“十二五”国家重点图书出版规划项目

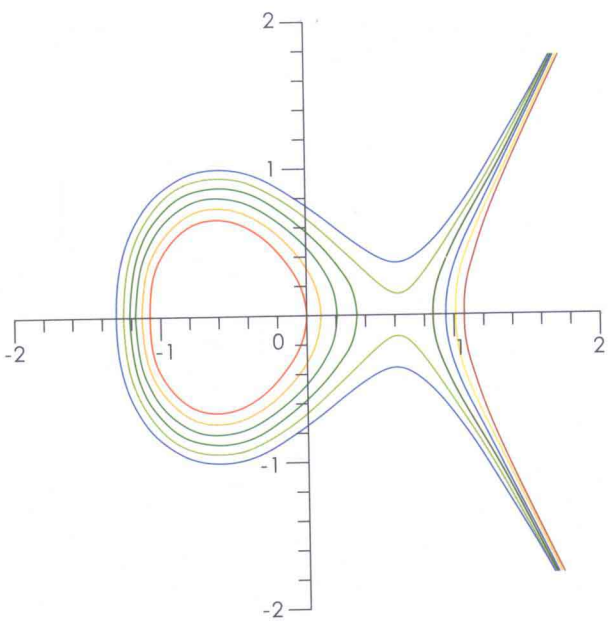
走向数学丛书

SCIENCE & HUMANITIES

椭圆曲线

ELLIPTIC CURVES

著　颜松远



大连理工大学出版社
DALIAN UNIVERSITY OF TECHNOLOGY PRESS

出版规划项目

走向数学丛书

椭圆曲线

ELLIPTIC CURVES

著　颜松远

大连理工大学出版社
DALIAN UNIVERSITY OF TECHNOLOGY PRESS

图书在版编目(CIP)数据

椭圆曲线 / 颜松远著. — 大连:大连理工大学出版社,2011.5
(走向数学丛书)
ISBN 978-7-5611-6176-0

Ⅰ. ①椭… Ⅱ. ①颜… Ⅲ. ①椭圆曲线 Ⅳ. ①O187.1

中国版本图书馆 CIP 数据核字(2011)第 066464 号

大连理工大学出版社出版
地址:大连市软件园路 80 号　邮政编码:116023
发行:0411-84708842　邮购:0411-84703636　传真:0411-84701466
E-mail:dutp@dutp.cn　URL:http://www.dutp.cn
沈阳新华印刷厂印刷　　大连理工大学出版社发行

幅面尺寸:147mm×210mm　印张:4.625　字数:81 千字
2011 年 5 月第 1 版　　2011 年 5 月第 1 次印刷

责任编辑:刘新彦　王　伟　　责任校对:李　慧　任俊杰
封面设计:孙　元　齐冰洁

ISBN 978-7-5611-6176-0　　定　价:20.00 元

续编说明

自从1991年“走向数学”丛书出版以来，已经出版了三辑，颇受我国读者的欢迎，成为我国数学传播与普及著作的一个品牌。我想，取得这样可喜的成绩主要原因是：中国数学家的支持，大家在百忙中抽出宝贵时间来撰写此丛书；天元基金的支持；与湖南教育出版社出色的出版工作。

但由于我国毕竟还不是数学强国，很多重要的数学领域尚属空缺，所以暂停些年不出版亦属正常。另外，有一段时间来考验一下已经出版的书，也是必要的。看来考验后是及格了。

中国数学界屡屡发出继续出版这套丛书的呼声。大连理工大学出版社热心于继续出版；世界科学出版社（新加坡）愿意出某些书的英文版；湖南教育出版社也乐成其事，

尽量帮忙。总之，大家愿意为中国数学的普及工作尽心尽力。在这样的大好形势下，“走向数学”丛书组成了以冯克勤教授为主编的编委会，领导继续出版工作，这实在是一件大好事。

首先要挑选修订重印一批已出版的书；继续组稿新书；由于我国的数学水平距国际先进水平尚有距离，我们的作者应面向全世界，甚至翻译他们的优秀著作。

我相信在新的编委会的领导下，丛书必有一番新气象。

我预祝丛书取得更大成功。

王　元

2010 年 5 月于北京

编写说明

从力学、物理学、天文学，直到化学、生物学、经济学与工程技术，无不用到数学. 一个人从入小学到大学毕业的十六年中，有十三四年有数学课. 可见数学之重要与其应用之广泛.

