现代数学基础丛书 103

椭圆曲线公钥密码导引

祝跃飞　张亚娟　著

科学出版社
www.sciencep.com

现代数学基础丛书　103

椭圆曲线公钥密码导引

祝跃飞　张亚娟　著

科学出版社

北京

内 容 简 介

椭圆曲线是一门古老而内容丰富的数学分支，ECC 理论涉及了许多深奥的椭圆曲线算数理论，要系统详细地讲授 ECC 理论需要较深的数学基础. 本书的目的是在交换代数的基础上系统阐述 ECC 理论，为有志于从事该方向研究的人员提供一本系统全面的基础性教材. 本书围绕 ECC 的理论和实践分三部分：第一部分介绍椭圆曲线的算术理论，主要是有限域上椭圆曲线的相关理论；第二部分为 ECC 的密码理论，重点论述了有限域上椭圆曲线的求阶算法，椭圆曲线上的离散对数求解算法和椭圆曲线公钥密码体制，椭圆曲线的素性证明和大数分解算法；第三部分为椭圆曲线公钥密码的有效实现，重点论述椭圆曲线公钥密码体制中的关键算子；标量乘法和双标量乘法的快速实现.

本书可以作为信息安全和密码学专业研究生的教材，也可供相关的研究人员参考.

图书在版编目(CIP)数据

椭圆曲线公钥密码导引/祝跃飞，张亚娟著. —北京：科学出版社，2006
(现代数学基础丛书；103)
ISBN 7-03-017360-0

I. 椭… II. ①祝… ②张… III. 密码-理论 IV. TN918.1

中国版本图书馆 CIP 数据核字(2006)第 057326 号

责任编辑：陈玉琢 贾瑞娜/责任校对：刘亚琦
责任印制：安春生/封面设计：王 浩

科学出版社出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

源海印刷有限责任公司印刷
科学出版社编务公司排版制作
科学出版社发行 各地新华书店经销
*
2006 年 10 月第 一 版 开本：B5 (720×1000)
2006 年 10 月第一次印刷 印张：16
印数：1—3 000 字数：298 000

定价：36.00 元

(如有印装质量问题，我社负责调换〈路通〉)

《现代数学基础丛书》编委会

《现代数学基础丛书》序

对于数学研究与培养青年数学人才而言，书籍与期刊起着特殊重要的作用．许多成就卓越的数学家在青年时代都曾钻研或参考过一些优秀书籍，从中汲取营养，获得教益．

20 世纪 70 年代后期，我国的数学研究与数学书刊的出版由于文化大革命的浩劫已经破坏与中断了十余年，而在这期间国际上数学研究却在迅猛地发展着．1978 年以后，我国青年学子重新获得了学习、钻研与深造的机会．当时他们的参考书籍大多还是 50 年代甚至更早期的著述．据此，科学出版社陆续推出了多套数学丛书，其中《纯粹数学与应用数学专著》丛书与《现代数学基础丛书》更为突出，前者出版约 40 卷，后者则逾 80 卷．它们质量甚高，影响颇大，对我国数学研究、交流与人才培养发挥了显著效用．

《现代数学基础丛书》的宗旨是面向大学数学专业的高年级学生、研究生以及青年学者，针对一些重要的数学领域与研究方向，作较系统的介绍．既注意该领域的基础知识，又反映其新发展，力求深入浅出，简明扼要，注重创新．

近年来，数学在各门科学、高新技术、经济、管理等方面取得了更加广泛与深入的应用，还形成了一些交叉学科．我们希望这套丛书的内容由基础数学拓展到应用数学、计算数学以及数学交叉学科的各个领域．

这套丛书得到了许多数学家长期的大力支持，编辑人员也为其付出了艰辛的劳动．它获得了广大读者的喜爱．我们诚挚地希望大家更加关心与支持它的发展，使它越办越好，为我国数学研究与教育水平的进一步提高作出贡献．

