

《数论算法（研究生）》

书籍信息

版次：1

页数：

字数：

印刷时间：2014年05月01日

开本：16开

纸张：胶版纸

包装：平装

是否套装：否

国际标准书号ISBN：9787560633022

内容简介

数论是研究整数性质的一个数学分支，它历史悠久，有着强大的生命力。数论问题叙述简明，“很多数论问题可以从经验中归纳出来，并且仅用三言两语就能向一个行外人解释清楚，但要证明它却远非易事”，因而有人说：“用以发现天才，在初等数学中再也没有比数论更好的课程了”，所以在国内外各级各类的数学竞赛中，数论问题总是占有相当大的比重。

随着科学技术的发展，将经典理论与现代应用相结合已成为发展的一种趋势，故数论的应用领域也逐渐扩展开来，顺应发展趋势，推动数论应用，正是本书的编写目的和出发点。实际上，目前数论的有关理论和方法在计算机、通信等领域有着大量的应用，尤其在信息和网络安全、数字信号处理等方面应用更加广泛，而本书也主要从应用角度出发来研究数论问题，尤其是有关整数运算中实用的方法和具体算法。

本书共分9章，各章的主要内容概括如下：

第1章整数的可除性，主要介绍整除概念及与其相关的问题，如整除的定义及其性质，重点介绍了求*公因数的有关算法。

第2章数论函数，给出了几种常用数论函数并讨论了其性质，同时介绍了函数的积性和函数的Dirichlet乘积等概念及性质。

[显示全部信息](#)

目录

第1章 整数的可除性

1.1 整除的概念与带余除法

1.1.1 整除及其性质

1.1.2 素数

1.1.3 带余除法

1.2 整数的表示

1.3 最大公因数与辗转相除法

1.3.1 最大公因数

1.3.2 辗转相除法

1.3.3 求 (a, b) 的算法

1.3.4 (a, b) 与 a 、 b 的关系

1.3.5 其他性质

1.4 整除的进一步性质及最小公倍数

1.4.1 整除和最大公因数的其他性质

整数的可除性

1.1

整除的概念与带余除法

1.1.1

整除及其性质

1.1.2

素数	1.1.3	
带余除法	1.2	
整数的表示	1.3	
最大公因数与辗转相除法		1.3.1
最大公因数	1.3.2	
辗转相除法	1.3.3	
求 (a, b) 的算法		1.3.4
(a, b) 与 a, b 的关系		1.3.5
其他性质	1.4	
整除的进一步性质及最小公倍数		
1.4.1 整除和最大公因数的其他性质		
1.4.2 最小公倍数及其性质		1.5
算术基本定理		
习题1	第2章	
数论函数	2.1	
数论函数	2.2 函数 $\{x\}$ 、 $\lfloor x \rfloor$ 、	
$[x]$	2.2.1	
下整数函数 $\{x\}$		2.2.2
上整数函数 $\lfloor x \rfloor$		2.2.3
四舍五入函数 $[x]$		2.3
函数 $\text{pot}_p n$	2.4	
Euler函数 $\phi(n)$		2.5
墨比乌斯函数 $\mu(n)$		2.5.1
墨比乌斯函数		2.5.2
墨比乌斯反演公式		2.6
素数个数函数 $\pi(n)$		2.7
数论函数的狄利克雷乘积		2.8
积性函数	2.8.1	
积性函数的定义		2.8.2
积性函数的性质		
习题2	第3章	
同余及其运算	3.1	
同余的概念及基本性质		3.2
剩余类及完全剩余系		3.2.1
剩余类和完全剩余系		3.2.2
剩余类的性质	3.3	
既约剩余系	3.3.1	
既约剩余系	3.3.2	
整数 a 模 m 的逆	3.4	
欧拉定理和费马小定理		3.4.1
欧拉定理	3.4.2	
费马小定理	3.5	

