华章数学译丛

55

Elementary Number Theory and Its Applications

(Sixth Edition)

初等数论及其应用

（原书第6版）

（美）Kenneth H. Rosen 著

夏鸿刚 译

机械工业出版社
China Machine Press

华 章 数 学

55

Elementary Number Theory and Its Applications

(Sixth Edition)

初等数论及其应用

（原书第6版）

（美）Kenneth H. Rosen 著

夏鸿刚 译

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

初等数论及其应用（原书第6版）/（美）罗森（Rosen，K. H.）著；夏鸿刚译．—北京：机械工业出版社，2015.2
（华章数学译丛）
书名原文：Elementary Number Theory and Its Applications, Sixth Edition

ISBN 978-7-111-48697-8

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（2014）第281426号

本书版权登记号：图字：01-2014-2864

本书以经典理论与现代应用相结合的方式介绍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．

出版发行：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　　责任校对：董纪丽
印　　刷：三河市宏图印务有限公司　　版　　次：2015年4月第1版第1次印刷
开　　本：186mm×240mm　1/16　　印　　张：31.25
书　　号：ISBN 978-7-111-48697-8　　定　　价：89.00元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88378991　88361066　　投稿热线：（010）88379604
购书热线：（010）68326294　88379649　68995259　　读者信箱：hzjsj@hzbook.com

前　言

我编著本书的目的是想写一本关于数论的入门级读物. 起初我的想法是制作一个教学上的有效工具，希望能展示数论这一数学分支中丰富的题材以及出乎意料的实用性. 数论既是经典的又是现代的，同时它既是理论化的又是实用化的. 在本书中，我力求抓住这一对立面，并最大限度地将它们糅合在一起.

本书是本科阶段理想的数论教材. 除了一些必要的数学素养和大学代数知识外不需要别的预备知识. 本书也可以作为初等数论的资料读物，既可作为计算机科学类课程的有益补充，也可作为有兴趣学习数论和密码学进展的读者的初级读物. 由于它的广泛性，它既可作为教科书，也可作为初等数论及其广泛应用的长期参考书.

本版的发行正好是庆祝该书的银质纪年. 在过去的25年里，前面的版本大约被十万名学生学习过. 本书每个成功的版本都得益于许多师生及审稿者的反馈与建议. 本次新版延续了前面版本的基本框架，但有许多补充与改进. 希望对本书不熟悉的教师或没有读过前面几版的读者仔细通读这一新的第6版，相信你们会喜欢本书中丰富的习题、有趣的人物传记和历史注记、最新进展的跟踪、缜密的证明、有用的例子、丰富的应用、对数学计算软件(例如 Maple 和 Mathematica)的支持以及网络上的大量资源.

第6版的变化

第6版的改动是为了使本书更易于教学和更有趣味性，以及尽可能及时更新诸多进展. 许多改动是应第5版的读者和审阅者的要求而进行的. 下面列出了本版的一些改动之处.

·新的发现

本版追踪了数值计算和理论证明这两方面的最新发现. 这其中包括四个新的梅森素数的发现以及许多未解决猜想的新证据，还有证明了任意长度的素数级数存在性的 Tao-Green 定理，这是本版收集的最新的理论证明方面的成果之一.

·人物传记和历史注记

我们在原来的丰富的人物传记基础上新添加了 Terence Tao(陶哲轩)、Etienne Bezout、Norman MacLeod Ferrers、Clifford Cocks 和 Waclaw Sierpiński 等人的小传，也增添了在 Rivest、Shamir、Adleman 等人的工作之前英国密码学上令人惊讶的秘密发现.

·猜想

新增了不少初等数论当中的猜想，特别是关于素数和丢番图方程的问题，这些问题中有的已经解决，而有的仍然悬而未决.

·组合数论

新增了一节关于拆分的介绍性内容，这是组合数论中很有意思的分支. 这一节中介绍了比较重要的概念，例如费勒斯图、拆分恒等式、拉马努扬在同余上的工作等. 在该节中，对于一些拆分恒等式，包括欧拉的重要工作，我们分别使用了母函数和建立双射对应来给出证明.