杨　乐

2003 年 8 月

前　言

1985 年，V. Miller 和 N. Koblitz 各自独立地提出椭圆曲线公钥密码 (elliptic curves cryptography,ECC)，这是继 Goldwasser 和 Kilian 的素性检验， Lenstra 的椭圆曲线大数分解后，椭圆曲线理论在密码学中的又一次全新的应用．它的思想仍然是在各种涉及有限域乘法群的公钥密码体制中，用有限域上的椭圆曲线构成的群来类比有限域的乘法群，从而获得类似的公钥密码体制．这类体制的安全性是基于椭圆曲线上离散对数问题求解的困难性，目前还没有找到解决此问题的次 (亚) 指数时间算法，因而它具有一些其他公钥密码体制无法比拟的优点，如在相同的安全强度下系统参数和密钥尺寸较短 (如 160bits 的 ECC 和 1024 bits 的 RSA 具有相当的安全强度)，选择余地较大等．正是这些特点，十几年来，一直引起数学家、密码学家和计算机科学家们的极大关注，在理论和技术上获得大量成果的同时，许多国际标准化组织 (政府、工业界、金融界、商业界等) 已将各种椭圆曲线密码体制作为其标准化文件向全球颁布．ECC 标准大体可以分为两种形式：一类是技术标准，即描述以技术支撑为主的 ECC 体制，主要有 IEEEP 1363 、 ANSI X9.62 、 ANSI X9.63 、 SEC 1 、 SEC 2 、 FIP 186-2 及 ISO/IEC 14888-3. 规范了 ECC 的各种参数的选择，并给出了各级安全强度下的一组 ECC 参数．另一类是应用标准，即在具体的应用环境中建议使用 ECC 技术，主要有 ISO/IEC 15946 、 IETFPKIX 、 IETF TLS 及 WAPWTLS 等．在标准化的同时，一些基于标准 (或草案) 的各种椭圆曲线加密、签名、密钥交换的软、硬件也相继问世．以加拿大 Certicom 为首的安全公司不仅和工业界联合共同研制、生产了以椭圆曲线密码算法为核心的密码产品，还提出了各种安全条件下对椭圆曲线离散对数攻击的悬赏挑战，这些举措大大刺激了 ECC 的理论和技术的发展．目前，国外已开发出含 ECC 的密码引擎协处理器的 SIM 卡、Smart 卡，也研制出含 ECC 的高速 DSP 芯片和 FPGA 、ASIC 芯片．在持续三年 (2000.01~2002.12) 的欧洲 NESSIE 工程中，及在日本电子政务的 CRYPTREC 工程中均有多个涉及 ECC 的候选方案．可以相信，凭借其自身的优势， ECC 技术在信息安全领域中会发挥越来越大的作用．

椭圆曲线是一门古老而且内容丰富的数学分支，ECC 理论涉及了许多深奥的

椭圆曲线算术理论，要系统详细地讲授 ECC 理论需要有较深的数学基础. 本书的目的是在交换代数的基础之上系统阐述 ECC 理论，为有志于从事该方向研究的人员提供一本系统全面的基础性教材. 本书是专业教材，国内还没有这方面的教材，与国外同类书籍比较，本书内容丰富，有理论，有应用，有实践，且将最新的研究成果融入其中；书中所有的结果尽可能自包含，以形成一个完整的体系；丰富的内容使得本书的阅读面较广，除代数、数论专业以及密码学的研究生和相关专业的研究人员外，第三部分的实践所涉及的算法，也可供信息安全方面的工程人员参考.

本书围绕着 ECC 的理论和实践分三部分内容撰写. 第一部分 (第 1 、2 章) 为椭圆曲线基础. 介绍了椭圆曲线的算术理论，主要是有限域上椭圆曲线的相关理论；第二部分 (第 3~6 章) 为 ECC 的密码理论，重点论述了有限域上椭圆曲线的求阶算法，椭圆曲线上的离散对数求解算法和椭圆曲线公钥密码体制，椭圆曲线的素性证明和大数分解算法；第三部分 (第 7 章) 为椭圆曲线公钥密码的有效实现，重点论述椭圆曲线公钥密码体制中的关键算子：包括标量乘法和双标量乘法的快速实现. 书中的大部分内容曾多次在解放军信息工程大学作为硕士研究生教材使用.

