数学小品

椭圆曲线

John Stillwell

近年来，椭圆曲线在数论研究中一直起着主导作用，最著名的当属怀尔斯 (Wiles) 证明费马 (Fermat) 大定理的工作. 不过，由于这些研究需要极专门的技巧，非三言两语所能说清，所以返回去看看椭圆曲线早期的简单身世，倒也不失为有益之举. 从丢番图 (Diophantus) 到牛顿 (Newton) 大约 1500 年间，椭圆曲线只不过是指由某些三次方程定义的曲线. 人们只把它们看作由研究圆锥曲线向前迈出的一小步，事实上，它们的某些几何性质和算术性质可看成是圆锥曲线的性质的推广. 特别地，对于二次和三次方程，我们有可能用简单的几何作图法找出其有理解.

随着十七世纪微积分的发展，圆锥曲线和椭圆曲线之间的深刻的差别才开始显现. 圆锥曲线可用有理函数进行参数化. 例如，对于圆 $x^2+y^2=1$, 可由

$$x=\frac{1-t^2}{t+t^2}, \qquad y=\frac{2t}{1+t^2}$$

实现参数化，但是椭圆曲线不能. 用于椭圆曲线参数化的最简单的函数是椭圆函数，它来源于微积分中椭圆积分的反演，椭圆积分这个名称的由来是由于其中最典型的例子恰为求椭圆上的弧长的积分. 仅仅因为这一偶然的理由，它们才被称作椭圆曲线 —— 这是个不幸的偶然，实际上椭圆本身不是椭圆曲线.

17 世纪人们尚不知道三次曲线的参数化，但从椭圆积分很难对付这点上已经“感觉”到了圆锥曲线和椭圆曲线之间的不同. 通过椭圆积分的反演产生椭圆曲线的想法要等到 19 世纪早期才出现. 对椭圆曲线的非有理性的完全理解则是 19 世纪中期的事，当时导入了复坐标，从而揭示了它们跟圆锥曲线在拓扑方面的差异. 这使我们踏进了以现代眼光看椭圆曲线的门槛 —— 它们是数论、几何、代数、分析和拓扑的奇异的综合. 下面我将试图描述到达这一境界的过程.

丢番图. 对丢番图我们知之甚少，只知他生活于公元 150 年至 350 年之间，是位求二元或多元多项式方程有理解的奇才. 他的《算术》(Arithmetica, 英译本见 Heath[4]) 中列有数百个方程的解，下面就是其中颇具启发性的例子.

1. 方程 $x^2+y^2=16$ 的一个 (不同于诸如 $x=0, y=4$ 这样显然的解的) 有理解，可通过解下述联立方程得到：

原题: Elliptic Curves. 译自: *Amer. Math. Monthly*, Vol. 102, No. 9, 1995, pp. 831–837.

$$x^2+y^2=16,$$

$$y=2x-4,$$

它导出的解是 $x=16/5, y=12/5$(参见 Heath[4]p.145)

2. 方程 $x^3-3x^2+3x+1=y^2$ 的一个 (不同于 $x=0, y=1$ 这个显然的解的) 有理解，可通过下述联立方程得到：

$$x^3-3x^2+3x+1=y^2$$

$$y=\frac{3}{2}x+1,$$

它导出的解是 $x=21/4, y=71/8$(参见 Heath[3],p.242).

在这两个例子中，丢番图是如何选定那些一次方程的呢？最简单的解释是基于几何的考虑，尽管他没提到几何.

第一个例子中，那个一次方程代表经过 "显然" 的有理点 (0,-4) 的一条直线. 该直线的斜率为何并不重要，因为任何一条经过 (0, 4) 、斜率为有理数 t 的直线都将在第二个有理点 $(8t/(1-t^2), (4t^2-4)/(1+t^2))$ 跟圆相遇. 反之，用这种方法可以得到圆上的所有的有理点，所以，丢番图本质上利用有理参数 t 的有理函数实现了圆上有理点的参数化.

