华章数学译丛

HZ BOOKS
华章教育

42

PEARSON
Addison Wesley

Elementary Number Theory and Its Applications
(Fifth Edition)

初等数论及其应用
（原书第5版）

（美）Kenneth H. Rosen 著

夏鸿刚 译

机械工业出版社
China Machine Press

华 章 数 学 译 丛

42

Elementary Number Theory and Its Applications
(Fifth Edition)

初等数论及其应用
（原书第5版）

(美) Kenneth H. Rosen 著
夏鸿刚 译

机械工业出版社
China Machine Press

本书以经典理论与现代应用相结合的方式介绍了初等数论的基本概念和方法，内容包括整除、同余、二次剩余、原根以及整数的阶的讨论和计算. 此外，书中附有60多位对数论有贡献的数学家的传略.

本书内容丰富，趣味性强，条理清晰，既可以作为高等院校计算机及相关专业的数论教材，也可以作为对数论和密码学感兴趣的读者的初级读物.

本书版权登记号：图字：01-2005-0901

图书在版编目（CIP）数据

初等数论及其应用（原书第5版）/（美）罗森（Rosen, K. H.）著；夏鸿刚译. —北京：机械工业出版社，2009.6

（华章数学译丛）

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

ISBN 978-7-111-26520-7

Ⅰ. 初… Ⅱ. ①罗… ②夏… Ⅲ. 初等数论 Ⅳ. O156.1

中国版本图书馆CIP数据核字（2009）第031376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

北京瑞德印刷有限公司印刷

2009年6月第1版第1次印刷

186mm×240mm · 30.25印张

标准书号：ISBN 978-7-111-26520-7

定价：68.00元

凡购本书，如有倒页、脱页、缺页，由本社发行部调换

本社购书热线：（010）68326294

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，适用于任何水平. 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将会乐于使用这个新版本. 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. 熟悉先前版本的教师将会发现新版本变得更灵活且更易于教学，也更加有趣和引人入胜，他们还将发现对于数论成果的历史渊源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，也更有趣和令人大开眼界. 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：

• 更灵活的题材组织

第 4 版的 1.1 节分成了较短的两节. 1.1 节涵盖了数和序列，并介绍丢番图逼近. 1.2 节涵盖了和与积. 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丢番图逼近的材料. 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

通过引进卡西斯基测试和重合次数，加进维吉尼亚密码分析，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 密码系统实施攻击的方法. 第 12 章通过使用来自用连分数的丢番图逼近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.

• 最新发现

数论的最新发现在本书中得到了反映，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，还有关于卡塔兰猜想的结论．计算方面的发现也加进书中，例如三个新的梅森素数．本书的网站特别重视数论方面的最新结果，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 节介绍了丢番图逼近的内容，加入了有理数逼近实数的狄利克雷定理，给出了一个应用鸽巢原理的证明．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，对丢番图方程的内容作了扩充．这一版包括对比尔猜想、卡塔兰猜想及其新近分析的简要讨论，还有对费马－卡塔兰猜想的讨论．对 *abc* 猜想也作了讨论，并说明如何用它来证明一些关于丢番图方程的结果．

增加了关于高斯整数的新的一章．这一章介绍高斯素数、高斯整数的最大公因子、高斯整数的欧几里得算法(辗转相除法)以及高斯整数分解成高斯素数的唯一性．这新的一章还阐明怎样用高斯整数求把正整数表示为两个整数的平方和有多少方式．

● 改进了例题和证明

这一版给出了欧几里得关于存在无穷多素数的证明．许多关于无穷多素数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说明．

● 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 版中发现的题意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．补充了涉及斐波那契恒等式的习题．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，其中不少涉及维吉尼亚密码和 RSA 密码系统．在一道习题中简述了二次互反律的最新证明．还新添了更多有关非线性丢番图方程(如巴舍方程、马尔可夫方程和同余数)的习题．

● 扩充了历史渊源的叙述和人物传记

黎曼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，包括伯特兰、费瑞、华林、巴舍、克罗内克、莱维本热尔松和卡塔兰等．人物传记中添加了照片．

● 增强了对数学软件 Maple 和 Mathematica 的辅助读物和支持

用高斯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使本书尽可能避免差错．

● 扩充了网站内容

本书的网站(www. awlonline. com/rosen)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本书. 应用设计成有助于扩展理论的应用范围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、分组密码及流密码、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、伪随机数及校验位. 对于许多其他领域的应用，例如调度、电话、昆虫学和动物学，也可在书中找到.

