數學傳播　40卷1期, pp. 31-38

數論淺談: 整數解之奧秘

魏福村

本文原載中央研究院週報第1538期「知識天地」, 經作者及週報同意轉載, 僅此致謝。

— 編輯室

在數學的學習過程中, 我們最早開始接觸的數字便是整數, 但其卻也是數學裡最難掌握的其中之一。數論研究中除了最近很紅的質數分佈問題之外 (2013年被張益唐院士打開了一道關鍵大門), 另一大類研究便是方程式的整數解問題。整數解的問題敘述常常很簡單, 然而目前可以說還沒有一個一統天下的辦法。二十世紀末數學界裡最重要的工作之一便是 Andrew Wiles 證明了費馬最後定理:

$$X^n + Y^n = Z^n \text{ 在 } n \geq 3 \text{ 時沒有非零 (即 } X, Y, Z \text{ 均不爲零) 的整數解。}$$

這短短一小句話, 背後竟藏著非常高深抽象的理論並開啟了二十一世紀許多新的數學領域。但若把這個方程式小改一下, 便又可以考倒絕大多數的人了。整數解的問題討論在基礎教育中其實很少, 因爲實在是太深不見底了。不過也透過整數解問題的這種渾沌美, 讓我們可以應用在資訊傳輸的安全上 (例如密碼與編碼系統)。在這篇文章裡, 我們回憶一些熟悉的整數解問題 (韓信點兵和畢氏三元數), 進而介紹費馬最後定理以及七個「一百萬問題」之一:
Birch and Swinnerton-Dyer 猜想。希望透過這篇文章能讓讀者對於整數解的研究有所認識。

1. 中國剩餘定理與線性方程組

「兵不知數, 三三數之剩二, 五五數之剩三, 七七數之剩二」

— 出自『孫子算經』。

這題相信大家或多或少都曾見過的韓信點兵, 用現代的數學符號描述如下:

$$N \equiv 2 \bmod 3, \quad N \equiv 3 \bmod 5, \quad N \equiv 2 \bmod 7, \quad \text{求 } N \equiv ? \bmod 105。$$

心算快的或是很會猜數字的人可以很快得知 $N \equiv 23 \bmod 105$。但是若是將 3, 5, 7 改爲更爲

複雜的數字便會大大增加求解之困難度。現在讓我們來回憶一下一般求其通解的過程:

(1) 先解 $\begin{cases} N_1 \equiv 1 \bmod 3, & N_1 \equiv 0 \bmod 5, & N_1 \equiv 0 \bmod 7 \\ N_2 \equiv 0 \bmod 3, & N_2 \equiv 1 \bmod 5, & N_2 \equiv 0 \bmod 7 \\ N_3 \equiv 0 \bmod 3, & N_3 \equiv 0 \bmod 5, & N_3 \equiv 1 \bmod 7 \end{cases}$;

(2) 令 $N \equiv 2 \cdot N_1 + 3 \cdot N_2 + 2 \cdot N_3 \bmod 105$ 即爲答案。

第一步解出 N_1, N_2, N_3 的方法主要是透過長除法: 利用 3 和 $5 \cdot 7 = 35$ 互質, 透過長除法得到 $1 = 3 - 2 = 3 - (35 - 11 \cdot 3) = 12 \cdot 3 - 35$, 因此

$$N_1 \equiv -35 \bmod 105 \equiv 70 \bmod 105。$$

同理得 $N_2 \equiv 21 \bmod 105$ 和 $N_3 \equiv 15 \bmod 105$。從第二步可知

$$N \equiv 2 \cdot 70 + 3 \cdot 21 + 2 \cdot 15 \bmod 105 \equiv 23 \bmod 105。$$

上述過程主要的運算就是透過長除法, 因此對於韓信點兵這類同餘問題求通解的方法是非常有效率的 (in polynomial time)。

上面這個經典的同餘問題其實也可以看做一個「線性方程組」的整數解問題:

$$N = 2 + 3x, \quad N = 3 + 5y, \quad N = 2 + 7z, \qquad N, x, y, z \in \mathbb{Z}$$

