HZ BOOKS

经 典 原 版 书 库

PEARSON Addison Wesley

初等数论及其应用

（英文版 · 第5版）

本书只供在
中国大陆销售

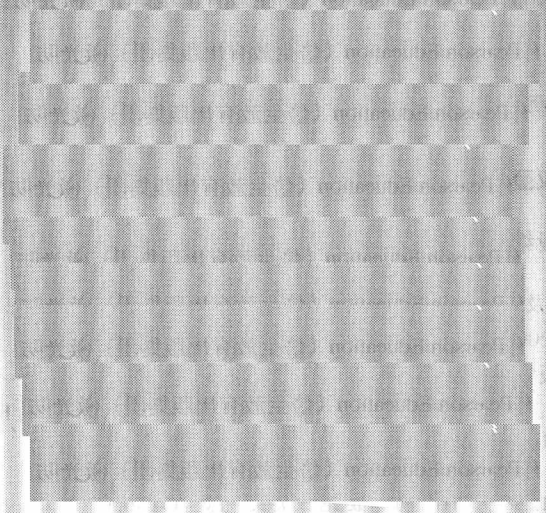
（美）肯尼斯 H. 罗森 著

机械工业出版社
China Machine Press

经 典 原 版 书 库

初等数论及其应用

（英文版 · 第5版）



（美）肯尼斯 H. 罗森 著

机械工业出版社
China Machine Press

本书版权登记号：图字：01-2005-1174

图书在版编目（CIP）数据

初等数论及其应用（英文版·第5版）/（美）罗森（Rosen, K. H.）著. -北京：机械工业出版社，2005.3

（经典原版书库）

书名原文：Elementary Number Theory and Its Applications, Fifth Edition

ISBN 7-111-15914-4

I. 初… II. 罗… III. 初等数论-英文 IV. O156.1

中国版本图书馆CIP数据核字（2004）第141001号

机械工业出版社（北京市西城区百万庄大街22号　邮政编码　100037）

责任编辑：迟振春

北京中兴印刷有限公司印刷·新华书店北京发行所发行

2005年3月第1版第1次印刷

787mm×1092mm 1/16·46.25印张

印数：0 001-3 000册

定价：69.00元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

本社购书热线：（010）68326294

List of Symbols

$[x]$	Greatest integer, 7
$\sum$	Summation, 16
$\prod$	Product, 20
$n!$	Factorial, 20
f_n	Fibonacci number, 30
$a \mid b$	Divides, 37
$a \nmid b$	Does not divide, 37
$(a_k a_{k-1} \ldots a_1 a_0)_b$	Base b expansion, 46
$O(f)$	Big-O notation, 60
$\pi(x)$	Number of primes, 71
$f(x) \sim g(x)$	Asymptotic to, 79
(a, b)	Greatest common divisor, 90
$(a_1 a_2, \ldots, a_n)$	Greatest common divisor (of n integers), 94
$\mathcal{F}_n$	Farey series of order n, 96
$[a, b]$	Least common multiple, 112
$\min(x, y)$	Minimum, 111
$\max(x, y)$	Maximum, 112
$p^a \parallel n$	Exactly divides, 117
$[a_1, a_2, \ldots, a_n]$	Least common multiple (of n integers), 120
F_n	Fermat number, 128
$a \equiv b \pmod{m}$	Congruent, 142
$a \not\equiv b \pmod{m}$	Incongruent, 142
$\overline{a}$	Inverse, 155
$\mathbf{A} \equiv \mathbf{B} \pmod{m}$	Congruent (matrices), 177
$\overline{\mathbf{A}}$	Inverse (of matrix), 178
$\mathbf{I}$	Identity matrix, 178