但提起数学，不少人仍觉得头痛，难以入门，甚至望而生畏. 我以为要克服这个鸿沟还是有可能的. 近代数学难于接触，原因之一大概是由于其符号、语言与概念陌生，兼之近代数学的高度抽象与概括，难于了解与掌握. 我想，如果知道讨论对象的具体背景，则有可能掌握其实质. 显然，一个非数学专业出身的人，要把数学专业的教科书都自修一遍，这在时间与精力上都不易做到. 若停留在初等数学水平上，哪怕做了很多难题，似亦不会有助于对近代数学的了

解.这就促使我们设想出一套“走向数学”小丛书,其中每本小册子尽量用深入浅出的语言来讲述数学的某一问题或方面,使工程技术人员、非数学专业的大学生,甚至具有中学数学水平的人,亦能懂得书中全部或部分含义与内容.这对提高我国人民的数学修养与水平,可能会起些作用.显然,要将一门数学深入浅出地讲出来,决非易事.首先要对这门数学有深入的研究与透彻的了解.从整体上说,我国的数学水平还不高,能否较好地完成这一任务还难说.但我了解很多数学家的积极性很高,他们愿意为“走向数学”撰稿.这很值得高兴与欢迎.

承蒙国家自然科学基金委员会、中国数学会数学传播委员会与湖南教育出版社的支持,得以出版这套“走向数学”丛书,谨致以感谢.

王　元

1990 年于北京

前 言

椭圆曲线意新颖，
到处可见其踪影.
费马定理显神通，
密码设计更称奇.

1997 年诺贝尔经济奖得主、哈佛大学商学院教授罗伯特-默顿 (Robert Merton)在其诺贝尔演讲报告中提到:“科学不一定是实用的,而实用的科学未必就具有优美性和挑战性”.很有幸的是,数论作为纯之又纯的数学学科(英国 20 世纪著名数学大师 G. H. Hardy 的名言),尤其是集数论、代数、几何和复变函数论为一体的椭圆曲线理论,则不仅具有极佳的优美性和挑战性,而且还具有很强的实用性和应用性.

所谓椭圆曲线(Elliptic Curve),可以认为是某一域(Field),比如说有理数域 $\mathbf{Q}$ 上三次不定方程 $y^2=x^3+ax+b$ 所定义的一种"平面"曲线,其中 a,b 为整数,$4a^3+27b^2\neq 0$. 这种貌似简单的曲线,简直就是一根"神线",因为它不仅具有很多优美漂亮的数学性质,而且还在众多的数学、计算机科学和密码学等领域中有着极为广泛而深入的应用. 比如悬而未决 350 多年的著名数学难题"费马猜想"(即"费马大定理"),就是由英国数学家 Andrew Wiles (现为美国普林斯顿大学教授)于 1994 年应用椭圆曲线的理论而彻底解决的(在问题解决的最后一步曾得到他昔日的博士生,现为美国哈佛大学教授 Richard Taylor 的帮助). 更为有意思的是,这种貌似简单的曲线,其理论却是十分的曲折深刻. 比如,关于这种曲线上有理点的一些基本性质和分布,人们至今仍不太清楚,著名的 21 世纪 7 个"千禧难题"之一的"Birch 和 Swinnerton-Dyer 猜想"就是与椭圆曲线有理点分布有关的一个极具挑战性的难题,由英国数学家 Bryan Birch (现为牛津大学教授)和 Peter Swinnerton-Dyer (现为剑桥大学教授)于 1960 年代初期提出来的一个悬而未决 50 余年的著名数学难题;美国 Clay 数学研究所悬赏一百万美元征寻其解. 因此椭圆曲线的理论及其应用作为现代数论中的一个分支学科,可以说是集纯粹性、优美性、挑战性、应用性、实用性为一体的一个"突出例子". 如果说"数论

是数学的皇后”(高斯的名言)的话,那么椭圆曲线理论就是皇后的皇冠上的一颗闪亮的“明珠”.