對於線性方程組, 利用線性代數裡所學的高斯消去法, 我們可以很容易地求得「有理數解」(即 N, x, y, z 爲有理數):

$$x = \frac{N-2}{3}, \quad y = \frac{N-3}{5}, \quad z = \frac{N-2}{7}, \qquad N \in \mathbb{Q}。$$

但其整數解透過上面的討論可知, 相對來說更爲複雜。我們再來考慮另一個線性方程組:

$$\begin{cases} 2x + 3y = 5 \\ 5y + 7z = 11 \end{cases}$$

可以用矩陣表示成:

$$\begin{bmatrix} 2 & 3 & 0 \\ 0 & 5 & 7 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 5 \\ 11 \end{bmatrix}。 \qquad (*)$$

其有理數解很快地可描述如下:

$$y = \frac{5-2x}{3}, \quad z = \frac{11-5y}{7} = \frac{8+10x}{21}, \qquad x \in \mathbb{Q}。$$

當然描述法不止一種。但是若想要把所有的整數解找出來, 上面的描述方式就很難看出其通解。因此原本的高斯消去法必須做調整。一樣是透過長除法, 對於整係數矩陣我們有所謂的「Smith normal form」。簡而言之, 就是只透過整係數並且行列式值爲 ± 1 的基本矩陣乘在左右使原矩陣變爲下面的形式:

$$\begin{bmatrix} d_1 & & \\ & d_2 & \\ & & \ddots \end{bmatrix}, \qquad d_1 \mid d_2 \mid \cdots 。$$

像在上面的例子 $(*)$ 可寫成如下:

$$\begin{bmatrix} 1 & 0 \\ -5 & 1 \end{bmatrix} \begin{bmatrix} 2 & 3 & 0 \\ 0 & 5 & 7 \end{bmatrix} A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix},$$

其中矩陣 A 爲下列基本矩陣相乘:

$$\begin{bmatrix} -1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & -3 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 2 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -6 \\ 0 & 0 & 1 \end{bmatrix}$$
$$= \begin{bmatrix} -1 & 6 & -33 \\ 1 & -4 & 22 \\ 0 & 3 & -16 \end{bmatrix} 。$$

所以原方程組可改寫成:

$$\begin{bmatrix} 1 & 0 \\ -5 & 1 \end{bmatrix}^{-1} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} -1 & 6 & -33 \\ 1 & -4 & 22 \\ 0 & 3 & -16 \end{bmatrix}^{-1} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 5 \\ 11 \end{bmatrix},$$

而通解則爲:

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} \begin{bmatrix} -1 & 6 & -33 \\ 1 & -4 & 22 \\ 0 & 3 & -16 \end{bmatrix} \begin{bmatrix} -5 \\ -14 \\ k \end{bmatrix} = \begin{bmatrix} -89 - 21k \\ 61 + 14k \\ -42 - 10k \end{bmatrix}, \qquad k \in \mathbb{Z}。$$

透過上面的過程, 我們知道線性方程組的整數解問題可用高斯消去法的精神加上長除法的輔助來求解。雖然沒有像在求有理數解時那麼快速, 但是跟同餘問題解法一樣也是很有效率的 (in polynomial time)。

2. 畢氏三元數與 Pell 方程

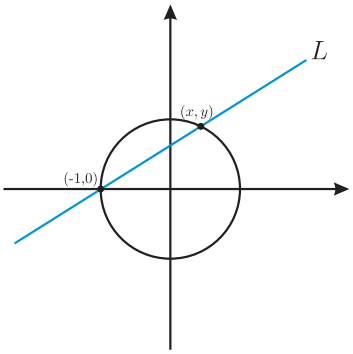
給定一直角三角形, 假設兩股長爲 a, b, 斜邊長爲 c, 則畢氏定理 (或稱勾股弦定理) 告訴我們:

$$a^2 + b^2 = c^2。$$

當 a, b, c 均爲正整數時, 我們稱 (a, b, c) 爲一組畢氏三元數 (Pythagorean triples)。找出所有的畢氏三元數即可看成 $X^2 + Y^2 = Z^2$ 的正整數解問題。其通解爲:

$$a = l(m^2 - n^2), \quad b = 2lmn, \quad c = l(m^2 + n^2), \qquad m, n, l \in \mathbb{N},\ m > n。$$

