 1950's and 1960's asserts that every elliptic curve over $\mathbf{Q}$ is modular. However, it only became widely known through its publication in a paper of Weil in 1967 [Wej (as an exercise for the interested reader!), in which, moreover, Weil gave conceptual evidence for the conjecture. Although it had been numerically verified in many cases, prior to the results described in this paper it had only been known that finitely many j-invariants were modular.

In 1985 Frey made the remarkable observation that this conjecture should imply Fermat's Last Theorem. The precise mechanism relating the two was formulated by Serre as the ε-conjecture and this was then proved by Ribet in the summer of 1986. Ribet's result only requires one to prove the conjecture for semistable elliptic curves in order to deduce Fermat's Last Theorem.

最後勝利

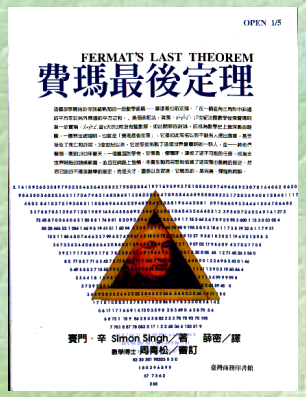
- 1995 年 5 月，懷爾斯長一百頁的證明，在雜誌《數學年鑑》中發表。
- 1997 年 6 月 27 日，懷爾斯獲得價值五萬美元的「沃爾夫斯凱爾獎金」。

懷爾斯的話



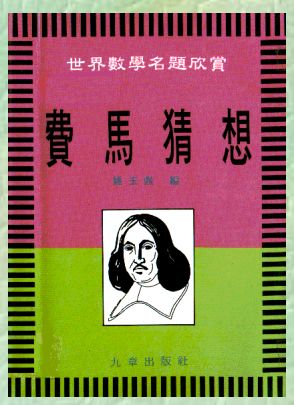
- 「設想你進入大廈的第一個房間，裏面很黑。你在家俱之間跌跌撞撞，但是逐漸你搞清楚了每一件家俱所在的位置。最後...你找到了電燈開關，打開了燈。突然...你能確切地明白你身在何處。」
- 「這是我童年時代的戀情，沒有東西能夠取代它...如果你能在成年時期解決某個對你來說非常重要的事，那麼再也找不出甚麼比這更有意義了。」

參考書籍



《費瑪最後定理》　作者：賽門　辛
出版社：臺灣商務印書館
故事：☺☺☺☺　數學：☺☺
易讀：☺☺☺

《費馬最後定理》　作者：艾克塞爾
出版社：時報出版
故事：☺☺☺　數學：☺☺☺
易讀：☺☺☺☺



《費馬猜想》　作者：姚玉強
出版社：九章出版社
故事：☺☺　數學：☺☺☺☺
易讀：☺

參考網頁

- 有關「費馬最後定理」
  - http://www.ams.org/new-in-math/fermat.html
  - http://www-history.mcs.st-and.ac.uk/~history/HistTopics/Fermat's_last_theorem.html
- 有關數學家生平、相片及有關資料
  - http://www-history.mcs.st-and.ac.uk/~history/index.html
- 有關數學歷史故事的中文網頁
  - http://www.edp.ust.hk/math