这是一本为大学生、研究生、广大数学爱好者以及对椭圆曲线感兴趣的科技人员而写作的一本比较通俗易懂的书籍.我们试图用简单浅显的语言向读者介绍曲折深刻的椭圆曲线理论及其应用.一般来讲,具有中等数学水平的读者,都可以读懂本书大部分的内容(略过有关复杂的数学公式).全书共分八章:第一章介绍与椭圆曲线有关的不定方程的知识,第二章介绍椭圆曲线的历史起源,第三章介绍椭圆曲线的重要性质,第四章介绍与椭圆曲线理论有关的一个极为重要的猜想,即 Birch 和 Swinnerton-Dyer 猜想(简称为 BSD 猜想),第五章介绍椭圆曲线在证明费马大定理中的应用,第六章介绍椭圆曲线在质数判定中的应用,第七章介绍椭圆曲线在整数分解中的应用,第八章介绍椭圆曲线在现代公钥密码体制中的应用.在每章中,如果需要用到一些比较深刻的或读者不太熟悉的概念,如同余、群、环、域、ζ 函数、L 函数、模形式等,我们都会适时的在适当的地方予以介绍.在本书的正文前给出了一些常用的符号及其说明,书末则给出进一步阅读的有关(英文)参考文献.为了节省篇幅,在本书中我们一般不给出定理的详细证明.另外,在每章的章末,都给出了一些思考题和科研题,供读者练习和研习之用.所谓思考题,就是一些可以做得出来的问

题.所谓科研题,就是目前还没有答案或定论的悬而未决的难题;这些难题有的悬而未决数千年,有的奖金高达百万美元;当然科研不是为了获奖,但科研奖项确实又是社会对历经艰辛而取得成就的科研人员的承认和回报.

作者衷心感谢本丛书的主编冯克勤教授(清华大学数学系)和顾问王元院士(中国科学院数学研究所),以及万哲先院士(中国科学院系统科学研究所)和王梓坤院士(北京师范大学数学系)对作者的鼓励、支持和帮助.国防科技大学数学与系统科学系谢端强教授帮助阅读过本书初稿.在本书的写作过程中,曾得到邹建成教授和何炎祥教授的鼓励和支持,谨此一并致以衷心感谢.由于作者学识浅陋,书中缺点错误在所难免.不当之处,敬请读者不吝指教;来信可寄:songyuanyan@gmail.com,syan@math.harvard.edu 或 syan@math.mit.edu.