讓我們回憶一下其中一種求法 (歐幾里得): 首先帶入可知上述形式的 (a, b, c) 必爲畢氏三元數。另一方面, 當給定一組畢氏三元數 (a, b, c) 時, 令 $x = a/c$, $y = b/c$。則 $0 < x, y < 1$ 且 (x, y) 爲單位圓上一點。考慮在平面上通過 (x, y) 和 $(-1, 0)$ 的直線 L (如下圖):



則 L 的斜率 $r = y/(x+1) \in \mathbb{Q}$ 且 $0 < r < 1$。將 $y = r(x+1)$ 帶入圓方程式 $x^2 + y^2 = 1$ 得到一個 x 的二次方程式:

$$(r^2 + 1)x^2 + 2r^2x + (r^2 - 1) = 0。$$

利用公式解可求得

$$x = \frac{1 - r^2}{1 + r^2} \quad 和 \quad y = \frac{2r}{1 + r^2}。$$

將 r 寫成 $r = n/m$, $m > n$, 且 m 和 n 互質, 我們便可以找到一個正整數 l 使得

$$a = l(m^2 - n^2), \quad b = 2lmn, \quad c = l(m^2 + n^2)。$$

上面所述方法也可以幫助我們找出 $X^2 - DY^2 = Z^2$ $(D \in \mathbb{Z})$ 整數解的一個生成公式:

$$X = l(m^2 + Dn^2), \quad Y = 2lmn, \quad Z = l(m^2 - Dn^2), \quad l, m, n \in \mathbb{Z}。$$

接下來我們考慮一個相關的變形 —「Pell 方程」:

$$X^2 - DY^2 = 1, \qquad D \in \mathbb{Z}。$$

這問題是爲了了解 $\sqrt{2}$ 而衍生的。當 $D < 0$ 或 D 是完全平方數時我們可以很容易得知其 Pell 方程的整數解只有有限個且可以很清楚的寫下來。然而當 $D > 0$ 且不是平方數的時候, 如何描述其所有整數解並不是一個容易的問題。假設能找出一組解 (a_1, b_1) (當 $b_1 \neq 0$ 時), 那便可利用下列遞迴式創造出無限多組解:

$$(a_{n+1}, b_{n+1}) = (a_n a_1 + D b_n b_1, a_n b_1 + b_n a_1), n \in \mathbb{N}。$$

這些解其實是從 $(a_n + b_n\sqrt{D}) = (a_1 + b_1\sqrt{D})^n$ 這個等式而來。因爲

$$(a_1 + b_1\sqrt{D})(a_1 - b_1\sqrt{D}) = 1,$$

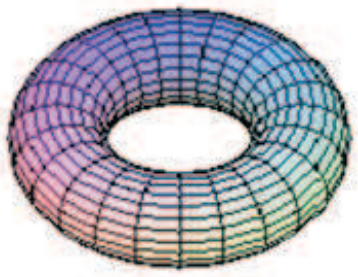
我們可以利用 $(a_1 - b_1\sqrt{D})^n = (a'_n + b'_n\sqrt{D})$ 又得到另一群解 (a'_n, b'_n)。如何先找出一組解, 這個問題早在 12 世紀中便已知道。但是對於找出所有整數解的問題, 卻又過了很久才有解答。對這問題可證明存在一個「基本解」(fundamental solution) (A_1, B_1) 使得其他的解均由 (A_1, B_1) 透過上面所述方法來生成。換句話說, 這些解構成一個「無限循環群」(infinite cyclic group), 而 (A_1, B_1) 爲其生成元。這個基本解可以透過將 $\sqrt{D}$ 寫成「連分數」來得到, 但是已知的演算法並非“polynomial time”。因此當 D 很複雜時我們暫時還沒有一個有效率的解法。

