數學傳播　45卷1期, pp. 24-32

理想類群、橢圓曲線及 zeta 函數

演講者：謝銘倫教授

時　間：民國 109 年 6 月 15 日

地　點：天文數學館 202 演講廳

本文從費馬最後定理出發, 嘗試沿著歷史的軌跡來說明數論中一些著名問題和各種 zeta 函數的關係。

費馬最後定理

20世紀末數學的最大成就之一是 Andrew Wiles 在 1995 完成了費馬最後定理的證明。其陳述如下:

費馬最後定理：設 n 爲大於 2 的整數, 則任意的正整數 X, Y, Z 都必

$$X^n + Y^n \neq Z^n.$$

Pierre de Fermat (1607∼1665)

Andrew Wiles (1953∼)

此問題敘述簡單, 在找不到費馬宣稱的證明後, 很快地引起一般大衆興趣並吸引到一些有名的數學家嘗試證明。不過嚴格來說, 這類問題是一類特殊方程式求整數解的問題, 在數學上是

*本文根據民國 109 年 6 月 15 日演講者於台大-中研院 Basic Notion Seminar 演講內容改寫而成。

一個孤立的問題, 並不具備一般的興趣, 因此並不是被所有的數論學家都認同這問題的重要性。例如在 1816 年, Gauss 寫下：「費馬最後定理是一個孤立的命題, 我承認自己對它少有興趣。我可以輕易寫下許多這種命題, 它們既無法被證明也無法被反證。」

Carl Friedrich Gauss (1777∼1855)

但日後 Wiles 在費馬最後定理的工作用到所有二十世紀末最前端的數學理論, 集結了代數數論、算術幾何及交換代數的數十年成果。他的工作在數論上的歷史是一個偉大的里程坤。數論學家在費馬最後定理上的研究建立了數論和自守表現論之間的橋樑, 對後來的 Sato-Tate 猜想的證明乃至 Langlands 綱領的進展都有巨大的影響, 這或許是 Gauss 當時始料未及的。

Kummer

第一位對費馬最後定理進行有系統性的研究是代數數論開拓者, 德國數學家 Kummer。他在 1850 年得到費馬最後定理證明的初步進展。他證明：若 p 是正則質數 (regular prime), 則費馬方程式 $X^p + Y^p = Z^p$ 無正整數解。

Kummer (1810∼1893)

Kummer **觀察到**：對任意正整數 n, 令

$$\zeta_n = e^{2\pi\sqrt{-1}/n} = \cos\frac{2\pi}{n} + \sqrt{-1}\sin\frac{2\pi}{n}\mathbb{C}$$

爲n次單位根。對任意奇質數 p, 費馬方程$X^p+Y^p=Z^p$可寫爲

$$X^p = (Z-Y)(Z-\zeta_p Y)(Z-\zeta_p^2 Y)\cdots(Z-\zeta_p^{p-1}Y).$$

若 X, Y, Z 是上面費馬方程的正整數解, 則

$$\{Z-\zeta_p^i Y,\ 0\le i\le p-1\}$$

的公因數會是 p 在環 $\mathbb{Z}[\zeta_p]$ 的因子 (divisor)。因此他發想到若 p 是正則質數, 也就是說當環 $\mathbb{Z}[\zeta_p]$ 有類似整數的「質因數分解唯一性」的性質, 或可證明費馬方程無正整數解。

理想類群

爲了給出正則質數的嚴格定義, 我們介紹理想類群的概念。若一個數體 (number field) K 是有理數體 $\mathbb{Q}$ 的有限擴展, 我們記 $\mathcal{O}_K$ 爲 K 的整數環。例如, 若 $K = \mathbb{Q}(\sqrt{-5})$, 則 $\mathcal{O}_K = \{a + b\sqrt{-5}, a, b \in \mathbb{Z}\}$。我們有：

定義：理想類群 (ideal class group) $\mathrm{Cl}(K)$ 爲

$$\mathrm{Cl}(K) = \{\mathcal{O}_K \text{ 的理想}\}/\sim,$$

其中 $a \sim b \Leftrightarrow$ 存在 $\alpha \in K^x = K\backslash\{0\}$ 使得 $a = \alpha \cdot b$ 。