颜松远

2010 年夏

完稿于伦敦和波士顿

常用符号一览表

符　号	说明及含义
$:=$	定义为
$\mid$	整除，如 $3 \mid 6$
gcd	最大公约数，如 $\gcd(3,6)=3$
$a \equiv b \pmod n$	a 和 b 在模 n 下同余，如 $8 \equiv 1 \pmod 7$
$\mathbf{Z}$	整数集合：$\mathbf{Z}=\{0,\pm 1,\pm 2,\pm 3,\cdots\}$
$\mathbf{Z}^+$	正整数集合：$\mathbf{Z}^+=\{1,2,3,\cdots\}$
$\mathbf{Q}$	有理数集合：$\mathbf{Q}=\{\frac{a}{b}: a,b \in \mathbf{Z}, b \neq 0\}$
$\mathbf{R}$	实数集合： $\mathbf{R}=\{n+0.d_1d_2d_3\cdots: n \in \mathbf{Z}, d_i \in \{0,1,\cdots,9\}$， 其中数字 9 不能无限连续重复出现$\}$
$\mathbf{C}$	复数集合： $\mathbf{C}=\{a+b\mathrm{i}: a,b \in \mathbf{R}, \mathrm{i}\sqrt{-1}\}$
$\mathbf{Z}/n\mathbf{Z}$	整数模 n 剩余类集合或整数环（可简记为 $\mathbf{Z}_n$）： $\mathbf{Z}/n\mathbf{Z}=\{0,1,2,\cdots,n-1\}$， 当 n 为质数 p 时，$\mathbf{Z}/p\mathbf{Z}$ 为一（有限）域
$(\mathbf{Z}/n\mathbf{Z})^*$	乘法群（可简记为 $\mathbf{Z}_n^*$）： $(\mathbf{Z}/n\mathbf{Z})^*=\{a \in \mathbf{Z}/n\mathbf{Z}: \gcd(a,n)=1\}$
$\lvert\mathbf{Z}/n\mathbf{Z}\rvert$	集合 $\mathbf{Z}/n\mathbf{Z}$ 中元素的个数
$\mathbf{F}_p$	有限域，$\mathbf{F}_p=\mathbf{Z}/p\mathbf{Z}$，$p$ 为质数
$\mathbf{F}_q$	有限域，$q=p^k$ 为质数幂
$\mathcal{A}$	任意域
$\mathrm{char}(\mathcal{A})$	域之特征（数）
E	椭圆曲线：$y^2=x^3+ax+b$，其中 $a,b \in \mathbf{Z}, 4a^3+27b^2 \neq 0$

$\mathcal{O}_E$	椭圆曲线上的无穷远点
$E\backslash\mathcal{K}$	定义在域 $\mathcal{K}$ 上的椭圆曲线 E
$E\backslash\mathbf{Q}$	定义在有理域 $\mathbf{Q}$ 上的椭圆曲线 E
$E\backslash\mathbf{F}_p$	定义在有限域 $\mathbf{F}_p$ 上的椭圆曲线 E
$E(\mathbf{Q}),E(\mathbf{F})_p$	$\mathbf{Q}$ 或 $\mathbf{F}_p$ 上椭圆曲线 E 的点之集合
$\lvert E(\mathbf{Q})\rvert,\lvert E(\mathbf{F})_p\rvert$	集合 $E(\mathbf{Q})$ 或 $E(\mathbf{Q})$ 中元素(点)之数目
$\mathrm{rank}(E(\mathbf{Q}))$	$E(\mathbf{Q})$ 之秩;也可记作 $\mathrm{rank}E(\mathbf{Q})$ 或 $r(E(\mathbf{Q}))$
N_p	$N_p=\lvert E(\mathbf{F}_p)\rvert$
a_p	$a_p=p+1-N_p$
$\zeta(s)$	黎曼 ζ 函数:

$$\zeta(s)=\sum_{i=1}^{\infty}n^{-s}=\prod_{p}(1-p^{-s})^{-1},$$

其中 $s=\sigma+it$ 为复数,$\sigma>1$,

p 过所有质数

$L(s,\chi)$ Dirichlet L 函数:

$$L(s,\chi)=\sum_{n=1}^{\infty}\chi(n)n^{-s}=\prod_{p}(1-\chi(p)p^{-s})^{-1},$$

其中 $s=\sigma+it$ 为复数,$\sigma>1$,

$\chi(n)$ 为模 m 之 Dirichlet 特征:

$$\chi(n)=\begin{cases}\chi(n \bmod m), & \text{如果 } \gcd(n,m)=1,\\ 0, & \text{如果 } \gcd(n,m)>1\end{cases}$$

$L(E,s)$ 椭圆曲线的 Mordell-Weil L 函数:

$$L(E,s)=\sum_{n=1}^{\infty}a_n n^{-s}=\prod_{p\nmid 2\triangle(E)}(1-a_p p^{-s}+p^{1-2s})^{-1},$$