第二个例子中的一次方程具有更浓的几何味儿. 它是 $x^3-3x^2+3x+1=y^2$ 在 "显然" 的有理点 (0,1) 处的 切线. 这里不能任意选择斜率，因为一条直线跟一条三次曲线相交，为使第三个交点是有理点，它必须跟该曲线交于 两个 有理点. 当只知道一个有理点时，这就迫使我们只好利用切线：切线通过两个 "重合的" 点.

当然，也可能丢番图是从纯代数的角度发现这些事实的，而根本没有注意到它们的几何解释；然而，这就完全离开了他那个时代的希腊数学文化传统，令人费解. 即使在代数文化更兴旺的 17 世纪，费马和牛顿也是立即认出了丢番图工作的几何特征，牛顿 [6] 明确地把丢番图的解法说成是弦和切线的作图. 我们将看到，其后的发现更加重了这种几何解释的份量.

费马和牛顿. 费马是继丢番图之后第一位在数论领域作出较大贡献的数学家. 在他的众多发现中，有一项是给出了证明某些方程 不存在 整数或有理数解的方法. 例如，他证明了不存在正有理数 a, b, c, 使得

$$a^4 \pm b^4 = c^4$$

这一结果蕴含了如下结论：不存在正整数的四次幂的和等于一个四次幂 (即 $n=4$ 时的费马大定理). 不过，这也是有关椭圆曲线的一个陈述，即：在曲线

$$y^2=1-x^4$$

上不存在非平凡的有理点；因为若 $p, q \neq 0$ 且

$$\frac{p^2}{r^2}=1-\frac{q^4}{r^4},$$

则有理点 $(p/r, q/r)$ 必给出 $a^4 - b^4 = c^4$ 的非零整解 $a = r, b = q, c = pr$.

我记得我曾说过椭圆曲线是三次的曲线，不过它们是在一个适当的坐标系内的三次曲线. 任一形如

$$y^2 = (x-\alpha)(x-\xi)(x-\gamma)(x-\delta)$$

的四次曲线都可写成

$$\left(\frac{y}{x-\alpha^2}\right)^2 = \left(1-\frac{\beta-\alpha}{x-\alpha}\right)\left(1-\frac{\gamma-\alpha}{x-\alpha}\right)\left(1-\frac{\delta-\alpha}{x-\alpha}\right),$$

因此它在坐标系

$$X = \frac{1}{x-\alpha}, \qquad Y = \frac{y}{x-\alpha^2},$$

之中是三次的. 特别地，$y^2 = 1 - x^4$ 在坐标 $X = 1/(1-x), Y = y/(1-x)^2$ 之下化为三次的：$Y^2 = 4X^3 - 6X^2 + 4X - 1$. 注意，从数论的观点看，这是一个适当的坐标变换，因为它使得位于一条曲线上的有理点 (x, y) 对应于另一条上的有理点 (X, Y). 这样的坐标变换称为双有理的.

牛顿发现了惊人的事实：所有关于 x, y 的三次方程皆可通过双有理坐标变换化为如下形式的方程

$$Y^2 = X^3 + aX + b.$$

事实上，他所用的变换就是射影变换，他称之为“影子产生曲线”. 他的结果可视为关于二阶曲线的那个著名定理的类似物，那个定理说：二阶曲线皆为圆锥曲线，故在非退化的情形都是圆的射影. 退化的三次曲线相应于方程右边 $X^3 + aX + b$ 具有重因子. 相应的重根 $X = \alpha$ 或者是曲线上的二重点 (图 1), 或者是曲线上的尖点 (图 2); 过这种点画斜率为 t 的直线，我们便可得到曲线上构成 t 的有理函数的那些点的坐标.

