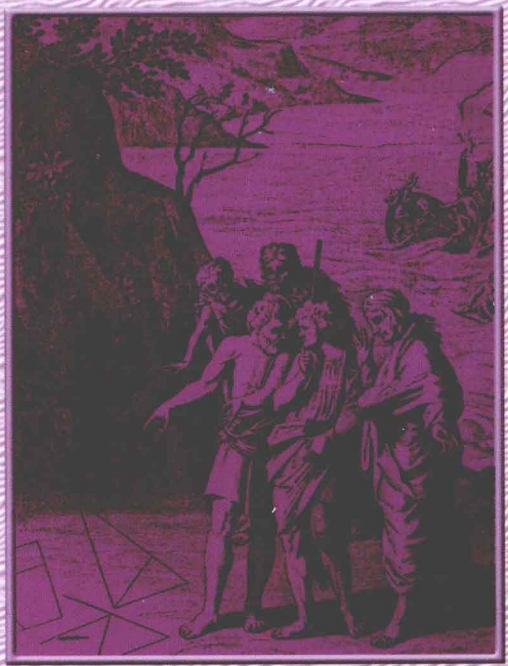
《数学中的小问题大定理》丛书（第二辑）

雅可比定理

——从一道日本数学奥林匹克试题谈起



梅根 佩捷 编著

◎椭圆曲线密码体制
◎刘维尔定理
◎雅可比函数
◎算术-几何平均值
◎希策布鲁赫的公式

HITP
哈爾濱工業大學出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS

《数学中的小问题大定理》丛书（第二辑）

雅可比定理

——从一道日本数学奥林匹克试题谈起

梅根 佩捷 编著

◎椭圆曲线密码体制

◎刘维尔定理

◎雅可比函数

◎算术—几何平均值

◎蒂策和鲁赫的公式

HITP
哈爾濱工業大學出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS

内容简介

本书是“数学中的小问题大定理”之一，通过一道日本数学奥林匹克试题研究讨论雅可比定理及其相关知识.

本书可供从事这一数学分支或相关学科的数学工作者、大学生以及数学爱好者研读.

图书在版编目(CIP)数据

雅可比定理:从一道日本数学奥林匹克试题谈起/梅根,佩捷编著. -- 哈尔滨:哈尔滨工业大学出版社,2013.4

ISBN 978-7-5603-4044-9

Ⅰ.①雅… Ⅱ.①梅… ②佩… Ⅲ.①数学—研究 Ⅳ.①O1-0

中国版本图书馆 CIP 数据核字(2013)第 078485 号

策划编辑 刘培杰 张永芹
责任编辑 张永芹 徐 丽
封面设计 孙茵艾
出版发行 哈尔滨工业大学出版社
社 址 哈尔滨市南岗区复华四道街 10 号 邮编 150006
传 真 0451-86414749
网 址 http://hitpress.hit.edu.cn
印 刷 哈尔滨市工大节能印刷厂
开 本 787mm×960mm 1/16 印张 14.5 字数 139 千字
版 次 2013 年 4 月第 1 版 2013 年 4 月第 1 次印刷
书 号 ISBN 978-7-5603-4044-9
定 价 48.00 元

⊙目录

椭圆曲线及其在密码学中的应用

⊙ 绪 论

1. 引　言

日本数学奥林匹克与日本制造一样缺乏原创性，但工于模仿且能推陈出新. 与我国的 CMO 相比虽技巧性稍逊一筹，但能紧跟世界数学主流且命题者颇具数学鉴赏力，知道哪些是“好数学”，哪些是包装精美的学术垃圾. 随着时间的推移，我们越来越能体会到其眼光的独到以及将尖端理论通俗化的非凡能力. 例如 1992 年日本数学奥林匹克预赛题第 3 题为：

试题　坐标平面上，设方程

$$y^2 = x^3 + 2\,691x - 8\,019$$

所确定的曲线为 E，连接该曲线上的两点 $(3,9)$ 和 $(4,53)$ 的直线交曲线 E 于另一点，求该点的坐标.

