# 數 甚麼是橢圓曲線？

作者：丹尼爾斯 Harris B. Daniels．羅札諾 - 羅布雷多 Alvaro Lozano-Robledo 譯者：王夏聲
丹尼爾斯是美國安默斯特學院數學系助理教授
羅札諾 - 羅布雷多是美國康乃狄克大學數學系副教授。

作者合影，羅札諾 - 羅布雷多（左）和丹尼爾斯（右）。（Keith Conrad 攝，羅札諾 - 羅布雷多提供）。

在數論、代數幾何、複分析、密碼學和物理等領域的研究裡，橢圓曲線（elliptic curve）無所不在。橢圓曲線也是算術幾何（arithmetic geometry）的研究前沿，出現在懷爾斯（Andrew Wiles）的費馬最後定理證明中（請參見本期〈2016 年阿貝爾獎得主懷爾斯訪談〉）。一般來說，算術幾何的研究目標是找出一數體（number field）$K$ 代數解形（algebraic variety）$C$ 上的 $K$ 有理點集 $C(K)$，亦即 $C$ 上坐標屬於 $K$ 的點。例如，費馬最後定理可以敘述成：當 $n \geq 3$ 時，有理數體（$\mathbb{Q}$）代數解形 $x^n + y^n = z^n$ 只有無聊解（trivial solution）。

在本文中，我們僅探討一維數體 $K$ 的代數解形，也就是代數曲線 $C$。其中，$K$ 通常是有理數體 $\mathbb{Q}$ 或高斯有理數體 $\mathbb{Q}(i)$，亦即實、虛部皆為有理數的複數體。

一維複曲線通常稱為黎曼面（Riemann surface），根據黎曼曲面的分類，曲線是依幾何虧格（genus）來分類。當 $C$ 的虧格為 0 時，運用歐幾里得、丟番圖（Diophantus）、婆羅摩笈多（Brahmagupta）、勒讓德（Adrien-Marie Legendre）、高斯、哈澤（Helmut Hasse），閔可夫斯基（Hermann Minkowski）等人的經典方法，可以完全決定 $C$ 上的 $K$ 有理點。例如：

$C_1: 37x + 39y = 1$ 和 $C_2: x^2 - 13y^2 = 1$

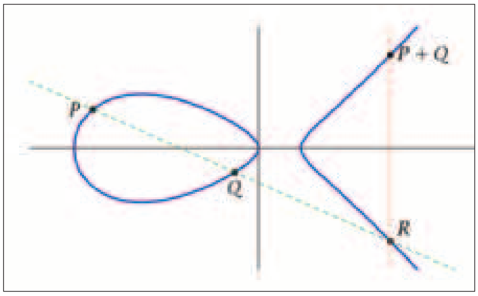
用基本方法便能完全找出上面所有的無窮多個有理點。但是一般而言，當 $C$ 的虧格是 1 時，我們甚至無法確定 $C$ 是否有 $K$ 有理點，遑論找出所有屬於 $C(K)$ 的點。

舉例來說，在虧格為 0 時，我們可以用局部性質來決定大域有理點的存在性。但是這個方法無法用在底下的虧格 1 曲線上：

$C: 3x^3 + 4y^3 = 5$

事實上，在此曲線上不含任何 $\mathbb{Q}$ 有理點 ❶。

虧格為 1 的複曲線，相當於實二維曲面。



在橢圓曲線上的群運算（加法）規則。

## 橢圓曲線

所謂的橢圓曲線 $E$ 是一定義於 $K$，虧格為 1 的光滑射影曲線（smooth projective curve）[2]，而且曲線上至少含一 $K$ 有理點。如果 $K$ 的特徵（characteristic）是 0（例如數體）或 $p>3$，則任何橢圓曲線在夠好的坐標下，可以寫成短懷爾斯查司模型（short Weierstrass model）：

$$E: y^2 = x^3 + Ax + B$$

其中 $A, B \in K$，而且判別式 $4A^3 + 27B^2 \neq 0$ 以確保曲線的光滑性。在這個模型下，曲線只有一無窮遠的 $K$ 有理點 $\mathcal{O}$。