3. 費馬最後定理與橢圓曲線

費馬最後定理所考慮的方程式 $X^n + Y^n = Z^n$ 可以看作是尋找畢氏三元數的一種推廣。該定理由費馬 (17世紀) 所提出, 但是費馬並沒有附上證明。這問題一直到20世紀末才由英國數學家 Andrew Wiles 所解決。然而 Wiles 的證明運用了許多近代數學才有的工具, 因此也有不少人相信這個定理應該還有其他的證明方式。近代數論研究的主要方程之一: 橢圓曲線, Wiles 的證明便是透過了關於橢圓曲線的研究。所謂的橢圓曲線, 我們可以用下面這類方程式 (Weierstrass 方程) 來描述:

$$E : Y^2 = X^3 + aX^2 + bX + c, \qquad a, b, c \in \mathbb{Z}。$$

這類方程式的特別之處在於其解集合有很漂亮的代數結構。更精確地說, 可利用「切線割線法」使其解集合構成一個「交換群」。若考慮其所有複數解, 可形成一個像輪胎的黎曼面 (如下圖)。



對橢圓曲線基本性質有興趣的讀者可以參考 [7] 及 [8]。

在 20 世紀中期, Taniyama-Shimura 猜想橢圓曲線必具有一個特殊的性質:「模」(modular)。進而在 80 年代, Frey 將費馬最後定理和橢圓曲線牽上關係: 假設存在 $X^p + Y^p = Z^p$ 的一組非零整數解 (a, b, c) (其中 $p > 2$ 爲質數), 考慮一個對應於這組解的橢圓曲線:

$$E_{a,b} \ : \ Y^2 = X(X - a^p)(X + b^p)。$$

Frey 提出而由 Serre 及 Ribet 證明了 (利用 $a^p + b^p = c^p$ 這個等式) 橢圓曲線 $E_{a,b}$ 必不具備「模」的性質。也就是說, 若解 (a, b, c) 存在的話, $E_{a,b}$ 便成爲 Taniyama-Shimura 猜想的一個反例。Wiles 的工作便是說明了某一類 (所謂的 semi-stable) 的橢圓曲線滿足 Taniyama-Shimura 猜想, 而這類型的橢圓曲線包含了 $E_{a,b}$。因此透過 Wiles 最後的臨門一腳 (卻也是最艱難的一步) 使得費馬最後定理得證。而整個 Taniyama-Shimura 猜想也在之後由 Wiles 及其研究團隊完整地證明。讀者若想知道更多的細節, 可以參考 [1] 以及 [2]。

橢圓曲線的「模」性質, 主要是在描述橢圓曲線以及複數上半平面的一種特殊解析函數 — 模形式 (modular form) — 之間的關係。模形式是近代數論研究中非常重要的函數, 可以看作「自守型式」(automorphic form) 的一種。這類解析函數具有非常多面向的幾何與算術意義。利用其傅立葉係數所造的生成函數 — L 函數, 除了有非常好的解析性質與對稱性之外, 其特殊值 (special value) 闡述了非常深奧的幾何與算術不變量 (cf. [9] 和 [10])。讀者若對於模形式有興趣, 相關的基本介紹可以參考 [6]。利用 Taniyama-Shimura 猜想以及 Wiles 的工作, 近代數學家透過對模形式的了解來幫助在橢圓曲線上的研究, 進而希望對於下一節的「一百萬問題」— Birch and Swinnerton-Dyer 猜想 — 有所突破。

4. Birch and Swinnerton-Dyer 猜想

這個近代數論熱門猜想之一, 目的是爲了了解橢圓曲線上的所有有理數解。當我們把橢圓曲線的方程式齊次化

$$E : Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3,$$

問題便轉化爲考慮 E 的整數解問題。上面有提到橢圓曲線特別之處就在於其解集合構成一個交換群, 而由 Mordell-Weil 定理可知整數解的集合所形成的是「有限生成」交換群。有限生成交換群具有和整數相似的代數結構, 因此在資訊安全的應用上有所謂的「橢圓曲線加密解密系統」(elliptic curve cryptosystem, 請參考 [5])。其好處便在於橢圓曲線上的加減法比整數來說相對複雜不少, 因此要被破解也相對困難。建立此系統的前提便是要先能了解橢圓曲線上的所有整數解, 而和第二節的 Pell 方程解集合一樣, 問題便成爲如何找出解集合的生成元。