$\mathrm{adj}(\mathbf{A})$	Adjoint, 180
$h(k)$	Hashing function, 203
$\phi(n)$	Euler's phi-function, 233
$\sum_{d\|n}$	Summatory function, 243
$f * g$	Dirichlet product, 247
$\lambda(n)$	Liouville's function, 247
$\sigma(n)$	Sum of divisors functions, 250
$\tau(n)$	Number of divisors function, 250
M_n	Mersenne number, 258
$\mu(n)$	Möbius function, 270
$E_k(P)$	Enciphering transformation, 278
$D_k(P)$	Deciphering transformation, 278
$\mathcal{K}$	Keyspace, 278
$\mathrm{ord}_m(a)$	Order of a modulo m, 334
$\mathrm{ind}_r(a)$	Index of a to the base r, 355
$\lambda(n)$	Minimal universal exponent, 372
$\lambda_0(n)$	Maximal ± 1–exponent, 394
$\left(\frac{a}{p}\right)$	Legendre symbol, 404
$\left(\frac{a}{n}\right)$	Jacobi symbol, 430
$(.c_1c_2c_3\ldots)_b$	Base b expansion, 457
$(.c_1\ldots c_{n-1}\overline{c_n\ldots c_{n+k-1}})_b$	Periodic base b expansion, 460
$[a_0; a_1, a_2, \ldots, a_n]$	Finite simple continued fraction, 469
$C_k = p_k/q_k$	Convergent of a continued fraction, 471
$[a_0; a_1, a_2, \ldots]$	Infinite simple continued fraction, 478
$[a_0; a_1, \ldots, a_{N-1}, \overline{a_N, \ldots, a_{N+k-1}}]$	Periodic continued fraction, 490
α'	Conjugate, 492
$N(z)$	Norm of complex number, 548
$\overline{z}$	Complex conjugate, 548
$\binom{m}{k}$	Binomial coefficient, 581

前　言

自古（姑且说1975年以前）数论拥有数学最纯粹部分的美称. 人们之所以研究数论，是因为它历史悠久且硕果累累，也因为它有大量易于理解而令人着迷的问题，更因为它富于智慧的魅力. 但是前些年人们已经从新的角度来审视数论了. 今天人们研究数论既出于传统的原因，又出于数论已成为密码学的基础这一引人注目的理由. 本书第1版是将初等数论的现代应用与传统主题相结合的最早的教材，第5版延续了原先版本的基本思路. 还没有其他的教材像本书一样以如此深思熟虑的方式介绍初等数论及其应用，使用本书的教师将会惊喜地看到现代的应用是怎样天衣无缝地融入到数论课程中去的.

本书是为大学本科的数论课程而写的，适用于任何年级. 除了一定的数学素养外，本书的大部分材料不需要什么预备知识. 本书既可以作为计算机科学课程的有益补充，也可以作为有兴趣学习数论和密码学新进展的读者的初级读物.

第5版保持了先前版本的长处，并加以充实、改进. 熟悉先前版本的教师对这个新版本也会感到满意. 初次使用本书的教师则会看到这样一本最新的教材，其中将跨越几千年的数论精华与最近不到十年的新进展加以整合. 熟悉先前版本的读者将会发现新版本变得更具柔性且更易于教学，也更加有趣和引人注目，他们还将发现对于数论成果的历史沿革及数论的实验方面的额外关注.

第5版的变化

应读者和审阅人的要求，新版本进行了多方面改进. 新版本应该更易于教学，更易于阅读，也更有趣和更有参考价值. 新版本更有效地表达了数论的数学美和它的应用价值. 值得注意的变化包括：

- **更具有柔性的题材组织**

第4版的1.1节分成了较短的两节. 1.1节包括数和数列的类型，并介绍Diophantine逼近. 1.2节包括求和与求积. 如果认为没有必要，教师可以略去这两节的大部分内容，不过很多人可能会选用关于Diophantine逼近的材料. 第4版的3.1节也分成了两节. 3.1节介绍素数，证明素数有无穷多个，并讨论如何寻找素数. 3.2节讨论素数的分布，并介绍素数定理及许多关于素数的猜想.

