Birch 與 Swinnerton-Dyer 猜測
—— 價值百萬美金的數學謎題

余文卿

英國的克雷數學研究所 (Clay Institute of Mathematics) 於2000年五月底在巴黎舉行記者發表會, 提出數學上急切需要解決的七個難題, 並提供百萬美金的獎金給解決其中之一問題的人。現討論其中之一的 Birch 與 Swinnerton-Dyer 猜測。根據網路所下載的資料如下:

數學家一直著迷於像求代數方程式

$$x^2 + y^2 = z^2$$

的所有整數解的問題。歐基里德 (Euclid) 曾給出這方程式的完全解。對於較複雜的方程, 求解變成困難的問題。事實上, Yu V. Matiyasevich 於1970年證明了 Hilbert 的第十個問題無解, 即當這類方程式有整數解時, 判別有無整數解的方法是不存在的。但在一些特殊情形, 我們會額外有所寄望。當解形成一交換曲體 (abelian variety) 上的所有點時, Birch 與 Swinner-Dyer 猜測斷言有理點的個數與附於曲線上面的 zeta 函數 $\zeta_E(s)$ 在 $s = 1$ 的取值有關。特別是這猜測斷言, 若 $\zeta_E(1) = 0$, 則 E 上有無窮多個有理點 (方程式有無窮多個有理解), 且反過來, 若 $\zeta_E(1) \neq 0$ 則只會有有限多個這類有理點。

1. 猜測的進一步說明與證據

因問題的對象是一般的大衆, 故說明中未用上很多的專業術語。現加以補充說明, 這裡所指的交換曲體應是橢圓曲線, 其一般方程式爲

$y^2 = ax^3+bx^2+cx+d, \quad a, b, c, d$ 是整數。

這方程式的複數解形成一加法群, 加上無窮遠點後會同構於 $\mathbb{C}/L$, 其中 L 是 $\mathbb{C}$ 上的方格點:

$$L = \mathbb{Z}w_1 + \mathbb{Z}w_2$$

設 p 是一質數, 考慮橢圓曲線在有限體 $F_p = \mathbb{Z}/p\mathbb{Z}$ 的點個數, 而得出附在 E 上的 Hasse-Weil zeta 函數爲

$$\zeta_E(s) = \prod_{p|N_E} (1 - a_p p^{-s})^{-1}$$

$$\cdot \prod_{p\nmid N_E} (1-a_p p^{-s}+p^{1-2s})^{-1}$$

其中 N_E 是 E 的引導子 (conductor), 是 E 上一些壞因子的乘積, 只限於有限多個, 而 $1+p-a_p$ 是 E 在有限體 F_p 的元素個數。

知道橢圓曲線上的 Hasse-Weil zeta 函數後, 我們重新敍述原先的猜測如下:

猜測 (B. J. Birch 與 H. P. F. Swin -nerton-Dyer): $\zeta_E(1)=0 \Leftrightarrow E$ 具有無窮多個有理點。

上面這猜測稱爲"弱性 Birch 與 Swinnerton -Dyer 猜測"。因爲原先於1963年提出的猜測尙包括下列幾點:

(a) $\zeta_E(s)$ 在 $s=1$ 的零點重數等於$E(\mathbb{Q})$ (有理點所形成的交換群)的階數(rank)。

(b) $\zeta_E(s)$ 在 $s=1$ 的泰勒展開式的第一個非零係數有明顯的表現式。

對具有複數乘法 (complex multiplication) 的橢圓曲線, 其 zeta 函數可做解析延拓並滿足泛方程式, 而有底下的結果。

定理 (J. Coates* 與 A. Wiles): 設 E 是定義於 $\mathbb{Q}$ 的橢圓曲線且 E 具有複數乘法。若 E 有無窮多個有理點, 則 $\zeta_E(1)=0$。