解　由两点式易得所给直线的方程为 $y = 44x - 123$. 将它代入曲线方程并整理得

$$x^3 - 1\,936x^2 + (2 \times 44 \times 123 + 2\,691)x - (123^2 + 8\,019) = 0$$

由韦达定理得

$$x + 3 + 4 = 1\,936$$

所以所求点 x 的横坐标为

$$x = 1\,936 - (3 + 4) = 1\,929$$

这道貌似简单的试题实际上是一道具有深刻背景的椭圆曲线特例.

2. 牛顿对曲线的分类

笛卡儿早就讨论过一些高次方程及其代表的曲线. 次数高于2的曲线的研究变成众所周知的高次平面曲线理论,尽管它是坐标几何的组成部分. 18世纪所研究的曲线都是代数曲线,即它们的方程由 $f(x,y) = 0$ 给出,其中 f 是 x 和 y 的多项式. 曲线的次数或阶数就是项的最高次数.

牛顿第一个对高次平面曲线进行了广泛的研究. 笛卡儿按照曲线方程的次数来对曲线进行分类的计划深深地打动了牛顿,于是牛顿用适合于各该次曲线的方法系统地研究了各次曲线,他从研究三次曲线着手. 这个工作出现在他的《三次曲线例举》(Enumeratio Linearum Tertil Ordinis)中,这是作为他的 Opticks(光学)英文版的附录在1704年出版的. 但实际上大约在1676年就做出来了,虽然在 La Hire 和 Wallis 的著作

中使用了负 x 值,但牛顿不仅用了两个坐标轴和负 x 负 y 值,而且还在所有四个象限中作图.

牛顿证明了怎样能够把一般的三次方程

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + fy^2 + hx + jy + k = 0$$

所代表的一切曲线通过坐标轴的变换化为下列四种形式之一:

(1) $xy^2 + ey = ax^3 + bx^2 + cx + d.$

(2) $xy = ax^3 + bx^2 + cx + d.$

(3) $y^2 = ax^3 + bx^2 + cx + d.$

(4) $y = ax^3 + bx^2 + cx + d.$

牛顿把第三类曲线叫做发散抛物线(diverging parabolas),它包括如图 1 所示的五种曲线. 这五种曲线是根据右边三次式的根的性质来区分的:全部是相异实根;两个根是复根;都是实根但有两个相等而且复根大于或小于单根;三个根都相等. 牛顿断言,光从一点出发对这五种曲线之一作射影,然后取射影的交线就能分别得到每一个三次曲线.

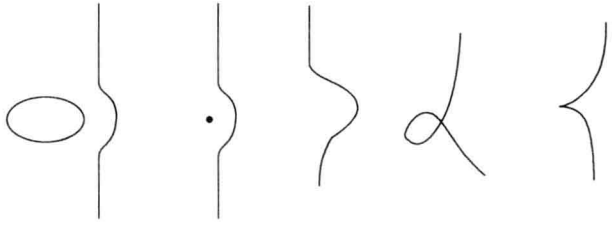


图 1

牛顿对他在《三次曲线例举》中的许多断言都没有给出证明. 斯特灵在《三次曲线》中证明了或用别的

方法重新证明了牛顿的大多数断言,但是没有证明射影定理,射影定理是由法国数学家克莱罗(Clairaut Alexis - Claude,1715—1763)和弗朗塞兄弟(Francois Nicole,1683—1758)证明的. 其实牛顿识别了 72 种三次曲线. 英国数学家斯特灵(Stirling James,1692—1770)加上了四种,修道院院长 Jean - Paul de Gua de Malves 在他 1740 年题为《利用笛卡儿的分析而不借助于微积分去进行发现……》(Usage de Vanalyse de Descartes pourdécouvrir sans le Secours du calcul differential…)的书里又加了两种.

