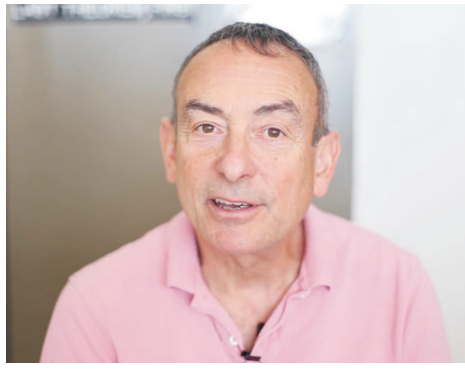
數學傳播　42卷2期, pp. 34-43

# 費馬最後定理及理想類

## 演講者：Kenneth A. Ribet 教授



時　間：民國 106 年 8 月 1 日
地　點：天文數學館一樓國際會議廳
整　理：陳其誠、梁惠禎

Kenneth Alan Ribet 教授於 1948 年出生於美國, 目前任教於加州大學柏克萊分校。他爲 Andrew Wiles 對費馬最後定理的證明, 完成了關鍵性的前置工作。

很榮幸在 NCTS 週年慶演講[1]。我在柏克萊的第一批研究生中就有一位來自台灣, 他是在座的紀文鎮教授。很久以前他邀請我來台灣, 今天算是我第三或第四次訪問, 記得在三年前參加過 NCTS 的研討會, 印象深刻。

請容我先問：在座有多少人是專業數學家? 有多少人不是專業數學家? 這個演講的前半部本來是講給非專業數學家聽的。近結尾時, 我會談到屬於代數數論的理想類 (ideal classes)。代數數論可說是源自數學家對費馬最後定理的研究, 是數學的一門分支。

談費馬最後定理必須提到它長遠的歷史。它起源於十七世紀, 會成爲數學的核心問題, 是基於各種各樣的原因, 其中一些純屬偶然。而它在數學上所以重要, 其中一個原因是它引導出一些重要的理論, 這些理論的應用範圍遠遠超過費馬最後定理本身的研究。

1993 年 6 月, 年輕的英國數學家 Andrew Wiles 在劍橋大學的數學會議上宣布：他已證明費馬最後定理, 350 多年來衆人對此問題的探索於焉完滿。這全然令人驚訝。從公衆的角度來看, 這無疑是數學上最令人興奮的消息; 因此, 隔天早上, 我的名字、當然還有 Andrew 的名

[1]影音檔請見 https://www.youtube.com/watch?v=NwGX6hGSzxY

字, 都上了紐約時報的頭版。

稍後我會給出定理的實際敘述; 它攸關方程式的解, 基本上是說任何正整數 $a, b$ 和 $c$ 都不能使某件事成立。1993 年, 記者常問我的一個問題是：「能否藉由電腦來驗證這個定理? 是否只要檢查了足夠的數據, 就能確信它是對的?」身爲專業數學家, 我們當然必須向記者及公衆解釋：數學定理通常不能藉由有限的計算來證明。數論是我的研究主題, 其中恰巧有許多表面上看似不怎麼樣複雜的問題, 其所牽涉到的數值卻出奇的大。譬如所謂的 Pell 方程式： $x^2 - cy^2 = 1$, $c$： 常數; 費馬就觀察到, 若取 $c = 109$, 則方程式 $x^2 - cy^2 = 1$ 的最小解是 $x = 158070671986249$, $y = 15140424455100$; 比起 109, $x$ 很大, $y$ 的值較 $x$ 稍小, 也很大 (譯註：所以你若只檢查比較小的 $x$ 或 $y$, 會以爲此方程式沒有整數解)。

另一個有名的例子是 Euler 在十八世紀提出的一個猜想：方程式 $a^4+b^4+c^4 = d^4$ 沒有正整數解; 換句話說, 三個整數四次冪的總和永遠不可能是整數的四次冪。到了 60 年代及 70 年代, 人們開始懷疑這個猜想可能是錯的, 結果哈佛的 Noam Elkies 首先找到反例 $2682440^4 + 15365639^4 + 18796760^4 = 20615673^4$。後來我們知道, 這不是最小的反例, 但最小的反例並不比它小很多。Elkies 是用電腦找到反例的, 但在他讓筆記本電腦作運算之前, 已用紙筆做了很多腦力工作。