橢圓曲線論之所以如此豐富，原因之一是因為 $E$ 上的 $K$ 有理點集 $E(K)$ 可賦予具有幾何意義的交換群（abelian group）結構（圖 3），其中 $\mathcal{O}$ 是群的單位元素。換一個說法，就是橢圓曲線是 1 維的阿貝爾解形（Abelian varieties）。

20 世紀初，龐卡赫（Henri Poincaré）提出「交換群 $E(K)$ 是有限生成（finitely generated）」的猜想。當 $K=\mathbb{Q}$ 時，摩岱爾（Louis J. Mordell）在 1922 年證明了這個猜想。1928 年，威伊（André Weil）將這個結果推廣到任何數體的阿貝爾解形，這是今日廣為人知的摩岱爾／威伊定理（Mordell-Weil Theorem）。從有限生成交換群的分類結果，$E(K)$ 可寫成一撓子群（torsion subgroup）與另一秩（rank）為 $r \geq 0$ 的自由（free）交換群的直和（direct sum），也就是：

$$E(K) \cong E(K)_{\text{tors}} \oplus \mathbb{Z}^r$$

我們稱 $r = r_{E/K}$ 是 $K$ 橢圓曲線 $E/K$ 的秩。舉例來說，對於橢圓曲線

$$E: y^2 + y = x^3 - 10x + 10$$

群 $E(\mathbb{Q})$ 是由 $P=(2,-2)$ 和 $Q=(-4,1)$ 所生成的。這裡 $P$ 點的階（order）是 5（亦即 $5P=\mathcal{O}$），而 $Q$ 點的階是無窮大，所以 $E/\mathbb{Q}$ 的秩等於 1，且 $E(\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}$

固定數體 $K$，哪些有限生成的交換群可以作為 $K$ 橢圓曲線 $K$ 的子群呢？關於撓子群 $E(K)_{\text{tors}}$，目前已知只有在 $K=\mathbb{Q}$ 或 $K$ 是二次或三次數體（例如 $\mathbb{Q}(i)$ 或 $\mathbb{Q}(\sqrt[3]{2})$）時可完全決定。在 $K=\mathbb{Q}$ 的情況，李維（Beppo Levi）在 1908 年提出了關於其撓子群清單的猜想。這個猜想被遺忘近 60 年後，1970 年又由歐格（Andrew P. Ogg）重新提出。最後在 1976 年，由梅哲（Barry Mazur）證明 $E(\mathbb{Q})_{\text{tors}}$ 只可能是下列情況之一

$$\begin{cases} \mathbb{Z}/N & 1 \leq N \leq 10,\ N = 12 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2M\mathbb{Z} & 1 \leq M \leq 4 \end{cases}$$

相較之下，即使是 $K=\mathbb{Q}$，我們也完全不清楚秩 $r_{E/K}$ 的清單是什麼。對任何固定數體，我們甚至不知道這清單是有限還是無限。在 $\mathbb{Q}$ 時，艾爾奇斯（Noam D. Elkies）找到一條橢圓曲線，其秩 28 是目前已知的最大秩。

---

[1] 這是塞爾莫（Ernst S. Selmer）所舉的的一個局部到大域原則（local-to-global principle）不適用的例子。對於任何 $\mathbb{Q}$ 的完備化（completion）體 $K$ ──亦即實數體 $\mathbb{R}$ 及任何質數 $p$ 的 $p$ 進數體（$p$-adic）$\mathbb{Q}_p$，雖然 $C$ 上都存在 $K$ 有理點，但是 $C$ 卻不含 $\mathbb{Q}$ 有理點。