牛顿关于三次曲线的工作激发了关于高次平面曲线的许多其他研究工作. 按照这个或那个原则对三次和四次曲线进行分类的课题继续使 18 和 19 世纪的数学家们感兴趣. 随着分类方法的不同所找到的分类数目也不同.

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

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

的四次曲线可以写成

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

因此它在坐标为

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

之中是三次的,特别地,$y^2 = 1 - x^4$ 在坐标 $X = \frac{1}{x-\alpha}$,

$Y=\frac{y}{(x-\alpha)^2}$之下化为三次的：$Y^2=4X^3-6X^2+4X-1$.

这一变换在数论中尤为重要，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.

牛顿发现了一个惊人的事实：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

$$y^2=x^3+ax+b$$

1995年证明了费马大定理的安德鲁·怀尔斯就是椭圆曲线这一领域的专家. 1975年安德鲁·怀尔斯开始了他在剑桥大学的研究生生活. 怀尔斯的导师是澳大利亚人约翰·科茨(John Coates)，他是伊曼纽尔学院的教授，来自澳大利亚新南威尔士州的波森拉什. 他决定让怀尔斯研究椭圆曲线，这个决定后来证明是怀尔斯职业生涯的一个转折点，为他提供了攻克费马大定理的新方法所需要的工具. 研究数论中的椭圆曲线方程的任务(像研究费马大定理一样)是当它们有整数解时把它算出来，并且如果有解，要算出有多少个解，如$y^2=x^3-2$只有一组整数解$5^2=3^3-2$.

3. 椭圆曲线与椭圆积分

“椭圆曲线”这个名称有点使人误解，因为在正常意义上它们即不是椭圆又不弯曲，它们只是如下形式的任何方程

$$y^2 = x^3 + ax^2 + bx + c, \text{这里 } a,b,c \in \mathbf{Z}$$

它们之所以有这个名称是因为在过去它们被用来度量椭圆的周长和行星轨道的长度.

有一个美国大学的数学竞赛试题说明了这点:

试题 半轴为 a 与 b 的椭圆,它的周长有两个显然的近似值,即 $\pi(a+b)$ 与 $2\pi(ab)^{\frac{1}{2}}$. 当比值 $\frac{b}{a}$ 很接近 1 时,哪一个比较接近真实值?

解 椭圆参数表示为 $x = a\cos t, y = b\sin t$. 由椭圆的长度公式知长度

$$L = \int_0^{2\pi} \sqrt{\left(\frac{\mathrm{d}x}{\mathrm{d}t}\right)^2 + \left(\frac{\mathrm{d}y}{\mathrm{d}t}\right)^2}\,\mathrm{d}t = \int_0^{2\pi} \sqrt{a^2\sin^2 t + b^2\cos^2 t}\,\mathrm{d}t$$

为周知的椭圆积分. 当 $\frac{b}{a}$ 接近 1 时考虑 L,置 $b = (1+\lambda)a$ 且考虑

$$L(\lambda) = a\int_0^{2\pi} \sqrt{1 + (2\lambda + \lambda^2)\cos^2 t}\,\mathrm{d}t$$

显然为 λ 的一个解析函数. 求它的幂级数至二次项

$$L(\lambda) = a\int_0^{2\pi} \left(1 + \frac{1}{2}(2\lambda+\lambda^2)\cos^2 t - \frac{1}{8}(2\lambda+\lambda^2)^2\cos^2 t + \cdots\right)\mathrm{d}t$$

$$= 2\pi a\left(1 + \frac{1}{4}(2\lambda+\lambda^2) - \frac{3}{64}(2\lambda+\lambda^2)^2 + \cdots\right)$$

$$= 2\pi a\left(1 + \frac{1}{2}\lambda + \frac{1}{16}\lambda^2 + \cdots\right)$$

后者表示式是由 $(1+z)^{\frac{1}{2}}$ 的二项式展开而得的,后来略去 λ 的三次以上的所有的项.

