數論淺談：整數解的奧秘

魏福村

國立中央大學數學系

26 December 2017

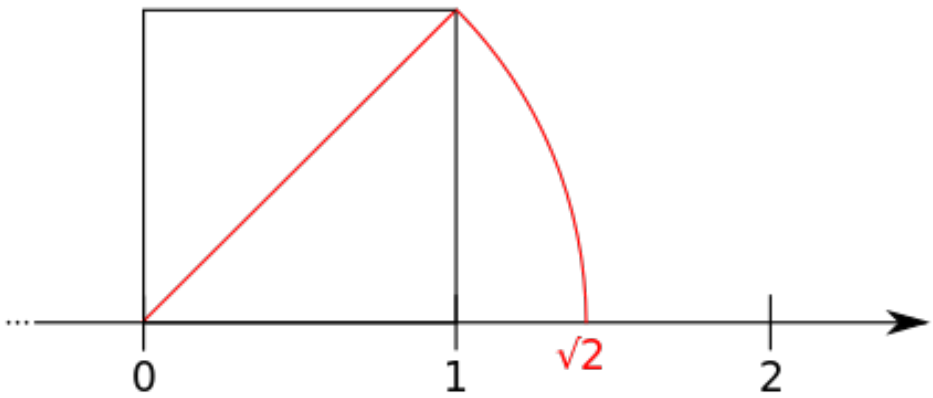
Outline

第一次數學危機

古希臘的畢達哥拉斯學派信奉「數即萬物」，並認為宇宙間各種關係都可以用整數或整數之比（有理數）來表達。但是.....

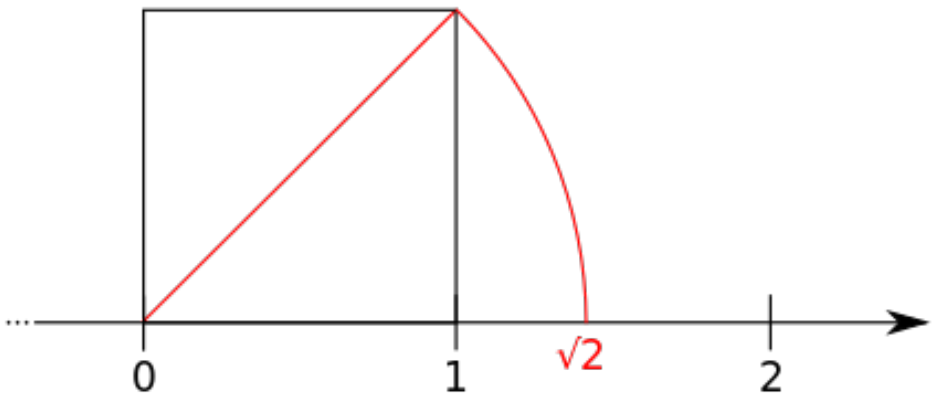
第一次數學危機

古希臘的畢達哥拉斯學派信奉「數即萬物」，並認為宇宙間各種關係都可以用整數或整數之比（有理數）來表達。但是.....



第一次數學危機

古希臘的畢達哥拉斯學派信奉「數即萬物」，並認為宇宙間各種關係都可以用整數或整數之比（有理數）來表達。但是.....



相傳畢達哥拉斯有一位學生希帕索斯 (Hippasus) 無意中對外人洩漏了這個驚人秘密，因而.....V_V

無理數：$\sqrt{2}$

說明 $\sqrt{2}$ 為無理數，可以將問題轉換成證明

$$x^2 - 2 = 0 \text{ 沒有有理數解。}$$

無理數：$\sqrt{2}$

說明 $\sqrt{2}$ 為無理數，可以將問題轉換成證明

$$x^2 - 2 = 0 \text{ 沒有有理數解。}$$

證明：假設存在兩互質的整數 a 和 b 滿足 $a^2 = 2b^2$。則 a 和 b 必須均為偶數，因此得到矛盾。Q.E.D.