- **扩充了与密码学有关的内容**

通过引进Kasiski测试和重合指标，加进Vigènere密码分析，提到包括AES加密标准在内的新近的密码学进展，描述了对RSA密码体制实施攻击的方法. 第12章通过使用Diophantine逼近利用连分数的概念开发了这类攻击中的一种方法，在习题中指出了推荐的零知识证明方案的缺陷.

• **新近的发现**

数论的最新发现在教材中得到了反映，其中包括一批理论上的发现以及关于证明一个整数是素数的多项式时间算法的讨论，还有关于Catalan猜想的结论．计算方面的发现也加进教材中，例如三个新的Mersenne素数．本书的网站将特别重视数论方面的最新新闻，并提供本书出版之后新发现的种种链接．

• **新的和扩充的论题**

1.1节介绍了Diophantine逼近的内容，加入了有理数逼近实数的Dirichlet定理，给出了一个应用鸽巢原理的证明．完整论述超出初等数论范围的许多重要论题现在也得以讨论，目的是使学生对数论有一个比较全面的评价．出于类似的思考，对Diophantine方程的内容作了扩充．这一版包括对Beal猜想、Catalan猜想及其新近分析的简要讨论，还有对Fermat-Catalan猜想的讨论．对abc猜想也作了讨论，并说明如何用它来证明一些关于Diophantine方程的结果．

增加了关于Gauss整数的新的一章．这一章介绍Gauss素数、Gauss整数的最大公约数、Gauss整数的Euclid算法（辗转相除法）以及Gauss整数分解成Gauss素数的唯一性．这新的一章还阐明怎样用Gauss整数求正整数表示为两整数平方和的方案数．

• **改进了例题和证明**

这一版给出了Euclid关于存在无穷多素数的证明．一大批素数无穷多的其他证明可在习题中找到．很多证明作了改进，其中包括简化或补充论证．

• **加强了习题**

本书以其别具一格的习题而久负盛名，这一版的习题更为出色．书中全部习题已作过检查和求解；在第4版中发现的题义含糊或者条件缺失的习题得以澄清．

加入了几百道新的习题．补充了涉及Fibonacci恒等式的习题．新增的习题用不同方法证明存在无穷多素数．新增了许多与密码学有关的习题，其中不少涉及Vigènere密码和RSA密码系统．在一道习题中简述了二次互反率的最新证明．还新添了更多有关非线性Diophantine方程（如Bachet方程、Markov方程和同余数）的习题．

• **扩充了历史沿革的叙述和人物传记**

Riemann假设的历史和现状包含在这一版内．对Skewes常数作了介绍，这是在一个数学证明中出现的最大数字之一．增加了关于Thomas Nicely发现奔腾芯片著名的除法缺陷的报道，这一发现是由于涉及孪生素数的两次计算不一致而引起的．这一版增加了很多新的人物传记，包括Bertrand、Farey、Waring、Bachet、Kronecker、Levi ben Gerson和Catalan等．人物传记中添加了照片．

• **对数学软件Maple和Mathematica的支持**

用Gauss整数进行计算的指令已增添到附录中，在这个附录中描述了用数学软件Maple和Mathematica进行数论计算的指令．

• **对正确性的格外关注**

这一版得益于为确保教材的正文、习题和解答的正确性而格外进行的工作，三位精心的校对费时多日以使本书尽可能避免差错．

• **扩充了网站**

本书的网站通过多种重要途径加以扩充和增强．“数论新闻”是一个特别关注数论新近发

现的新专栏．与本书相关的包罗甚广的数论网站表已得到扩充，所有链接都已更新．这些链接将在这一版的生存期内定期更新．该网站现在还支持收罗广泛的数论与密码学的应用小程序集，这些小程序可用于相关计算和探索，该网站也支持关于PARI/GP的辅导，PARI/GP是一个用于快速数论计算的计算系统，这些应用小程序建立在这个系统之上．推荐用于学生小组或个人的题目库也可在该网站找到．