因为对于较小的 λ 的值(事实上是当 $|2\lambda| + \lambda^2 <$

1)级数绝对收敛. 上面的运算合理.

题中提出的周长近似式是

$$\pi(a+b)=2\pi a\left(1+\frac{1}{2}\lambda\right)$$

与

$$2\pi\sqrt{ab}=2\pi a\sqrt{1+\lambda}=2\pi a\left(1+\frac{1}{2}\lambda-\frac{1}{8}\lambda^2+\cdots\right)$$

因为三个函数有相同的常数项与一次项,所以它们的差别是对于较小的 λ 的二次项,有

$$L(\lambda)>2\pi a\left(1+\frac{1}{2}\lambda\right)>2\pi a\left(1+\frac{1}{2}\lambda-\frac{1}{8}\lambda^2+\cdots\right)$$

所以椭圆周长 $\pi(a+b)$ 比 $\pi\sqrt{ab}$ 好,几乎好三倍. 事实上

$$L(\lambda)-2\pi a\left(1+\frac{1}{2}\lambda\right)\sim\frac{1}{16}\lambda^2$$

而

$$L(\lambda)-2\pi a\sqrt{1+\lambda}\sim\frac{3}{16}\lambda^2$$

在一定意义上说,椭圆积分是不能表为初等函数的积分的最简单者,椭圆函数则以某些椭圆积分的反函数形式出现.

设 R 为 x 与 y 的有理函数. 令 $I=\int R(x,y)\mathrm{d}x$. 如果 y^2 为 x 的二次或更低次的多项式,则 I 可用初等函数表示. 如果 y^2 为 x 的三次或四次多项式,则 I 一般不能用初等函数表示,并叫做椭圆积分(Ellipticintegral)

在椭圆积分中一个重要的贡献是以德国数学家维

尔斯特拉斯名字命名的:用一个适当的变换

$$x' = \frac{ax + b}{cx + d}, ad - bc \neq 0$$

可把椭圆积分 I 化为一个这样的椭圆积分,其中多项式 y^2 具有规范形式. 勒让德规范形式和维尔斯特拉斯典则形式. 其维尔斯特拉斯典则形式为 $y^2 = 4x^3 - g_2x - g_3$. 这里 g_2, g_3 为不变量,是实数或复数. I 恒可表示为有理函数的积分与第一第二第三种椭圆积分的线性组合. 在维尔斯特拉斯典则形式中可表为

$$\int \frac{dx}{y}, \int \frac{xdx}{y}, \int \frac{dx}{(x - c)y}$$

其中 $y = \sqrt{4x^3 - g_2x - g_3}$.

维尔斯特拉斯生于德国西部威斯特伐利里(Westphalia)的小村落奥斯腾费尔德(Ostenfelde),曾从师以研究椭圆函数著称的古德曼(C. Gudermann).

椭圆积分应用很广. 在几何中,椭圆函数或椭圆积分出现于下列问题的求解之中:决定椭圆、双曲线或双纽线的弧长、求椭球的面积、求旋转二次曲面上的测地线、求平面三次曲线或更一般地一个亏格 1 的曲线的参数表示、求保形问题等. 在分析中,它们可用于微分方程(拉梅方程、扩散方程等);在数论中则应用于包括费马大定理等各种问题中,在物理科学里,椭圆函数及椭圆积分出现在位势理论中,或者通过保形表示或者通过椭球的位势,出现在弹性理论、刚体运动、热传导或扩散论的格林函数以及其他一些问题中.

4. 阿贝尔·雅可比·艾森斯坦和黎曼

在19世纪20年代,阿贝尔(Abel)和雅可比(Jacobi)终于发现了对付椭圆积分的方法. 那就是研究他们的反演. 比如说,要研究积分

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

我们转而研究它的反函数 $x = g(u)$,这样一来可将问题大大简化,就如同我们研究函数 $x = \sin u$ 来代替研究 $\sin^{-1} x = \int_0^x \frac{\mathrm{d}t}{\sqrt{1 - t^2}}$,特别这时我们面对的已不是多值积分而是一个周期函数 $x = g(x)$.

