

<<椭圆曲线算术>>

图书基本信息

书名：<<椭圆曲线算术>>

13位ISBN编号：9787510037443

10位ISBN编号：7510037441

出版时间：2011-7

出版时间：世界图书出版公司

作者：希尔弗曼

页数：513

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## &lt;&lt;椭圆曲线算术&gt;&gt;

## 内容概要

美国哈佛大学从1977年以来曾多次举办“椭圆曲线”班，《椭圆曲线算术(第2版)(英文版)》作者是该讨论班成员之一。

椭圆曲线是一个古老的数学课题，最近由于代数数论和代数几何等现代数学的进展，使它得到了新的活力。

本书则是以上述观点处理椭圆函数的算术理论，包括椭圆曲线的几何背景，椭圆曲线的形式群，有限域上的椭圆函数、复数、局部域和整体域等基本内容，最后两章讨论整数和有理数。

书末有三个附录。

这是第二版，在第一版的基础上增加了“椭圆曲线的代数方面”全新一章，重在强调有限域上的算术，包括lenstra因式分解算术，schoof点计算算术，计算tate和weil派对的miller算术。

新增加了一部分讲述szpir ó猜想和abc，扩展和更新了大量的最新进展和大量新的练习。

目次：代数变量；代数曲线；椭圆曲线几何；椭圆曲线的标准群；有限域上的椭圆曲线； $\mathbb{C}$ 上的椭圆曲线；局部域上的椭圆曲线；全局域上的椭圆曲线；椭圆曲线的整数点；mordell-weil群上的计算；椭圆曲线的算术方面。

读者对象：数学专业的研究生教材、科研人员和相关的科技工作者。

<<椭圆曲线算术>>

作者简介

作者：(美国)希尔弗曼 (Joseph H.Silverman)

## &lt;&lt;椭圆曲线算术&gt;&gt;

## 书籍目录

- preface to the second edition
- preface to the first edition
- introduction
- chapter i algebraic varieties
  - § 1. affine varieties
  - § 2. projective varieties
  - § 3. maps between varieties
- exercises
- chapter ii algebraic curves
  - § 1. curves
  - § 2. maps between curves
  - § 3. divisors
  - § 4. differentials
  - § 5. the riemann-roch theorem
- exercises
- chapter iii the geometry of elliptic curves
  - § 1. weierstrass equations
  - § 2. the group law
  - § 3. elliptic curves
  - § 4. isogenies
  - § 5. the invariant differential
  - § 6. the dual isogeny
  - § 7. the tate module
  - § 8. the weil pairing
  - § 9. the endomorphism ring
  - § 10. the automorphism group
- exercises
- chapter iv the formal group of an elliptic curve
  - § 1. expansion around  $o$
  - § 2. formal groups
  - § 3. groups associated to formal groups
  - § 4. the invariant differential
  - § 5. the formal logarithm
  - § 6. formal groups over discrete valuation rings
  - § 7. formal groups in characteristic  $p$
- exercises
- chapter v elliptic curves over finite fields
  - § 1. number of rational points
  - § 2. the weil conjectures
  - § 3. the endomorphism ring
  - § 4. calculating the hasse invariant
- exercises
- chapter vi elliptic curves over  $\mathbb{C}$ 
  - § 1. elliptic integrals
  - § 2. elliptic functions

## &lt;&lt;椭圆曲线算术&gt;&gt;

§ 3. construction of elliptic functions

§ 4. maps analytic and maps algebraic

§ 5. uniformization

§ 6. the lefschetz principle

exercises

chapter vii elliptic curves over local fields

§ 1. minimal weierstrass equations

§ 2. reduction modulo

§ 3. points of finite order

§ 4. the action of inertia

§ 5. good and bad reduction

§ 6. the group  $e/e_0$

§ 7. the criterion of  $n$ -non-oggg-shafarevich

exercises

chapter viii elliptic curves over global fields

§ 1. the weak mordell-weil theorem

§ 2. the kummer pairing via cohomology

§ 3. the descent procedure

§ 4. the mordell-weil theorem over  $q$

§ 5. heights on projective space

§ 6. heights on elliptic curves

§ 7. torsion points

§ 8. the minimal discriminant

§ 9. the canonical height

§ 10. the rank of an elliptic curve

§ 11. szpiro's conjecture and abc

exercises

chapter ix integral points on elliptic curves

§ 1. diophantine approximation

§ 2. distance functions

§ 3. siegel's theorem

§ 4. the  $s$ -unit equation

§ 5. effective methods

§ 6. shafarevich's theorem

§ 7. the curve  $ye = x^3 + d$

§ 8. roth's theorem--an overview

exercises

chapter x computing the mordell-weil group

§ 1. an example

§ 2. twisting--general theory

§ 3. homogeneous spaces

§ 4. the selmer and shafarevich-tate groups

§ 5. twisting--elliptic curves

§ 6. the curve  $y^2 = xa + dx$

exercises

chapter xi algorithmic aspects of elliptic curves

§ 1. double-and-add algorithms

<<椭圆曲线算术>>

- § 2. lenstra's elliptic curve factorization algorithm
- § 3. counting the number of points in  $e(fq)$
- § 4. elliptic curve cryptography
- § 5. solving the ecdlp: the general case
- § 6. solving the ecdlp: special cases
- § 7. pairing-based cryptography
- § 8. computing the weil pairing
- § 9. the tatae-lichtenbanm pairing
- exercises
- appendix a elliptic curves in characteristics 2 and 3
- exercises
- appendix b group cohomology ( $h_0$  and  $h_1$ )
- § 1. cohomology of finite groups
- § 2. galois cohomology
- § 3. nonabelian cohomology
- exercises
- appendix c further topics: an overview
- § 11. complex multiplication
- § 12. modular functions
- § 13. modular curves
- § 14. tate curves
- § 15. neron models and tate's algorithm
- § 16. l-series
- § 17. duality theory
- § 18. local height functions
- § 19. the image of galois
- § 20. function fields and specialization theorems
- § 21. variation of  $a_p$  and the sato-tate conjecture
- notes on exercises
- list of notation
- references
- index

<<椭圆曲线算术>>

章节摘录

版权页：插图：

<<椭圆曲线算术>>

编辑推荐

《椭圆曲线算术(第2版)(英文)》由世界图书出版公司出版。



<<椭圆曲线算术>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>