第一图书网, tushu007.com

<<算法数论>>

图书基本信息

书名：<<算法数论>>

13位ISBN编号：9787030106834

10位ISBN编号：7030106830

出版时间：2002年09月

出版时间：科学出版社

作者：裴定一,祝跃飞

页数：233

字数：196000

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

第一图书网, tushu007.com

<<算法数论>>

内容概要

本书论述了算法数论的基本内容，其中包括：连分数、代数数域、椭圆曲线、素性检验、大整数因子分解算法、椭圆曲线上的离散对数、超椭圆曲线。
本书的特点是内容涉及面广，在有限的篇幅内，包含了必要的预备知识和数学证明，尽可能形成一个完整的体系。
并且本书的部分内容曾多次在中国科学院研究生院信息安全国家重点实验室和广州大学作为硕士研究生教材使用。
本书可作为信息安全、数论等专业的研究生教材及相关专业的研究人员、高等学校的教师和高年级学生的参考。

第一图书网, tushu007.com

<<算法数论>>

书籍目录

序前言第一章 整数的因子分解 1.1 唯一分解定理 1.2 辗转相除法（欧氏除法） 1.3 Mersenne素数和Fermat素数 1.4 整系数多项式 1.5 环Z[i]和Z[ω] 习题一第二章 同余式 2.1 孙子定理 2.2 剩余类环 2.3 Euler函数ρ（m） 2.4 同余方程 2.5 原根 2.6 缩系的构造 习题二第三章 二次剩余 3.1 定义及Euler判别条件 3.2 Legendre符号 3.3 Jacobi符号 习题三第四章 特征 4.1 剩余系的表示 4.2 特征 4.3 原特征 4.4 特征和 4.5 Gauss和 习题四第五章 连分数 5.1 简单连分数 5.2 用连分数表实数 5.3 最佳渐近分数 5.4 Legendre判别条件 习题五第六章 代数数域 6.1 代数整数 6.2 Dedekind整环 6.3 阶的一些性质第七章 椭圆曲线 7.1 椭圆曲线的群结构 7.2 除子类群 7.3 同种映射 7.4 Tate模和Weil对 7.5 有限域上的椭圆曲线 习题七第八章 在密码学中的一些应用 8.1 RSA公钥密码 8.2 Uiffie-Hellman体制 8.3 ElGamal算法 8.4 基于背包问题的公钥密码 8.5 秘密共享第九章 素性检验 9.1 Fermat小定理及伪素数 9.2 强伪素数及Miller-Rabin检验 9.3 利用n-1的因子分解的素性检验 9.4 利用n+1的因子分解的素性检验 9.5 分圆环素性检验 9.6 基于椭圆曲线的素性检验第十章 大整数因子分解算法 10.1 连分数因子分解算法 10.2 二次筛法 10.3 Pollard的P-1因子分解算法 10.4 椭圆曲线因子分解算法 10.5 数域筛法 习题十第十一章 椭圆曲线上的离散对数 11.1 椭圆曲线公钥密码 11.2 小步-大步法 11.3 家袋鼠和野袋鼠 11.4 MOV约化 11.5 FR约化 11.6 SSSA约化 11.7 有限域上离散对数的计算第十二章 超椭圆曲线 12.1 超椭圆曲线的Jacobian 12.2 虚二次代数函数域 12.3 基于超椭圆曲线的公钥密码附录 一些常用算法 A.1 不可约多项式的判别 A.2 有限域中平方根的求解 A.3 有限域上的分解 A.4 Hensel引理 A.5 格 A.6 Z[x]中多项式的分解参考文献

第一图书网, tushu007.com

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