對費馬最後定理的描述通常始於畢氏定理, 其方程爲 $a^2 + b^2 = c^2$, 亦即, 你問： 兩個整數平方的和是否可以是某個整數的平方? 大多數人都知道, 3 的平方加上 4 的平方是5的平方, $3^2 + 4^2 = 5^2$, 而 5 的平方加上 12 的平方是 13 的平方, $5^2 + 12^2 = 13^2$。當然, 如果你隨機取兩個數, 並將它們平方後相加, 通常不會得到整數的平方; 譬如： 2 的平方加上 3 的平方是 $4 + 9 = 13$, 這不是整數的平方。你可能會得到一個完美的平方, 但通常並非如此。畢氏三元組是正整數 $a$, $b$ 和 $c$, 其中前兩個數的平方總和是第三個數的平方。所以 3, 4 和 5 及 5, 12 和 13 都是畢氏三元組。如果你嘗試去生成像 5, 12, 13 這樣的畢氏三元組, 你可能會想到一個簡單的代數等式, 利用它確實可以生成任意多的畢氏三元組。亦即, 取正整數 $n$ 及 $m$, 通常取 $m$ 大於 $n$, 而後取 $m$ 及 $n$ 的平方的差, 此即爲 $a$, 而 $b$ 是它們的乘積的兩倍。你將這兩個數平方後相加, 將得到一個完美的平方, 它是 $m$ 及 $n$ 的平方和的平方; 也就是說 $(m^2 - n^2)^2 + (2mn)^2 = (m^2 + n^2)^2$。若你爲 $n$ 和 $m$ 代入正整數, 會生成畢氏三元組 (譯註：例如代 $m = 3$, $n = 2$, 得 5, 12, 13)。如果我們選取互質且不全爲奇數的 $m$ 和 $n$, 則得到的畢氏三元組 $a, b, c$ 會互質且 $a$ 是奇數, 反之, 所有互質的且 $a$ 是奇數的畢氏三元組 $a, b, c$ 都可以這樣生成, 此爲這個主題的第一個定理, 已於 500 BC 被古希臘人證明。

若你考慮的不是平方, 會發生什麼事? 考慮立方、四次方, 或 $n$ 次方時, 會發生什麼事? 費馬最後定理的方程是 $a^n + b^n = c^n$。談到這個方程與費馬本人的關聯, 據說費馬在閱讀希臘數論家 Diophantus 的著作時, 常常在空白處做頁邊筆記, 其中一條寫道：「$a^n + b^n = c^n$ 無解, 其中 $a$, $b$ 和 $c$ 是正整數, $n > 2$」。我們知道的是：費馬的兒子 Samuel 在他父親過世後,

得到他父親的書, 發現他父親寫的頁邊筆記, 並出版附有他父親筆記的新版 Diophantus 著作。我們現在看得到的是 Samuel 的版本, 而有他父親實際手寫註記的 Diophantus 的原書丟失了, 我們沒有那個原本, 只有二手來源。之後發生的是, 頁邊筆記的其他內容, 都陸續由不同的數學家完成證明, 唯獨「$a^n + b^n = c^n$ $(n > 2)$ 無非平凡解解」的敘述無法證明。

費馬聲稱的敘述, 很可能是費馬之後會想要修改的 (如果他找到了這本書, 並回頭看頁邊筆記), 因爲他後來又寫出了 $n = 4$ 特殊情況的完整證明。如果他自認能解決一般次方, 就不會回到四次方, 提出那種費力的證明。作爲一個成熟的數學家, 他後來回頭處理特殊情況的事實, 通常被認爲是一個非常有力的證據, 顯示他意識到：自己寫下頁邊筆記時野心過大或者可能當時醉了。事實上, 費馬解決了比「四次方的總和是四次方」更爲一般性的問題。他證明了兩個 4 次方的和不可能是一個完美的平方, 也就是說方程式 $a^4 + b^4 = c^2$ 無正整數解, 這是一個更強的敘述。

他的證明實際上使用的, 是現今所謂的數學歸納法的變形。他的想法是 ： 如果你有一個 $a^4 + b^4 = c^2$ 的正整數解, 你可以對 $(a, b, c)$ 做一些我稍後將解說的分析, 得到一個更小的解 $(a', b', c')$。[2] 費馬繼續重複這個過程 ： 若有一個解, 你可以得到更小的解, 而後又有更小的解, 接續不絕。但因爲正整數不能小於 1, 你無法生成無限序列的正整數, 其中每個整數都小於先前的整數; 你不能無限下降。因此, 存在正整數解的假設是錯誤的。在邏輯上這與我們通常使用的數學歸納法一樣：你可先證明沒有小於某數值的解, 再以此證明沒有稍大的解, 再以此證明沒有更稍大的解, 一步一步的證下去, 來證明解不存在。這種方法因此有了一個浪漫的名稱：「無限下降的證明 (proof by infinite descent)」。