• 一体化的论题

取自初等数论的很多概念都被用于素性检验和因数分解. 进而，素性检验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. 所有依赖于超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

已付出极大的努力来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. 对这样的习题，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 或者由学生或

教师自编的计算程序可以完成的计算和研究问题，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．每节还包括一些程序设计题，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，也可以用另外的语言．

• 习题答案

奇数编号的习题答案请从本书网站下载．

• 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时所做的那样．

• 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，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，有多种计算最大公因子、素性检验和因数分解的算法．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．编写传记是为了让学生对这些有卓越贡献的人作出正确的评价，他们往往引领了(甚至仍然引领着)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，他们甚至可以看到他们可能如何参与发现新的素数．

• 参考文献

本书提供了内容广泛的参考文献目录．这个目录列出已出版的主要数论资源，包括书籍和论文．其中有很多有用的教材，诸如论述数论史的著作和数论特定主题领域的专著．此外，包

含许多原始文献，例如有关密码学的资料.

• 对数学软件 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. 这些命令是按照本书使用命令的各章列出的.

• 网络资源

本书的网站(www. awlonline. com/rosen)包括与本书相关的数论内容以及一大批其他资源. 为了方便起见，最重要的数论网站都在附录 D 中列出.

• 表格

附录 E 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进行模式搜索和提出猜想. 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. 网站还包括显示数论方面最新发现的部分，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

本书的设计极其灵活. 对于一门数论课程，基本的核心材料可以包括：讨论整数的整除性的 1.5 节，讨论素数、因子分解与最大公因子的第 3 章，讨论同余的 4.1 ~ 4.3 节，介绍包含费马小定理的重要同余式的第 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 ~ 1.4 节的材料是可选的. 1.1 节介绍整数的不同类型、整数序列与可数性，还介绍丢番图逼近的概念. 1.2 节可帮助有需求的学生复习和与积. 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 节介绍斐波那契数，这是许多教师喜爱的论题，学生可能在离散数学的课程中学过. 如前所述，1.5 节阐述关于整数整除性的核心材料，应当采用.

第 2 章是可选的，包括以 b 为基的整数表示、整数的计算机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时.

如前所述，第 3 章及 4.1 ~ 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，若不需要这两节可省略．4.6节介绍一种特殊的因子分解方法(波拉德ρ方法)，也可省略．

第5章是可选的．教师可从数论的不同应用中选讲一些．5.1节介绍整除性检验；5.2节涉及万年历；5.3节讨论循环赛赛程安排；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校验位．正如前面提到的，第6章讲述核心材料．

第7章讨论乘性函数．7.1节应予采用，介绍乘性函数的基本概念并研究欧拉ϕ函数．因子和及因子个数的函数在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梅森素数．

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节介绍这个主题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务必要采用这一节．8.2节介绍分组与流密码，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节包括基于模取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、原根及指数的算术等概念．9.1～9.4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检验，并论述费马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卡迈克尔数的有趣结果．

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、埃尔伽莫密码系统以及电话线缆绞接方案的三节，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节讨论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节讨论雅可比符号与欧拉伪素数，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．

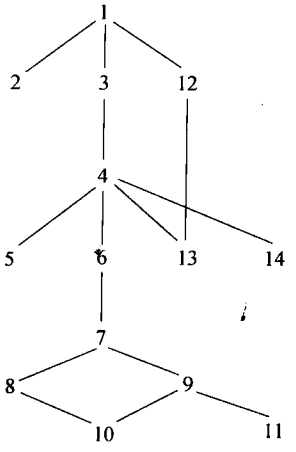
12.1节包括十进制分数，会被很多教师所采用．对连分数有兴趣的教师会采用12.2～12.4节，这几节建立了关于有限连分数与循环连分数的基本结果．12.5节讨论用连分数进行因子分解，是可选的．

大部分教师会采用13.1节及13.2节，这两节分别讨论毕达哥拉斯三元组及费马大定理．13.3节讨论平方和，13.4节讨论佩尔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，这一章包括高斯整数．这种数的许多与整数相似的性质在这一章阐述．特别是，引入高斯素数和证明高斯整数分解的唯一性．最后，使用高斯整数可得到把一个正整数表示为两个整数平方和的方式的数目．

下图表示各章之间的依赖关系，用于帮助教师规划课程．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，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.