模重复平方计算法		3.5.1	
算法原理	3.5.2		
模重复平方计算法		3.6	
一次不定方程		3.6.1	
二元一次(不定)方程			3.6.2
求特解的方法		3.6.3	
s元一次不定方程		3.6.4	
(s元)一次不定方程组			3.7
矩阵的同余运算		3.7.1	
矩阵及其线性运算		3.7.2	
矩阵乘法	3.7.3		
可逆矩阵	3.8		
同余的应用		3.8.1	
RSA公钥密码算法		3.8.2	
背包公钥密码算法		3.8.3	
希尔密码算法		3.8.4	
随机数的Lehmer生成算法			3.8.5
随机数的BBS生成算法			
习题3	第4章		
同余方程		4.1	
基本概念		4.2	
一次同余方程		4.3	
中国剩余定理		4.4	
高次同余方程的解数及解法			4.4.1
解数	4.4.2		
特殊情形的解法		4.4.3	
一般情形的解法		4.5	
素数模的同余方程		4.5.1	
同余方程的化简		4.5.2	
解数的判断		4.6	
同余方程的应用		4.6.1	
密钥分存		4.6.2	
数据库加密方案		4.6.3	
BBS流密码算法			
习题4	第5章		
二次同余方程与平方剩余			5.1
一般二次同余方程		5.1.1	
二次同余方程的化简		5.1.2	
平方剩余	5.2		
模为奇素数的平方剩余与平方非剩余			
5.2.1 平方剩余的判断条件			5.2.2
平方剩余的个数		5.3	

勒让德符号	5.4	
雅可比符号	5.5	
模 p 平方根	5.6	
模数为合数的情形		5.6.1
p 为奇素数	5.6.2	
$p = 2$	5.7	
解同余方程小结		
习题5	第6章	
原根与离散对数		6.1
整数的阶及其性质		6.1.1
整数的阶和原根		6.1.2
阶的性质与计算方法		6.2
原根的存在性与计算方法		6.3
离散对数	6.4	
离散对数的计算		6.4.1 Pohlid-
Hellman算法	6.4.2	
Shank算法	6.5	
二项同余方程与 n 次剩余		6.6
原根与离散对数的应用		6.6.1 Diffie-
Hellman密钥交换算法		6.6.2
EIGamal加密算法		6.6.3
改进的随机数生成算法		6.6.4
一种快速傅里叶变换算法		6.6.5
同余方程的求解	6.7	
单向函数		
习题6	第7章	
连分数	7.1	
连分数	7.1.1	
连分数的概念	7.1.2	
连分数性质与渐进连分数的计算		7.2
简单连分数	7.2.1	
实数的简单连分数的生成		7.2.2
有理分数的连分数表示		7.3
循环连分数		
习题7	第8章	
素性测试和整数分解		8.1
素性测试的精确方法		8.2
伪素数与Fermat测试算法		8.3
Euler伪素数与Solovay-Stassen测试算法		
8.3.1 Euler伪素数		8.3.2 Solovay-
Stassen测试算法	8.4	
强伪素数与Miller-Rabin测试算法		

8.4.1 强伪素数		8.4.2 Miller-
Rabin测试算法		8.5
正整数的分解		8.5.1
Fermat方法		8.5.2
Fermat方法的拓展		8.5.3
Legendre方法		8.5.4
Pollard方法		8.5.5
Kraitchik方法		8.5.6
B基数法——Brillhart-Morrison法		
8.5.7 连分数法		8.5.8
二次筛法		8.5.9
p-1法		
习题8		
有限域	第9章	
集合及其运算	9.1	9.1.1
集合	9.1.2	
映射	9.1.3	
代数运算		9.1.4
同构映射		9.2
群	9.3	
环	9.3.1	
环	9.3.2	
多项式环		9.4
域	9.4.1	
域的概念		9.4.2
域的特征和同构		9.4.3
有限域及其结构		9.4.4
有限域的构造		9.4.5
GF (2n) 域上的计算		习题
9	附录A	
素数表与最小正原根表(1200以内)		
附录B k的连分数		附录C
F2上的既约多项式(n 10)		
F2上的本原多项式		附录D
索引		
参考文献		
显示全部信息		

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www.tushupdf.com](http://www.tushupdf.com)