費馬如何由一組解 $(a, b, c)$ 得出另一組更小的解 $(a', b', c')$ 呢? 他考慮因式分解 ： $a^4 = c^2 - b^4$, 其中 $c^2 - b^4 = (c - b^2)(c + b^2)$。等號右邊的兩個因子都是正數, 它們的乘積是完美的四次方。如果你相信整數系具有質因數分解的唯一性, 而你有互質的兩個整數, 它們的乘積是某整數的 4 次方, 則每個因子本身必須也是整數的 4 次方, 於是你可以寫下一些輔助方程, 並做一點代數 (我不深入演算), 從而得更小的解 $(a', b', c')$, 以實現無限下降。上面說的其實尚有些漏洞。例如, 一開始 $a$ 和 $b$ 的公因數如果是 $d$ 的話, 則很容易看出 $d^2$ 整除 $c$; 如果 $d > 1$, 則 $c - b^2$ 和 $c + b^2$ 兩數也被 $d$ 整除, 故不會互質, 但在這種情況可取 $a' = a/d$, $b' = b/d$, $c' = c/d^2$ 得到更小的解; 如果 $d = 1$, 則 $b$ 和 $c$ 互質, 不過 $c - b^2$ 和 $c + b^2$ 兩數不一定會互質, 但你做一些分析後, 會發現2是唯一可能的公因數。在 2 整除 $c - b^2$ 和 $c + b^2$ 的的情況下[3], 做些類似的分析和演算, 也會得出較小解 $(a', b', c')$。

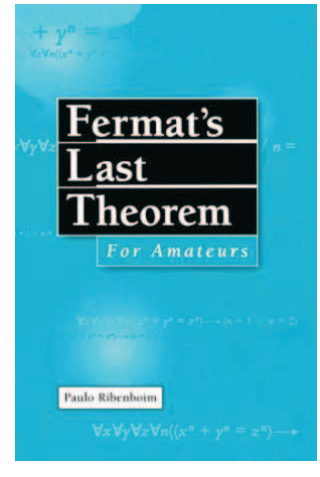
如果你是專業數學家, 且喜歡代數幾何, 則你甚或可把費馬的方法, 重新翻譯成橢圓曲線上的下降 (descent)。

對專業數學家來說, 令人尷尬的是, 我們並不確定費馬沒有證明這個所謂的定理 (它在

[2]有些判斷大小的方法, 譬如可比較 $a + b$ 及 $a' + b'$ 的大小。

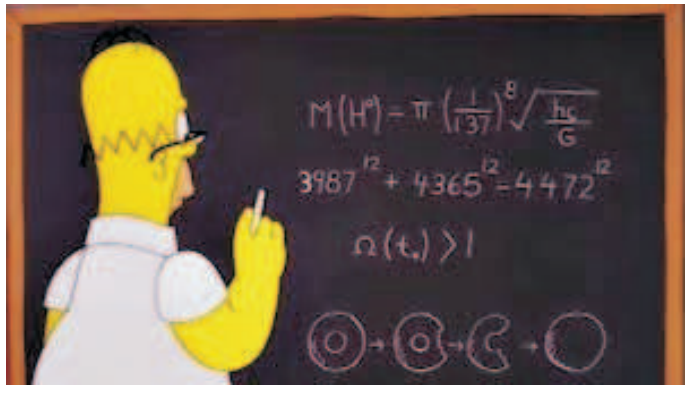
[3]見 https://en.wikipedia.org/wiki/Proof_of_Fermat%27s_Last_Theorem_for_specific_exponents.

1990 年代初期才成爲定理, 在 17 世紀或 18 世紀並不是定理)。我們相信費馬寫下頁邊筆記時構想的證明並不正確, 但也無法確定, 所以仍有一種合理的可能性 : 費馬確實發現了一些東西, 但因沒寫下來而已丟失, 世上某些聰明人, 仍有可能透過代數推演及因式分解, 提出聰明的方法來重建論證。這樣的想法導致, 每一份數學期刊, 特別是數論的期刊, 都會收到源源不絕的文稿, 聲稱重新發現了費馬在 17 世紀的論證。如果你是期刊編輯, 會深感困擾, 因爲你老是收到這些文稿, 而且知道它們是錯的。但你是從經驗判斷它們是錯的, 並非因讀完文稿才說它們是錯的。類似的投稿, 有解決 Goldbach 猜想的、黎曼猜想的, 或物理學的大統一等等的; 看到這些標題, 編輯們就知道麻煩又來了, 但邏輯上, 也不能完全否定它們之中有朝一日出現正確證明的可能。




數論學家 Paulo Ribenboims 是巴西人, 任教於加拿大安大略省的 Kingston 的 Queen's University (已退休)。他爲業餘人士寫了題爲《*Fermat's Last Theorem*》的書。這是一本相當厚實的書, 總結所有已知在費馬方程上基本技巧能做的事。如果你有雄心壯志, 想藉由基本技巧來證明費馬最後定理, 不防從閱讀本書起步, 學習所有的東西。也許你能找到些額外的東西, 足以證明這個定理。