本书的编写和出版得到国家 973 项目 (编号：G1999035804) 、国家自然科学基金项目 (编号：60473021) 的资助，特此感谢！

作 者

目　录

第 1 章　椭 圆 曲 线

1.1 概　　述

公元 250 年，古希腊的亚历山大 (Alexandia) 时代，出版了丢番图 (Diophantus [①]) 的巨作《算术》(Arithmatic, 共 13 卷). 该书在历史上首次引入代数、方程、负数，后几卷涉及了数论的内容. 不幸的是，它出版后没过多久就被遗失了. 一千多年后，直到 1570 年才找到几卷，现保存的只有 6 卷. 尽管丢失了这么长时间，但该书中的许多工作并没有被重新发展. 书中所考虑的基本问题是有理多项式是否有有理解的问题，此问题分成以下两种形式.

(1) 仿射 (affine)：问 $f(x,y)\in\mathbb{Q}[x,y]$ 有无有理数解. 显然，通过乘以一个整数，便可以去掉 $f(x,y)$ 系数的分母，从而使得 $f(x,y)\in\mathbb{Z}[x,y]$，则问题转化为 $f(x,y)\in\mathbb{Z}[x,y]$ 有无有理数解.

(2) 投射 (projective)：问齐次方程 $f(x,y,z)\in\mathbb{Q}[x,y,z]$ 有无有理数解，即是否存在 $(0,0,0)\neq(x,y,z)\in\mathbb{Q}^3$ 满足 $f(x,y,z)=0$. 因为对于任意的 $t\in\mathbb{Q}$ 有 $f(tx,ty,tz)=t^{\deg f}f(x,y,z)$，即若 (x,y,z) 是所求的解，则 (tx,ty,tz) 也是解，称 (x,y,z) 和 (tx,ty,tz) 是等价的，则该等价类中一定有 $\mathbb{Z}^3$ 中的元素；又因为乘以一个整数不会改变方程的解，所以只需考虑整系数齐次多项式 $f(x,y,z)$ 有无整数解的问题.

进一步，若上述问题有解，考虑所有的解是否能用参数化表示的问题. 为了

---

① Diophantus：生活于公元 250 年前后的古希腊. 对于丢番图的生平事迹，人们知之甚少. 但在一本《希腊诗文选》中，收录了他的墓志铭：坟中安葬着丢番图，多么令人惊讶，它忠实地记录了他所经历的道路. 上帝给予的童年占 1/6，又过 1/12，两颊长髯，再过 1/7，点燃起结婚的蜡烛. 五年之后天赐贵子，可怜迟到的宁馨儿，享年仅及其父之半，便进入冰冷的墓. 悲伤只能用数论的研究去弥补，又过四年，他也走完了人生的旅途. 由此知道丢番图享年 84 岁. 他有几本著作，最重要的是《算术》，还有一部《多角数》，另一些已遗失. 《算术》是一部划时代的著作，虽然其是讲数论的，但是它引入了未知数，并对未知数加以运算，故可将其划归为代数. 丢番图把代数解放出来，摆脱了几何的羁绊，他认为代数方法比几何的演绎陈述更适宜于解决问题，而在解题的过程中显示出的高度技巧和独创性，在希腊数学中独树一帜. 他被后人称为“代数学之父”.

纪念丢番图，上述问题通称为丢番图问题，所涉及的不定方程称为丢番图方程.

注意到，仿射和投射是可以互相转化的. 例如，考虑仿射方程 $u^n+v^n=1$ 是否有有理解的问题，通过变量代换

$$u \leftarrow \frac{x}{z}, v \leftarrow \frac{y}{z},$$

该问题转化为投射方程 $x^n+y^n=z^n$ 是否有非平凡的整数解 (即 $z \neq 0$) 的问题，当 $n=2$ 时，见习题 1.1；当 $n \geqslant 3$ 时，该问题即是著名的费马 (Fermat [①]) 问题. 1993 年，安得鲁 · 怀尔斯 (A.Wiles [②]) 用椭圆曲线等相关现代数学理论证明了费马大定理.

以下从一些简单的投射丢番图方程入手，考虑丢番图问题.