我們可以證明理想類群 $\mathrm{Cl}(K)$ 是個有限群, 其元素個數

$$h(K) = \#(\mathrm{Cl}(K))$$

被稱爲數體 K 的類數 (class number)。類數的重要性在於它刻畫一個數體的整數環是否具有一般整數的質因數分解唯一性。

定理：$h(K) = 1$ 若且唯若 $\mathcal{O}_K$ 具有質因數分解的唯一性。

例如：$h(\mathbb{Q}) = 1$, 而 $h(\sqrt{-5}) = 2$。也說明當 $K = \mathbb{Q}(\sqrt{-5})$, 整數環 $\mathcal{O}_K$ 裡的整數沒有質因數分解唯一性。例如 $6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$。

正則質數

對任意正整數 n, 令 $\mathbb{Q}(\zeta_n)$ 爲 $\mathbb{Q}$ 添加 ζ_n 生成的有限擴張。我們稱 $\mathbb{Q}(\zeta_n)$ 爲 n 次分圓體 (cyclotomic field)。

定義：稱質數 p 爲正則質數, 若且唯若 p 不整除 $h(\mathbb{Q}(\zeta_p))$。

Kummer 證明：若 p 是正則質數, 則方程式 $X^p + Y^p = Z^p$ 無正整數解。

可惜的是, 並非所有的質數都是正則質數。例如 : $p = 691$ 不是正則質數, 亦即 691 整除 $h(\mathbb{Q}(\zeta_{691}))$。事實上, 最小的非正則質數爲 37, 也因此 Kummer 證明了當 $n < 37$, 費馬最後定理成立。事實上, 德國的數學家 Carl Siegel 有以下猜想:

猜想 (Siegel): 約 65.65 % 的質數爲正則質數。

若上面的 Siegel 猜想爲真, Kummer 當時證明了約三分之二的費馬最後定理!

Zeta 值和岩澤理論

在 Kummer 的工作之後, 如何有效的判別一個質數是否正則形成一個重要的問題。定義類數 $h(\mathbb{Q}(\zeta_p))$ 雖然簡單, 但計算類數是一件十分困難的事。神奇的是, 我們能利用岩澤理論結合 zeta 函數以解析方法得到有效的正則質數判斷法。

定義：Riemann zeta 函數定義爲

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s},$$

其中 s 爲實部 $\mathrm{Re}\ s > 1$ 的複數。

Euler 曾計算 $\zeta(s)$ 在一些負奇數的取值：

$$\zeta(-1) = -\frac{1}{12}, \qquad \zeta(-3) = \frac{1}{120}, \qquad \zeta(-5) = -\frac{1}{2^2 \cdot 3^2 \cdot 7},$$
$$\zeta(-7) = \frac{1}{2^4 \cdot 3 \cdot 5}, \qquad \zeta(-9) = -\frac{1}{2^2 \cdot 3 \cdot 11},$$
$$\zeta(-11) = \frac{691}{2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13}, \ \cdots$$
$$\zeta(-31) = -\frac{37 \cdot 683 \cdot 305065927}{2 \cdot 3 \cdot 5 \cdot 7}, \ \cdots$$

我們注意到：質數 691 具有下列性質

- 691 是 $\zeta(-11)$ 的分子的質因數 (解析性質),
- 691 是類數 $h(\mathbb{Q}(\zeta_{691}))$ 的質因數 (算術性質)。

類似地, 質數 37 具有下列性質：

- 37 是 $\zeta(-31)$ 的分子的質因數 (解析性質),
- 37 是類數 $h(\mathbb{Q}(\zeta_{37}))$ 的質因數 (算術性質)。

為了進一步解釋這種觀察, 我們引進以下定義

定義：稱 $A_p := \mathrm{Cl}\Big(\mathbb{Q}(\zeta_p)\Big) \bigotimes_Z \mathbb{Z}_p$ 爲 $\mathrm{Cl}\Big(\mathbb{Q}(\zeta_p)\Big)$ 的 p-準素子群 (p-primary subgroup); 它具有自然的 Galois 作用 $\mathrm{Gal}\Big(\mathbb{Q}(\zeta_p)/\mathbb{Q}\Big) \times A_p \to A_p$ 。