暢銷書及大衆媒體常愛牽扯到費馬最後定理, 譬如《龍紋身的女孩》這部小說。我準備演講時, 向柏克萊的某位數論學者提及此事, 他說 :「我們應該告訴衆人星際爭霸戰 (Star Trek) 的事」。星際爭霸戰是 1960 年代的電視影集, 擁有廣大粉絲。你可以去 YouTube 看其中一集"*Fermat's Last Theorem of Star Trek*"; 在那集中, 主角討論著 :「費馬最初的斷言已延宕 700 年, 迄今懸而未決」。他們錯了, 不過當時寫劇本的人, 也無法從心所欲地展望未來。有許多與費馬最後定理相關的暢銷書, 你可在 Google 圖書搜尋關鍵字『費馬』, 並試圖排除任何疑似在討論數學的東西; 你會發現那些痴迷於費馬最後定理的小說人物及主角。




費馬也出現在名爲辛普森的電視影集。值得注意的是, 辛普森的大多數編劇, 在寫作時都堅持忠於各種數學。不久前賽蒙辛 (Simon Singh) 寫了一本關於辛普森的書。賽蒙辛是英國作家; 他起初是物理學家, 曾在瑞士擔任博士後, 之後爲 BBC 做紀錄片。他曾爲費馬最後定理製作紀錄片 (美國稱之爲 The Proof), 英

國廣播公司成片後數月, 在美國上映, 也在 YouTube 播出。他拍完這部紀錄片後, 熱衷於費馬最後定理, 寫了一本關於它的書。那是一本很棒的書。之後他繼續著述,「我曾是物理學家, 曾是紀錄片製作人, 現在是科普作家」。他正在寫宇宙學、數學、密碼學及其他主題的書。他非常棒, 我當然推薦這本關於費馬的書[4]。

現在我們稍微深入地談些較爲嚴肅的數學, 但仍以歷史的角度來看。費馬把 $n = 4$ 的情況分開處理。而 $n = 2$ 的情況是希臘人的研究, 實際上並不屬費馬最後定理; 費馬最後定理關乎 $n > 2$。你可能會問：已知 $n = 4$ 是如何, 那麼 $n = 3$ 或 $n = 5$ 時會是如何? 從基本觀點來看, 明顯的是： 若你能對某指數證明定理, 則也證明了 $n$ 爲該指數的倍數的情況。例如, 你不必擔心 8 次方, 因爲 8 次方也是 4 次方; 你不必擔心 12 次方, 因爲 12 次方也是 4 次方。如果你考慮比 2, 3, 4, 5 大的數字, 每個這樣的數字都可以用 4 或某奇數的質數來整除。既然費馬完成了 $n = 4$ 的情況, 你只需處理 $n$ 爲質數的情況, 而後套用這個基本的論證。你必須看的是其他質數： 3, 5, 7, 11, 13, 17等等。因此, 不用處理一般的 $a^n + b^n = c^n$, 你僅需考慮 $a^p + b^p = c^p$, $p$ 爲奇質數的情況, 費馬方程式通常採此形式。

費馬證明 $n = 4$ 的情況後, 下個世紀中 Euler 處理了 $n = 3$ 的情況, 他的論證與費馬的論證區別不大, 除了他把等號右邊 $c^3 - b^3$ 分解成 3 個因子[5], 而不是如同 $n = 4$時分解成兩個。在此情況有三個因子, 攸關 3 次單位根 $(-1 + \sqrt{-3})/2$, 因此會涉入更複雜的算術：不只有整數, 且有 $-3$ 的平方根。這是初等數論的好課題。今天下午有些想學初等數論的人要我推薦書, 我推薦 Niven、Zuckerman 及 Montgomery 寫的初等數論好書《*An Introduction to the Theory of Numbers*》第五版, 此書討論了在包含 3 次單位根 $(-1 + \sqrt{-3})/2$ 之數系的算術, 你可以從中理解 Euler 的論證, 確實僅有兩三頁, 很值得學。