(1) 一次的投射丢番图方程为投射线 $ax+by+cz=0$， $a,b,c \in \mathbb{Z}$ 不同时为 0. 其在 $\mathbb{Z}^3$ 的解是容易求得的，且所有的解可以参数化表示.

(2) 二次的投射丢番图方程，通过合适的线性变换，不妨设为 $ax^2+by^2+cz^2=0$， $a,b,c \in \mathbb{Z}$ 不同时为 0. 对该方程无解的判断相对来说容易得多，举例如下.

① $x^2+y^2+z^2=0$ 无平凡整数解：因为平方数均不小于 0，即在 $\mathbb{R}$ 中无解.

② $x^2+y^2=3z^2$ 无平凡整数解：因为任意整数解均可以诱导出一组互素的整数解，所以不妨设该方程有互素的整数解 $x,y,z \in \mathbb{Z}$，则方程两边同时模 3，可得 $x^2+y^2 \equiv 0 \mod 3$，显然 3 一定是 x,y,z 的公因子，矛盾.

---

①费马 (1601.8~1665.1)，法国数学家，生于图卢兹 (Toulouse) 附近的一个皮革商人家庭，他学习过法律并担任过律师，业余研究数学. 他受到由法国数学家 Bachet 翻译成拉丁文的丢番图《算术》(1621 年出版) 的影响，潜心研究数论，在看到毕达哥拉斯 (Pythagoras) 问题的章节时，他写道“$n \geqslant 3$ 时，$x^n+y^n=z^n$ 无平凡整数解，我已获得一个巧妙的证明方法，但由于书的空隙太小无法写下来”.

②怀尔斯 (1953~),1953 年 4 月 11 日生于英国剑桥. 1971 年入牛津大学莫顿 (Merton) 学院学习，1974 年获该校学士学位. 同年入剑桥大学柯雷尔 (Clare) 学院学习，1980 年获该校博士学位. 1977~1980 年，是柯雷尔学院的“青年研究会员”和哈佛大学的“本杰明 · 裴尔斯助教授”. 1981 年是波恩的“理论数学专门研究院”访问教授，此年稍后，为美国普林斯顿的“高等研究所”研究员. 1982 年成为普林斯顿大学教授，该年春是奥赛的巴黎大学访问教授. 作为古根海特别研究员，他在 1985~1986 年是科学高级研究所 (IHES) 和高级师范学校 (ENS) 的访问教授. 1988~1990 年是牛津大学皇家学会研究教授. 1994 年，他取得现在的普林斯顿大学欧根 · 黑金斯数学教授职位. 怀尔斯于 1989 年被选为在伦敦的皇家学会研究员. 1995 年获瑞典皇家科学院的数学韬克奖. 同年获费马奖，由保罗萨巴提尔大学和马特拉马克尼空间颁发. 1996 年获沃尔夫奖和 (美国) 国家科学院奖.

若丢番图方程有整数解，显然在实数域 $\mathbb{R}$ 中有解，在任意 p-adic 整环 $\mathbb{Z}_p$(或 p-adic 数域 $\mathbb{Q}_p$) 中有解. 反之是否成立呢？ Hasse [①] 对此给出了正式的归纳：若一个齐次方程在 $\mathbb{Q}$ 上有解当且仅当它在 $\mathbb{R}$ 和任意 $\mathbb{Q}_p$ 上有解，简述成整体有解当且仅当局部有解. 该命题称作局部整体原则 (local global principle)，由于 Hasse 是在 Minkowski [②] 已证明了对二次齐次方程局部整体原则是正确的基础上提出的，故又称之为 Hasse-Minkowski 原理. 利用局部整体原则，判别丢番图方程无整数解比有整数解要容易. Hensel [③] 证明了 $\mathbb{Q}_p$ 上的求解问题可以转化为 $\mathbb{F}_p$ 上的求解问题，所以丢番图方程求整数解的问题转化为在 $\mathbb{R}$ 和 $\mathbb{F}_p$ 中求解问题，其中 p 是所有的素数.

