1.9 三次曲線的切線

工作紙

題目

STEP I 2009，第 2 題

繼續閱讀之前，請先看題目（原題為英文）。題目載於 STEP Support Programme 的試題資料庫：

step.maths.org/questions/09-s1-q2

提示

請先自行嘗試解題。如果遇到困難，請逐一閱讀提示，每讀完一個便回到題目再試。標有停一停，試一試的提示是關鍵步驟。每個提示之後均留有空位供你演算。

想一想　點 $(-a, b)$ 在曲線上。為甚麼？這跟立方和又有甚麼關係？

階段 1 切線

想一想 對 $y^3 = x^3 + a^3 + b^3$ 進行隱函數求導（implicit differentiation）。記住 a 和 b 都是常數。

停一停，試一試 求出在 $(-a, b)$ 的斜率（gradient），寫出通過該點的直線方程，然後消去分數。

階段 2 切線與曲線再次相交之處

想一想 把切線（tangent）寫成 $y = \ldots$ 的形式，再代入 $y^3 = x^3 + 9$。

想一想 展開後把所有項移到同一邊，並找出各係數的公因數（common factor）。

階段 3　解三次方程

想一想 從切點（point of contact）可知，你已經掌握了這個三次方程（cubic）的一個根。

停一停，試一試 切線與曲線相切，所以切點對應的是一個重根（repeated root）。除去 $(x+1)^2$ 便可求出第三個根，從而得到切線與曲線再次相交的點。

想一想 該點位於 $y^3 = x^3 + 9$ 上。消去分母。餘下的那一項並不是立方數，但 $9 = 1^3 + 2^3$。

背後的數學

弦切法

取一條三次曲線（cubic curve），例如 $y^3 = x^3 + 9$，或者更標準的形式 $y^2 = x^3 + Ax + B$。假如你知道曲線上兩個坐標為有理數的點，那麼過這兩點的直線恰好與曲線再相交於一點，而該點的坐標也是有理數（理由見回顧中的論證）。假如你只知道一個點，就改用該點的切線。無論哪種情況，舊的有理點都能產生新的有理點。

值得注意的是，這個「弦切」（chord–tangent）作圖法可以變成一種把曲線上的點相加的方法，於是有理點便構成一個羣（group），這是你在大學一年級會學到的一種代數結構。莫德爾（Louis Mordell）在 1922 年證明了這個羣由有限個點生成：所有有理點，不論有多少個，都可以由一個有限集合出發，利用弦和切線構造出來。他的證明是 Section 1.5 中費馬（Fermat）下降法的一個版本。

今日的橢圓曲線

這類曲線稱為橢圓曲線（並非因為它們是橢圓，而是因為歷史上它們與橢圓的弧長有關）。它們在現代數學中無處不在。

- **費馬最後定理。**在 1980 年代，Gerhard Frey 留意到 $x^n + y^n = z^n$ 的一個解會產生一條非常古怪的橢圓曲線。懷爾斯（Andrew Wiles）在 1994 年證明了這樣古怪的曲線不可能存在，從而證明了費馬最後定理。
- **貝赫與斯維訥通－戴爾猜想（Birch and Swinnerton-Dyer conjecture）。**有理點所構成的羣需要多少個生成元（generators）？在 1960 年代，有人憑藉劍橋一些數學史上最早的電腦實驗提出了一個猜想，它用一個函數來預測答案，而這個函數是由點算

曲線在模質數之下的點數構造出來的。它是七條千禧年大獎難題（Millennium Prize Problems）之一。

- **密碼學（cryptography）。**在有限數系上的橢圓曲線上，把一個點 P 自己相加 n 次是很快的，即使 n 有數百位數字也一樣（把 P 反覆加倍，就像你用反覆平方來計算高次冪那樣）。但已知 P 和結果 nP，要找出 n 卻似乎極之困難：這就是*橢圓曲線離散對數問題*（elliptic-curve discrete logarithm problem）。這種不對稱性保護着今日大部分的網上通訊。

同次冪之和

能寫成三個正立方數之和的最小立方數是 $6^3 = 3^3 + 4^3 + 5^3$；切線法找到的是 $20^3 = 7^3 + 14^3 + 17^3$，它並非前者的倍數，而重複使用這個方法會不斷產生新的恆等式（雖然有些會涉及負數）。要多少個 k 次冪才能湊成另一個 k 次冪？歐拉（Euler）在 1769 年猜想，至少需要 k 個 k 次冪才能湊成另一個 k 次冪。對於四次冪和五次冪，他錯了：1966 年 Leon Lander 和 Thomas Parkin 以電腦搜尋找到

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5$$

而在 1988 年，Noam Elkies 利用橢圓曲線找到了四次冪的反例（counterexamples）。

延伸練習

1. **圓上的有理點。**過 $(-1, 0)$ 而斜率為 t 的直線與圓 $x^2 + y^2 = 1$ 再次相交。證明另一個交點是 $\left(\dfrac{1 - t^2}{1 + t^2}, \dfrac{2t}{1 + t^2}\right)$，並由此得出無窮多組畢氏三元數（Pythagorean triples）。

2. **一條落空的弦。**點 $(1, 2)$ 和 $(2, 1)$ 在 $x^3 + y^3 = 9$ 上。證明過這兩點的直線與曲線再沒有其他交點。那個「第三點」到哪裏去了？（查一查*無窮遠點*（point at infinity）。）

3. **故技重施。**求 $y^3 = x^3 + 9$ 在 $\left(\frac{17}{7}, \frac{20}{7}\right)$ 的切線，以及它與曲線相交的第三點。（使用電腦代數系統會有幫助；留意數字增長得有多快。）

4. **的士數（taxicab numbers）。**$1729 = 1^3 + 12^3 = 9^3 + 10^3$。求過 $(1, 12)$ 和 $(9, 10)$ 的直線與曲線 $x^3 + y^3 = 1729$ 相交的第三點，並由此推導出一條形如 $p^3 = q^3 + r^3 + s^3$ 的新恆等式。

延伸閱讀

- **Joseph Silverman & John Tate, *Rational Points on Elliptic Curves***（Springer）。為大學本科生而寫；第 1 章所需的知識不超出英國高考（A-level）程度。

- **Avner Ash & Robert Gross, *Elliptic Tales***（Princeton University Press）。一本普及讀物，一路講到貝赫與斯維訥通－戴爾猜想。
- **Simon Singh, *Fermat's Last Theorem***。講述橢圓曲線如何解決一個有 350 年歷史的難題。

完整的引導式解答見第 1.9 節：

https://beyondstep.keithmcnulty.org/zh-hant/ch01/tangents-cubic.html

每星期一道 STEP 題目，完整講解：The STEP Up，以電郵免費發送，訂閱網址：keithmcnulty.substack.com