費馬最後定理:
A. Wiles 的解決方法

李文卿

余文卿　合著

懸疑三百多年的費馬最後定理最近又引起世人的注意。原因是 A. Wiles 宣稱他解決了整個問題; 但不久, 證明中被找出有漏洞。爲此, 香港中文大學在 1993 年 12 月 18 日到 21 日舉行一 "橢圓曲線與模型式研討會", 邀請看過 Wiles 手稿的人以及 Wiles 所用到定理的關係人, 就 Wiles 工作做系統性的介紹。明顯的結論是: Wiles 的證明是建立在一不等式上, 這不等式是兩有限群之秩之間的關係式, 不等式一邊之有限群的秩有辦法計算, 但另一邊 Selmer 群的秩則難以估計。故實質上, Wiles 並未完全解決費馬最後定理。底下是李文卿教授在去年七月裡根據 e-mail 得到的信息所整理出來的摘要性文章, 部份內容經第二作者依據最新的發展修改過, 並寫成中文, 或能滿足讀者的好奇心。

1. 費馬最後定理與橢圓曲線的關連性

給定一定義在 Q 上的橢圓曲線

$$E : y^2 = x^3 + ax^2 + bx + c$$

以 $E(Q)$ 表示 E 上所有有理點所形成的群。根據 Mordell-Weil 定理, 我們知道群 $E(Q)$ 的結構, 是一有限群乘上階數有限的自由交換群 (free abelian group of finite rank), 而這有限群是 $E(Q)$ 的 torsion 部份 (即秩是有限的元素所形成的子群)。研究橢圓曲線的人曾提出一個問題: 當 E 變動的時候, $E(Q)$ 的 torsion 部份的秩是否會有上界, 且這上界只跟其定義域 Q 有關? Ogg 曾猜測 $E(Q)$ 的 torsion 部份所形成的子群只能有 15 種結構, 這猜測於 1976 年被 B. Mazur 所證實 [參考 7, 8, 9]。設 N 是不具平方因子的正整數。若 E 含有一秩爲 N 的有理點, 則它會給出模型曲線 (modular curve) $X_0(N)$ 上一有理點。Mazur 的證明中有一重要步驟是研究 Hecke 代數 T, 它是模型曲線 $X_0(N)$ 之 Jacobian 上的自同態環, 並且考慮 T 的 $p-$ 進位完備畢包

($p-$ adic completions)。在另一方面, 有一些人在研究使秩較大之元素不存在的局部條件時發現: $E(Q)$ 上若有秩是 $2p$ 的點且 p 相當大, 則可以找到三個這樣的點, 其三個 x 坐標正好是費馬方程式 $x^p + y^p = z^p$ 的一組非顯然的解。因此, Mazur 的結果多少肯定了費馬最後定理的眞實性。

反過來, G. Frey 提出下列有原創性的概念: 他從費馬方程式的非顯然解去建構一橢圓曲線, 其步驟如下。設 p 是一比 3 大的質數且假設 (a, b, c) 是方程式 $x^p + y^p + z^p = 0$ 的一組原始整數解 (無公因數)。定 $A = a^p, B = b^p$ 且 $C = c^p$, 考慮橢圓線

$$E_{A,B} : y^2 = x(x - A)(x - B)$$

這曲線也被稱爲 **Frey** 曲線。Frey [3, 4] (也參考 [11]) 證明 $E_{A,B}$ 具有很多好的性質, 包括底下這些:

(i) $E_{A,B}$ 的 conductor N_E 是 ABC 之質因數的乘積。

(ii) E 是半穩定 (semi-stable); 亦即 $E_{A,B}$ 若對某一質數 q 有壞的 reduction (即 $E_{A,B}$ mod q 後不再是一橢圓曲線), 則必是乘性 (multiplicative) reduction (換句話說, $E_{A,B}$ mod q 後的曲線上無尖點存在)。

對每一正整數 m, 以 $E[m]$ 表示 E 上的 $m-$ 等分點。那麼 $E[m]$ 同構於 $Z/mZ \times Z/mZ$, 且 Galois 群 $G_Q = Gal(\bar{Q}/Q)$ 作用在這群上, 以 $\rho_{E_{A,B},\ell}$ 表示當 m 爲一質數 ℓ 時所生成的 G_Q 的群表現。

(iii) $\ell \geq 11$ 時, $\rho_{E_{A,B},\ell}$ 的值域是群 $GL_2(Z/\ \ell Z)$ 的全部 (這是根據 Mazur 的一個定理 [9])。