(3) 三次投射丢番图方程没有一个一致的结果. 1951 年，Selmer 证明了方程 $3x^3+4y^3+5z^3=0$ 局部有解，但整体无解. 所以当方程次数为 3 时，局部整体原则不成立. 继续考虑下面几个三次方程的例子.

①三次 Fermat 方程 $x^3+y^3=z^3$：对其作变量代换为

$$\begin{cases} \dfrac{x}{z}=\dfrac{3u}{v} \\ \dfrac{y}{z}=\dfrac{v-9}{v} \end{cases}$$

则得 $v^2-9v=u^3-27$.

②同余 (congruent) 数问题：$r\in\mathbb{Q}$ 称作同余数，若 r 是一个有理数边构成的直角三角形的面积，即

$$r\text{是同余数} \Longleftrightarrow \text{存在 } x,y,z\in\mathbb{Q}\text{使得} \begin{cases} x^2+y^2=z^2 \\ r=\dfrac{1}{2}xy \end{cases}$$

同余数问题是指是否存在同余数. 如果 r 是同余数，则对于任意的 $s\in\mathbb{Q}$，

① Hasse (1898~1979), 德国哥廷根大学教授，师从 Hensel，在类域论、复乘等方面有过杰出的成果.

② Minkowski(1864~1909), 德国哥廷根大学教授，在二次型、连分式等方面有过杰出的成果.

③ Hensel(1861~1941), 德国 Marburg 大学教授, 师从 Weierstrass、Kirchhoff、Helmholtz 和 Kronecker，主要研究领域是代数数域.

均有 s^2r 是同余数，故同余数问题只需考虑无平方因子整数 r. 由方程

$$\begin{cases} x^2+y^2=z^2 \\ r=\dfrac{1}{2}xy \end{cases}$$

可得 $(x\pm y)^2=z^2\pm 4r$, $\left(\dfrac{x\pm y}{2}\right)^2=\left(\dfrac{z}{2}\right)^2\pm r$，则 $\left(\dfrac{x^2-y^2}{4}\right)^2=\left(\dfrac{z}{2}\right)^4-r^2$，令 $u=\dfrac{z}{2}, v=\dfrac{x^2-y^2}{4}$，有 $v^2=u^4-r^2$, $u^6-r^2u^2=(uv)^2$, 再令 $u^2=x, uv=y$, 可得 $x^3-r^2x=y^2$. 因此，若 $x^3-r^2xz^2=y^2z$ 在 $\mathbb{Q}$ 中有 $z\neq 0$ 的解，则 $y^2=x^3-r^2x$ 在 $\mathbb{Q}$ 中有解，从而

$$\begin{cases} x^2+y^2=z^2 \\ r=\dfrac{1}{2}xy \end{cases}$$

在 $\mathbb{Q}$ 中有解.

③对于给定的数，如 6，是否能将其分成两部分 (有理数)，使它们的乘积是一个数的立方和此数的差，即

$$6y-y^2=x^3-x$$

是否有有理数解？ $P=(x,y)=(-1,0)$ 是方程的一个解，考虑过 P 点的所有直线与上述方程的交点. 设直线为 $x=2y-1$，代入方程得

$$6y-y^2=8y^3-12y^2+6y-1-2y+1=8y^3-12y^2+4y,$$

显然 $y\neq 0$ 在 $\mathbb{R}$ 中无解. 即除了 P 点外，该直线和方程在实平面内没有其他的交点. 设直线为 $x=3y-1$，代入方程得

$$6y-y^2=27y^3-27y^2+6y,$$

故 $y=\dfrac{26}{27}, x=\dfrac{17}{9}$ 是直线与方程的交点，即其为方程的解.