無理數：$\sqrt{2}$

說明 $\sqrt{2}$ 為無理數，可以將問題轉換成證明

$$x^2 - 2 = 0 \text{ 沒有有理數解。}$$

證明：假設存在兩互質的整數 a 和 b 滿足 $a^2 = 2b^2$。則 a 和 b 必須均為偶數，因此得到矛盾。Q.E.D.

推廣： 給定一整係數多項式

$$c_0x^n + c_1x^{n-1} + \cdots + c_{n-1}x + c_n, \quad c_1, \ldots, c_n \in \mathbb{Z}。$$

若 a/b（a,b 互質）為其一有理解，則 $b \mid c_0$ 和 $a \mid c_n$。

韓信點兵

「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』。

韓信點兵

「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』。

用現代的數學符號描述如下：

$$\begin{cases} N \equiv 2 \bmod 3 \\ N \equiv 3 \bmod 5 \\ N \equiv 2 \bmod 7 \end{cases} \qquad \text{求 } N \equiv ? \bmod 105。$$

通解法

(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 $N \equiv 2 \cdot N_1 + 3 \cdot N_2 + 2 \cdot N_3 \mod 105$ 即為答案。

通解法

第一步解出 N_1, N_2, N_3 的工具為長除法 (division algorithm)：利用 3 和 $5 \cdot 7 = 35$ 互質，透過輾轉相除法得到

$$35 = 11 \cdot 3 + 2 \quad \text{以及} 3 = 2 + 1。$$

所以

$$1 = 3 - 2 = 3 - (35 - 11 \cdot 3) = 12 \cdot 3 - 35，$$

可得

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

通解法

第一步解出 N_1, N_2, N_3 的工具為長除法 (division algorithm)：利用 3 和 $5 \cdot 7 = 35$ 互質，透過輾轉相除法得到

$$35 = 11 \cdot 3 + 2 \quad \text{以及} 3 = 2 + 1。$$

所以

$$1 = 3 - 2 = 3 - (35 - 11 \cdot 3) = 12 \cdot 3 - 35，$$

可得

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

同理得 $N_2 \equiv 21 \bmod 105$ 和 $N_3 \equiv 15 \bmod 105$。

從第二步可知 $N \equiv 2 \cdot 70 + 3 \cdot 21 + 2 \cdot 15 \bmod 105 \equiv 23 \bmod 105$。

線性方程組

上述問題也可用「線性方程組」敘述如下：

$$\begin{cases} N = 2 + 3x\,, \\ N = 3 + 5y\,, \\ N = 2 + 7z\,, \end{cases} \qquad N, x, y, z \in \mathbb{Z}\,。$$

「有理解」(即 N, x, y, z 為有理數) 為：

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

線性方程組

考慮下面方程組

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

矩陣表示法：

$$\begin{pmatrix} 2 & 3 & 0 \\ 0 & 5 & 7 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 5 \\ 11 \end{pmatrix}\text{。}$$

Smith Normal Form

有理解可描述如下：

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

Smith Normal Form

有理解可描述如下：

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

然而，整數解的通解得透過「高斯消去法—修正版」將方程組的矩陣化為其"Smith normal form":

$$\begin{pmatrix} 1 & 0 \\ -5 & 1 \end{pmatrix} \begin{pmatrix} 2 & 3 & 0 \\ 0 & 5 & 7 \end{pmatrix} \cdot U = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}\,,$$

Smith Normal Form

其中

$$
\begin{aligned}
U &= \begin{pmatrix} -1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -3 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\
&\quad \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -6 \\ 0 & 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} -1 & 6 & -33 \\ 1 & -4 & 22 \\ 0 & 3 & -16 \end{pmatrix} .
\end{aligned}
$$

線性方程組

原方程組可改寫為

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} U^{-1} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -5 & 1 \end{pmatrix} \cdot \begin{pmatrix} 5 \\ 11 \end{pmatrix} = \begin{pmatrix} 5 \\ -14 \end{pmatrix} \circ$$

線性方程組

原方程組可改寫為

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} U^{-1} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -5 & 1 \end{pmatrix} \cdot \begin{pmatrix} 5 \\ 11 \end{pmatrix} = \begin{pmatrix} 5 \\ -14 \end{pmatrix} 。$$