現定義 $\omega : \mathrm{Gal}\Big(\mathbb{Q}(\zeta_p)/\mathbb{Q}\Big) \to \mathbb{Z}_p^{\times}$ 爲滿足

$$\sigma(\zeta_p) = \zeta_p^{\omega(p)}, \quad \forall\ \sigma \in \mathrm{Gal}\Big(\mathbb{Q}(\zeta_p)/\mathbb{Q}\Big)$$

的唯一特徵值。我們可進行依 Galois 群作用的譜分解, 將 A_p 分解爲

$$A_p = \bigoplus_{k=0}^{p-1} A_p(k),$$

其中 $A_p(k) = \{x \in A_p \mid \sigma(x) = \omega^k(\sigma)x,\ \sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p))/\mathbb{Q})\}$。根據以上分解, 我們對 $p = 691, 37$ 有以下更細緻的結果 (Herbrand - Ribet 定理) :

$$691 \mid \zeta(-11);\ 691 \mid \#(A_{691}(-11)).$$
$$37 \mid \zeta(-31);\ 37 \mid \#(A_{37}(-31)).$$

數論中的岩澤理論旨在系統性的研究上述現象及其推廣。粗略來說, 古典岩澤理論探討下述關聯 :

zeta 函數值 $\Leftrightarrow$ 具 Galois 作用的理想類群。

Dirichlet L-函數

1837 年, Dirichlet 推廣 Riemann zeta 函數, 對任意狄利克雷特徵 (Dirichlet character)

$$\chi : (\mathbb{Z}/p\mathbb{Z})^\times \to C^\times.$$

定義 L-**函數** :

$$L(s,\chi) = \sum_{n=1, p\nmid n}^{\infty} \frac{\chi(n)}{n^s}, \quad \text{其中 } s \in \mathbb{C},\ \mathrm{Re}\, s > 1.$$

Dirichlet (1805∼1859)

Dirichlet 建構此函數, 用以證明 : 對 $1 \le a < p$, 等比數列 $\{pn + a\}_{n=1,2,\ldots}$, 包含無限多個質數。

Dirichlet L-函數有解析延拓 (analytic continuation), 整個複平面。若 $\chi(-1) = -1$, 則可得知 $L(0,\chi) \neq 0$ 且

$$L(0,\chi) = \frac{1}{p}\sum_{a=1}^{p-1} \chi(a), \quad a \in \overline{\mathbb{Z}}.$$

我們若將 p-adic 特徵 $\omega : \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \to \mathbb{Z}_p^\times$ 視爲狄利克雷特徵 $\omega : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}^\times$; 則由上式可知

$$L(0,\omega^k) \in \mathbb{Z}_p \ \text{ 對任意奇數 } k。$$

理想類群與 Zeta 值的進一步關係

定理 (Mazur-Wiles, 1984)：設 p 爲任意奇質數。對任意奇數 k, 我們都有

$$\#(A_p(k)) = \#\Big(\mathbb{Z}_p/L(0,\omega^k)\Big).$$

備註：對任意負奇數 $k<0$, 我們有同餘關係如下：

$$L(0,\omega^k) \equiv \zeta(k) (\mathrm{mod}\, p).$$

取 $p=11$, $k=-11$, 則可解釋下述關係：

$$691 \mid \zeta(-11) \;\Leftrightarrow\; 691 \mid L(0,\omega^{-11}) \;\Leftrightarrow\; 691 \mid \#(A_{691}(-11)).$$

根據原來定義, 一個質數 p 爲正則質數若且唯若 p 不整除 $\#(A_p)$。另一方面, 我們有分解

$$A_p = \bigoplus_{k=0}^{p-1} A_p(k).$$

Mazur-Wiles 定理指出：若 k 爲奇數, 則 $\#(A_p(k))$ 可由計算 Dirichlet L-函數而得知。若 k 爲偶數, 我們有下述

猜想 (Vandier)：若 k 爲偶數, $\#(A_p(k)) = 1$。

當 $p < 125000$, 此猜想已被驗證屬實。

根據 Mazur-Wiles 定理, 若承認上面的 Vandier 猜想, 我們有一個奇質數 p 是正則質數若且唯若 p 整除 $\zeta(1-2k)$ 對所有 $k = 1, \ldots, (p-1)/2$。

備註：$\zeta(1-2k)$ 可以柏努力數來快速計算得出。

至此我們了解 zeta 函數的特殊值和類數之間的關系。下面我們從古老的同餘數問題 (congruent number problem) 出發, 說明 zeta 函數和橢圓曲線的關連。

同餘數問題 ($\sim$972 A.D.)

