

<<计算代数数值论教程>>

图书基本信息

书名：<<计算代数数值论教程>>

13位ISBN编号：9787506233101

10位ISBN编号：750623310X

出版时间：1997-9

出版人：世界图书出版公司

作者：H.Cohen

页数：545

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>

## <<计算代数数值论教程>>

### 内容概要

With the advent of powerful computing tools and numerous advances in mathematics, computer science and cryptography, algorithmic number theory has become an important subject in its own right. Both external and internal pressures gave a powerful impetus to the development of more powerful algorithms. These in turn led to a large number of spectacular breakthroughs. To mention but a few, the LLL algorithm which has a wide range of applications, including real world applications to integer programming, primality testing and factoring algorithms, sub-exponential class group and regulator algorithms, etc ...

<<计算代数数值论教程>>

书籍目录

Chapter 1 Fundamental Number-Theoretic Algorithms 1.1 Introduction 1.1.1 Algorithms 1.1.2 Multi-precision 1.1.3 Base Fields and Rings 1.1.4 Notations 1.2 The Powering Algorithms 1.3 Euclid's Algorithms 1.3.1 Euclid's and Lehmer's Algorithms 1.3.2 Euclid's Extended Algorithms 1.3.3 The Chinese Remainder Theorem 1.3.4 Continued Fraction Expansions of Real Numbers 1.4 The Legendre Symbol 1.4.1 The Groups  $(\mathbb{Z}/n\mathbb{Z})^*$  1.4.2 The Legendre-Jacobi-Kronecker Symbol 1.5 Computing Square Roots Modulo  $p$  1.5.1 The Algorithm of Tonelli and Shanks 1.5.2 The Algorithm of Cornacchia 1.6 Solving Polynomial Equations Modulo  $p$  1.7 Power Detection ..... 1.8 Exercises for Chapter 1

Chapter 2 Algorithms for Linear Algebra and Lattices 2.1 Introduction 2.2 Linear Algebra Algorithms on Square Matrices 2.3 Linear Algebra on General Matrices 2.4  $\mathbb{Z}$ -Modules and the Hermite and Smith Normal Forms 2.5 Generalities on Lattices 2.6 Lattice Reduction Algorithms 2.7 Applications of the LLL Algorithm 2.8 Exercises for Chapter 2

Chapter 3 Algorithms on Polynomials 3.1 Basic Algorithms 3.2 Euclid's Algorithms for Polynomials 3.3 The Sub-Resultant Algorithm 3.4 Factorization of Polynomials Modulo  $p$  3.5 Factorization of Polynomials over  $\mathbb{Z}$  or  $\mathbb{Q}$  3.6 Additional Polynomial Algorithms 3.7 Exercises for Chapter 3

Chapter 4 Algorithms for Algebraic Number Theory I

Chapter 5 Algorithms for Quadratic Fields

Chapter 6 Algorithms for Algebraic Number Theory II

Chapter 7 Introduction to Elliptic Curves

Chapter 8 Factoring in the Dark Ages

Chapter 9 Modern Primality Tests

Chapter 10 Modern Factoring Methods

Appendix A Packages for Number Theory

Appendix B Some Useful Tables

Bibliography

Index

<<计算代数数值论教程>>

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>