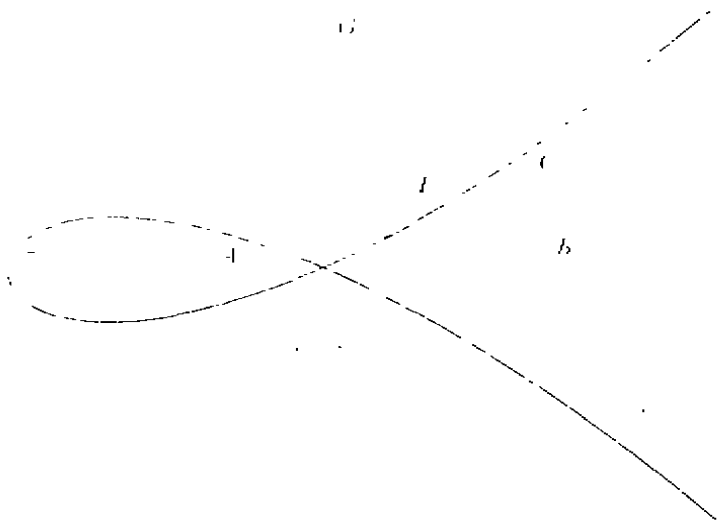

图 1. 具有二重点的三次曲线

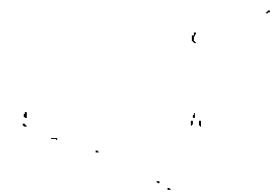

图 2. 具有尖点的三次曲线

对于 X^3+aX+b 不存在重因子的情形，曲线不能用有理函数参数化，此类曲线即我们现在所称的椭圆曲线 (图 3)

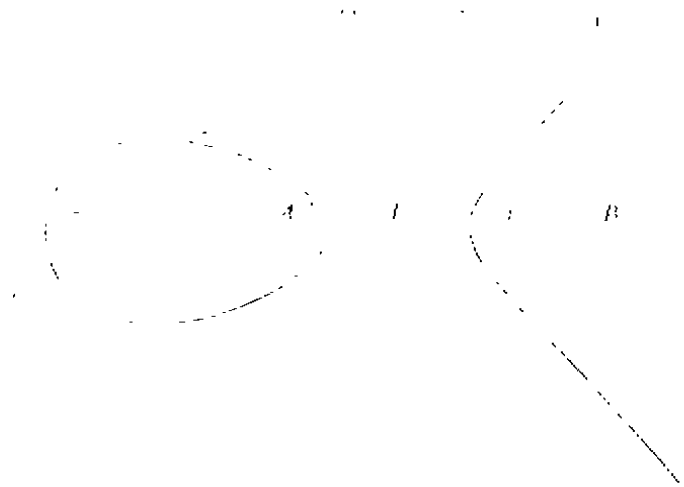

图 3. 非退化的三次曲线

椭圆积分. 在研究积分演算的早期，数学家们遇到了将多项式的平方根 "有理化" 的问题. 例如，为求圆的面积或弧长，你会遇到含有 $\sqrt{1-x^2}$ 的积分. 这可以通过 "丢番图" 代换 $x=(1-t^2)/1+t^2$ 来有理化，事实上雅可布·贝努利 (Jacob Bernoulli)[1] 在处理相类似的问题时确实把这一代换归功于丢番图. 他利用这一代换得到公式

$$\frac{\pi}{4}=\int_0^1 \frac{dt}{1+t^2},$$

由此出发，他将 $1/(1+t^2)$ 展成几何级数并逐项积分，从而得到著名的级数

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots$$

含有三次或四次多项式的平方根的积分更难处理，它们被称为**椭圆积分**，因为其中之一表示椭圆的弧长．三次和四次多项式归在一类是由于它们是双有理等价的，正如上面提到过的 $y^2 = 1 - x^4$ 和 $Y^2 = 4X^3 - 6X^2 + 4X - 1$ 一样．这类积分来源于大量普通的几何和力学问题，所以人们花了大力气来研究它们，可惜成效甚微．

第一位看出为什么不能有理化的人也许就是雅可布·贝努利，他注意到 $\sqrt{1-x^4}$ 的有理化至少要利用系数为有理数的有理函数 $x = f(t)$，而这违反了费马关于 $a^4 \pm b^4 = c^2$ 不存在正整数解的定理．事实上，只要反复使用费马的论证于多项式（代替原来的整数），你就能证明 $\sqrt{1+x^4}$ 不可能通过任意有理函数 $x = f(t)$ 实现有理化，所以雅可布·贝努利的思路是对的．不过这种类型的论证直到 19 世纪才出现，所以在这之前人们对椭圆积分的性质一直认识不清（到 19 世纪，不仅出自数论的思考，而且出自分析和拓扑的思考都指向了这个问题）．