[2] 射影曲線是在射影空間 $\mathbb{P}^2(K)$ 中的曲線，除了一般的仿射點（affine point）外，還可能包含無窮遠點。

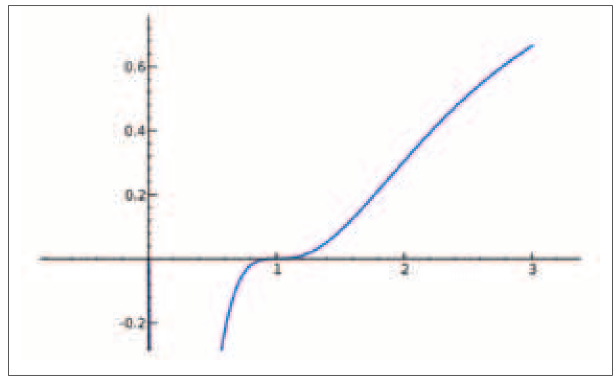
## BSD 猜想

橢圓曲線秩的未解問題是決定橢圓曲線 $K$ 有理點如此困難的核心因素。其中最困難之處，在於當曲線虧格大於 0 時，局部到全域原則（或哈澤原理）並不適用。對任何橢圓曲線 $E/K$，可定義泰特 / 薩法瑞維奇群（Tate-Shafarevich group，TS 群） $Ш = Ш_{E/K}$ 來衡量哈澤原理不適用的程度。在某種意義上，$Ш$ 扮演了在數體中理想類群（ideal class group）的角色。然而，我們並不確定 $Ш_{E/K}$ 是否總是有限群 [3]。如果 $Ш$ 總是有限的，那麼由費馬引介的無窮遞降法（method of infinite descent）應該足以得到一個決定 $E$ 上所有 $K$ 有理點的算則。

1960 年代，伯奇（Bryan Birch）和斯溫諾頓戴爾（Peter Swinnerton-Dyer）提出一個猜想（簡稱 BSD 猜想），想以分析方法來計算橢圓曲線的秩。這猜想之後被改善為以有理橢圓曲線的哈澤／威伊 $L$ 函數（Hasse-Weil $L$-function）來表示。這個函數它是以歐拉乘積來定義的：

$$L(E,s) = \prod_{p \text{ prime}} L_p(E, p^{-s})^{-1}$$

其中除有限質數外，$L_p(E,t) = 1 - a_p t + pt^2$，$a_p = p + 1 - \sharp E(\mathbb{F}_p)$，此處 $\sharp E(\mathbb{F}_p)$ 是 $E$ 以 $\mathbb{F}_p$ 為係數時，$\mathbb{F}_p$ 點的個數。依此定義，當 $s$ 的實部 $\mathrm{Re}(s) > 3/2$ 時，$L(E,s)$ 收斂。事實上，哈澤更猜測：任何 $\mathbb{Q}$ 橢圓曲線的 $L$ 函數有一全複平面的解析延拓（analytic continuation）。現在這猜想已被證明是模性定理（modularity theorem，見後述）的推論。BSD 猜想斷言 $L(E,s)$ 在 $s=1$ 的根重數




文中 $L$ 函數 $L(E,x)$ 在 $x=1$ 是三重根。

（order of vanishing）等於 $E(\mathbb{Q})$ 的秩 $r_{E/\mathbb{Q}}$。事實上，這猜想也預測在 $s=1$ 的留數（residue）可以用 $E/\mathbb{Q}$ 的不變量來表示。

例如 $E: y^2 + y = x^3 - 7x + 6$ 的秩是 3 且 $E(\mathbb{Q}) \cong \mathbb{Z}^3$。圖 4 是當 $0 \le x \le 3$ 時，$L(E,x)$ 的圖形。

透過寇茨（John Coates）和懷爾斯、格羅斯（Benedict Gross）和扎基爾（Don Zagier）、柯里維金、魯賓、斯金納（Christopher Skinner）、爾本（Eric Urban）等人的研究，現在只知道 BSD 猜想在某些秩為 0 或 1 的特定橢圓曲線成立。但是，巴噶瓦（Manjul Bhargava）、斯金納、張偉（Wei Zhang）已經證明，BSD 猜想至少對 66% 的 $\mathbb{Q}$ 橢圓曲線是成立的。

## 橢圓曲線與模性猜想

自從艾利瓜許（Yves Hellegouarch）、弗瑞（Gerhard Frey）和塞爾（Jean-Pierre Serre）提議透過某些橢圓曲線不可能存在，可描繪出證明費馬最後定理的藍圖，1980 年代橢圓曲線的研究日益受人矚目。