本书特色

• 经典数论的发展

本书的核心是以一种有助于理解和引人入胜的方式阐述经典初等数论，关键结果的史料和重要性得到记述．在精心开展每个论题的基本材料之后，接着论述同一论题更复杂的结果．

• 突出应用

本书的主要长处是包括了数论的种种应用．一旦需要的理论得以建立，应用就以灵活的方式编入教材．应用设计成有助于促进理论的扩展和阐明初等数论在不同方面的用处．数论广泛应用于密码学，经典密码、分组密码及序列密码、公钥密码系统和密码协议都被包括在内．对计算机科学的其他应用包括整数的快速乘法、伪随机数及校验数字．对于许多其他领域的应用，例如调度、电话、昆虫学和动物学，也可在教材中找到．

• 一体化的论题

取自初等数论的很多概念都被用于素性测试和因数分解．进而，素性测试和因数分解又在数论对于密码学的应用中起着关键作用．正是如此，这些主题作为一体化的论题而被反复论述．几乎每一章都包括涉及这些主题的材料．

• 易于入门

本书被设计成只需最低限度的预备知识．本书几乎是完全自足的，只需具备通常称为“大学代数”的知识．只有几处用到了一些微积分的概念（例如讨论素数分布及大O符号），少数几处用到离散数学及线性代数的概念．所有依赖于高出大学代数论题的内容都明确注明并且都是可选的．

• 准确性

已付出极大的努力以保证这一版的准确性．来自本书第4版的许多读者、审阅人及校对的意见帮助我们实现了这一目标．

• 收入习题广博

学习数学的最佳途径（也许是唯一途径）就是做习题．本教材包括极为广泛和多种多样的习题．收入许多常规习题是为了训练基本技能，已注意将带有奇数编号的和偶数编号的两种习题包含在这一类题中．大量中等难度的题有助于学生把若干概念结合起来形成新的结果．许多其他习题或习题组则是为发展新概念而设计的．具有挑战性的习题也是充足的，用单星号（*）表示难题，双星号（**）表示很难的题．有些题包含以后正文中要用到的结果，这些题用手指符号（☞）表示．这样的习题教师在适当的时候应尽可能布置．

提供了广泛的上机作业．每一节都包括借助于数学软件Maple、Mathematica或由学生或教

师自编的计算程序可以完成的计算和探索问题. 这类常规的习题可使学生学会如何应用Maple或Mathematica的基本指令（在附录D中描述），而更多开放性的问题是为实验及激发创造性而设计的. 每节还包括一批编程作业，要由学生使用自己选择的程序设计语言来完成，可以用Maple和Mathematica中的语言，也可以用另外的语言.

• 习题答案

奇数编号的习题答案附于书末.

• 以经验为依据的发现

在本书的许多地方，考察数值凭据有助于促使关键结果的产生. 这种做法使学生有机会运用猜想，这正如当初人们在获得许多数论结果所做的那样.

• 广泛的例题

本书包括阐明每个重要概念的例题. 这些例题是为阐明书中的定义、算法和证明而设计的. 这些例题也用以帮助学生完成每节之后的习题.

• 注意诱导式的证明

书中的许多证明用例题作为诱导，在正式证明和说明证明的关键思想之前先用例题作为诱导. 证明本身则以仔细、严谨和完全明白的方式表述. 证明的设计使学生对每一步和整个推理过程都能理解. 经常在正式证明之前给出说明证明步骤的数值例题.

• 关于算法的推导

有关初等数论算法的方方面面贯穿本书始终. 不仅描述算法，而且对其复杂性加以分析. 在本书描述的算法中，有多种计算最大公约数、素性测试和因数分解的算法. 本书包含算法复杂性的讨论，教师在自己的课程中可以随意取舍.