由上面性質可推出

(iv) 當 $l \geq 5$ 時, 群表現 $\rho_{E_{A,B},\ell}$ 是不可約 (irreducible), 且是非常溫和分歧 (mildly ramified)。因此它引出一平的 (flat) 的 group scheme。

2. Shimura-Taniyama-Weil 猜測與 Serre 猜測

設 E 是定義在 Q 上的橢圓曲線, 其 conductor 是 N_E, Shimura-Taniyama-Weil 猜測是說: 存在有一從模型曲線 $X_0(N_E)$ 到 E 的映型 (morphism) φ, 它把 $i\infty$ 映到 E 的原點, 且它把 E 上的標準全純微分形式 (Standard holomorphic differential form) 拉回到 $X_0(N_E)$ 上的微分形式, 後者能以 $f(z)dz$ 的非零有理數倍表之。在此 f 是同餘子群 (congruence group) $\Gamma_0(N_E)$ 的一個權 (weight) 爲 2 的正規化尖點新型式 (normalized cuspidal newform)。說得更精確一點, 若附著在 E 上的 L - 函數是

$$\begin{aligned} & L(s, E) \\ = & \prod_{p|N_E} (1 - a_p p^{-s})^{-1} \prod_{p \not| N_E} (1 - a_p p^{-s} + p^{1-2s})^{-1} \\ = & \sum_{n=1}^{\infty} a_n n^{-s}, \end{aligned}$$

則 $f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}$。此處, 當 $p \not| N_E$ 時, $E(mod\, p)$ 上的 Z/pZ 一點的個數是

$1+p-a_p$; 當 $p|N_E$ 時, a_p 爲 1, -1 或 0, 依 $E(mod\, p)$ 的情況而定。

從一橢圓曲線 E 以及一給定的質數 ℓ, 我們得出 Galois 群 G_Q 的兩種群表現。一是從 G_Q 作用在 $E[\ell]$ 所得出的表現 $\rho_{E,\ell}: G_Q \to GL_2(Z/\ell Z)$, 這已在上面解釋過; 另一是從 G_Q 作用在 Tate 模 (Tate module)

$$T_\ell = \lim_{\leftarrow n} E[\ell^n]$$

所得到的 ℓ- 進位表現 $\widetilde{\rho_{E,\ell}} : G_Q \to GL_2(Q_\ell)$。這是因爲 T_ℓ 是階數爲 2 的 Z_ℓ-模, 因此 $T_\ell \otimes_{Z_\ell} Q_\ell$ 是一佈於 Q_ℓ 上的 2 維向量空間。

顯然地, 限制在餘數體時, $\widetilde{\rho_{E,\ell}}$ 化爲 $\rho_{E,\ell}$, 這 ℓ- 進位表現有下面的性質: 對所有質數 $p \not| \ell N_E$ 而言, 我們有

$$a_p = \mathrm{Tr}(\widetilde{\rho_{E,\ell}}(\mathrm{Frob}\ p)),$$

且

$$p = \det(\widetilde{\rho_{E,\ell}}(\mathrm{Frob}\ p))。$$

當 ℓ 變動時, 稱 $\{\widetilde{\rho_{E,\ell}}\}$ 是附著在 E 上之 ℓ- 進位表現的一相容族 (compatible family)。(質言之, ℓ- 進位表現是 $Gal(Q^\ell/Q)$ 的群表現, 其中 Q^ℓ 是 Q 在 $\bar{Q}$ 中使得 ℓ 之外的位 (place) 皆不分歧的最大擴充體)。

另一方面, 一權 $k \geq 2$, 階數是 N 且特徵是 χ 的尖點新型式

$$g(z) = \sum_{n=1}^{\infty} b_n e^{2\pi i n z}$$

的 Fourier 係數 b_n 落在某一數體 K 的整數環 Q_k 中。Deligne [1] 證明了存在有一 λ-進位表現的相容族 $\{\widetilde{\rho_{g,\lambda}}\}$