·同余数与椭圆曲线

新增了一节讲述鼎鼎有名的同余数问题，同余数问题是指判断哪些正整数是边长为有理数的三角形的面积. 该节有椭圆曲线的简单介绍以及如何将同余数问题和特定的椭圆曲线上的有理点联系起来的内容，同时也有将同余数问题与三平方算术级数联系在一起的内容.

·几何推导

本版介绍了利用几何推导来研究丢番图问题的方法. 特别地，新增内容表明了找出单位圆周上的有理点对应于找出毕达哥拉斯三元组，找出以指定整数为面积的有理三角形等价于找出相应的椭圆曲线上的有理点.

·密码学

本版删去了 RSA 密码系统中待加密明文需与密钥中模互素这一不必要的限制.

·最大公因子

最大公因子和两整数互素都在第 1 章中引入. 本书也引入了 Bezout 系数这一概念.

·雅可比符号

给出雅可比符号实用性的动机，特别是给出了利用雅可比符号来计算勒让德符号的讨论.

·改进的习题

对习题的改进我们做了大量的工作，添加了从一般性的到有挑战性的数百道新习题，而且在计算和研究部分也有新习题.

·准确性

为本书的准确性我们付出了不少努力. 两个独立的审阅者分别检查了全部正文以及习题答案.

·网站 www. pearsonhighered. com/rosen

本版的网站也进行了大幅扩充，师生们可以在此找到许多与本书关联的资料. 新内容包括扩充的小应用程序列表、使用数学软件研究数论的手册以及一个专门刊发数论新闻的网页.

习题部分

鉴于习题的重要性，我在修改习题上花费了大量的时间. 学生应该记住学习数学的最好方法就是尽可能地多做习题. 下面我将简短地介绍本书中习题的类型以及答案的出处.

·普通习题

一般性的习题按照适当的次序排序，着重于训练基本的技能，奇偶号习题都有这种类型的题目. 大量中等难度的习题帮助学生将诸多概念融合在一起得出新的结果，也有很多习题是为了发展一些新的概念.

·有难度的习题

本书中有不少具有挑战性的习题，用“*”标记的是较难的习题，用“**”标记的是很难的习题. 有些习题的结论在后面章节中会被用到，这些习题用手形“☞”标记，这部分习题应该在教师的指定下去尝试.

·习题答案

本书的后面提供了所有奇数号习题的答案[⊖]. 更完整的习题答案可在英文书网站上的"Student's Solutions Manual"部分找到. 所有答案都被多次检查以保证准确性.

·计算类习题

每节后附有计算和研究题，需要用诸如 Maple、Mathematica、PARI/GP 或者 Sage 之类的软件或学生自己编写的程序来完成. 有些常规的习题可以让学生熟悉一些基本的命令(附录 D 中有关于 Maple、Mathemaica 的命令，PARI/GP 和 Sage 的命令可在英文书网站上找到)，而更多开放性的习题是为实验和激发创造性而设计的. 每节后还附有程序设计题，学生可以选用一种编程语言或一种程序来完成. 英文书网站上的"Student's Manual to Computations and Explorations"部分提供了答案或提示以帮助学生完成这些习题.

网站

学生和教师可以在 www.pearsonhighered.com/rosen 上找到各种类型的资源. 在 www.pearsonhighered.com/irc 上可以找到专门为教师提供的资源，这些资源的获取需要从 Pearson 那里获取密码.

·外部链接

该网站列有到许多与数论相关的网站的带说明的链接. 这些网站与书中相关材料的讨论关系密切. 附录 D 中列出了与数论相关的最重要的一些网址.

·数论新闻

该网站有一个专门刊登最新数论发现的页面.

·学生解题手册

学生解题手册包含所有奇数号习题的答案以及试题样本.

·学生计算和研究题手册

该手册为计算和研究题提供帮助，对此类习题提供完全或部分答案，或者给出提示. 该手册在不同程度上支持各种计算平台，包括 Maple、Mathematica 以及 PARI/GP.