• 人物传记和历史注释

这一版包括60多位对数论有贡献的数学家的传记. 这些有贡献的人包括古代的、中世纪的、16至18世纪的、19世纪的和20世纪的，既有东方的，也有西方的. 编写这些传记是为了让学生们对这些有卓越贡献的人作出正确的评价，他们往往引领了（乃至仍然引领着）有趣的研究方向.

• 未解决的问题

数论中未解决的问题在书中随处可见，有些在正文中，另一些则在习题中. 这些问题表明数论是一门仍在向前发展的学科. 读者应当认识到试图解决这些难题往往可能耗费大量时日而徒劳无功. 然而，如果其中某些问题在未来几年仍得不到解决，人们还是会感到惊奇.

• 最新的内容

书中包括数论的最新发现. 描述了许多未解决问题的现状，例如新的理论成果. 2004年9月关于素数和因数分解的新发现已列入这一版的第一次印刷之中. 这些发现将有助于读者理解数论是一个极为活跃的研究领域. 他们可以看到甚至他们自己有可能参与发现新的素数.

• 参考文献

本书提供了内容广泛的参考文献目录. 这个目录列出主要的已出版的数论资源，包括书籍和论文. 开列了很多有用的教材，诸如论述数论史的著作和数论方方面面的专著. 包含许多原始文献，例如有关密码学的资料.

• 数学软件Maple和Mathematica的支持

本书提供了一个附录，其中列出Maple 和Mathematica用于数论计算的命令. 这些命令是按

照有关章节中的内容列出的.

• **网络资源**

本书的网站包括与本书相关的数论的网络指南以及一大批其他资源. 访问本网站请进入www.awlonline.com/rosen. 为了方便起见, 最重要的数论网站都在附录D中重点列出.

• **表格**

包含帮助学生进行计算和实验的5个表格, 查看这些表格能帮助学生探寻建立相关模式及公式的猜想. 当这些表格不够用时, 建议使用诸如数学软件Maple和Mathematica这样的计算软件包.

• **符号表**

本书使用的符号表及对应定义的页码列于文前.

辅助材料

• **网站**

本书网站包含一大批与数论有关的网站的指南, 提供带有注释的链接. 这些网站与书中进行相关材料讨论的页面联系在一起, 具体位置在书中用符号()标出. 网站还包括显示数论方面最新发现的一部分, 同时也提供广泛的数论和密码学的应用小程序.

如何使用本书

本书的编排极具灵活性. 对于一门数论课程, 基本的核心材料可以包括: 讨论整数的除法的1.5节, 讨论素数、因数分解与最大公约数的第3章, 讨论同余式的4.1节~4.3节, 介绍Fermat小定理等重要同余式的第6章. 教师可选择其他内容对核心材料加以补充来设计自己的课程. 为了帮助教师选择课程所包含的章节, 将本书的不同部分概述如下:

1.1节~1.4节的材料是可选的. 1.1节介绍整数的不同类型、整数数列与可数性. 这一节还介绍Diophantine逼近的概念. 1.2节可帮助有需求的学生复习求和与求积. 1.3节介绍数学归纳法, 这些内容学生可能已在别处学习过了. (关于整数公理与二项式定理的材料可在附录中找到.) 1.4节介绍Fibonacci数, 这是许多教师喜爱的论题, 学生可能在一门离散数学的课程中学过这种数. 如前所述, 1.5节阐述关于整数除法的核心材料, 应当采用.

第2章是可选的, 包括以b为基的整数表示、整数的算术运算与整数运算的复杂性. 2.3节引入大O符号. 对于以前还未在别处见过这个符号的学生, 这是很重要的, 尤其是当教师要着重讲述数论中的计算复杂性的时候.

如前所述, 第3章及4.1节~4.3节讲述核心材料. 4.4节讨论的以素数幂为模的多项式同余方程的解法是可选的, 不过对发展p进数理论是很重要的. 4.5节需要一些线性代数的背景知识, 这一节的材料在8.2节用到, 若不需要这几节可省略. 4.6节介绍一种特殊的因数分解方法(Pollard rho方法), 也可省略.