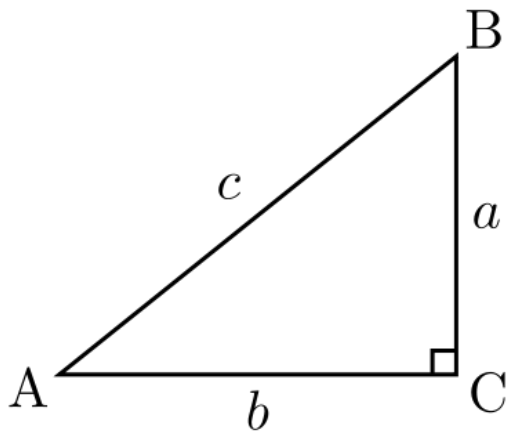
因此整數解可描述如下：

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = U \cdot \begin{pmatrix} 5 \\ -14 \\ k \end{pmatrix} = \begin{pmatrix} -89 - 21k \\ 61 + 14k \\ -42 - 10k \end{pmatrix} , \quad k \in \mathbb{Z} 。$$

畢式（勾股弦）定理

給定一直角三角形，假設兩股長為 a,b，斜邊長為 c，則：

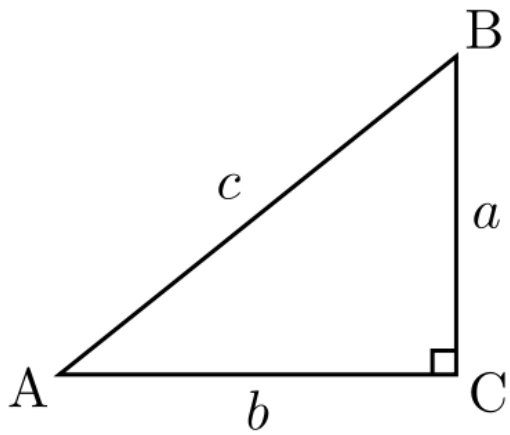
$$a^2 + b^2 = c^2 \circ$$



畢式（勾股弦）定理

給定一直角三角形，假設兩股長為 a,b，斜邊長為 c，則：

$$a^2 + b^2 = c^2 \circ$$



當 a, b, c 均為正整數時，我們稱 (a, b, c) 為一組畢氏三元數（Pythagorean triples）。

畢氏三元數

找出所有的畢氏三元數即可看成的下面方程

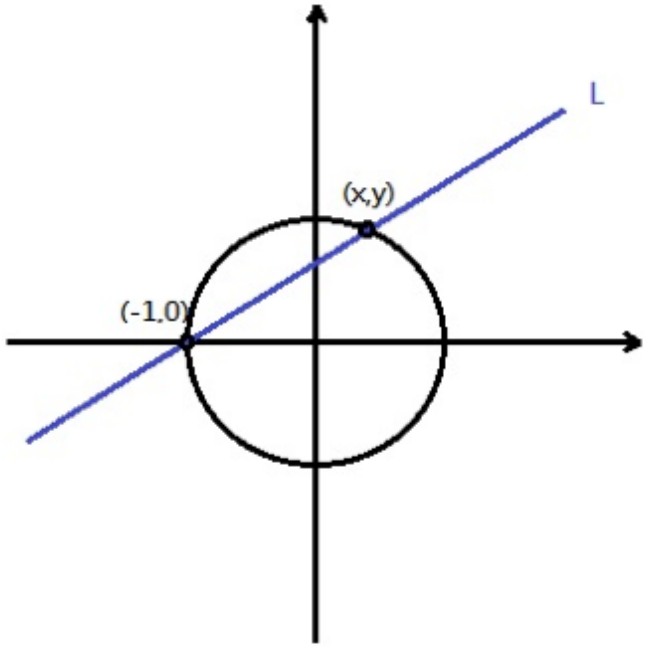
$$X^2 + Y^2 = Z^2$$

的正整數解問題。其通解 (a, b, c) 可描述如下：

$$\begin{cases} a = \ell(m^2 - n^2), \\ b = 2\ell mn, \\ c = \ell(m^2 + n^2), \end{cases} \qquad \ell, m, n \in \mathbb{Z}_{>0} \text{ and } m > n.$$