·应用小程序

该网站上有大量的应用小程序. 学生可以利用这些程序来进行数论上一般性的计算以及加深对概念的理解和研究未解决的猜想. 除了数论中的计算性算法程序外，我们也提供了密码学上的应用小程序，包括解密、加密、密码分析以及密码协议，兼顾了经典密码和 RSA 密码系统. 这些密码学上的应用小程序可被个人或组织使用，也可用于教学.

·建议性项目

该网站上有一批建议性项目，这些项目可用于学生或是学生小组的期末作业.

·教师手册

含有所有习题的答案，包括偶数号习题，也有大量不对学生开放的各种资源，包括课程表样本、课程范围的建议以及试题库等.

⊖ 限于篇幅，习题答案未出现在中文版中，有需要者可从华章网站(www.hzbook.com)下载. ——编辑注

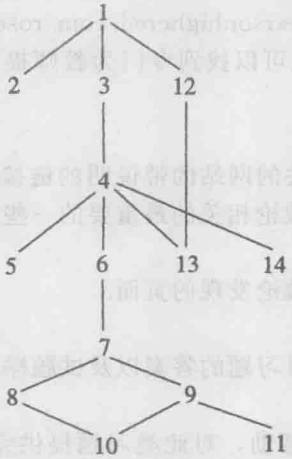
如何使用本书

本书可用作侧重点不同的各种级别的初等数论课程的教科书. 因此，教师用本书来安排课程有相当大的自由度. 对多数教师而言，第 1 章、2.1 节、第 3 章、4.1～4.3 节、第 6 章、7.1～7.3 节、9.1～9.2 节的主要内容是必需的.

教师可以用感兴趣的部分来充实自己的课程表. 一般而言，所有内容可粗略分为理论性和应用性两部分. 理论性部分有莫比乌斯反演(7.4 节)、整数的拆分(7.5 节)、原根(第 9 章)、连分数(第 12 章)、丢番图方程(第 13 章)、高斯整数(第 14 章)等.

有些教师也许想加入一些易于接受的应用，例如整除性检验、万年历、校验位(第 5 章). 而想侧重计算机应用和密码学的教师可以加入第 2 章和第 8 章，也可继续加入 9.3 节、9.4 节、第 10 章、11.5 节等.

在选好想要讲授的章节后，教师可参考下图所示的各章间的依赖关系：



虽然第 2 章在不需要时可省略，但其中解释了描述算法复杂度的贯穿全书的大 O 符号. 除了定理 12.4 依赖于第 9 章的内容外，第 12 章只依赖于第 1 章. 第 13 章中只有 13.4 节依赖于第 12 章. 若 9.1 节中有关原根的可选注释被略去，则可以不用学完第 9 章而学习第 11 章. 14.3 节应与 13.3 节一同被采用.

此外，教师可参阅网站上教师手册中侧重点不同的课程表.

致谢

感谢 Pearson 和 Addison-Wesley 的编辑 Bill Hoffman 和 Pearson 数学分部的主任 Greg Tobin 一如既往的热情支持，Bill Hoffman 是我在 Pearson 合作最多的编辑. 特别感谢我的助理编辑 Caroline Celano，在她的协助下本版得以出版. 感谢本书幕后的整个编辑、生产、营销和媒体团队，他们是 Pearson 的 Beth Houston(生产项目经理)、Maureen Raymond(插图编辑)、Carl Cottrell(媒体设计师)、Jeff Weidenaar(市场营销经理)、Kendra Bassi(营销助理)、Beth Paquin(设计师)以及 Windfall Software 的 Paul Anagnostopoulos(项目经理)、Jacqui Scarlott(排版)、Rick Camp(文字编辑和校对)、Laurel Muller(美工).

再次感谢为本书前五版提供支持的所有人，包括以前 Addison-Wesley 的许多编辑以及 AT&T 贝尔实验室的管理层(以及相关人员).

特别感谢 Bart Goddard，本书所有习题的答案均由他给出，同时他也审阅了本书. 感谢 Jean-Claude Evard 和 Roger Lipsett 一遍遍地检查了全部手稿，包括习题的答案. 感谢 David Wright 对本书网站所做的贡献，包括关于 PARI/GP 的材料、数论和密码学上的应用小程序、计算和研究手册和建议的作业. 感谢 Larry Washington 和 Keith Conrad 在同余数及椭圆曲线方面的建议.

