第一图书网, tushu007.com

<<数论与有限域>>

图书基本信息

书名：<<数论与有限域>>

13位ISBN编号：9787111315964

10位ISBN编号：7111315960

出版时间：2010-10

出版时间：机械工业出版社

作者：董丽华，胡予濮，曾勇　编著

页数：156

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

前言

长期以来，数论与有限域作为高度抽象的数学学科，对数学理论的发展起到了积极的作用，但其发展一直处于纯理论的研究状态，大多数人并不清楚它们的实际意义。
当今，随着近代计算机科学和应用数学的发展，数论与有限域已经不仅仅是优秀数学家大展才华的场所，在计算方法、编码学、密码学、计算机代数、组合论、通信工程、离散控制系统等许多领域得到日益广泛的实际应用，是许多从事应用和实际工作的工程技术人员必须掌握的数学基础知识。
本书试图使读者在较短时间内切实掌握数论与有限域的基本概念和基础知识，领会数论与有限域的精神实质和思想方法。

本书在编写过程中力求做到叙述简明，推理详尽，并不假定读者具有很多的数学知识，大学二年级的学生不查看其他参考书籍就能看懂本书。

内容概要

本书是初等数论与有限域的入门教材。
全书共分七章，前四章论述了数论中的基础知识，具体内容包括：整数的整除理论、同余理论、数论函数、二次剩余以及原根与指数等内容；随后两章重点论述了近世代数中群、环、域的基本概念，有限域的构造以及有限域中的计算；最后一章则讨论了数论与有限域的简单应用。
　本书结构紧凑、例题翔实，可作为高等院校网络工程、通信、信息工程、计算机、信息安全及其他相关专业本科生、研究生的教材和参考书，也可作为通信、计算机等领域中工程技术人员的参考书。

第一图书网, tushu007.com

书籍目录

前言教学和阅读建议第1章 整数与同余 1.1 整数 1.1.1 整数的定义 1.1.2 整除 1.2 整数的进位制表示法 1.2.1 带余除法 1.2.2 整数的二进制表示法 1.2.3 数制转换 1.3 整数分解 1.3.1 最大公因数 1.3.2 欧几里得算法 1.3.3 因式分解法 1.3.4 标准分解式 1.4 同余 1.4.1 同余的概念 1.4.2 线性同余式 1.4.3 中国剩余定理 1.4.4 威尔逊定理、费马小定理与欧拉定理 习题第2章 数论函数 2.1 积性函数 2.1.1 积性函数的定义 2.1.2 除数函数 2.2 高斯函数[x] 2.2.1 高斯函数[x]的性质 2.2.2 n！的标准分解式 2.3 欧拉函数φ(x) 2.4 默比乌斯函数 2.4.1 默比乌斯函数的概念 2.4.2 默比乌斯反演公式 2.5 完全数 2.5.1 完全数的概念 2.5.2 梅森数、费马数 习题第3章 二次剩余 3.1 二次剩余的概念 3.2 勒让德符号 3.3 高斯二次互反律 3.4 雅可比符号 3.5 二次同余式的解法和解数 习题第4章 原根和指数 4.1 原根 4.1.1 整数的阶 4.1.2 原根的概念 4.1.3 原根的存在性 4.1.4 原根的求法 4.2 指数 4.2.1 指数的性质 4.2.2 指数表 习题第5章 有限域的概念 5.1 群 5.1.1 群的概念 5.1.2 子群、陪集与拉格朗日定理 5.2 环 5.2.1 环的定义 5.2.2 多项式环 5.3 整环中的因子分解 5.3.1 一些基本概念 5.3.2 唯一分解整环 5.4 由整环构造域 习题第6章 有限域的抽象性质 6.1 有限域的加法结构 6.2 有限域的乘法结构 6.2.1 元素的阶 6.2.2 本原元 6.2.3 最小多项式与本原多项式 习题129第7章 数论与有限域的应用 7.1 同余式的简单应用 7.1.1 正整数能否被除尽 7.1.2 弃九法 7.1.3 计算星期几 7.1.4 循环赛 7.2 二次剩余的应用 7.2.1 Blum通信游戏 7.2.2 欧拉伪素数 7.3 信息加密 7.3.1 文件集合的加密 7.3.2 rsa公钥密码体制 7.4 正交拉丁方 7.5 阿达玛阵 7.6 纠错码 7.6.1 循环码 7.6.2 循环冗余校验码 习题参考文献

编辑推荐

《数论与有限域》内容涵盖数论与有限域的核心基础知识，叙述简明、推理详尽，展现有限域的本质，通过例题提示数论与有限域在网络工程、编码学、密码学、通信工程等方面的实际应用。

随着计算机科学和应用数学的发展，数论与有限域已经不仅仅是优秀数学家大展才华的场所，在计算方法、编码学、密码学、计算机代数、组合论、通信工程、离散控制系统等许多领域也得到日益广泛的实际应用。

是许多从事应用和实际工作的工程技术人员必须掌握的数学基础知识。

《数论与有限域》是初等数论与有限域的入门教材，在编写过程中，力求做到从具体实例出发。

引出抽象概念，强调计算而不只是偏重理论推导。

叙述尽量简洁易懂。

推理严谨，重点突出，试图使读者在较短时间内切实掌握数论与有限域的基本概念和基础知识，领会数论与有限域的精神实质和思想方法。

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