定義：設正整數 n 無任何整數的平方爲其因數。稱此正整數 n 爲同餘數 (congruence number), 若且唯若 n 是某三邊長都是有理數的直角三角形的面積。換言之, 存在正的有理數 A, B, C 使得

$$n = \frac{1}{2}AB, \quad C^2 = A^2 + B^2.$$

若 A, B, C 爲上述方程的解, 我們令

$$x = C^2\!\diagup_4, \qquad y = \frac{(A^2-B^2)C}{2},$$

立即可知 $(x,y)\in\mathbb{Q}^2$ 爲三次方程式

$$y^2=x(x-n)(x+n)$$

的有理解。這是橢圓曲線的一例。

橢圓曲線

令 $a,b\in\mathbb{Z}$ 使得 $\triangle:=4a^3+27b^2\neq 0$。令

$$f(X,Y,Z)=Y^2Z-(X^3+aXZ^2+bZ^3)$$

且令 $E\subset\mathbb{P}^2$ 爲 f 在 $\mathbb{P}^2$ 的零集, 則 E 定義了一個 $\mathbb{Q}$ 上無奇異點的投影曲線。給定體 L, 令 $E(L)$ 爲 E 的 L-有理點 :

$$\begin{aligned}E(L)&=\{[a_0:a_1:a_2]\in\mathbb{P}^2(L)\mid f(a_0,a_1,a_2)=0\}\\&=\{(x,y)\in L^2\mid y^2=x^3+ax+b\}\cup\{0:1:0\}.\end{aligned}$$

我們知道

- $O:=[0:1:0]\in E(\mathbb{Q})$.
- $E(\mathbb{C})$ 爲虧格爲一的黎曼曲面。

我們稱 (E,O) 爲 $\mathbb{Q}$ 上由 $y^2=x^3+ax+b$ 定義的橢圓曲線。

Mordell-Weil 定理

我們有如下的同構關係 :

$$E(L)\simeq \mathrm{Pic}^0E(L),\qquad P\mapsto(P)-(O).$$

這給了 $E(L)$ 交換群的結構。

定理 (Mordell-Weil) : 若 L 是 $\mathbb{Q}$ 的有限擴張體, 則 $E(L)$ 是有限生成的交換群。

定義 : 我們稱 $\mathrm{rank}_{\mathbb{Z}}E(L)$ 爲 E 佈於 L 上的代數秩 (algebraic rank)。

現在我們把同餘數問題翻譯成佈於有理數體的橢圓曲線的代數秩的問題。

定義 : 對任意正整數 n, 令 $\mathcal{E}_n$ 爲三次方程式

$$y^2=x(x-n)(x+n)$$

所定義的橢圓曲線。

命題：正整數 n 是同餘數, 若且唯若

$$\begin{aligned}\mathrm{rank}_{\mathbb{Z}}\mathcal{E}_n(\mathbb{Q})>0 &\Leftrightarrow \#(\mathcal{E}_n(\mathbb{Q}))=\infty\\ &\Leftrightarrow \mathcal{E}_n(\mathbb{Q})\text{ 有一個 non-torsion 點 (亦即, 階爲無限的點)。}\end{aligned}$$

我們考慮橢圓曲線

$$\mathcal{E}_{157}: y^2=x(x-157)(x+157).$$

可證明其 torsion 點爲

$$\mathcal{E}_{157}(\mathbb{Q})_{\mathrm{tor}}=\{(0,0),(157,0),(-157,0),[0:1:0]\}.$$

最簡單的 non-torsion 點 (x_0,y_0) 爲

$$\begin{aligned}x_0&=\frac{9573235935450158125836445 3}{27748778743924463216912 1},\\ y_0&=\frac{8340627641289489440728570857011032229 40}{1461725457917215265681552594381960 81}.\end{aligned}$$