审阅人

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，他们的许多想法已体现在这一版中. 在此特别感谢为第 6 版提供帮助的审阅人：

Jennifer Beineke，西部新英格兰学院
David Bradley，缅因-阿让诺大学
Flavia Colonna，乔治梅森大学
Keith Conrad，康涅狄格大学
Pavel Guerzhoy，夏威夷大学
Paul E. Gunnells，马萨诸塞大学阿默斯特分校
Charles Parry，弗吉尼亚理工学院和州立大学
Holly Swisher，俄勒冈州立大学
Lawrence Sze，加州理工大学 Pomona 分校

在此也感谢前几版的大约 50 位审阅人，他们一直为改进本书提供着帮助. 最后，提前感谢以后给我发送建议和勘误的读者，相关内容可由 math@pearson.com 转发给我.

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
$\sum$	求和号
$\prod$	连乘积
$n!$	阶乘
f_n	斐波那契数
$a \mid b$	整除
$a \nmid b$	不整除
(a, b)	最大公因子
$(a_k a_{k-1} \cdots a_1 a_0)_b$	b 进制展开
$O(f)$	大 O 符号
$\pi(x)$	素数的个数
$f(x) \sim g(x)$	渐近，近似于
$(a_1, a_2, \cdots, a_n)$	最大公因子(n 个整数)
$\mathscr{F}_n$	n 阶费瑞级数
$\min(x, y)$	最小值
$\max(x, y)$	最大值
$[a, b]$	最小公倍数
$p^a \parallel n$	恰整除，$p^a \mid n$ 但是 $p^{a+1} \nmid n$
$[a_1, a_2, \cdots, a_n]$	最小公倍数(n 个整数)
F_n	费马数
$a \equiv b \pmod m$	同余
$a \not\equiv b \pmod m$	不同余
$\overline{a}$	逆
$\boldsymbol{A} \equiv \boldsymbol{B} \pmod m$	同余(矩阵)
$\boldsymbol{I}$	单位矩阵
$\overline{\boldsymbol{A}}$	逆(矩阵)
$\mathrm{adj}(\boldsymbol{A})$	伴随
$h(k)$	散列函数
$\phi(n)$	欧拉 ϕ 函数
$\sum_{d \mid n}$	对 n 的所有正因子 d 求和
$f * g$	狄利克雷积
$\lambda(n)$	刘维尔函数
$\sigma(n)$	因子和函数
$\tau(n)$	因子个数函数
M_n	梅森数
$\mu(n)$	莫比乌斯函数
$p(n)$	拆分函数
$E_k(P)$	加密变换
$D_k(P)$	解密变换
$\mathscr{K}$	密钥空间
$\mathrm{ord}_m(a)$	a 模 m 的阶
$\mathrm{ind}_r(a)$	以 r 为底 a 的指数
$\lambda(n)$	最小通用指数
$\lambda_0(n)$	最大±1-指数
$\left(\frac{a}{p}\right)$	勒让德符号
$\left(\frac{a}{n}\right)$	雅可比符号
$(.c_1 c_2 c_3 \cdots)_b$	b 进制展开
$(.c_1 \cdots c_{n-1} \overline{c_n \cdots c_{n+k-1}})_b$	循环 b 进制展开
$[a_0; a_1, a_2, \cdots, a_n]$	有限简单连分数
$C_k = p_k / q_k$	连分数的第 k 个收敛子
$[a_0; a_1, a_2, \cdots]$	无限简单连分数
$[a_0; a_1, \cdots, a_{N-1}, \overline{a_N, \cdots, a_{N+k-1}}]$	循环连分数
a'	共轭
$N(z)$	复数的范数
$\overline{z}$	复共轭
$\binom{m}{k}$	二项式系数

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顺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. 这个证明被认为是所有数学证明中最漂亮的证明之一. 17 和 18 世纪研究素数的热情之火被重新点燃，数学家费马(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. 最近 100 年来发明了研究素数的许多强大的技术方法，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悬而未决的问题.