椭圆函数．在 19 世纪 20 年代，阿贝尔 (Abel) 和雅可比 (Jacobi) 终于看出了该怎样对付椭圆积分——研究它们的反演．比如说，代替研究积分

$$u = g^{-1}(x) = \int_0^x = \frac{dt}{\sqrt{t^3 + at + b}},$$

我们来研究它的反函数 $x = g(u)$．这样做，问题变得简单的程度，可跟我们用研究函数 $x = \sin u$ 来代替研究 $\sin^{-1} x = \int_0^x (dt/\sqrt{1-t^2})$ 相媲美．特别地，此时你面对的是个周期函数 $x = g(u)$ 而不是一个多值积分 $g^{-1}(x)$ 了．

$\sin u$ 和 $g(u)$ 之间的差异在于：只有当允许变量取复数值时，才能真正看出 $g(u)$ 的周期性，而且 $g(u)$ 有两个周期，即存在非零的 $\omega_1, \omega_2 \in \boldsymbol{C}$，$\omega_1/\omega_2 \notin \mathbb{R}$，使得

$$g(u) = g(u + \omega_1) = g(u + \omega_2).$$

有许多方法可让这两个周期显露出来．一种方法是艾森斯坦 (Eisenstein) 最早提出的 [1847]，今日还在普遍使用，要点是先写出显然具有周期 ω_1 和 ω_2 的一个函数

$$g(u) = \sum_{m,n \in \mathbb{Z}} \frac{1}{(u + m\omega_1 + m\omega_2)^2},$$

然后通过无穷级数的巧妙演算导出其性质．最终你会发现 $g^{-1}(x)$ 正是我们开始时考虑的那类积分．

另一种方法是研究 t 在复平面上变化时被积函数 $1/\sqrt{t^3 + at + b}$ 的行为．按照黎曼 (Riemann) 的观点，视双值“函数” $1/\sqrt{t^3 + at + b}$ 为 $\boldsymbol{C}$ 上的双叶曲面，你将发现两个独立的闭积分路径，其上的积分值为 ω_1 和 ω_2．这说明反函数 $g(u)$ 的周期为 ω_1 和 ω_2．这种方法更深刻，但要严格化也更困难．

由于 $g(u)=x$，根据基本的微积分知识可知

$$g'(u)=\frac{dx}{du}=\frac{1}{du/dx}=\frac{1}{1/\sqrt{x^3+ax+b}}=\sqrt{x^3+ax+b}=y,$$

所以，$x=g(u), y=g'(u)$ 给出了曲线 $y^2=x^3+ax+b$ 的参数化. 稍微再前进一步便可证明，$u\mapsto(g(u),g'(u))$ 事实上是 $C/\langle\omega_1,\omega_2\rangle$ 和曲线之间的连续的一一对应. $C/\langle\omega_1,\omega_2\rangle$ 是 C 相对于 ω_1 和 ω_2 生成的子群的商，从拓扑角度看是个环面，因此它就是曲线 $y^2=x^3+ax+b$. 这就是为什么椭圆曲线不能实现有理地参数化的更深层的原因. 可以用有理函数 $x=p(u), y=q(u)$ 实现参数化的曲线是 u 取值的全平面 $C\cup\{\infty\}$ 的拓扑象，而 $C\cup\{\infty\}$ 在拓扑上是个球.