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，他们对本书的初始思想深表赞同并认识到本书的潜在魅力，而在当时其他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，印第安纳大学 - 普度大学印第安纳波利斯分校
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'S ullivan，圣迭戈州立大学
David Wright，俄克拉何马州立大学
Gary Towsley，纽约州立大学 Geneseo 分校

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，南卡罗来纳大学 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．

Kenneth H. Rosen
于新泽西州米德尔顿

符 号 表

$[x]$	不超过 x 的最大整数，4
Σ	求和号，11
Π	连乘积，13
$n!$	阶乘，14
f_n	斐波那契数，22
$a \mid b$	整除，27
$a \nmid b$	不整除，27
$(a_k a_{k-1} \cdots a_1 a_0)_b$	b 进制展开，33
$O(f)$	大 O 符号，43
$\pi(x)$	素数的个数，52
$f(x) \sim g(x)$	渐近，近似于，58
(a, b)	最大公因子，66
$(a_1, a_2, \cdots, a_n)$	最大公因子(n 个整数)，69
$\mathscr{F}_n$	n 阶费瑞级数，70
$[a, b]$	最小公倍数，82
$\min(x, y)$	最小值，82
$\max(x, y)$	最大值，82
$p^a \parallel n$	$p^a \mid n$ 但是 $p^{a+1} \nmid n$，86
$[a_1, a_2, \cdots, a_n]$	最小公倍数(n 个整数)，88
F_n	费马数，94
$a \equiv b \pmod{m}$	同余，104
$a \not\equiv b \pmod{m}$	不同余，104
$\overline{a}$	逆，114
$\boldsymbol{A} \equiv \boldsymbol{B} \pmod{m}$	同余(矩阵)，130
$\overline{\boldsymbol{A}}$	逆(矩阵)，131
$\boldsymbol{I}$	单位矩阵，131
$\operatorname{adj}(\boldsymbol{A})$	伴随，132
$h(k)$	散列函数，148
$\phi(n)$	欧拉 ϕ 函数，171
$\sum_{d \mid n}$	对 n 的所有正因子 d 求和，177
$f * g$	狄利克雷积，180

目　录

何谓数论

关于数论流传着多种说法：成千上万的人们在网上研究共同关心的数论问题. PBS 电视系列节目 NOVA 报道了一个著名数论问题被解决的新闻. 人们研究数论是为了理解信息加密系统. 这门学问到底是什么？今天为何有那么多人对它感兴趣？

数论是数学的一个分支，研究一类特殊数的性质和相互关系. 在数论所研究的数当中，最重要的是正整数集合. 更具体地说，特别重要的是*素数*，即那些没有大于 1 并且小于自身的正因子的正整数. 数论的一个很重要的结果表明，素数是正整数的乘法结构的基石. 这个叫做*算术基本定理*的结果告诉我们，每个正整数可以按递增次序唯一地写成素数的乘积. 对于素数的兴趣要追溯到 2500 年前古希腊数学家的研究工作. 人们思考的第一个问题可能是：素数是否有无穷多个. 在《几何原本》(The Elements)中，古希腊数学家欧几里得(Euclid)对于素数的无穷性给出了证明. 17 和 18 世纪研究素数的热情之火被重新点燃，费马(Fermat)和欧拉(Euler)证明了许多重要结果，并且对素数的生成提出许多猜想. 素数的研究在 19 世纪取得重大进展，其结果包括：在等差数列中有无穷多素数，对不超过正数 x 的素数个数作了精细的估计等. 在 20 世纪发明了研究素数的许多有威力的技术方法，但是许多问题用这些方法仍不能解决. 比如说，一个未解决的问题是：孪生素数（即相差为 2 的两个素数）是否有无穷多对？下一个十年里肯定还会有新的结果，因为专家们仍在致力于研究与素数有关的许多未解问题.

现代数论的发展始于德国数学家高斯(Gauss)，他是历史上最伟大的数学家之一，在 19 世纪初期发明了同余的语言. 我们称两个整数 a 和 b 是模 m 同余的(其中 m 为正整数)，是指 m 整除 $a-b$. 这种语言使我们在研究整除性关系的时候，变得像研究方程那样容易. 高斯提出了数论中的许多重要概念. 例如，他证明了最具有智慧和美感的一个结果：*二次互反律*. 这个定律把素数 p 是否为模另一个素数 q 的完全平方与 q 是否为模 p 的完全平方联系起来. 高斯给出二次互反律的许多不同的证明，其中有些证明开启了数论的一些新领域.