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.

将素数从合数中区分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. 多种方法被用于确定某个整数是否为素数. 例如，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 必为素数). 但这是不成立的，在 19 世纪初期人们找到反例：对于合数 $n=341$，n 整除 2^n-2. 这样的整数叫做*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. 然而这种方法并不能用来确定一个整数为素数。寻求有效算法来证明一个整数为素数是一个有几百年历史的问题，但令数学界惊讶的是在 2002 年，这个问题已经由三位印度计算机科学家 Manindra Agrawal，Neeraj Kayal 和 Nitin Saxena 解决。他们

的算法能在多项式时间内证明一个整数 n 是素数(即 n 的位数的多项式时间).

将正整数进行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 30 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,我们可以很容易地找到几百位甚至几千位长的素数,但是要把同样位长的整数进行因子分解,目前最快的计算机还不能胜任.

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,在此类系统中,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 密码系统的工作机制就必须要懂得一些数论的基础知识,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. 一个方程若要求解仅为整数,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,则这个方程没有整数解 (x, y, z),其中 $xyz\neq 0$. 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(Andrew 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的研究步伐大大提高. 每个人都能加入这项研究的队伍中,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,其中 p 也是素数. 2008 年 8 月,第一个超过 1000 万位的素数被发现,即梅森数 $2^{43\,112\,609}-1$,该发现获得了由电子前沿基金颁发的十万美元大奖. 大家正在协同努力去寻找超过一亿位的素数,这个素数奖金有 15 万美元. 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. 有志于继续学习数学的学生会学到数论的更高深内容,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,要记住数论是一门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,它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.

动手实验和探索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. 他们努力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，我建议你考察大量的例子，从中寻找规律，形成你自己的猜测. 你可以自己动手研究一些小的例子，就像数论的奠基者所做的那样，但与这些先行者不同的是，你可以利用当今强大的计算能力和计算工具. 通过手工或借助计算机来研究这些例子，会帮助你学习这门学科，甚至你也会得到自己的一些新结果.

第1章 整 数

在最一般的意义下，数论研究各种数集合的性质. 在本章中我们讨论某些特别重要的数的集合，包括整数、有理数和代数数集合. 我们将简单介绍用有理数逼近实数的概念，也介绍序列(特别是整数序列)的概念，包括古希腊人所研究的一些垛积数序列. 一个常见问题是如何由一些初始项来判定一个特别的整数序列. 我们将简单讨论一下如何解决这种问题.

利用序列概念，我们定义可数集合并且证明有理数集合是可数的. 我们还引进了求和符号和求积符号，并建立一些有用的求和公式.

数学归纳法是数论(和许多数学分支)中最重要的证明方法之一. 我们讨论数学归纳法的两种形式，说明如何用它们来证明各种结果，并且解释数学归纳法为什么是一种有效的证明手段.

然后我们介绍著名的斐波那契(Fibonacci)数序列，讲述引出这种数的原始问题. 我们将建立与斐波那契数有关的一些恒等式和不等式，其中有些证明就使用了数学归纳法.

本章最后一节讲述数论的一个基本概念：整除性. 我们将建立整数除法的基本性质，包括“带余除法”，还将解释如何用最大整数函数来表示一个整数去除另一个整数的商和余数. (也讲述了最大整数函数许多有用的性质.)

1.1 数和序列

本节将介绍一些基础知识，它们在本书中通篇使用. 特别地，我们将涉及数论中所研究的重要的数集合、整数序列的概念、求和与求积符号.

数

首先，我们介绍一些不同类型的数. 整数是集合{…，−3，−2，−1，0，1，2，3，…}中的数. 整数在数论的研究中扮演着重要的角色. 关于正整数的一个性质是值得关注的.

良序性质(The Well-Ordering Property) *每个非空的正整数集合都有一个最小元.*

良序性质看起来是显然的，但是在1.3节中我们将看到这是能够帮助证明关于整数集合的许多结果的一个基本性质.