$$\widetilde{\rho_{g,\lambda}} : G_Q \longrightarrow GL_2(K_\lambda)。$$

其中 λ 跑遍 K 中不整除 N 的所有有限位置。對幾乎所有的質數 p, 下列關係成立。

$$b_p = \mathrm{Tr}(\widetilde{\rho_{g,\lambda}}(\mathrm{Frob}\ p))$$

且

$$\chi(p)p^{k-1} = \det(\widetilde{\rho_{g,\lambda}}(\mathrm{Frob}\ p))。$$

對一 G_Q 的 λ- 進位表現而言, 若它同構於某一 $\widetilde{\rho_{g,\lambda}}$, 其中 g 是一新型式, 則稱它是模型 (modular) 表現。因此, 一定義在 Q 上的橢圓曲線 E 滿足 Shimura-Taniyama-Weil 猜測的充要條件是存在有一質數 ℓ 使得 $\widetilde{\rho_{E,\ell}}$ 是模型表現; 且因 Dirichlet 級數 $L(s,E)$ 有整係數, 存在一個質數 ℓ 使 $\widetilde{\rho_{E,\ell}}$ 是模型表現的充要條件是對所有質數 ℓ 而言, $\widetilde{\rho_{E,\ell}}$ 都是模型表現; 這可視爲 Shimura-Taniyama-Weil 猜測的局部版本。

上面所談到 g 的 λ- 進位表現 $\widetilde{\rho_{g,\lambda}}$ 引出另一佈於有限域的 G_Q 的表現

$$\rho_{g,\lambda} : G_Q \to GL_2(k),$$

其中 k 是質理想 λ 在 K 中的餘數體。對幾乎所有的質數 p, 我們有

$$b_p \equiv \mathrm{Tr}(\rho_{g,\lambda}(\mathrm{Frob}\ p)) \ (\mathrm{mod}\ \lambda)$$

和

$$\chi(p)p^{k-1} \equiv \det\left(\rho_{g,\lambda}(\mathrm{Frob}\ p)\right) \ (\mathrm{mod}\ \lambda)。$$

更進一步, 以 c 表示 Q 上將元素映至其共軛複數的自同構, 則 $\det \rho_{g,\lambda}(c) = -1$。一般來說, G_Q 的表現 ρ 若滿足 $\det \rho(c) = -1$,

則稱之爲奇表現, 在 1987 年, Serre 在 [11] 中提出下列猜測: 任一 (連續) 不可約佈於有限體 k 的奇表現

$$\rho : G_Q \to GL_2(k)$$

必是模型表現。換句話說, 存在某一 g 與 λ, 使得 $\rho = \rho_{g,\lambda}$。我們注意到對一模型表現 ρ 而言, g 的選擇性並不唯一。Serre 進一步給一個推測描述某一特定 g 的存在性, 並給出 g 的權數, 階數與其特徵。1990 年, K. Ribet [10] 證明 Serre 猜測的後半部伴隨著前半部成立而成立。而由這結果推出費馬最後定理隨著 Shimura-Taniyama-Weil 猜測成立而成立, 理由如下。

假設不然, 從 $x^p+y^p+z^p = 0, p \geq 11$ 的一組非顯然原始解, 我們得到一 §1 中討論過的 Frey 曲線因 Shimura-Tariyama-Weil 猜測對 $E_{A,B}$ 成立, 其 p- 進位表現 $\rho_{\widetilde{E_{A,B},p}}$ 是一模型表現, 因此 $\rho_{E_{A,B},p}$ 也是。更進一步, $\rho_{E_{A,B},p}$ 是一不可約奇表現, 則根據 Serre 推測的後半部, 存在有一 $\Gamma_0(2)$ 的新型式 g, 其權爲 2, 使得 $\rho_{E_{A,B},p} = \rho_{g,p}$。另一方面, 已知 $\Gamma_0(2)$ 的虧格 (genus) 數是零, 這類的模型式並不存在, 故費馬最後定理成立。

[註記] Serre 在 [11] 中得證: Shimura-Tariyama-Weil 猜測隨著 Serre 猜測成立而成立。

因 Frey 曲線 $E_{A,B}$ 是半穩定, 利用上面的論點, 要證明費馬最後定理, 我們只要證明

Shimura-Taniyama-Weil 猜測對定義在 Q 上的半穩定橢圓曲線成立。

這就是 Wiles 所要證明的。底下, 我們描述一下他的處理方式以及困難所在。

3. 尋求一質數 ℓ 使得$\rho_{E,l}$ 是模型表現

此後, 設 E 是定義在 Q 上的半穩定橢圓曲線, 如 §2 中所解釋, 只要證明對某一 ℓ 而言, $\widetilde{\rho_{E,\ell}}$ 是模型表現即可。如此, 對同一 ℓ, $\rho_{E,\ell}$ 也是模型表現。爲尋找可能的 ℓ, 我們看一下表現 $\rho_{E,l}$ 上的信息。取 $\ell = 3$, 群 $GL_2(Z/3Z)$ 是 $PGL_2(Z/3Z)$ 的二次中心擴充 (central extension)。由 $PGL_2(Z/3Z)$ 在投影線 $P^1(Z/3Z)$ 的作用可看出 $PGL_2(Z/3Z)$ 同構於置換群 S_4。由於 S_4 的二次中心擴充可嵌入 $CL_2(Z[\sqrt{-2}])$ 中, 我們可將特徵是 3 的表現