Euler 以降的數年及數世紀裡, 數學家確實處理了 $p = 5$ 及 $7$ 的情況, 但進度緩慢[6]。值得注意的是, 之後數學家開發出一種方法, 能夠快速檢查：對於給定的 $p$, 費馬方程式是否沒有正整數解 (或說費馬最後定理在 $p$ 成立)。這正是你很難向紐約時報記者解釋的： 你不能靠有限的計算來真正證明定理, 但對於任何給定的 $p$, 費馬最後定理在 $p$ 是否成立, 確實存在可用數值檢驗的判別法。檢驗大的質數 $p$ 需要使用電腦。例如在 1950、1960 年代, 就能檢驗出費馬最後定理在 $p = 144169$ 成立。如此藉由電腦的計算來檢驗費馬最後定理, 著實成果驚人。在 Wiles 宣布結果時, 電腦計算已經驗證出： 費馬最後定理在小於 400 萬的質數都成立, 這是 Buhler, Crandall, Ernvall, Metsänkylä 的工作。有趣的是, 四人的工作發表在 *Mathematics of Computation* (該期刊發表一些有關計算的成果) 時, 並不被看重。大家都知道 *MathSciNet*, 這是美國數學學會的線上系統, 用以對數學論文進行編目及評論; 是美國數學學會的一項傑出產品。實際上, 當時 *MathSciNet* 評論者對於四人的工作, 只是說：「常見的

[4]此書及賽蒙辛的另一本著作 "*The Code Book*"《碼書》有中譯本. 由台灣商物印書館發行。

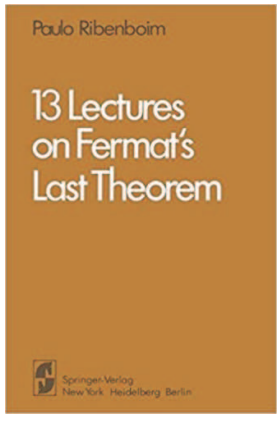
[5]$c^3 - b^3 = (c - b)(c - \omega b)(c - \omega^2 b)$, 其中 $\omega$ 是單元的立方根。

[6]見 https://en.wikipedia.org/wiki/Proof_of_Fermat%27s_Last_Theorem_for_specific_exponents.

猜測得到證實：費馬最後定理」。箇中牽涉到的運算確實很普通, 而你可以輸入任何質數 $p$, 只要大小在電腦可以處理的範圍, 即可經由電腦運算檢驗費馬最後定理在 $p$ 的情況。

回顧歷史, Euler 處理了 $p = 3$, 而 Dirichilet 及 Lamé 等人處理了 $p = 5$ 或 7。在電腦科學時代, 如何從 20 世紀之前的一位數、兩位數的 $p$, 轉化爲非常大的 $p$? 何以致之? 答案如我之前所述：你必須做因數分解。費馬的論證把等號右邊分解爲兩個因子; Euler 的論證則有三個因子。對於質數 $p$, $c^p - b^p$ 是 $p$ 個不同因子的乘積[7]。你必須引入 $p$ 次單位根, 它不是 1, 但其 $p$ 次方是 1; 如果你想把它記成複數, 你可取它爲 $e^{2\pi i/p}$; 如果你想抽象些, 你就說你選取了一個, 但不明確說出它的值。現有 $p$ 個不同因子, 我們可否重複費馬在 $n = 4$ 的論證? 你或許認爲：不同的因數的乘積爲完美的 $p$ 次方時, 每個因數都應爲完美的 $p$ 次方。事實上, 這個想法導致許多人提出了費馬最後定理的錯誤證明。這種證明是錯誤的, 因爲有這種「$p$ 次方必爲 $p$ 次方的乘積」的想法是有問題的。在較複雜的數字系統時, 質因數分解不具唯一性; 如果你的參考經驗是普通整數的算術, 可能不會預期此事; 事情並不像你想像的那麼好。

人們好奇：是否這正是費馬寫下頁邊筆記時所犯的錯誤。但數學史學者會告訴你, 在費馬的時代, 人們尚未想到這種複雜系統的質因數分解唯一性的問題; 但我們當然不知道實情。對費馬能做什麼、不能做什麼的看法, 總帶著臆測性。




有一本書解說了這整個主題, 也是 Paulo Ribenboims 的著作, 是本令人愉快的書。它出版於 1979 年, 以非常親切的方式向專業數學家講述費馬最後定理迄至當時的一切。這是一本很好的書。

在這次演講的最後, 我想談談我在理想類方面的論文。我本可把時間全用在談論 Andrew Wiles 以及 1993 年、94 年及 95 年發生的事, 其中有許多重大的歷史值得談, 但我選擇最後回到質因數分解的議題。費馬最後定理的研究衍生出許多理論, 有些並未被 Andrew Wiles 用於費馬最後定理的證明, 但並不意味它們沒有價值或有所缺失。費馬最後定理的研究, 提供了數學各種不同的工具, 迄今仍被使用。