另一方面, 具模的橢圓曲線稱爲模型曲線, 這類曲線的 zeta 函數是權爲2之模型式的 Mellin 轉換, 自然具有解析延拓與泛方程式, 而有底下的已知結果。

定理 (Gross 與 Zagier): 若 E 是定義於 $\mathbb{Q}$ 的橢圓曲線, $\zeta_E(1)=0$ 且 $\zeta_E'(1)\neq 0$, 則 $E(\mathbb{Q})$ 的階數至少爲1。

*即是本期「有朋自遠方來」專訪的 John Coates 教授

有名的谷山–志村猜測 (Tanigama-Shimura Conjecture) 斷言每一橢圓曲線都是模型曲線, 而這猜測已得到證實 (1999), 而猜測的特殊情形也被 Wiles 用於費馬最後定理的證明。無論如何, 現在問題的困難度已縮減, 完全沒有解析延拓與泛方程式的問題。

2. 定義於複數的橢圓曲線

給定複數平面上的方格點 $L=\mathbb{Z}w_1+\mathbb{Z}w_2$, 其中 $0, w_1, w_2$ 在複數平面上所表示的三點不共線, 現欲建構一橢圓曲線 E, 使 $E\cong \mathbb{C}/L$, 採取的方式是考慮雙週期函數

$$\wp(z)=\frac{1}{z^2}+\sum_{\lambda\in L,\lambda\neq 0}\left(\frac{1}{(z-\lambda)^2}-\frac{1}{z^2}\right)$$

這級數在 $\mathbb{C}$ 上的任一緊緻集上絕對收斂, 而定義 $\mathbb{C}$ 上的半純函數 (meromorphic function), 這函數滿足

$$\wp(z+w_1)=\wp(z) \qquad 且\wp(z+w_2)=\wp(z)$$

是一典型的 雙週期函數 。在 $z=0$ 附近, $\wp(z)$ 的展開式爲

$$\wp(z)=\frac{1}{z^2}+3G_4z^2+5G_6z^4+\ldots +(2n+1)G_{2n+2}z^{2n}+\ldots$$

其中

$$G_k(w_1,w_2)=G_k(L)=\sum_{\lambda\in L,\lambda\neq 0}\lambda^{-k} =\sum_{(m,n)\neq(0,0)}(mw_1+nw_2)^{-k}$$

是 Eisenstein 級數, $G_k(z) = G_k(z,1)$ 是權爲 k 的模型式, 即對 $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z})$,

$$G_k(\frac{az+b}{cz+d}) = (cz+d)^k G_k(z).$$

現把 $\wp(z)$ 的展開式逐項對 z 微分得

$$\wp'(z) = -\frac{2}{z^3} + 6G_4 z + 20G_6 z^3 + 42G_8 z^5 + \cdots$$

因而

$$\begin{aligned} \left[\wp'(z)\right]^2 &= \frac{4}{z^6} - 24G_4\frac{1}{z^2} - 80G_6 \\ &\quad +(36G_4^2 - 168G_8)z^2 + \cdots \\ \left[\wp(z)\right]^3 &= \frac{1}{z^6} + 9G_4\frac{1}{z^2} + 15G_6 \\ &\quad +(21G_8 + 27G_4^2)z^2 + \cdots \end{aligned}$$

觀察到

$$\begin{aligned} H(z) = &\left[\wp'(z)\right]^2 - \left[4\wp^3(z)\right. \\ &\left. - 60G_4\wp(z) - 140G_6\right] \end{aligned}$$