$$\rho_{E,3} : G_Q \to GL_2(Z/3Z)$$

提升爲特徵是 0 的表現

$$\rho : G_Q \to GL_2(Z[\sqrt{-2}]) \subset GL_2(C)。$$

假設 $\rho_{E,3}(G_Q) = GL_2(Z/3Z)$, 那麼表現 ρ 是奇, 不可約且是 S_4 型, 根據 Langlands [6] 與 Tunnell [12] 在 GL_2 的基底變換 (base change) 理論, 存在有一尖點模型式 f, 其權是 1, 階數等於 ρ 的 conductor, 且滿足 $L(s,f) = L(s,\rho)$。再利用整係數 Eisenstin series 的同餘性質, 可證明存在一權數爲 2 的模型式 g 使得 $\rho_{E,3} = \rho_{g,3}$是模型表現。

當 $\rho_{E,3}(G_Q)$ 只是 $GL_2(Z/3Z)$ 的眞子集時該怎麼辦? 這發生在 E 具有一秩是 3 的有理群的情況。因 E 是半穩定, 故 E 沒有秩是 5 的有理群; 否則的話, 將給出 $X_0(15)$ 上一個 non-cuspidal 有理點。但已知 $X_0(15)$ 具有 4 個 non-cuspidal 有理點, 它們都由非半穩定的橢圓曲線所給出。因此

$$\rho_{E,5} : G_Q \to GL_2(Z/5Z)$$

是蓋射(surjective)。在這情形下, 將找出 Q 上另一半穩定橢圓曲線 E' 使得 $E'[5]$ 同構於 $E[5]$ (故 $\rho_{E,5} = \rho_{E',5}$) 且 $\rho_{E',3}$ 是模型表現。爲找到這樣的 E', 考慮模型曲線 X, 它由定義於 Q 上, 且 5- 等分點同構於 $E[5]$ 之橢圓曲線的等價類所組成。這曲線是 $X(5)$ 的一 "扭曲"(twist), 其虧格數是零且含有一有理點, 亦即 E 所代表的等價類; 因此它是一投影線, 從而包含無窮多個有理點。利用 Hilbert 的不可約定理以及 Čebotarev 密度定理, Wiles 證明並非所有 X 上的有理點都可由定義於 Q 上的橢圓曲線 E'' 使得 $\rho_{E'',3}(G_Q) \neq GL_2(Z/3Z)$ 來代表。因此, 所要的 E' 確實存在。爲確保 E' 的半穩定性, 選擇 E' 與 E 在 5 的位非常靠近 (E' close to E 5-adically), 如此 E' 在位 5 爲半穩定, 從而在其他位上也半穩定, 原因是 $\rho_{E',5}(G_Q) = GL_2(Z/5Z)$。暫時假設我們能證明: 對任意質數 ℓ 而言, 若 $\rho_{E,l}$ 是模型表現, 則其提升 $\widetilde{\rho_{E,\ell}}$ 也是模型表現。那麼在 $\rho_{E,3}(G_Q) = GL_2(Z/3Z)$ 的情況下, 我們得出 $\widetilde{\rho_{E,3}}$ 是模型表現, 從而得所欲證。當 $\rho_{E,3}(G_Q)$ 爲 $GL_2(Z/3Z)$ 的眞子群時, 我們知道 $\widetilde{\rho_{E',3}}$ 是模型表現, 因此, 如 §2 所注意到, $\widetilde{\rho_{E',5}}$ 也是, 所以 $\rho_{E',5}$ 也是模型表現, 但這表現與 $\rho_{E,5}$ 一樣, 由此得出 $\widetilde{\rho_{E,5}}$ 是模型表現, 這就是所要的。

由上面的推理看出, 整個定理已演變至證實上述假設的正確性, 這是 Wiles 所要證明的, 我們留在下節討論。

4. 模型表現$\rho_{E,l}$的提升

從一定義在 Q 上的橢圓曲線 E 以及一模型表現

$$\rho_{E,\ell} : G_Q \to GL_2(Z/lZ)。$$

我們想證明其 ℓ- 進位提升 $\widetilde{\rho_{E,\ell}}$ 也是模型表現, Wiles 利用到 Mazur 的變形理論 (theory of deformation)。