但在此之前, 容我在很短的時間內, 談談 90 年代中葉費馬最後定理的實際證明。令人驚嘆的是, 它涉及到一個小小的輔助建構, 這個輔助建構源自德國數學家 Gerhardt Frey 在 80 年代初期的構想。Frey 的構想是：假設 $a, b, c$ 是費馬方程式的正整數解, $a^n + b^n = c^n$, 考慮輔助的三次方程式：$y^2 = x(x - a^n)(x + b^n)$, 這定義了一條所謂的橢圓曲線, 然後再試圖導出矛盾。Frey 想到的矛盾的性質是 Wiles 在 Richard Taylor 的幫助下證明的, 他們證明這條橢圓曲線是模的 (modular), 這是說它與模形式 (modular form) 有某種關聯。而我在 1986 年證明了該曲線不是模的。這是個反證法, 邏輯上有些複雜難懂。1993 年, 向電視記者解說時,

[7] $c^p - b^p = (c - b)(c - \omega b) \cdots (c - \omega^i b) \cdots (c - \omega^{p-1} b)$, 其中 $\omega$ 是選定的 $p$ 次單位根。

我必須仔細地考慮自己到底能說什麼。

現在來談談質因數分解。首先, 把所有的整數及一個 $p$ 次單位根做所有可能的、有限多次的加、減、乘運算, 建構成了由 $p$ 次單位根所生成的環 (ring)。這個環是否具有質因數分解的唯一性? 答案是: 當 $p$ 等於 3, 5, 7, 11, 13, 17 和 19 時, 確實如此, 但僅止於這些。不能超過 19; 這是已知的, 23 不是如此。John Masley 和 Hugh Montogomery 在 1970 年代證明[8]: 對於超過 19 的質數, 質因數分解在其對應的環不具唯一性。如果你的論證用到質因數分解的唯一性, 你可能要放棄它, 因爲它只適用於我列出的質數, 不能大於 19。

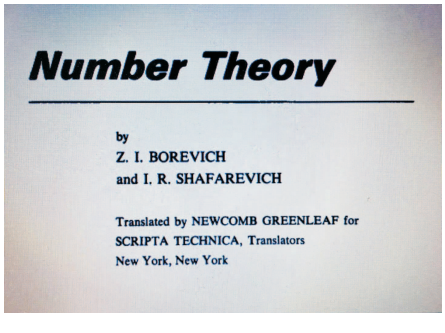
現在來講一些研究生該知道的專業數學。當你嘗試在數學中研習某件事時, 必須有阻礙物 (obstruction) 的概念, 它阻礙某事發生。在目前情況, 質因數分解唯一性的阻礙物是個有限群, 被稱爲類群 (class group), 因其依賴於其所對應的質數 $p$, 我們寫下足標 $p$ 並記之爲 $\mathcal{G}_p$ 。它是有限的阿貝爾群 (abelian group)。(事實上, 在代數數論, 它爲有限並非明顯的事實, 必須用一些論證才能證明)。由 $p$ 次單位根所生成的環具有質因數分解的唯一性, 若且唯若它所對應的類群只有一個元素 (亦即是平凡群)。令人驚訝的是, Masley 和 Montogomery 證明, 這個群僅當 $p$ 不大於 19 時才爲平凡群。而你所要做的就是弄清楚超過 19 的情況。


Ernst Kummer

這個主題的大英雄顯然是 19 世紀的 Ernst Kummer, 他催生了當代代數數論。他審視涉及質因數分解的論證後證明: 若類群 $\mathcal{G}_p$ 的階 (order) 不能被 $p$ 整除, 費馬最後定理在 $p$ 仍成立。這是 Kummer 的定理。

類群的階被稱爲類數 (class number)。結構上, 你取此阿貝爾群的 $p$-part[9], 這個子群是平凡群, 恰當 $p$ 不能整除類數。譬如, 質因式分解非唯一的首個質數是 $p = 23$, 類數爲 3, 不能被 23 整除。當 $p = 29$, 類數不能被 29 整除。當 $p = 31$, 類數也不能被 31 整除。但當 $p = 37$, 類數被 37 整除。如是, Kummer 的定理不適用於所有質數, 但它適用於許多質數。

聽衆中有人曾問我: 該讀什麼數論的書? 較進階的, 我在演講廳外提到了 Borevich 及 Shafarevich 的書, 我曾從中學習 Kummer 的論證, 你不妨把它當作這個演講的參考文獻。




Kummer 不僅在類數不能被 $p$ 整除時, 證明了費馬最後定理, 而且給出了數值判別法, 使你能夠很快判斷類數是否可被 $p$ 整除。

[8] J. M. Masley and H. L. Montgomery, *Cyclotomic fields with unique factorization*, J. Reine Angew. Math. **286/287** (1976), 248-256.

[9] 即 the Sylow $p$-subgroup of $\mathcal{G}_p$.