畢氏三元數

證法：(歐幾里德) 給一畢氏三元數 (a, b, c), 令 $(x, y) = (a/c, b/c) \in \mathbb{R}^2$。考慮線 L



畢氏三元數

則線 L 的斜率為 $r = y/(x+1) \in \mathbb{Q}$ 且 $0 < r < 1$。

畢氏三元數

則線 L 的斜率為 $r = y/(x+1) \in \mathbb{Q}$ 且 $0 < r < 1$。
將 $y = r(x+1)$ 帶入 $x^2 + y^2 = 1$ 可得

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

畢氏三元數

則線 L 的斜率為 $r = y/(x+1) \in \mathbb{Q}$ 且 $0 < r < 1$。
將 $y = r(x+1)$ 帶入 $x^2 + y^2 = 1$ 可得

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

公式解得出

$$x = \frac{1-r^2}{1+r^2}, \quad y = \frac{2r}{1+r^2}.$$

畢氏三元數

則線 L 的斜率為 $r = y/(x+1) \in \mathbb{Q}$ 且 $0 < r < 1$。
將 $y = r(x+1)$ 帶入 $x^2 + y^2 = 1$ 可得

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

公式解得出

$$x = \frac{1-r^2}{1+r^2}, \quad y = \frac{2r}{1+r^2}.$$

令 $r = n/m$, $m, n \in \mathbb{Z}_{>0}$, $m > n$, 且 m, n 互質。則存在 $\ell \in \mathbb{Z}_{>0}$ 使得

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

畢氏三元數

推廣：$X^2 - 2Y^2 = Z^2$ 的整數解 (a, b, c) 可描述如下：

$$\begin{cases} a = \ell(m^2 + 2n^2), \\ b = 4\ell mn, \\ c = \ell(m^2 - 2n^2), \end{cases} \qquad \ell, m, n \in \mathbb{Z}.$$

畢氏三元數

推廣：$X^2 - 2Y^2 = Z^2$ 的整數解 (a, b, c) 可描述如下：

$$\begin{cases} a = \ell(m^2 + 2n^2), \\ b = 4\ell mn, \\ c = \ell(m^2 - 2n^2), \end{cases} \qquad \ell, m, n \in \mathbb{Z}.$$

- 當限制 $c = 0 \Longrightarrow a = b = 0$（因為 $\sqrt{2}$ 為無理數）。
- 當限制 $c = 1 \Longrightarrow$ Pell 方程。

Pell 方程

給一整數 D, 考慮下列方程

$$X^2 - DY^2 = 1.$$

Pell 方程

給一整數 D, 考慮下列方程

$$X^2 - DY^2 = 1.$$

- 當 $D \leq 0$ 或 D 為完全平方數時，有限多組整數解 (easy exercise)。

Pell 方程

給一整數 D, 考慮下列方程

$$X^2 - DY^2 = 1.$$

- 當 $D \leq 0$ 或 D 為完全平方數時，有限多組整數解 (easy exercise)。
- 當 $D > 0$ 且 D 不為完全平方數時，無限多組整數解 (not easy)。

當 $D<0$ 且 D 不為完全平方數

假設有一組解 (a_1, b_1) 其中 $b_1 \neq 0$，則

$$(a_{n+1}, b_{n+1}) := (a_n a_1 + D b_n b_1, a_n b_1 + b_n a_1), \quad n \in \mathbb{Z}_{>0}$$

均為其解。

當 $D<0$ 且 D 不為完全平方數

假設有一組解 (a_1, b_1) 其中 $b_1 \neq 0$，則

$$(a_{n+1}, b_{n+1}) := (a_n a_1 + D b_n b_1, a_n b_1 + b_n a_1), \quad n \in \mathbb{Z}_{>0}$$

