1.9 三次曲线的切线

工作纸

题目

STEP I 2009，第 2 题

继续阅读之前，请先看题目（原题为英文）。题目载于 STEP Support Programme 的试题资料库：

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

提示

请先自行尝试解题。如果遇到困难，请逐一阅读提示，每读完一个便回到题目再试。标有“停一停”或“试一试”的提示是关键步骤。每个提示之后均留有空位供你演算。

> **想一想**　点 $(-a, b)$ 在曲线上。为甚么？这跟立方和又有甚么关系？

阶段 1 切线

想一想 对 $y^3 = x^3 + a^3 + b^3$ 进行隐函数求导（implicit differentiation）。记住 a 和 b 都是常数。

停一停，试一试 求出在 $(-a, b)$ 的斜率（gradient），写出通过该点的直线方程，然后消去分数。

阶段 2 切线与曲线再次相交之处

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

想一想　展开后把所有项移到同一边，并找出各系数的公因数（common factor）。

阶段 3　解三次方程

想一想　从切点（point of contact）可知，你已经掌握了这个三次方程（cubic）的一个根。

停一停，试一试　切线与曲线相切，所以切点对应的是一个重根（repeated root）。除去 $(x+1)^2$ 便可求出第三个根，从而得到切线与曲线再次相交的点。

想一想 该点位于 $y^3 = x^3 + 9$ 上。消去分母。余下的那一项并不是立方数，但 $9 = 1^3 + 2^3$。

背后的数学

弦切法

取一条三次曲线 (cubic curve)，例如 $y^3 = x^3 + 9$，或者更标准的形式 $y^2 = x^3 + Ax + B$。假如你知道曲线上两个坐标为有理数的点，那么过这两点的直线恰好与曲线再相交于一点，而该点的坐标也是有理数（理由见回顾中的论证）。假如你只知道一个点，就改用该点的切线。无论哪种情况，旧的有理点都能产生新的有理点。

值得注意的是，这个“弦切”(chord–tangent) 作图法可以变成一种把曲线上的点相加的方法，于是有理点便构成一个群 (group)，这是你在大学一年级会学到的一种代数结构。莫德尔 (Louis Mordell) 在 1922 年证明了这个群由有限个点生成：所有有理点，不论有多少个，都可以由一个有限集合出发，利用弦和切线构造出来。他的证明是 Section 1.5 中费马（Fermat）下降法的一个版本。

今日的椭圆曲线

这类曲线称为椭圆曲线（并非因为它们是椭圆，而是因为历史上它们与椭圆的弧长有关）。它们在现代数学中无处不在。

- **费马最后定理。**在 1980 年代，Gerhard Frey 留意到 $x^n + y^n = z^n$ 的一个解会产生一条非常古怪的椭圆曲线。怀尔斯（Andrew Wiles）在 1994 年证明了这样古怪的曲线不可能存在，从而证明了费马最后定理。
- **贝赫与斯维讷通－戴尔猜想 (Birch and Swinnerton-Dyer conjecture)。**有理点所构成的群需要多少个生成元 (generators)？在 1960 年代，有人凭借剑桥一些数学史上最早的电脑实验提出了一个猜想，它用一个函数来预测答案，而这个函数是由计数曲线在模

质数之下的点数构造出来的。它是七条千禧年大奖难题（Millennium Prize Problems）之一。

- **密码学（cryptography）。**在有限数系上的椭圆曲线上，把一个点 P 自己相加 n 次是很快的，即使 n 有数百位数字也一样（把 P 反复加倍，就像你用反复平方来计算高次幂那样）。但已知 P 和结果 nP，要找出 n 却似乎极之困难：这就是*椭圆曲线离散对数问题*（elliptic-curve discrete logarithm problem）。这种不对称性保护着今日大部分的网上通讯。

同次幂之和

能写成三个正立方数之和的最小立方数是 $6^3 = 3^3 + 4^3 + 5^3$；切线法找到的是 $20^3 = 7^3 + 14^3 + 17^3$，它并非前者的倍数，而重复使用这个方法会不断产生新的恒等式（虽然有些会涉及负数）。要多少个 k 次幂才能凑成另一个 k 次幂？欧拉（Euler）在 1769 年猜想，至少需要 k 个 k 次幂才能凑成另一个 k 次幂。对于四次幂和五次幂，他错了：1966 年 Leon Lander 和 Thomas Parkin 以电脑搜索找到

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

而在 1988 年，Noam Elkies 利用椭圆曲线找到了四次幂的反例（counterexamples）。

延伸练习

1. **圆上的有理点。**过 $(-1, 0)$ 而斜率为 t 的直线与圆 $x^2 + y^2 = 1$ 再次相交。证明另一个交点是 $\left(\dfrac{1 - t^2}{1 + t^2}, \dfrac{2t}{1 + t^2}\right)$，并由此得出无穷多组毕氏三元数（Pythagorean triples）。

2. **一条落空的弦。**点 $(1, 2)$ 和 $(2, 1)$ 在 $x^3 + y^3 = 9$ 上。证明过这两点的直线与曲线再没有其他交点。那个“第三点”到哪里去了？（查一查*无穷远点*（point at infinity）。）

3. **故技重施。**求 $y^3 = x^3 + 9$ 在 $\left(\frac{17}{7}, \frac{20}{7}\right)$ 的切线，以及它与曲线相交的第三点。（使用电脑代数系统会有帮助；留意数字增长得有多快。）

4. **的士数（taxicab numbers）。**$1729 = 1^3 + 12^3 = 9^3 + 10^3$。求过 $(1, 12)$ 和 $(9, 10)$ 的直线与曲线 $x^3 + y^3 = 1729$ 相交的第三点，并由此推导出一条形如 $p^3 = q^3 + r^3 + s^3$ 的新恒等式。

延伸阅读

- **Joseph Silverman & John Tate, *Rational Points on Elliptic Curves***（Springer）。为大学本科生而写；第 1 章所需的知识不超出英国高考（A-level）程度。

- **Avner Ash & Robert Gross, *Elliptic Tales***（Princeton University Press）。一本普及读物，一路讲到贝赫与斯维讷通－戴尔猜想。
- **Simon Singh, *Fermat's Last Theorem***。讲述椭圆曲线如何解决一个有 350 年历史的难题。

完整的引导式解答见第 1.9 节：

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

每星期一道 STEP 题目，完整讲解：The STEP Up，以电子邮件免费发送，订阅网址：keithmcnulty.substack.com