每一個有限生成交換群都有一個不變量: 秩 (rank)。這個不變量 (大致上) 給了這個群的生成元個數。而 Birch and Swinnerton-Dyer 猜想第一部分 (最原始的猜想) 便是希望透過

橢圓曲線的 L 函數 $L(E,s)$ 來得到秩這個不變量。橢圓曲線的 L 函數是來自原方程式 E 在每個質數 p 的同餘解個數, 即對每個質數 p 考慮下面同餘方程:

$$Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3 \bmod p。$$

同餘解的個數是有限的, 因此某個程度上來說 $L(E,s)$ 是可以計算的。上一節所提到的 Taniyama-Shimura 猜想更精確地說法爲: 每個橢圓曲線的 L 函數 $L(E,s)$ 都是來自於一個對應的模形式。因此這類的 L 函數都是"解析"的且滿足一個非常漂亮的對稱性 (連接 $L(E,s)$ 和 $L(E,2-s)$)。在中心點 $s=1$ 做泰勒展開式時可將 $L(E,s)$ 寫成

$$L(E,s) = c_r(s-1)^r + c_{r+1}(s-1)^{r+1} + \cdots, \qquad c_r \neq 0。$$

其中 r 爲一個非負的整數。Birch and Swinnerton-Dyer 猜想第一部分 (也是最原始的猜想) 便是:

r 等於 E 的整數解集合的秩。

從 L 函數的構造方式, 可知 r 這個數字是可計算的。因此若這個猜想正確, 我們便可得到生成元的個數。而 Birch and Swinnerton-Dyer 猜想的第二個部分爲:

係數 c_r 包含了 E 的"所有"幾何不變量。

對於找出橢圓曲線整數解的生成元, 現在已知的演算法 (例如"descent") 其有效性便是建立在 Birch and Swinnerton-Dyer 猜想這兩個敘述的正確性之上。目前現有的演算法 (假設 Birch and Swinnerton-Dyer 猜想正確) 在實際問題上均可找出所有的生成元。然而不止是其有效性都還不知道, 這些方法的效率也是另一個問題。

透過橢圓曲線的「模」的性質, Gross-Zagier 以及 Kolyvagin 的工作證明了當 $r \leq 1$ 時這整個猜想是正確的。雖然現有理論已知有很大一部分的橢圓曲線其秩均小於等於 1, 但是現在對於 $r \geq 2$ 的情況並沒有太多的進展。因此目前離完整證明 Birch and Swinnerton-Dyer 猜想還有很長很長的一段路要走。

參考資料

1. 于靖, 數論三講, 數學傳播, 十八卷二期。
2. 李文卿, 余文卿, 費馬最後理: A. Wiles 的解決方法, 數學傳播, 十八卷二期。
3. Barbeau, Edward J. (2003), *Pell's Equation*, Problem Books in Mathematics, Springer-Verlag.
4. Edwards, Harold M. (1996), *Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory*, Graduate Texts in Mathematics 50, Springer-Verlag.
5. Koblitz, N. (1994). *A Course in Number Theory and Cryptography*, Graduate Texts in Mathematics 114, 2nd edition, Springer-Verlag.

6. Serre, J.-P. (1973). *A Course in Arithmetic*, Graduate Texts in Mathematics 7, Springer-Verlag.
7. Silverman, J. H. (2009). *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 106, 2nd edition, Springer-Verlag.
8. Silverman, J. H. and Tate, J. (2015). *Rational Points on Elliptic Curves*, Undergraduate Texts in Mathematics, 2nd edition, Springer-Verlag.
9. Wei, F.-T. (2013). *On metaplectic forms over function fields*, Mathmatische Annalen Volume 355 Issue 1 235-258.
10. Wei, F.-T. (2014). On Rankin triple product L-functions over function fields: central critical values, *Mathematische Zeitschrift*, Volume 276, Issue 3-4 925-951.
11. Wiles, A. (2006). The Birch and Swinnerton-Dyer Conjecture, in The Millennium prize problems, American Mathematical Society, 31-44.

—本文作者爲中研院數學所研究學者—