良序性质可以作为定义正整数集合的公理，或者由一组公理推导出来. (附录A列出了整数集合的这组公理.)我们说正整数集合是良序的. 但是所有整数的集合不是良序的，因为在有些整数集合中没有最小的元素，例如负整数的集合、小于100的偶数集合和全体整数的集合.

在数论学习中的另一类重要的数是那些可以被写为整数的比的数的集合.

定义 *如果存在整数 p 和 $q\neq 0$，使得 $r=p/q$，则称实数 r 是*有理数*. 如果 r 不是有理的，则称为*无理数*.*

例 1.1 $-22/7$，$0=0/1$，$2/17$ 和 $1111/41$ 都是有理数. ◀

注意每个整数 n 都是有理数，因为 $n=n/1$. 无理数的例子有$\sqrt{2}$，π 和 e. 我们可以用正整数集合的良序性质证明$\sqrt{2}$是无理数. 我们给出的证明尽管技巧性较强，但却不是证明$\sqrt{2}$是无理数的最简单的方法. 读者可以参考我们在第 4 章给出的证明，该证明基于第 4 章中所给出的概念. (e 是无理数的证明作为习题 44. 关于 π 是无理数的证明并不容易，请参考[HaWr08].)

定理 1.1 *$\sqrt{2}$是无理数.*

证明 假设$\sqrt{2}$是有理数，那么存在正整数 a 和 b 使得$\sqrt{2}=a/b$. 因此，$S=\{k\sqrt{2}\mid k$ 和 $k\sqrt{2}$为正整数$\}$是一个非空的正整数集合(非空是因为 $a=b\sqrt{2}$是 S 的一个元素). 因此，由良序性质，S 有最小元，比如 $s=t\sqrt{2}$.

$s\sqrt{2}-s=s\sqrt{2}-t\sqrt{2}=(s-t)\sqrt{2}$. 由于 $s\sqrt{2}=2t$ 和 s 都是整数，故 $s\sqrt{2}-s=s\sqrt{2}-t\sqrt{2}=(s-t)\sqrt{2}$也必是整数. 进一步，这个数是正的，这是因为 $s\sqrt{2}-s=s(\sqrt{2}-1)$并且$\sqrt{2}>1$. 而这个数又小于 s，这是因为$\sqrt{2}<2$，从而$\sqrt{2}-1<1$. 这与 s 是 S 中的最小元矛盾. 因此$\sqrt{2}$是无理数. ■

整数集合、正整数集合、有理数集合和实数集合通常分别记为 $\mathbb{Z}$，$\mathbb{Z}^+$，$\mathbb{Q}$ 和 $\mathbb{R}$. 我们也用 $x\in S$ 来表示 x 属于集合 S. 在本书中我们偶尔会使用这些记号.

这里我们简要地提及几种其他类型的数，之后在第 12 章才会再涉及它们.

定义 *数 α 称为***代数数***，如果它是整系数多项式的根；也就是说，α 是代数数，如果存在整数 a_0，…，a_n 使得 $a_n\alpha^n+a_{n-1}\alpha^{n-1}+\cdots+a_0=0$. 如果数 α 不是代数数，则称为***超越数***.*

例 1.2 无理数$\sqrt{2}$是代数数，因为它是多项式 x^2-2 的根. ◀

注意每个有理数都是代数数，这是因为数 a/b 是多项式 $bx-a$ 的根，其中 a，b 是整数且$b\neq 0$. 在第 12 章中，我们将给出超越数的一个例子. e 和 π 也是超越数，但是这些事实的证明超出了本书的范围(可参看[HaWr08]).

最大整数函数

在数论中我们用一个特别的符号来表示小于或等于一个给定的实数的最大整数.

定义 *实数 x 中的***最大整数***(greatest integer)记为$[x]$，是小于或等于 x 的最大整数，即$[x]$是满足*

$$[x]\leqslant x<[x]+1$$

的整数.