将素数从合数中挑选出来是数论的一个关键问题. 这方面的工作发展出了大量的*素性检验法*. 最简单的素性检验是检查一个正整数是否被不超过此数平方根的每个素数所整除. 不幸的是，对于非常大的正整数，这个试验方法效率很低. 在 17 世纪，费马证明了：若 p 为素数，则 p 整除 2^p-2，一些数学家考虑反过来是否也对(即若 n 整除 2^n-2，则 n 为素数). 但是在 19 世纪初期人们找到反例：对于合成数 $n=341$，n 整除 2^n-2. 这样的正数叫做*伪素数*. 尽管存在伪素数，但是多数合数都不是伪素数，基于这个事实给出的素性检验现在仍可用来快速找到一些非常大的素数.

将正整数素因子分解是数论中的另一个核心问题. 可以用试除法把一个正整数分解，但是这种方法非常费时间. 费马、欧拉和许多其他数学家提出了一些富有想象力的分解算法，这些算法在过去的 25 年中扩展成一大批因子分解方法. 用目前已知的最先进技术，我们可以很容易找到几百位长的素数，但是要把同样长的整数因子分解，最快的计算机目前还不能胜任.

找出大素数和分解大数在时间上的强反差是当今一种非常重要的称为 RSA 密码系统的基

础. RSA 系统是一种公钥密码系统. 在些类系统中，每个用户有公私两把密钥. 每个用户可以用别人的公钥来加密信息，但只有拥有相应私钥的用户才能解密. 要明白 RSA 的工作机制就必须要懂得一些数论基础知识. 现代密码学的其他分支也要求这一点. 数论在密码学上的极端重要性推翻了早期许多数学家的看法，那就是数论在现实世界的应用中并不重要. 具有讽刺意味的是历史上的一些著名的数学家，像哈代(G. H. Hardy)还为数论没有像今天这样得到广泛应用而沾沾自喜.

寻求方程的整数解是数论的又一个重要内容. 一个方程若要求解为整数，则称为*丢番图方程*，以纪念古希腊数学家丢番图(Diophantus). 人们研究了许多不同类型的丢番图方程，其中最著名的是*费马方程* $x^n+y^n=z^n$. *费马大定理*说：若 n 是大于 2 的整数，这个方程没有整数解 (x, y, z)，这里 $xyz\neq 0$. 费马在 17 世纪猜想这个定理是对的. 在随后的 300 多年里数学家们(和其他人)一直在努力地寻求证明，直到 1995 年才由怀尔斯(Andre Wiles)给出第一个证明.

正像怀尔斯的证明中所显示的，数论不是一个静止的对象!新的发现不停地产生，研究人员经常得到重大的理论结果. 今天计算机联网所产生的巨大威力，使数论在计算方面大大提高了研究的步伐. 每个人都能加入到这项研究的队伍中. 比如说，你可以一起来寻找新的*梅森*(Mersenne)*素数*，即形为 2^p-1 的素数，这里 p 也是素数. 1999 年 6 月，第一个具有 100 万位的素数被发现，即梅森数 $2^{6\,972\,593}-1$，然后大家又致力于寻找多于 1000 万位的素数. 在学过本书的某些内容之后，你也能够决定是否涉猎于这项活动，使你的计算资源用于有益的事业.

何谓初等数论? 你可能会想，为什么书名上冠以“初等”二字. 这本书只考虑数论的一部分，即称为*初等数论*的那部分，它不依赖于诸如复变函数、抽象代数或者代数几何等高等数学. 有志继续学习数学的学生会学到数论的更高深领域，如解析数论(使用复变函数)和代数数论(用抽象代数的概念证明代数数域的有趣结果).

一些建议 在你开始学数论的时候，要记住数论是一个具有几千年历史的经典学科，也是很现代的学科，新的发现不断快速地涌现. 它是最富含人类智慧的一个纯数学分支，也是应用数学，在密码学和计算机科学以及电子工程方面有重要的应用. 我希望你能捕捉到数论的多种面孔，就像在你之前的许多数学迷那样，在离开学校之后仍旧对数论保持浓厚的兴趣.

动手实验是研究数论所不可缺少的部分. 本书的所有成果都是数学家们不断考察大量的数值计算现象，寻找规律并作出猜测而得到的. 他们拼命地工作以证明他们的猜测，一些猜想被证明而成为定理，另一些由于找到反例而被否定，还剩下一些未被解决. 在你学习数论的时候，我建议你要考察大量的例子，从中寻找规律，形成你自己的猜测. 这会帮助你学习这门学问，甚至你也会得到你自己的一些新结果.