如何得知 37 整除 $\mathcal{G}_{37}$ 的階? Kummer 的判別法涉及伯努利數 (Bernoulli number), 它是與指數函數非常相關的某函數之泰勒係數。考慮指數函數, $e^x$ 的冪級數從 1 起頭, 將它減去 1, 則差的冪級數以 $x$ 起頭, 將其除以 $x$, 則冪級數再次從 1 起頭。對這個從 1 起頭的冪級數取倒數, 得到從 1 起頭的如下冪級數 :

$$\frac{x}{e^x-1}=1-\frac{x}{2}+\frac{x^2}{12}-\frac{x^4}{720}+\frac{x^6}{30240}-\cdots .$$

審視它時, 會發現一些你能很快證明的性質。其一是僅 $x$ 的偶次冪有非零係數, 唯一的例外是 $x$ 本身, 其係數爲 $-1/2$。另外, 非零係數出現於平方項、四次方項等等, 正負號交替。將 $x^i$ 的係數乘以階乘 $i!$ 即爲第 $i$ 個伯努利數 $B_i$。因此, $B_1=-1/2$, $B_2=1/6$, 而 $B_4$ 是 $-720$ 除以 $4!$ 之後取倒數 :

$$B_2=\frac{1}{6},\ B_4=-\frac{1}{30},\ B_6=\frac{1}{42},\ B_{12}=-\frac{691}{2730},\cdots .$$

開頭幾個伯努利數都是分子爲 1 的分數; $B_{12}$ 是首個分子不爲 1 的分數, 其分子爲 691。Kummer 的判別法可由這些伯努利數描述。他證明 : 類數不能被 $p$ 整除若且唯若伯努利數串 $B_2, B_4, \ldots, B_{p-3}$ 中各個分數的分子都不能被 $p$ 整除。你須取成串的伯努利數, 共有 $p-3$ 個, 其實是 $(p-3)/2$ 個, 因爲其中一半爲零, 你希望其中沒有一個分數的分子能被 $p$ 整除 : 若是這樣, 則 Kummer 定理的條件就成立, 你就能確定費馬最後定理在 $p$ 成立。

來談談它們不能被 $p$ 整除的機率。不妨將各個分子當成隨機數, 則其不被 $p$ 整除的機率爲 $1-(1/p)$。因此, 粗略來說, $p$ 滿足 Kummer 定理的條件的機率爲 $(1-1/p)^{(p-3)/2}$, 其中 $(p-3)/2$ 是你必須檢查的伯努利數的個數。令 $p$ 趨近無窮大, 由微積分得知該機率的極限值爲 $e^{-1/2}$。這粗略意味著, 對指數 $p$ 證得費馬最後定理的機率爲 $e^{-1/2}$, 約爲 60.65%。亦即, 直觀的說, 全部質數中約有三分之二的 $p$, 可據此證明對應的費馬方程式 $x^p+y^p=z^p$ 沒有非零正整數解。

你或許會問 : 1993 年 Buhler, Crandall, Ernvall, Metsänkylä 爲上達 400 萬的數字證明了定理, 這些數字都屬這三分之二嗎? 如果你閱讀那些書, 會看到改良過的條件。在 Kummer 定理的條件 (意即 $p$ 不整除類數) 不被滿足的情況, 後繼者發現了越來越多關於 $p$ 的條件, 來證明費馬最後定理在 $p$ 成立。它們都是很好的條件, 分別適用於某些質數。而且, 400 萬以內的每一個質數 $p$, 都有一個適用條件。但我應該舉幾個例子來說明 Kummer 判別法失靈的情況。例如, 取 $p=37$, 則你必須檢查 $B_2$ 及 $B_{34}$ 之間的伯努利數, 其中 $B_{32}$ 的分子可被 37 整除 :

$$B_{32}=\frac{37\cdot 783\cdot 305065927}{510};$$

因此 Kummer 的條件對 37 不奏效。另外, 極其著名的是, Kummer 條件在 $p$ 爲質數 691 時也不被滿足; 此時你考慮 $B_2$ 及 $B_{689}$ 之間的伯努利數, 其中 $B_{12}$ 的分子爲 691。這些是不滿足 Kummer 條件的質數, 稱爲不規則質數 (irregular primes)。

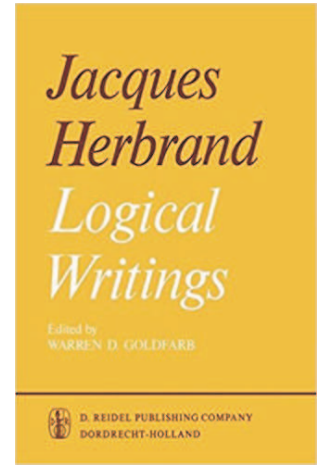
2001 年, Buhler, Crandall, Ernvall, Metsänkylä, Shorkrollahi 合寫的一篇論文驗證了：若你取 1200 萬以內的質數, 共有比例約 61% 的質數 $p$ 滿足 Kummer 的條件, 此數值非常接近直觀猜測的 $e^{-1/2}$。