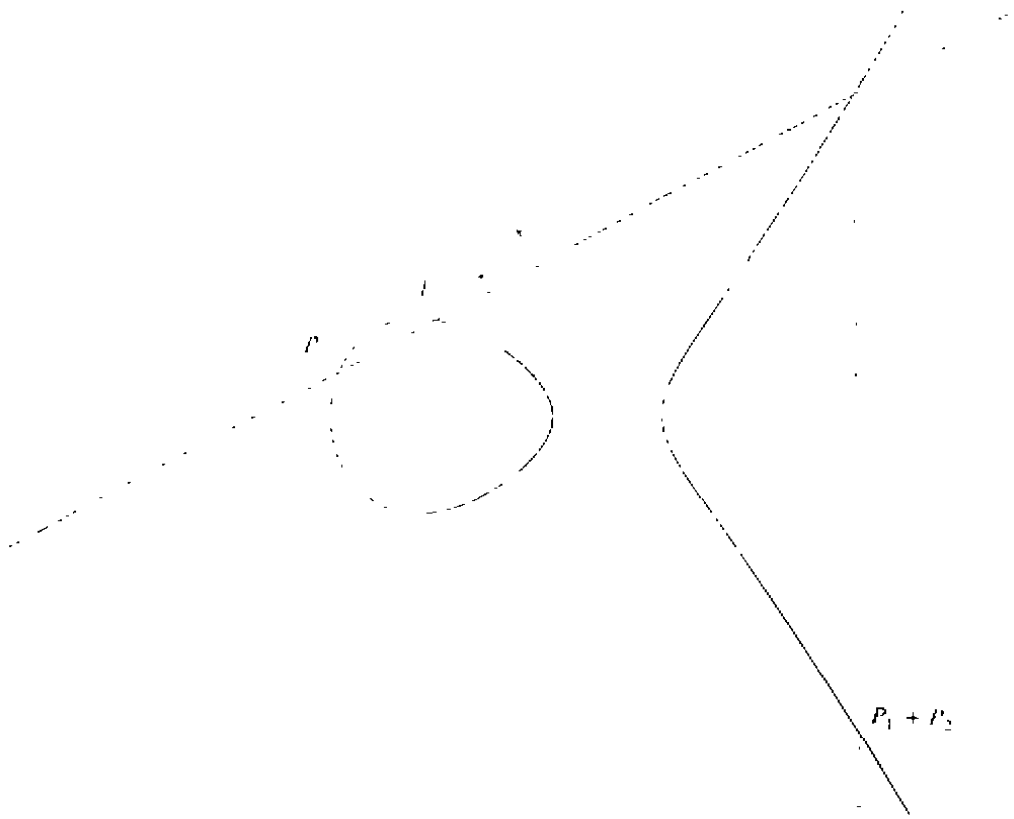

图 4. 椭圆曲线上点的和 (取自 Koblitz[5])

经 $x=g(u), y=g'(u)$ 参数化可得的另一推论是：曲线 $y^3=x^3+ax+b$ 是个阿尔贝群. 对应于参数值 u_1, u_2 的点的 "和" 就是对应于参数值 u_1+u_2 的点. 按照这一 "和" 的定义，该曲线跟群 $C/\langle\omega_1,\omega_2\rangle$ 是同构的. 令人惊讶的是，还有一种关于 "和" 的等价的定义，丢番图可能已经理解到了 (这也许有助于解释清楚为什么椭圆函数在数论中那么有用)：点 P_1 和 P_2 的和就是跟 P_1 和 P_2 共线的曲线上第三个点关于 x 轴的反射 (图 4). 对于这一结论的解释，我们必须建议读者参阅近期出版的有关椭圆

曲线的书，比如科布利茨 (Koblitz)[5]. 在这本书里，你还将读到古代的数论和几何问题所激发出的椭圆曲线的许多漂亮的现代成果.

参 考 文 献

[1] Bernoulli, Jakob (1696) Positionum de seriebus infinitis pars tertia *Werke*, **4**, 85–106.

[2] Bernoulli, Jakob (1704) Positionum de seriebus infinitis ... pars quinta. Werke, **4**, 127–147.

[3] Eisenstein, G.(1847) Beiträge zur Theorie der elliptischen Functionen. *J. reine angew. Math.* **35**, 137–274.

[4] Heath, T.L. (1910) *Diophantus of Alexandria*, Cambridge University Press.

[5] Koblitz, N. (1985) *Introduction to Elliptic Curves and Modular Forms*, Springer-Verlag, New York.

[6] Newton, I. (late 1670s) De resolutione quaestionum circa numeros. *Math. Papers* **4**, 110–115.

[7] Riemann, G. B H. (1851) Grudlagen für eine allgemeine Theorie der Functionen einer veränderlichen complexen Grösse. *Werke*, 2nd ed., 3 48.

(袁向东 译　冯绪宁 校)