關於懷爾斯解決費馬最後定理的一些補充說明

余文卿

今年5月20日, 筆者應邀到建國中學對師生做專題演講, 其中談到德數學家庫麥爾 (Kummer) 在數論上的主要貢獻, 自然也談到他對規則質數冪次之費馬最後定理的證明, 不免也提到懷爾斯的證明過程手法。演講後, 建中任教的林礽堂老師問到三個數論上的專有名詞: 橢圓曲線、模型曲線與模型式, 前兩個名詞出現於爭議性頗多的谷山一志村猜想 (Taniyama-Shimura Conjecture) 中:

> 每一橢圓曲線都是模型曲線。

而懷爾斯則是證明谷山一志村猜想對半穩定橢圓曲線成立:

> 每一半穩定橢圓曲線都是模型曲線。

爲什麼這樣就證明了費馬最後定理? 底下我們提出一些補充說明。

一. 橢圓曲線

對任意有理數 p, q, r, 二元三次方程式 $y^2 = x^3 + px^2 + qx + r$, 其中 $x^3 + px^2 + qx + r = 0$ 沒有重根, 定義一佈於有理數體 $\mathbb{Q}$ 的橢圓曲線 E, 若考慮這方程式的所有複數解, 則其解集合與一輪胎面 (torus) 同構。在數學上, 所謂的輪胎面是複數平面 $\mathbb{C}$ 被其上方格點

$$\Lambda = \{aw_1 + bw_2 | a, b \text{ 是整數}, w_1, w_2 \text{ 是固定複數且 } w_2/w_1 \notin \mathbb{R}\}$$

所除的商群 $\mathbb{C}/\Lambda$, 這商群是一加法交換群, 因而橢圓曲線 E 上的點也構成一加法子群。

弗維 (Frey) 的嶄新構想是從費馬方程式的解去建構橢圓曲線。設費馬最後定理對質數 p 不成立 (且 $p \geq 5$), 而 a, b, c 是費馬方程式 $x^p + y^p + z^p = 0$ 的一組非顯然

的整數解, 則

$$y^2 = x(x-a^p)(x+b^p)$$

是一半穩定的橢圓曲線 E, 這也被稱爲弗維曲線 (Frey curve), 而其引導子 (conductor) N_E 是 $a^pb^pc^p$ 的因數。

二. 模型式與模型曲線

設 Γ 是模型群, 其元素是二階方陣 $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $ad-bc=1$, a,b,c,d 是整數, Γ 透過模型變換 $z \to (az+b)/(cz+d)$ 而作用在複數半平面 $H=\{z=x+iy|y>0\}$ 上, 而所謂 Γ 之權爲 k 的模型式是滿足下列兩條件的 H 上的解析函數 f:

(a) 對任意 $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma$, $f(\frac{az+b}{cz+d}) = (cz+d)^k f(z)$,

(b) $f(z)=\sum_{n=0}^{\infty} a_n e^{2\pi inz}$。

因而模型式只是一種較特殊的週期函數, 對模型 Γ 的子群 Γ', 自然可定義 Γ' 的模型式, 只要將條件 (a) 限制於 Γ' 上即可。

對任意正整數 N, 定 $\Gamma_0(N)$ 是 Γ 的一同餘子群, 是由滿足 $c \equiv 0 \pmod N$ 之元素 $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ 所成的集合, 而 H^* 是上半平面 H 與有理數的聯集, 一樣透過模型轉換 $z \to (az+b)/(cz+d)$, $\Gamma_0(N)$ 作用在 H^*, 其軌道空間 (orbit space) $H^*/\Gamma_0(N)$ 是一緊緻的里曼面, 透過解析同構而得出一模型曲線 $X_0(N)$, 而谷山一志村猜測斷言: 對任意定義於 $\mathbb{Q}$ 的橢圓曲線 E, 存在有一正整數 N 及一映成 (surjective) 的代數幾何映射 ϕ: $X_0(N) \to E$, 把 $X_0(N)$ 的無窮遠點映到 E 的原點, 而附在 E 上的 L-函數若爲

$$L(s,E)=\sum_{n=1}^{\infty} a_n n^{-s},$$

則 $f(z)=\sum_{n=1}^{\infty} a_n e^{2\pi inz}$ 是一 $\Gamma_0(N)$ 的模型式。

三. L-函數

古典的里曼 zeta 函數 $\zeta(s)=\sum_{n=1}^{\infty} n^{-s}$ 在 s 大於1時有無窮乘積展開式

$$\zeta(s)=\prod_p (1-p^{-s})^{-1}。$$

而附著於橢圓曲線的 L-函數也是類似的無窮乘積:

$$\begin{aligned} L(s,E) = & \prod_{p|N_E} (1-a_p p^{-s})^{-1} \\ & \cdot \prod_{p\nmid N_E} (1-a_p p^{-s}+p^{1-2s})^{-1}, \end{aligned}$$

其中 N_E 是 E 的引導子。當 $p \nmid N_E$, $1+p-a_p$ 表示 E 在有限體 $F_p=\mathbb{Z}/p\mathbb{Z}$ 中的元素個數, 對模型曲線而言, 其 L-函數是一模型式的梅林轉換 (Mellin tranform)。即若

$$L(s,E)=\sum_{n=1}^{\infty} a_n n^{-s},$$

則 $f(z)=\sum_{n=1}^{\infty} a_n e^{2\pi inz}$ 是某一同餘子群 $\Gamma_0(N)$ 的模型式

四. 最後階段。

證明費馬最後定理的最後階段得借重模型式方面的理論, 假設費馬最後定理對某一質數 p 不成立 (且 $p \geq 5$), 則費馬方程式

$$x^p + y^p + z^p = 0,$$

有一組整數解 (a, b, c) 且 $abc \neq 0$ 如此可用於建構一弗維曲線 $E: y^2 = x(x - a^p)(x + b^p)$, 懷爾斯所證明的谷山一志村猜想適用於這樣的半穩定的橢圓曲線, 也就是, 任意的半穩定橢圓曲線都是模曲線 (見"二"!)。但是, 我們又知道弗維曲線是一種半穩定橢圓曲線卻又不是模型曲線, 因爲根據謝爾 (Serre) 提出的秘方, 並且經過里貝 (Ribet) 給予完整的證明, 有一權爲2的 $\Gamma_0(2)$ 的模型式, 但另一方面 $H^*/\Gamma_0(2)$ 的虧格數爲零, 根本不會有這樣的模型式存在, 而得出矛盾, 因而得證了費馬最後定理。

參考資料

1. Amir D. Aczel, Fermat's Last Theorem, unlocking the secret of an ancient mathematical problem, 中譯本林祕堂譯, 余文卿審訂, 時報出版社。

—本文作者任教於國立中正大學數學系—