均為其解。其實：

$$a_n + b_n\sqrt{D} = (a_1 + b_1\sqrt{D})^n.$$

利用 $(a_1 - b_1\sqrt{D})^n$ 可得另一群解 (a'_n, b'_n)。

當 $D<0$ 且 D 不為完全平方數

假設有一組解 (a_1, b_1) 其中 $b_1 \neq 0$，則

$$(a_{n+1}, b_{n+1}) := (a_n a_1 + D b_n b_1, a_n b_1 + b_n a_1), \quad n \in \mathbb{Z}_{>0}$$

均為其解。其實：

$$a_n + b_n\sqrt{D} = (a_1 + b_1\sqrt{D})^n.$$

利用 $(a_1 - b_1\sqrt{D})^n$ 可得另一群解 (a'_n, b'_n)。

可證明：存在一基本解（fundamental solution）$(A_1, B_1) \in \mathbb{Z}^2$ 使得所有解均由上面方式所得。$\Longrightarrow$ 所有解構成一個「無限循環群」（infinite cyclic group）。

當 $D<0$ 且 D 不為完全平方數

假設有一組解 (a_1, b_1) 其中 $b_1 \neq 0$，則

$$(a_{n+1}, b_{n+1}) := (a_n a_1 + D b_n b_1, a_n b_1 + b_n a_1), \quad n \in \mathbb{Z}_{>0}$$

均為其解。其實：

$$a_n + b_n\sqrt{D} = (a_1 + b_1\sqrt{D})^n.$$

利用 $(a_1 - b_1\sqrt{D})^n$ 可得另一群解 (a'_n, b'_n)。

可證明：存在一基本解（fundamental solution）$(A_1, B_1) \in \mathbb{Z}^2$ 使得所有解均由上面方式所得。$\Longrightarrow$ 所有解構成一個「無限循環群」（infinite cyclic group）。

找 (A_1, B_1) 可透過 $\sqrt{D}$ 的「連分數表示法」。

Pierre de Fermat

17 世紀中，費馬閱讀丟番圖（Diophantus）的「算術」（Arithmetica）時註解寫道：當 $n \geq 3$ 時，

$$X^n + Y^n = Z^n$$

找不到非零整數解。

Andrew Wiles

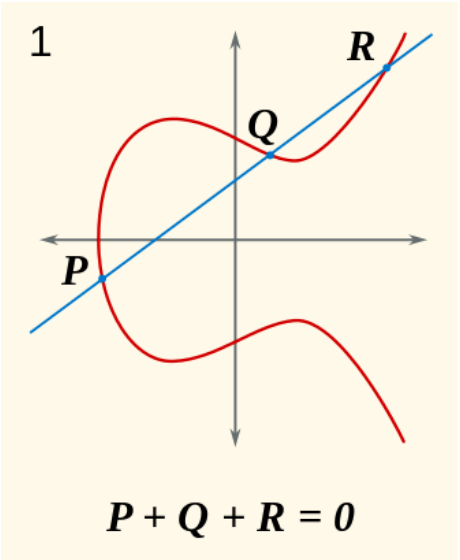
此定理一直到了 1995 年由 Andrew Wiles（及其助手 Richard Taylor）才完整證明。