④ Bacht 问题：考虑一个有理数 c 如何写成一个平方 (有理) 数和一个立方 (有理) 数之差. 即可描述成 Bacht 方程： $y^2-x^3=c$ 是否有有理数解？ 1621 年， Bacht 证明了若 (x,y) 是一个解，则

$$\left(\frac{x^4-8cx}{4y^2}, \frac{-x^6-20cx^3+8c^2}{8y^3}\right)$$

也是一个解. 令人惊讶的是 Bacht 如何找到这样的非平凡的解呢？后人用③中所述的直线和方程相交的思想给出了解释. 然而，要知道笛卡儿 [①] 在 1637 年出版《几何学》，才引入坐标系、用符号代数来研究轨迹等几何问题，而 Bacht 生活在笛卡儿之前，难道那时 Bacht 的思维里已有坐标系的概念了吗？

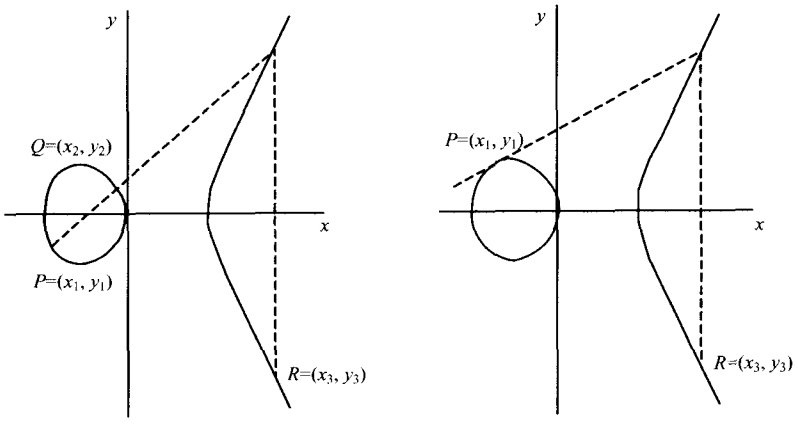
上述四个例子均可归结为一类三次方程，即所谓的 Weierstrass 方程

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad a_i \in \mathbb{Q}.$$

光滑的 Weierstrass 方程所确定的曲线加上一个特定点 O (无穷远点) 称为 $\mathbb{Q}$ 上的椭圆曲线. 同样，可定义 $\mathbb{R}, \mathbb{C}, \mathbb{Q}_p, \mathbb{F}_p$ 上的椭圆曲线，如

$$E(\mathbb{R}) = \{(x, y) \in \mathbb{R}^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{O\}$$

从几何角度利用弦切法可以在 $E(\mathbb{R})$ 上定义“ + ”运算：对于椭圆曲线上的点 P,Q，过点 P,Q 的直线 (若 $P = Q$，则取过点 P 的切线) 和椭圆曲线必有第三个交点 (考虑重数)，过该点和 O 的直线与椭圆曲线的另一交点即定义为 $P+Q$. 如图 1.1 所示.



弦切法： $R = P + Q$ $R = P + P = 2P$

图 1.1 弦切法示意

①笛卡儿 (Descart,1596~1650)，生于法国土伦省莱耳市的一个贵族之家，卒于斯德哥尔摩. 1612 年在普瓦捷大学攻读法学，四年后获博士学位； 1628 年移居荷兰； 1637 年发表的《几何学》标志着解析几何学的诞生，确定了其在数学史上的地位； 1649 年到斯德哥尔摩任宫廷哲学家，为瑞典女王授课；其在数学、物理及哲学等众多领域都有杰出贡献，堪称 17 世纪及其后的欧洲哲学界和科学界最有影响的巨匠之一，被誉为“近代科学的始祖”.

则 $(E(\mathbb{R}),+)$ 构成群 (Poincaré [①] 定理),$(E(\mathbb{Q}),+)$ 是其子群. 对于域 K 上 Weierstrass 方程的解确定的椭圆曲线 $E(K)$，虽然没有几何图像直观表示，但利用弦切法所决定的代数公式，自然可以定义 $E(K)$ 上的加法，使其构成一个加法群. 本书重点论述 K 为有限域 $\mathbb{F}_q$ 的情况. 一方面从前面论述已知，判断 E 有无非有理数解，根据局部整体原则和 Hensel 引理，需要研究 $E(\mathbb{Q}_p)$, $E(\mathbb{R})$, $E(\mathbb{C})$, $E(\mathbb{F}_q)$ 的结构和相关性质及理论. 另一方面，椭圆曲线能够在密码中应用的关键是椭圆曲线的群结构，由于密码系统是个离散的系统，它需要用有限群来构筑系统的基础，因此 $E(\mathbb{F}_q)$ 的结构和性质是本书的讲述重点. 若没有特殊声明，$\mathbb{Z}_n$ 均表示商群 $\mathbb{Z}/n\mathbb{Z}$.