第5章是可选的. 教师可从多种数论的应用中选讲一些. 5.1节介绍可除性判定; 5.2节包括万年历; 5.3节讨论循环赛的轮次安排; 5.4节说明怎样将同余式用于散列函数; 5.5节描述如何寻找和使用数字串错误中的检查数字.

第7章包括积性函数．7.1节应予采用，介绍积性函数的基本概念并研究Euler ϕ函数．因数和及因数的个数函数在7.2节讨论，这一节推荐所有教师采用．所有教师大概都会采用7.3节，这一节介绍完全数的概念并描述如何寻找Mersenne素数．

第8章包括数论在密码学中的应用．竭力推荐这一论题，因为这很重要，并且学生也会发现它极为有趣．8.1节介绍这门学科的基本术语以及一些经典的字符密码，计划在课程中包括密码学内容的教师应确信采用这一节材料的必要性．8.2节介绍分组与序列密码，这是两类重要的密码，并且给出这两类密码基于数论的例子．8.3节包括基于模幂运算的特殊类型的分组密码．8.4节应为所有的教师采用，这一节介绍公钥密码的基本概念，并用RSA密码系统加以说明．8.5节讨论背包密码，这一节是可选的．8.6节提供关于密码协议的导引，向对现代密码学的应用感兴趣的教师竭力推荐这一节．（密码学的其他论题包含在第9~11章内．）

第9章涉及整数的阶、原根及指标算术等概念．9.1节~9.4节在可能的情况下应予采用．9.5节讨论如何将这一章的概念用于素性测试，并论述Fermat小定理的部分逆命题．9.6节讨论通用指数，是可选的，这一节包括一些关于Carmichael数的有趣结果．

第10章介绍一些使用第9章材料的应用．这一章包括讨论伪随机数、ElGamal密码系统以及电话电缆连接方案的三节，这些材料是可选的．强调密码学应用的教师会特别愿意采用10.2节．

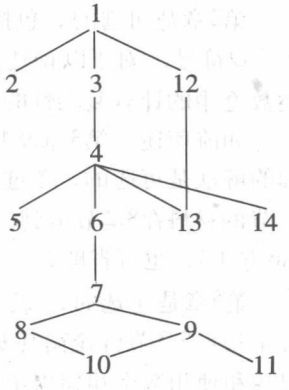
11.1节及11.2节包括二次剩余及二次互反律，这是数论的一个主要结果，只要可能就应采用．11.3节及11.4节讨论Jacobi符号与Euler伪素数，是可选的．11.5节包括零知识证明，对密码学感兴趣的教师只要有可能就会采用这一节．

12.1节包括十进制小数，会被很多教师所采用．对连分数有兴趣的教师会采用12.2节~12.4节，这几节建立了关于有限连分数与循环连分数的基本结果．12.5节讨论用连分数进行因数分解，是可选的．

大部分教师会采用13.1节及13.2节，这两节分别讨论Pythagoras三元组及Fermat大定理．13.3节包括平方和，13.4节讨论Pell方程的解及用连分数求解，这两节是可选的．

第14章是可选的，这一章包括Gauss整数．这种数的许多与整数相似的性质在这一章阐述．特别是，引入Gauss素数和建立Gauss整数分解唯一性的结论．最后，使用Gauss整数可得到一正整数表示为两整数平方和的方案数．

右图表示各章之间的依赖关系，可帮助教师计划课程．虽然第2章在不需要时可省略，但其中清楚说明了描述算法复杂性的贯穿全书的大O符号．除了定理12.4依赖于第9章的材料外，如图所示，第12章只依赖于第1章．在第13章中只有13.4节依赖于第12章．如果9.1节中有关原根的可选注释被略去，则可以采用第11章而不采用第9章．14.3节可以与13.3节一同采用．