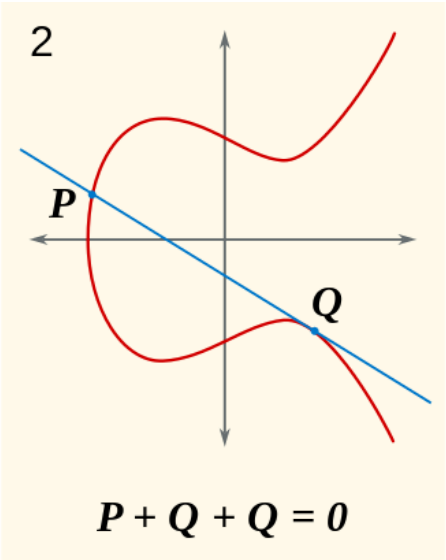
橢圓曲線

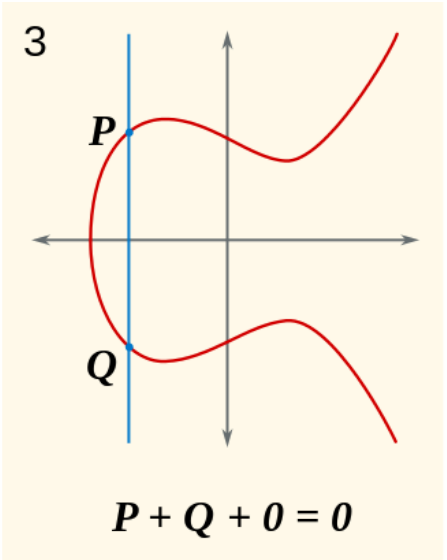
給定 $a, b, c \in \mathbb{Z}$，考慮下列 Weierstrass 方程：

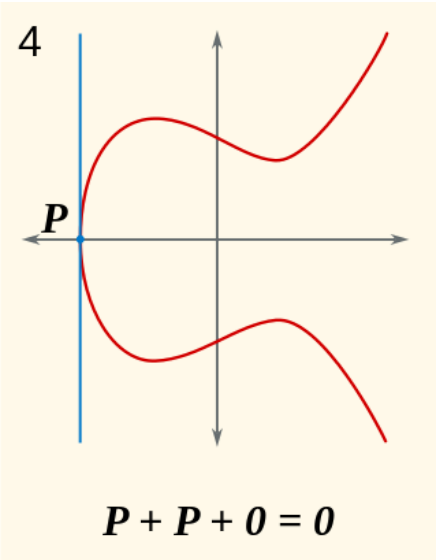
$$E : Y^2 = X^3 + aX^2 + bX + c.$$

「切線割線法」$\longrightarrow$ 解集合構成「交換群」：



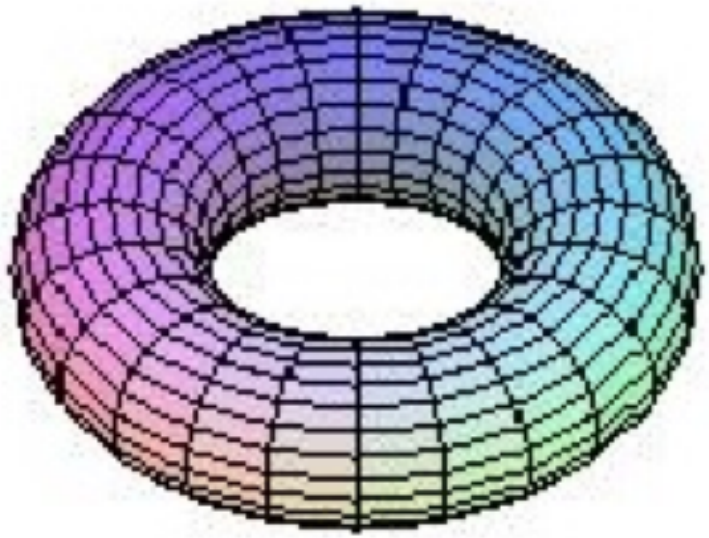






橢圓曲線

透過複變數函數論，可描述其複數解如下：



Wiles 的證明

- 問題可以化為只考慮 $n = p$ 為一質數的情況。

Wiles 的證明

- 問題可以化為只考慮 $n = p$ 為一質數的情況。
- 20 世紀中期，Taniyama-Shimura 猜想所有（整係數）橢圓曲線均具有一特殊性質：「模」(Modular)。

Wiles 的證明

- 問題可以化為只考慮 $n = p$ 為一質數的情況。
- 20 世紀中期，Taniyama-Shimura 猜想所有（整係數）橢圓曲線均具有一特殊性質：「模」(Modular)。
- 假設存在非零整數 a, b, c 滿足 $a^p + b^p = c^p$（其中 p 為質數），Frey (1980) 考慮下面的橢圓曲線

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

Wiles 的證明

- 問題可以化為只考慮 $n = p$ 為一質數的情況。
- 20 世紀中期，Taniyama-Shimura 猜想所有（整係數）橢圓曲線均具有一特殊性質：「模」(Modular)。
- 假設存在非零整數 a, b, c 滿足 $a^p + b^p = c^p$（其中 p 為質數），Frey (1980) 考慮下面的橢圓曲線