定理 1.1.1 (Poincaré 定理) $(E(\mathbb{F}_q),+)$ 是一个阿贝尔群.

定理 1.1.2 (Hasse 定理) $|E(\mathbb{F}_q)|=1+q-t$，其中 t 满足 $|t|\leqslant 2\sqrt{q}$.

定理 1.1.3 (群结构) $E(\mathbb{F}_q)\cong\mathbb{Z}_{n_1}\times\mathbb{Z}_{n_2}$，其中 $n_1|n_2, n_1|q-1$.

1.2 仿射平面曲线

本章用 K 表示代数闭域. 本节介绍了仿射曲线的概念及基本性质.

定义 1.2.1 集合 $K\times K$ 称为 K 上的仿射平面 (affine plane)，记作 $A^2(K)$.

定义 1.2.2 K 上的一条仿射曲线是指 $K[X,Y]$ 中一个不可约多项式 C 的零点集，即 $C(K)=\{(a,b)\in A^2(K): C(a,b)=0\}$.

若给定 K 上的不可约多项式 C 也可看作 K 的某个子集 k 上的多项式，即 $C\in k[X,Y]$，则以后常称仿射曲线 $C(K)$ 的子集 $C(k)=\{(a,b)\in k^2: C(a,b)=0\}$ 为 C 在 k 上的有理点集.

例 1.1 令 $k=\mathbb{R}, K=\mathbb{C}$，曲线 D,E,F 在 $\mathbb{R}$ 上的有理点集的构成如图 1.2 所示.

因为 K 是代数闭域，所以任意曲线均有无限多个点：对于任意 $x\in K$，方程 $C(x,Y)$ 在 K 中至少有一个解，记作 y，则 $P=(x,y)$ 是曲线上的点. 为描述方便起见，以下将曲线和不可约多项式不加区别 (参见习题 1.2)，常称 C 是一条曲线或曲线 C，在不引起混淆的情况下，曲线可简记为 C.

---

① Poincaré(1854~1912), 生于法国南锡 (Nancy)，1879 年在巴黎大学获数学博士学位，同年任教于 Caen 大学，1887 年当选为法国科学院 (the Académie des Sciences) 院士，1906 年成为科学院主席，在数学分析、代数、拓扑、应用数学等领域均有杰出贡献.

D： $Y^2-(X^3+X^2)$ E： $Y^2-(X^3-X)$ F： Y^2-X^3

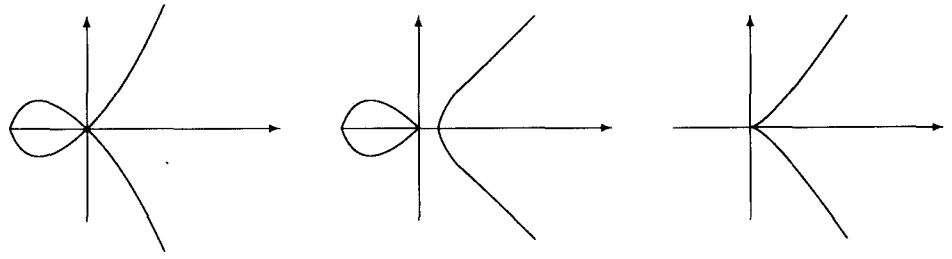


图 1.2 例 1.1 图

定义 1.2.3 设 C 是一条曲线，$P=(a,b)$ 是 C 上一个点. 若 $\frac{\partial C}{\partial X}|_{(a,b)}=\frac{\partial C}{\partial Y}|_{(a,b)}=0$，则称 P 是 C 上奇异点. 否则，称 P 是 C 上的非奇异点或光滑点，且称 $\frac{\partial C}{\partial X}|_P(X-a)+\frac{\partial C}{\partial Y}|_P(Y-b)=0$ 为 C 在 P 点的切线. 一条含有奇异点的曲线称为奇异曲线，否则称为非奇异曲线或光滑曲线.