固定某些提升用的 "提升數據", 包括所允許的分歧以及在 ℓ 位的局部動態等, 這就定義出一提升問題。Mazur 證明存在有一廣泛提升 (universal lifting), 亦即一局部環 (local ring) R 以及 G_Q 到 $GL_2(R)$ 的表現, 使得某種適當類型的提升皆可由廣泛提升分解出來, 特別是 $\widetilde{\rho_{E,\ell}}$ 也可以。另一方面, $\rho_{E,\ell}$ 是模型表現, 因而附著於一模型式, 此時, 存在一 Hecke 環 T, 它是 R 中具有下述獨特性質的最大商環; 這獨特性質是: 所有 $\rho_{E,\ell}$ 的模型提升皆可經其分解出來。Mazur 猜測說 $R = T$。若然, 則馬上得出 $\widetilde{\rho_{E,\ell}}$ 是模型表現, 而結束整個定理的證明。

已知 T 是一 Gorenstein 環, 同構於其對偶, 且是一局部完備交集 (local complets intersection), 利一些交換代數上的結

果, Wiles 把 $R = T$ 的問題轉化成檢定兩個有限群大小的不等式:

$$^{\#}(\mathcal{P}_R/\mathcal{P}_R^2) \leq {}^{\#}(\mathcal{P}_T/\mathcal{P}_T^2)$$

其中 $\mathcal{P}_R$, $\mathcal{P}_T$ 分別是 R 及 T 的最大理想。根據 Hida 的工作, $\mathcal{P}_T/\mathcal{P}_T^2$ 的秩與某一 L-函數值有關, 而 $\mathcal{P}_R/\mathcal{R}_R^2$ 與附著於 $\rho_{E,\ell}$ 的模型式之 Sym^2 的 Selmer 群的秩有關, 但後者在計算上非常困難。Wiles 仿照 Kolyvagin 構造 Euler 系統 [5] 的方法來計算。他利用模型單位 (modular units) 去建構他所謂上同調類的 "幾何 Euler 系統"。這概念源自 Flach [2], 不過, Flach 只做了 Wiles 所需要的底層部份; Wiles 曾試把這推到更高層次, 但並不十分成功。

5. 結論

對 Wiles 所提出費馬定理的解決方法, 因尚有很大的漏洞, 故一些代數幾何與數論專家皆不願下定論; 看過他手稿的如 K. Ribet 與 R. Taylor 嘗試把 Wiles 的工作介紹出來, 但在場的大師 Serre 在演講後都承認無法理解; 在此我們期待不久的將來, 會有新的版本出現。

參考文獻

1. P. Deligne: Formes modulaires et représentations $l-$adiques. In: Séminaire Bourbaki vol. 1968/69, Lecture Notes in Math. 179, Springer–Verlag, Berlin, Heidelberg, New York (1971).
2. M. Flach: A generalization of the Cas- sels—Tate pairing, J. reine angew. Math. 412 (1990), 113-127.
3. G. Frey: Rationale Punkte anf Fer- matkurven und getwisteten Modulkurven, J. Crelle 331 (1982), 185-191.
4. G. Frey: Links between stable elliptic curves and certain Diophantine equations, Ann. Univ. Saraviensis, Ser. Math. 1 (1986), 1-40.
5. V. A. Kolyvagin: Euler systems. In: The Grothendieck Festschrift, vol. II, Prog. in Math. 87, Birkhäuser Boston, Boston, MA. (1990), 435-483.
6. R. Langlands: Base Change for GL_2, Princeton Univ. Press (1980).
7. B. Mazur: Rational points on modular curves. In: Modular Functions of One Variable, Lecture Notes in Math. 601, Springer–Verlag, Berlin, Heidelberg, New York (1977).
8. B. Mazur: Modular curves and the Eisenstein ideal, Publ. Math. I.H.E.S. 47 (1977).
9. B. Mazur: Rational isogenies of prime degree, Invent. Math. 44 (1978), 129-162.
10. K. Ribet: On modular representations of $Gal(\bar{\mathbf{Q}}\,/\,\mathbf{Q})$ arising from modular forms, Invent. Math. 100 (1990), 431-476.
11. J. -P. Serre: Sur les représentations modulaires de degré 2 de $Gal(\bar{\mathbf{Q}}/\mathbf{Q})$, Duke Math. J. 54 (1987), 179-230.
12. J. Tunnell: Artin's conjecture for representations of octahedral type, Bull. A.M.S. 5 (1981), 173-175.

—本文作者分別任教於美國賓州州立大學數學系與國立中正大學數學系—