要找出該點, 需美妙地結合代數幾何、代數數論及複分析的工具。

此外, 從這個解的複雜度可看出一般同餘數問題求解的困難度。不過我們期望利用橢圓曲線 $\mathcal{E}_n$ 的 zeta 函數來快速計算 $\mathcal{E}_n$ 佈於有理數體的代數秩。

$E/\mathbb{Q}$ 的 zeta 函數

設 ℓ 爲質數。令 $\mathbb{F}_\ell=\mathbb{Z}/\ell\mathbb{Z}$ 並

定義 $a_\ell(E)\in\mathbb{Z}$ 如下：

$$a_\ell(E)=\#(\mathbb{P}^1(\mathbb{F}_\ell))-\#(E(\mathbb{F}_\ell))=1+\ell-\#(E(\mathbb{F}_\ell))\in\mathbb{Z}.$$

定義 $E/\mathbb{Q}$ 的 zeta 函數如下：

$$L(E/\mathbb{Q},s)=\prod_{\ell\nmid\triangle}\frac{1}{1-a_\ell(E)\ell^{-s}+\ell^{1-2s}},\quad(\mathrm{Re}\,s>\frac{3}{2}).$$

定理 (Wiles 等, 1995)：$L(E/\mathbb{Q},s)$ 可解析延拓至整個複平面。

定義：我們稱 $\mathrm{ord}_{s=1}L(E/\mathbb{Q},s)$ 爲 E 的解析秩 (analytic rank)。

存在唯一的正整數 N_E (E 的 conductor) 使得

$$\Lambda_E(s):=\left(\frac{\sqrt{N_E}}{2\pi}\right)^s\cdot\Gamma(s)\cdot L(E/\mathbb{Q},s)$$

滿足函數方程

$\Lambda_E(s)=w(E/\mathbb{Q})\cdot\Lambda_E(2-s)$, 其中 $w(E/\mathbb{Q})\in\{\pm1\}$ 稱爲 E 的根數 (root number)。

千禧年大獎難題

猜想 (Birch 及 Swinnerton-Dyer)

$$\mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}) = \mathrm{ord}_{s=1} L(E/\mathbb{Q}, s).$$

Birch 及 Swinnerton-Dyer

該猜想有個較弱的版本：

$$L(E/\mathbb{Q}) = 0 \ \Leftrightarrow\ \mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}) > 0 \ \Leftrightarrow\ E(\mathbb{Q}) \text{ 有無限多點。}$$

在前述之例子 $\mathcal{E}_{157}$, 不難計算其根數 $w(\mathcal{E}_{157}/\mathbb{Q}) = -1$, 因此由函數方程我們得到 $L(\mathcal{E}_{157}/\mathbb{Q}) = 0$。

定理 (Coates - Wiles, 1977; Kolyvagin, 1995)：
若 $\mathrm{ord}_{s=1} L(E/\mathbb{Q}, s) = 0$, 則 $\mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}) = 0$。

換言之, 若 $L(E/\mathbb{Q}, 1) \neq 0$ 或解析秩爲零時, 則 $E(\mathbb{Q})$ 是有限群。

因此, 若 $L(\mathcal{E}_n/\mathbb{Q}, 1) \neq 0$, 則 n 不爲同餘數。若解析秩爲一時, 我們有

定理 (Gross - Zagier , 1986; Kolyvagin, 1995)：
若 $\mathrm{ord}_{s=1} L(E/\mathbb{Q}, s) = 1$, 則 $\mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}) = 1$。

也因此若 $\mathcal{E}_n/\mathbb{Q}$ 的解析秩等於一時, n 爲同餘數。一般而言, 對解析秩大於一的橢圓曲線, 逆反命題的驗證

$$L(E/\mathbb{Q}, 1) = 0 \ \Rightarrow\ \mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}) > 0$$

極爲困難。但在適當條件下, 可藉橢圓曲線的岩澤理論解決。

結語：數論有著問題的簡單性與方法的複雜性; 數論之美, 源於兩者之間的矛盾。也正因如此, 我們往往從一個重要數論問題的解決中, 看到數學各個分支之間的和諧共融。希望本文能傳達給讀者這樣的訊息。

—本文作者任職中央研究院數學研究所—