$\sin u$ 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 $w_1, w_2 \in \mathbf{C}, \frac{w_1}{w_2} \notin \mathbf{R}$,使得

$$g(u) = g(u + w_1) = g(u + w_2)$$

有许多方法可让这两个周期显露出来,一种方法是德国数学家艾森斯坦(Eisenstein Ferdinand Gotthold Max,1823—1852)最早提出的,今天还在普遍使用,要点是先写出显然具有周期 w_1, w_2 的一个函数

$$g(u) = \sum_{m,n \in \mathbf{z}} \frac{1}{(u + mw_1 + mw_2)^2}$$

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 $\frac{1}{\sqrt{t^3+at+b}}$ 的行为,按照黎曼(Riemann Georg Friedrich Bernhard,1826—1866)的观点,视双值"函数" $\frac{1}{\sqrt{t^3+at+b}}$ 为 **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 w_1 和 w_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

$$g'(u)=\frac{\mathrm{d}x}{\mathrm{d}u}=\frac{1}{\frac{\mathrm{d}x}{\mathrm{d}u}}=\frac{1}{\frac{1}{\sqrt{x^3+ax+b}}}=\sqrt{x^3+ax+b}=y$$

所以 $x=g(u)$,$y=g'(u)$ 给出了曲线 $y^2=x^3+ax+b$ 的参数化.

椭圆 $\frac{x^2}{a^2}+\frac{y^2}{b^2}=1$ 的弧长的计算可化到椭圆积分.实际上,对应于横坐标自 0 变到 x 的那一段弧,等于

$$l(x)=\int_0^x\sqrt{1+y'^2}\,\mathrm{d}x=a\int_0^{\frac{x}{a}}\sqrt{\frac{1-k^2t^2}{1-t^2}}\,\mathrm{d}t$$

其中 $t=\frac{x}{a}$,$k^2=\frac{a^2-b^2}{a^2}$,这是勒让德形式的第二种椭圆积分.椭圆的全长可用完全椭圆积分来表示 $l=4a\cdot\int\sqrt{\frac{1-k^2t^2}{1-t^2}}\,\mathrm{d}t=4aE(k)$,这就是我们称其为椭圆积分而称它们的反函数为椭圆函数的根据.

5. 椭圆曲线的加法

实数域中加法规则的几何描述如图 2 所示.

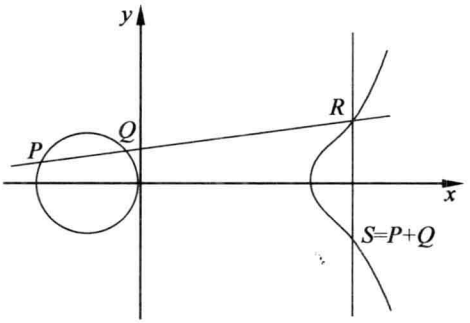


图 2

要对点 $P(x_1, y_1)$ 和 $Q(x_2, y_2)$ 做加法，首先过 P 和 Q 画直线（如果 $P = Q$ 就过点 P 画曲线的切线）与椭圆曲线相交于点 $R(x_3, -y_3)$，再过无穷远点和点 R 画直线（即过点 R 做 x 轴的垂线）与椭圆曲线相交于点 $S(x_3, y_3)$，则点 S 就是 P 和 Q 的和，即 $S = P + Q$.

讨论：

情形一：$x_1 \neq x_2$.

设通过点 $P(x_1, y_1)$ 和 $Q(x_2, y_2)$ 的直线为 L，情形一实际上是点 $P(x_1, y_1)$ 与自己相加，即倍点运算. 这时定义直线 $L: y = \lambda x + \gamma$ 是椭圆曲线 $y^2 = x^3 + ax + b$ 在点 $P(x_1, y_1)$ 的切线，根据微积分理论可知，直线的斜率等于曲线的一阶导数，即