你可回到 Borevich 和 Shafarevich 的書, 從而可用一些簡單的技巧來產生不規則質數, 因而得到無限多個不規則質數。對我來說, 真正神奇的是, 規則質數 (regular primes) 理應占多數, 但我們竟不知它們的個數是否無限。在數論中有很多這類的尷尬：許多非常簡單的問題, 答案仍屬未知。回首 19 世紀, Kummer 的條件看似適用於大多數質數; 但我們其實無法證明如此的質數有無限多個。這真的非常令人驚訝。

因爲演講的時間有限, 對我在 1976 年左右關於 Kummer 判別法的工作, 我將僅做非常簡單的描述。Kummer 判別法是一個非常明確的敘述：若且爲若某件事是對的, 另一件事才是對的。1976 年時我還在用熟悉的打字機打論文。我在巴黎 IHÉS 研究所使用秘書的辦公室, 因爲秘書的打字機比數學家的好, 而且我想仔細打些符號及希臘字母。我在午餐時間借用秘書的辦公室。哈佛的某著名數學家進來說：「你在做什麼?」我說：「我正在改進 Kummer 判別法」。他說：「爲什麼要改進 Kummer 判別法? 這是一個判別法, 還有什麼可說的? 」答案是： 這個判別法中有 $(p-3)/2$ 個不同的伯努利數。而你可以把我之前介紹過的類群分解成 $(p-3)/2$ 個不同的分部 (component)。我初次證明的是： 不同的伯努利數對應於不同的分部。我所以會做這個, 是要檢查我正在著手的工作。我不認爲這有甚麼了不起, 以爲這已衆所周知。我在 IHÉS 吃午餐時 (你知道這是該研究所的價值：你可以在與同事共進午餐時討論數學), 提到我在檢查某事, 於是 John Coates 抬頭說道：「等一下。這是未知的。誰證明了它? 它還未被證明。」我很困惑, 這有點像天啟的感覺, 我頓時不知道自己正在做什麼; 我之前以爲這是個已被證明的定理, 我只是給它一個新的證明。

我會再次跳過一些投影片, 因爲演講時間很短。但我想給你看一張 Jaques Herbrand 的照片, 他是 20 世紀早期的邏輯學家兼數論學家。他在畫面中央, 非常、非常年輕。他出生於 1908 年, 1931 年去世, 兩個年份的間隔不大。他在拍攝這張照片的山中失足身亡, 得年 23 歲或 22 歲。我還是一名學生時, 獲悉他的故事, 因爲我的室友是一位邏輯學家, 正在翻譯他的書"*Ecrits logiques*" (邏輯寫作), 我幫室友翻譯與 cyclotomic fields (分圓體) 有關的部分; cyclotomic 意味著切割圓。在書中 cyclotomic fields 被稱爲 corpus circulaires。我和室友想了解 corpus circulaires 意味著什麼, 而我發現它就是 cyclotomic fields (分圓體), 並如此翻譯。結果是, 我爲伯努利數及類群的分部建立聯繫時所證明的, 實際上是 Herbrand 過世前隱微證明之敘述的逆命題。他證明：若伯努利數不能被 $p$ 整除, 則相應的分部是平凡群。我證明：若伯努利數被

$p$ 整除, 則相應的分部就非平群。我藉由模形式來證明; 我用模形式構建出該分部所對應的類體 (class field)。




我的工作遵循 Serre 在 1967 年撰寫的文章, 他在文章中首次將 Galois 表示與模形式聯繫起來, 或者至少他看到了這種聯繫; 他沒有確實把它們聯繫起來, 幾個月後, Deligne 證明了 Serre 隱微認爲必然爲真的聯繫。Serre 這篇具有巴黎風格的數論文章, 充溢著改變數論的奇妙想法, 是我非常用心去了解的。但回溯 MathSciNet 對那篇文章的評論, 評論者對此全然不感興趣 :「作者對拉瑪努嘉 $\tau$ 函數的結果做了全面評述」。這是整個評論。但 Serre 做的不僅僅這些。他介紹了模形式與 Galois 表示之間的整個聯繫; 用此聯繫, 我們才得以證明 Herbrand 的結果的逆命題。

我不會瀏覽隨後的投影片。但事實顯示, 在分圓體、有理數等情況下, 觀察其擴展, 以及將其嵌入更複雜的事物, 是一種很好的解決問題方式。它讓你從試圖了解的群, 轉換到資訊豐富的、較大的群。許多人發現我的技巧適用於其他情況, 而對數論產生了相應的影響。

—整理者陳其誠任教於台灣大學數學系—