是 z 的解析函數且依然是雙週期函數, 必是常數, 而得出

$$\left[\wp'(z)\right]^2 = 4\wp^3(z) - 60G_4\wp(z) - 140G_6$$

表示點 $(\wp(z), \wp'(z))$ 落在橢圓曲線

$$y^2 = 4x^3 - 60G_4 x - 140G_6$$

上。把 $(\wp(z)\,,\, \wp'(z))$ 視爲 $\mathbb{P}^2_{\mathbb{C}}$ 上的點 $(\wp(z),\, \wp'(z)\,,\, 1)$ 而定

$$z \to (\wp(z), \wp'(z), 1)$$

這建立了 $\mathbb{C}/L$ 與橢圓曲線

$$E : y^2 = 4x^3 - 60G_4 x - 140G_6$$

在 $\mathbb{P}^2_{\mathbb{C}}$ 上點的一一對應關係。

對於兩條橢圓曲線 $E = \mathbb{C}/L$ 與 $E' = \mathbb{C}/L'$。其中

$$L = \mathbb{Z}w_1 + \mathbb{Z}w_2, \qquad L' = \mathbb{Z}w_1' + \mathbb{Z}w_2'.$$

定 $z = \frac{w_1}{w_2}$, $z' = \frac{w_1'}{w_2'}$, 則 $E \cong E'$ 的充要條件是存在 $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z})$, 使得

$$\frac{az+b}{cz+d} = z'.$$

另一方面, 像 $E = \mathbb{C}/L$, $L = \mathbb{Z}i + \mathbb{Z}$, 乘上 i 把 L 映至本身, 而對應到 E 的一自同構, 這樣的 E 稱爲具複數乘法。又如, $E = \mathbb{C}/L$, $L = \mathbb{Z}w + \mathbb{Z}$, $w = e^{\frac{2\pi i}{3}}$ 也具有複數乘法。絕大多數的橢圓曲線不具複數乘法。

3. 定義於有限體上的橢圓曲線

設 F_q 是一具有 q 個元素的有限體, 當然這裡的 q 一定是某一質數 p 的正整數冪次, $q = p^n$, 定義於 F_q 的橢圓曲線 E 的方程式爲

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4 + a_6$$

固定每一 x 的值, y 至多有兩個解, 因而解的個數至多是 $2q+1$ 個, 但任一隨機的二次方程式, 有50% 的機會沒有實數解, 因而解的個數約爲 $q+1$ 個。底下的定理來自 E. Artin 的猜測而被 Hasse 於1930年左右得到證明

定理 (Hasse): 設 E 是定義於 F_q 的橢圓曲線, $^{\#}E(F_q)$ 表示曲線上點的個數, 則

$$|^{\#}E(F_q) - q - 1| \le 2\sqrt{q}$$

設 F_{q^n} 是 F_q 的 n 次擴充體, 附著於 E 的 zeta 函數定義爲

$$Z(E/F_q;T)=\exp\{\sum_{n=1}^{\infty}(^{\#}E(F_{q^n}))\frac{T^n}{n}\}$$

Weil 猜測到這函數是 T 的有理數且已得到證實, 即

$$Z(E/F_q;T)=\frac{1-a_qT+qT^2}{(1-T)(1-qT)}$$

其中 $q+1-a_q=^{\#}E(F_q)$。

現附於橢圓曲線 E 上的 Hasse-Weil zeta 函數就是以 $Z(E/F_q;T)$爲根據的 zeta 函數, 定爲

$$\zeta_E(s)=\prod_{p|N_E}(1-a_pp^{-s})^{-1}\prod_{p\nmid N_E}(1-a_pp^{-s}+p^{1-2s})^{-1}$$

其中 N_E 是 E 的引導子, 是一些使 E/F_p 具有節點 (node) 或尖點 (cusp) 之質數 p 的冪次方乘積。

4. 結語

相較於里曼假設, Hodge 猜測, Poin-caré 猜測等難以捉摸的難題, Birch 與 Swinnerton-Dyer 猜測算是較具體的, 尤其谷山一志村猜測已得到證明, 考慮的對象就是模型曲線。但若像網路上所提的交換曲體, 那問題又另當別論了。

參考文獻

1 N. Koblitz, *Introduction to Elliptic Curves and Modular Forms.*

2 J. H. Silverman, *The Arithmetic of Elliptic Curves.*

—本文作者任教於國立中正大學數學系—