粗略的說，當 $p \geq 11$ 且 $a^p + b^p = c^p$ 是費馬方程 $x^p + y^p = z^p$ 的非無聊解時，所謂的弗瑞／艾利瓜許曲線（Frey-Hellegouarch curve）$y^2 = x(x - a^p)(x + b^p)$ 將具備兩個一般認為是矛盾的性質。一是這曲線是半穩的（semistable）。這是關於曲線 $E/\mathbb{F}_p$ 類型的溫和技術性條件。二是這曲線是模曲線（modular curve）（見後）。

1986 年，李比特（Kenneth Ribet）證明了塞爾的猜想「弗瑞／艾利瓜許曲線是半穩橢圓曲線，但不是模曲線」。因此根據李比特的結果，想要證明費馬最後定理，我們「只」需要證明「任何半穩 $\mathbb{Q}$ 橢圓曲線都是模曲線」即可。

這項敘述肇始於 1950 年代，有時被稱為模性猜想（modularity conjecture）或谷山／志村／威伊猜想（Taniyama-Shimura-Weil conjecture）[1]。模性猜想連結了兩個看似極為不同的數學分支——橢圓曲線與模形式（modular form）。

模形式是定義在上半複數平面且滿足某種對稱性質的複解析函數 $f(s)$。特別的是，$f(s)$ 可以做傅立葉級數展開 $f(s) = \sum_{n \geq 0} a_n q^n$，其中 $q = e^{2\pi i s}$。而且，模形式 $f$ 對應一 $L$ 函數 $L(f, s) = \sum_{n \geq 0} a_n / n^s$。模性猜想告訴我們：任何橢圓曲線 $E$ 都是模曲線，可對應到某一模形式 $f$，使得 $L(E, s) = L(f, s)$。換句話說，兩者所對應的 $L$ 函數是相同的。這特別意味著 $L(E, s)$ 可解析研拓到 $\mathbb{C}$，因為已知這對 $L(f, s)$ 是成立的。

1993 年，懷爾斯宣稱證明了半穩條件下的模性猜想 [2]，卻被發現證明有瑕疵，最後泰勒（Richard Taylor）與懷爾斯在 1995 年修正了證明，完成費馬最後定理的證明。2001 年，布賀耶（Christophe Breuil）、康拉德（Brian Conrad），戴蒙德（Fred Diamond）與泰勒證明對所有 $\mathbb{Q}$ 橢圓曲線模性猜想都成立。2015 年弗雷特斯（Nuno Freitas），黎雄（Bao V. Le Hung）與希克賽克（Samir Siksek）將模性定理推廣到實二次體（real quadratic fields）。就如季辛（Mark Kisin）所描述的 [3]，模性定理與朗蘭茲綱領（Langlands Program）、方丹諾／梅哲猜想（Fontaine-Masur conjecture）已經整合成一個更大的研究脈絡。

想要學習橢圓曲線的研究生，希爾弗曼（Joseph H. Silverman）所著的《橢圓曲線算術》（*The Arithmetic of Elliptic Curves*）是標準的入門書。而他與泰特合寫的《橢圓曲線的有理點》（*Rational Points on Elliptic Curves*）則更為淺顯。∞

本文參考資料請見〈數理人文資料網頁〉http://yaucenter.nctu.edu.tw/periodical.php

本文出處

"What is ... an Elliptic Curve?" *Notices* 64 （2017） No. 3, AMS。
本刊感謝作者與 AMS 同意轉載翻譯。

譯者簡介

王夏聲為交通大學應用數學系副教授。

延伸閱讀

▶ Silverman, Joseph H. *The Arithmetic of Elliptic Curves*, 2nd Edition, Springer-Verlag, 2009. 研究生學習橢圓曲線標準入門書

▶ Silverman, Joseph H. & Tate, John T. *Rational Points on Elliptic Curves* 2nd Edition, Springer-Verlag, 1992. 比前書更淺顯。

3 目前只有在某些秩 $\leq 1$ 的情形下可確認 Ш 是有限的，這是柯里維金（Victor Kolyvagin）與魯賓（Karl Rubin）的工作。