致谢

我要对我在AT&T实验室的管理同仁表示感谢，他们对这一版的准备工作给予了大力支持，并提供了一种富于激励性的专

业环境．特别要感谢Bart Goddard，他为本书准备了辅助材料，并要特别感谢Douglas Eubert、Tom Wegleitner和Steve Whalen，他们协助审阅手稿以保证正确性，并对习题求解提供帮助以及反复核对习题的答案和求解．

感谢本版编辑Bill Hoffman的支持，感谢本书前几版的Addison-Wesley公司的编辑们，特别需要提到Wayne Yuhasz和Jeff Pepper，他们对本书的原始概念深表赞同并认识到本书的潜在魅力，而在当时其出版商都认为数论已是一门失去生命力的课程，毫无出版新书的价值．我还要感谢本书幕后的整个编辑、印制、营销和媒体团队，他们是Mary Reynolds、Julie LaChance、Jeffrey Holcomb、Barbara Atkinson、Beth Anderson、Barbara Pendergast、Paul Anagnostopoulos、Emily Portwood、Lynne Blaszak、Greg Tobin和Phyllis Hubbard．我同样对David Wright表示感谢，他对本书网站作出多方面的贡献，包括有关PARI/GP的材料、数论和密码学的应用小程序以及推荐的作业．

我从本书前几版读者的深思熟虑的评论和建议中受益匪浅，他们的许多思想已体现在这一版中．

我对下列审阅人在本版的准备过程中提供的帮助深表谢意：

Ruth Berger, 路德学院

Joel Cohen, 马里兰大学

Michael Cullinane, Keene 州立大学

Mark Dickinson, 密歇根大学

George Greaves, 加的夫大学

Kerry Jones, 保尔州立大学

Slawomir Klimek, 印地安那大学－普度大学印地安那波利斯分校

Stephen Kudla, 马里兰大学

Jennifer McNulty, 蒙大拿大学

Stephen Miller, 拉特格大学

Michael Mossinghoff, Davidson 学院

Michael E. O'sullivan, 圣迭哥州立大学

Gary Towsley, 纽约州立大学 Geneseo 分校

David Wright, 俄克拉何马州立大学

我还要再次感谢本书前几版的审阅人，他们帮助一版一版地改进本书，对他们一次又一次参与本书的审阅我会铭记在心．他们是：

David Bressoud, 宾夕法尼亚州立大学

Sydney Bulman-Fleming, Wilfred Laurier 大学

Richard Bumby, 拉特格大学

Charles Cook, 南卡罗来那大学Sumter分校

Christopher Cotter, 北科罗拉多大学

Euda Dean, Tarleton 州立大学

Daniel Drucker, 韦恩州立大学

Bob Gold, 俄亥俄州立大学
Fernando Gouvea, 库尔比学院
Jennifer Johnson, 犹他大学
Roy Jordan, Monmouth 学院
Herbert Kasube, 布拉德雷大学
Neil Koblitz, 华盛顿大学
Steven Leonhardi, Winona 州立大学
Charles Lewis, Monmouth 学院
James McKay, 奥克兰大学
John Mairhuber, Maine-Orono大学
Alexsandrs Mihailovs, 宾夕法尼亚大学
Rudolf Najar, 加州州立大学Fresno分校
Carl Pomerance, 乔治亚大学
Sinai Robins, 神学院
Tom Shemanske, 达特茅斯学院
Leslie Vaaler, 得克萨斯大学奥斯汀分校
Evelyn Bender Vaskas, 克拉克大学
Samuel Wagstaff, 普度大学
Edward Wang, Wilfred Laurier 大学
Betsey Whitman, Framingham 州立大学
David Wright, 俄克拉何马州立大学
Paul Zwier, 卡尔文学院

最后，我要提前感谢未来对我提出建议和更正意见的诸位．您可把这样的材料按照Addison-Wesley的电子邮件地址math@awl.com发送给我．

肯尼斯 H.罗森
于新泽西州米德尔顿

Contents