

<<数论基础>>

图书基本信息

书名：<<数论基础>>

13位ISBN编号：9787510004674

10位ISBN编号：7510004675

出版时间：2009-5

出版公司：世界图书出版公司

作者：史迪威

页数：254

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>

<<数论基础>>

内容概要

This book is intended to complement my Elements of Algebra , and it is similarly motivated by the problem of solving polynomial equations. However , it is independent of the algebra book , and probably easier.

In Elements of Algebra we sought solution by radicals , and this led to the concepts of fields and groups and their fusion in the celebrated theory of Galois. In the present book we seek integer solutions , and this leads to the concepts of rings and ideals which merge in the equally celebrated theory of ideals due to Kummer and Dedekind. The book is based on two short courses (about 20 lectures each) given at Monash University in recent years; one on elementary number theory and one on ring theory with applications to algebraic number theory. Thus the amount of material is suitable for a one-semester course , with some variation possible through omission of the optional starred sections. A slower~paced course could stop at the end of Chapter 9 , at which point most of the standard results have been covered , from Euclid's theorem that there are infinitely many primes to quadratic reciprocity.

<<数论基础>>

书籍目录

Preface
 1 Natural numbers and integers
 1.1 Natural numbers
 1.2 Induction
 1.3 Integers
 1.4 Division with remainder
 1.5 Binary notation
 1.6 Diophantine equations
 1.7 The Diophantus chord method
 1.8 Gaussian integers
 1.9 Discussion
 2 The Euclidean algorithm
 2.1 The gcd by subtraction
 2.2 The gcd by division with remainder
 2.3 Linear representation of the gcd
 2.4 Primes and factorization
 2.5 Consequences of unique prime factorization
 2.6 Linear Diophantine equations
 2.7 The vector Euclidean algorithm
 2.8 The map of relatively prime pairs
 2.9 Discussion
 3 Congruence arithmetic
 3.1 Congruence mod n
 3.2 Congruence classes and their arithmetic
 3.3 Inverses mod p
 3.4 Fermat's little theorem
 3.5 Congruence theorems of Wilson and Lagrange
 3.6 Inverses mod k
 3.7 Quadratic Diophantine equations
 3.8 Primitive roots
 3.9 Existence of primitive roots
 3.10 Discussion
 4 The RSA cryptosystem
 4.1 Trapdoor functions
 4.2 Ingredients of RSA
 4.3 Exponentiation mod n
 4.4 RSA encryption and decryption
 4.5 Digital signatures
 4.6 Other computational issues
 4.7 Discussion
 5 The Pell equation
 6 The Gaussian integers
 7 Quadratic integers
 8 The four square theorem
 9 Quadratic reciprocity
 10 Rings
 11 Ideals
 12 Prime ideals
 Bibliography
 Index

<<数论基础>>

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>