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

- Frey 和 Serre-Ribet 證明此橢圓曲線必不具備「模」(modular)。

Wiles 的證明

- 問題可以化為只考慮 $n = p$ 為一質數的情況。
- 20 世紀中期，Taniyama-Shimura 猜想所有（整係數）橢圓曲線均具有一特殊性質：「模」(Modular)。
- 假設存在非零整數 a, b, c 滿足 $a^p + b^p = c^p$（其中 p 為質數），Frey (1980) 考慮下面的橢圓曲線

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

- Frey 和 Serre-Ribet 證明此橢圓曲線必不具備「模」(modular)。

Wiles 的工作主要其實是在證明 Taniyama-Shimura 猜想，進而說明此組解 (a, b, c) 必不存在！

「模」性質

給定一橢圓曲線 $E: Y^2 = X^3 + aX^2 + bX + c$，其中 $a, b, c \in \mathbb{Z}$。對一質數 p，考慮

$$E(p) := \left\{ (x, y) \in \mathbb{Z}^2 \;\middle|\; \begin{array}{l} 0 \le x, y \le p-1 \\ y^2 \equiv x^3 + ax^2 + bx + c \mod p \end{array} \right\}.$$

「模」性質

給定一橢圓曲線 $E: Y^2 = X^3 + aX^2 + bX + c$，其中 $a, b, c \in \mathbb{Z}$。對一質數 p，考慮

$$E(p) := \left\{ (x, y) \in \mathbb{Z}^2 \;\middle|\; \begin{array}{l} 0 \le x, y \le p-1 \\ y^2 \equiv x^3 + ax^2 + bx + c \mod p \end{array} \right\}.$$

令 $c_p := p - \#(E(p))$. 利用同餘解可以定義 E 的Hasse-Weil L-函數:

$$L(E, s) \text{ ”} = \text{”} \prod_p (1 - c_p p^{-s} + p^{1-2s})^{-1} = \sum_{n=1}^{\infty} \frac{c_n}{n^s}, \quad s \in \mathbb{C}.$$

「模」性質

考慮 $L(E,s)$ 的"Mellin inversion transform", i.e. 考慮下面生成函數：

$$f_E(z) := \sum_{n=1}^{n} c_n q^n, \quad q = e^{2\pi iz}, \quad z = x + yi \in \mathbb{C} \text{ with } y > 0$$

則 Taniyama-Shimura 猜想此生成函數 $f_E(z)$ 必為一個「模型式」（Modular Form）。

「模」性質

考慮 $L(E,s)$ 的"Mellin inversion transform", i.e. 考慮下面生成函數：

$$f_E(z) := \sum_{n=1}^{n} c_n q^n, \quad q = e^{2\pi iz}, \quad z = x + yi \in \mathbb{C} \text{ with } y > 0$$

則 Taniyama-Shimura 猜想此生成函數 $f_E(z)$ 必為一個「模型式」(Modular Form)。

- 在近代數論研究中，發現幾乎所有特別的數列所造的生成函數均為模型式（或其推廣——「自守型式」(Automorphic Form)）。
- 模型式所對應的 L-函數具有很好的解析性質，且其" 特殊值" 含有非常深的幾何與算術意義。

Mordell-Weil 定理

給一橢圓曲線 $E: Y^2 = X^3 + aX^2 + bX + c$，其中 $a, b, c \in \mathbb{Z}$，考慮其對應在" 攝影平面" 的方程：

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

考慮其整數解集合

$$E(\mathbb{Z}) := \left\{ (x, y, z) \in \mathbb{Z}^3 \;\middle|\; \begin{array}{l} \gcd(x, y, z) = 1 \\ y^2z = x^3 + ax^2z + bxz^2 + cz^3 \end{array} \right\}$$

