第一图书网, tushu007.com

<<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

出版时间：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

内容概要

This book is intended to complement my Elements of Algebra， and itis similarly motivated by the problem of solving polynomial equations.However， it is independent of the algebra book， and probably easier. InElements of Algebra we sought solution by radicals， and this led to theconcepts of fields and groups and their fusion in the celebrated theory ofGalois. In the present book we seek integer solutions， and this leads to theconcepts of rings and ideals which merge in the equally celebrated theoryof ideals due to Kummer and Dedekind. The book is based on two short courses （about 20 lectures each） givenat Monash University in recent years; one on elementary number theoryand one on ring theory with applications to algebraic number theory. Thusthe amount of material is suitable for a one-semester course， with somevariation possible through omission of the optional starred sections. Aslower~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 infinitelv many primes to quadratic reciprocity.

书籍目录

Preface1 Natural numbers and integers1.1 Natural numbers1.2 Induction1.3 Integers1.4 Division with remainder1.5 Binary notation1.6 Diophantine equations1.7 The Diophantus chord method1.8 Gaussianintegers1.9 Doscission2 The Euclidean algorithm2.1 The gcd by subtraction2.2 The gcd by division with remainder2.3 Linearrepresentation ofthe god2.4 Primes and factorization2.5 Consequences of unique prime factorization2.6 Linear Diophantine equations2.7 The vector Eudidean algorithm2.8 The map ofre latively prime pairs2.9 Doscission3 Congruencearithmetic3.1 Congruencemodn3.2 Congruence classes and their arithmetic3.3 Inverses mod p3.4 Fermat's little theorem3.5 Congruence theorems of Wilson and Lagrange3.6 Inverses mod k3.7 Quadratic Diophantine equations3.8 Primitive roots3.9 Existence ofprimitive roots3.10 Discussion4 The RSA cryptosystem4.1 Trapdoorfunctions4.2 Ingredients of RSA4.3 Exponentiation mod n4.4 RSA encryption and decryption4.5 Digitalsignatures4.6 0thercomputationalissues4.7 Discussion5 The Pell equation6 The Gaussian integers7 Quadratic integers _8 The four square theorem9 Quadratic reciprocity10 Rings11 Ideals12 Prime idealsBibliographyIndex

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