例 1.2 仿射曲线 D、E、F 同例 1.1.

(1) 因为

$$\begin{aligned}\frac{\partial D}{\partial X}(0,0)=\frac{\partial D}{\partial Y} &= 0,\\ \frac{\partial F}{\partial X}(0,0)=\frac{\partial F}{\partial Y} &= 0.\end{aligned}$$

所以 $(0,0)$ 是 D 和 F 上的奇异点.

(2) 因为

$$\frac{\partial E}{\partial X}(0,0)=(-3X^2+1)|_{X=0}=1\neq 0,$$

所以 $(0,0)$ 是 E 上的非奇异点.

将 $C(X,Y)$ 在 $P=(a,b)$ 点展开，一定有形式

$$C(X,Y)=\frac{\partial C}{\partial X}|_P(X-a)+\frac{\partial C}{\partial Y}|_P(Y-b)+\text{高次项},$$

所以可以知道，$C(X,Y)$ 在 $P=(a,b)$ 奇异当且仅当上式没有一次项，否则一次项就是在 P 点的切线.

在代数闭域上，一个二次项一定能写成两个一次项的乘积，即

$$\begin{aligned}&\alpha(X-a)^2+\beta(X-a)(Y-b)+\gamma(Y-b)^2\\ &=(\alpha_1(X-a)+\beta_1(Y-b))(\alpha_2(X-a)+\beta_2(Y-b)),\end{aligned}$$

设 P 是奇异点，若 $\alpha_1(X-a)+\beta_1(Y-b)=\alpha_2(X-a)+\beta_2(Y-b)$，称 P 为尖点 (cusp)，否则称为叉点 (node). 例如，曲线 D 在 $(0,0)$ 点有 2 条切线，$Y=\pm X$，故 $(0,0)$ 是叉点；曲线 E 在 $(0,0)$ 点有一条二重的切线 $X=0$，故 $(0,0)$ 是尖点.

对于 $g(X,Y)\in K[X,Y]$，可以如下定义 C 到 K 的映射，即

$$g(X,Y):\quad \begin{cases} C\longrightarrow K \\ (a,b)\mapsto g(a,b) \end{cases}$$

该映射常称为多项式映射. 显然对于多项式 $f(X,Y)$,$g(X,Y)\in K[X,Y]$，其作为多项式映射相等当且仅当 $C|f-g$.

定义 1.2.4 *曲线 C 上的多项式环为 $K[C]=K[X,Y]/(C)$，即是全体多项式映射构成的集合.*

为描述方便，以下将 X,Y 在 $K[C]$ 中的剩余类仍记作 X,Y，其真正的含义可从上下文得知. 因为 C 不可约，所以 $K[C]$ 是整环.

定义 1.2.5 *$K[C]$ 的分式域称为 C 上的有理函数域，记作 $K(C)$.*

定义 1.2.6 *设有理函数 $r\in K(C),P\in C$，若存在 $f,g\in K[C]$，使得 $r=\dfrac{f}{g}$ 且 $g(P)\neq 0$，则称 r 在 P 点正则 (regular)，记 $r(P)=\dfrac{f(P)}{g(P)}$；在 P 点正则的有理函数的全体构成环，称为 C 在 P 的局部环，记作 $O_P(C)$. 若 r 在 P 点不正则，常记作 $r(P)=\infty$.*

所有在 P 点正则的有理函数在 P 点的取值是与有理函数的表示无关的：假设

$$r=\frac{f_1}{g_1}=\frac{f_2}{g_2},$$

其中，$f_1,g_1,f_2,g_2\in K[C],g_1(P)\neq 0,g_2(P)\neq 0$，则在 $K[C]$ 中有

$$f_1g_2=f_2g_1,$$

所以存在 $h\in K[X,Y]$，使得在 $K[X,Y]$ 中有

$$f_1g_2-f_2g_1=hC,$$

因此

$$f_1(P)g_2(P)-f_2(P)g_1(P)=h(P)C(P)=0,$$