Mordell-Weil 定理

Mordell-Weil 定理

利用切憲哥線法，其整數解集合 $E(\mathbb{Z})$ 構成一個「有限生成交換群」。

Mordell-Weil 定理

Mordell-Weil 定理

利用切憲哥線法，其整數解集合 $E(\mathbb{Z})$ 構成一個「有限生成交換群」。

- 有限生成交換群具有和整數類似的運算結構
  $\Longrightarrow$ 橢圓曲線加密解密系統 (Elliptic curve cyptosystem)。
- Google (2011) 和 Facebook (2015) 已在使用此套系統。

BSD 猜想

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）代表這個群的最少生成元個數。

BSD 猜想

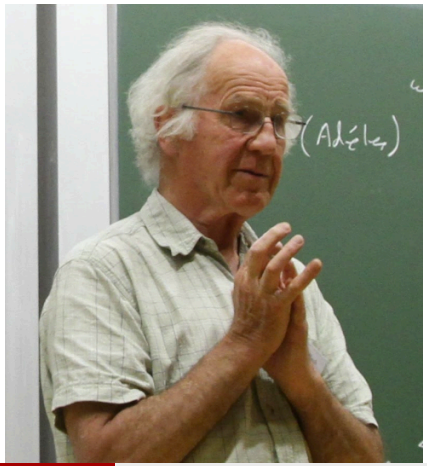
每一個有限生成交換群都有一個不變量：秩（rank）。這個不變量（大致上）代表這個群的最少生成元個數。
問題：如何計算 $E(\mathbb{Q})$ 的秩 (令為 $r_{\mathrm{MW}}(E)$)？

BSD 猜想

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）代表這個群的最少生成元個數。

問題：如何計算 $E(\mathbb{Z})$ 的秩 (令為 $r_{\mathrm{MW}}(E)$)？

$\Longrightarrow$ Birch and Swinnerton-Dyer.



BSD 猜想

回到 Hasse-Weil L-函數

$$L(E,s)" = "\prod_p \left(1-(p-\#(E(p)))p^{-s}+p^{1-2s}\right) = \sum_{n=1}^{\infty}\frac{c_n}{n^s}.$$

考慮 $L(E,s)$ 對 $s=1$ 做泰勒展開，得到

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

令 $r_{\mathrm{an}}(E) := r$。則：

BSD 猜想

回到 Hasse-Weil L-函數

$$L(E,s)" = "\prod_p \left(1-(p-\#(E(p)))p^{-s}+p^{1-2s}\right) = \sum_{n=1}^{\infty}\frac{c_n}{n^s}.$$

考慮 $L(E,s)$ 對 $s=1$ 做泰勒展開，得到

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

令 $r_{\mathrm{an}}(E) := r$。則：

Birch and Swinnerton-Dyer Conjecture

- $r_{\mathrm{an}}(E) = r_{\mathrm{MW}}(E)$。
- c_r 包含了橢圓曲線 E 的" 所有" 幾何不變量。

已知結果

- 透過橢圓曲線「模」的性質，Gross 和 Zagier 以及 Kolyvagin 的工作證明了此猜想在 $r_{\mathsf{an}}(E) \leq 1$ 的情況。
- 很大一部分的橢圓曲線滿足 $r_{\mathsf{an}}(E) \leq 1$。
- 當 $r_{\mathsf{an}}(E) \geq 2$：

已知結果

- 透過橢圓曲線「模」的性質，Gross 和 Zagier 以及 Kolyvagin 的工作證明了此猜想在 $r_{\mathsf{an}}(E) \leq 1$ 的情況。
- 很大一部分的橢圓曲線滿足 $r_{\mathsf{an}}(E) \leq 1$。
- 當 $r_{\mathsf{an}}(E) \geq 2$：**Nothing has been proved..... V_V**。

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, 費馬最後定理: A. Wiles 的解決方法, 數學傳播, 十八卷二期。
3. Edwards, Harold M. (1996), Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory, Graduate Texts in Mathematics 50, Springer-Verlag.
4. Koblitz, N., (1994) A Course in Number Theory and Cryptography, Graduate Texts in Mathematics 114, 2nd edition, Springer-Verlag.
5. Wiles, A., (2006) The Birch and Swinnerton-Dyer Conjecture, in The Millennium prize problems, American Mathematical Society 31–44.