例 1.3 $[5/2]=2$，$[-5/2]=-3$，$[\pi]=3$，$[-2]=-2$，$[0]=0$. ◀

注记 最大整数函数也被称为取整函数(floor function). 在计算机科学中通常用记号$\lfloor x\rfloor$来代替$[x]$. 上整数函数(ceiling function)是在计算机科学中常用的相关函数. 一个实数 x 的上整数函数记为$\lceil x\rceil$，是大于或等于 x 的最小整数. 例如$\lceil 5/2\rceil=3$，$\lceil -5/2\rceil=-2$.

最大整数函数出现在许多情况下. 除了在数论中有重要应用之外，我们在这本书中也会看到，它在计算机科学的一个分支——算法分析中也扮演着重要角色. 下面的例子体现了这个函数的一个非常有用的性质. 最大整数函数的其他性质可参看本节后的习题和[GrKnPa94].

例 1.4 证明：如果 n 是整数，则对于任意实数 x，都有 $[x+n]=[x]+n$. 为了证明这个性质，设 $[x]=m$，则 m 是整数，即 $m\leqslant x<m+1$. 我们在这个不等式上加上 n 得到 $m+n\leqslant x+n<m+n+1$. 这说明 $m+n=[x]+n$ 是小于或等于 $x+n$ 的最大整数，从而 $[x+n]=[x]+n$.

定义 *实数 x 的* **分数部分**(fractional part)*记为 $\{x\}$，是 x 与 $[x]$ 的差，即 $\{x\}=x-[x]$.*

由于 $[x]\leqslant x<[x]+1$，从而对任意实数 x，有 $0\leqslant\{x\}=x-[x]<1$. 因为 $x=[x]+\{x\}$，所以 x 的最大取整也叫做 x 的整数部分.

例 1.5 $\{5/4\}=5/4-[5/4]=5/4-1=1/4$. $\{-2/3\}=-2/3-[-2/3]=-2/3-(-1)=1/3$.

丢番图逼近

我们知道一个实数和与之最接近的整数的距离不超过 1/2. 但是我们可否证明一个实数的前 k 个倍数中的某一个一定更接近某个整数？数论中一个很重要的部分称为*丢番图逼近*，它正是研究这类问题的. 特别地，丢番图逼近着重研究用有理数逼近实数的问题. (*丢番图*这个词来自古希腊数学家丢番图(Diophantus)，他的传记见 13.1 节.)

这里我们将要证明在实数 α 的前 n 个倍数中至少有一个实数与最接近它的整数的距离小于 $1/n$. 这个证明是基于德国数学家狄利克雷(Dirichlet)提出的*鸽笼原理*[⊖](pigeonhole principle). 简单地说，这个原理告诉我们，如果有比盒子多的物体，那么当要把这些物体放进盒子中时，至少有两个物体被放入同一个盒子里. 尽管这个想法看起来特别简单，但是它在数论和组合数学中非常有用. 我们现在陈述并证明这个重要的事实. 如果你所拥有的鸽子数多于鸽笼数，那么必有两只鸽子栖息在同一个鸽笼中，因此我们把它称为鸽笼原理.

定理 1.2(*鸽笼原理*) *如果把 $k+1$ 个或者更多的物体放入 k 个盒子中，那么至少有一个盒子中有两个或者更多的物体.*

证明 如果 k 个盒子中的任何一个中都没有多于一个的物体，那么所有物体的总数至多为 k. 这个矛盾说明有一个盒子中至少有两个或者更多的物体. ■

现在我们来叙述并证明狄利克雷逼近定理，它能够保证一个实数的前 n 个倍数之一必定在某个整数的 $1/n$ 邻域内. 我们给出的证明说明了鸽笼原理很有用. (关于鸽笼原理的更多应用参见[Ro07].)(注意在证明中我们用到了*绝对值函数*(absolute value function). 在这里我们先回顾一下，x 的绝对值 $|x|$ 当 $x\geqslant 0$ 时等于 x，当 $x<0$ 时等于 $-x$. $|x-y|$ 给出了 x 与 y 之

⊖ 狄利克雷并未把定理 1.2 称为鸽笼原理，而是用德语称为 Schubfachprinzip，译为英语是抽屉原理(drawer principle). 狄利克雷的传记见 3.1 节.