其中 $s=\sigma+it$ 为复数,$\sigma>1$,

p 过所有质数

$$a_n=\begin{cases}1, & \text{如果 } n=1,\\ p-N_p, & \text{如果 } n=p,p \text{ 为质数},\\ a_p a_{p^{r-1}}-pa_{p^{r-1}}, & \text{如果 } n=p^r \text{ 为质数幂},\\ \prod_{i=1}^{k}a_{p_i^{\alpha_i}}, & \text{如果 } n=\prod_{i=1}^{k}p_i^{\alpha_i}\end{cases}$$

$\mathcal{P}$	在确定型图灵机上以多项式时间解决的问题之集合
$\mathcal{NP}$	在非确定型图灵机上以多项式时间解决的问题之集合
O	符号 O 定义为：当 $x\to\infty$，$f(x)=O(g(x))$，如果存在 $c\in\mathbf{R}_{>0}$，使之 $f(x)<cg(x)$.

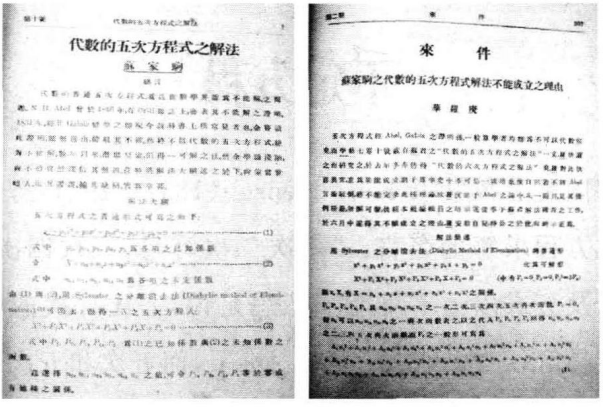
目 录

一

不定方程

德国著名数学家 Kurt Hensel (1861－1941)有一句关于代数方程求解的名言："一次二次容易，三次四次困难，五次以及五次以上不可能."意思是说，一次二次的代数方程很容易解，三次四次就比较困难了，而五次和五次以上的代数方程是没有求解公式的. 其实，我国著名数学家华罗庚(1910－1985)先生早期出名也就是出名在有关代数方程的解法上. 1926 年上海的《学艺》杂志在其第 7 卷第 10 期上刊登了苏家驹先生的文章《代数的五次方程式之解法》(见图 1 的左图). 当时年轻的华罗庚先生看到这篇文章后就感到非常纳闷，因为早在 1820 年左右挪威天才数学家阿贝尔(1802－1829)就证明了五次以及五次以上的代数方程是没有代数解的，即没有"通用的代数求根公式". 经过反复推算

验证，华先生发现苏文中的一个阶为 12 的行列式的计算有误，从而导致出错误的结果，为此写出《苏家驹之代数的五次方程式解法不能成立之理由》的文章（见图 1 的右图），在 1930 年上海的《科学》杂志第 15 卷第 2 期上刊出. 正是这篇文章，导致当时清华大学数学系主任熊庆来（1893—1969）教授邀请仅有初中文凭的华罗庚先生到清华大学工作，并最终将他培养成国际著名数学大师（这是后话）.


代数的五次方程式之解法

苏 家 驹

来 件

苏家驹之代数的五次方程式解法不能成立之理由

华 罗 庚

图 1　苏家驹和华罗庚文章的首页

对于一次二次的代数方程，一般中学生都会解. 比如对于一般形式的一元二次方程

$$ax^2+bx+c=0, \tag{1}$$

其解法有“万能”的通用求根公式

$$x=\frac{-b\pm\sqrt{b^2-4ac}}{2a}, \tag{2}$$

并且根据其判别式 $\Delta=b^2-4ac$，可以唯一确定其解的结