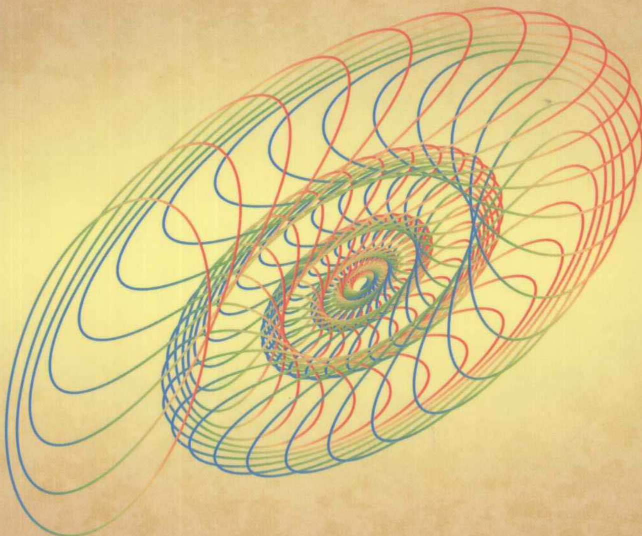
TURING 图灵数学·统计学丛书 46



An Introduction to the Theory of Numbers

哈代数论

（第6版）

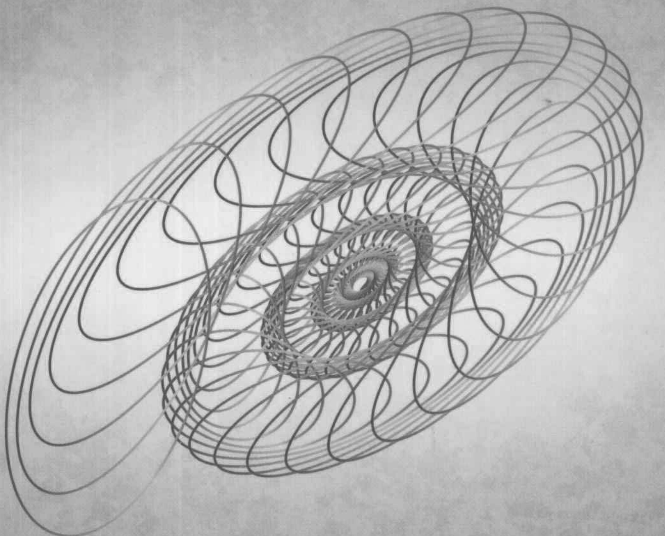
[英] G. H. Hardy E. M. Wright 著

[英] D. R. Heath-Brown [美] J. H. Silverman 修订

张明尧 张 凡 译

人民邮电出版社
POSTS & TELECOM PRESS

TURING 图灵数学·统计学丛书 46



An Introduction to the Theory of Numbers

哈代数论

（第6版）

[英] G. H. Hardy E. M. Wright 著

[英] D. R. Heath-Brown [美] J. H. Silverman 修订

张明尧 张凡 译

人民邮电出版社
POSTS & TELECOM PRESS

图书在版编目(CIP)数据

哈代数论：第 6 版/（英）哈代（Hardy, G. H.），（英）赖特（Wright, E. M.）著；张明尧，张凡译. —北京：人民邮电出版社，2010. 10
(图灵数学 · 统计学丛书)
书名原文： An Introduction to the Theory of Numbers
ISBN 978-7-115-23203-8

Ⅰ. ①哈… Ⅱ. ①哈… ②赖… ③张… ④张… Ⅲ. ①数论 Ⅳ. ①O156

中国版本图书馆 CIP 数据核字(2010)第 122111 号

内 容 提 要

本书是一本经典的数论名著，取材于作者在牛津大学、剑桥大学等大学授课的讲义. 主要包括素数理论、无理数、费马定理、同余式理论、连分数、用有理数逼近无理数、不定方程、二次域、算术函数、数的分划等内容. 每章章末都提供了相关的附注，书后还附有译者编写的相关内容的最新进展，便于读者进一步学习.

本书可供数学专业高年级学生、研究生、大学老师以及对数论感兴趣的专业读者学习参考.

图灵数学 · 统计学丛书

哈代数论(第 6 版)

◆ 著 [英] G. H. Hardy E. M. Wright
修订 [英] D. R. Heath-Brown [美] J. H. Silverman
译 张明尧 张 凡
责任编辑 明永玲
执行编辑 卢秀丽

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号
邮编 100061 电子函件 315@ptpress.com.cn
网址：http://www.ptpress.com.cn
北京铭成印刷有限公司印刷

◆ 开本：700×1000 1/16
印张：30.75
字数：655 千字 2010 年 10 月第 1 版
印数：1–3 000 册 2010 年 10 月北京第 1 次印刷

著作权合同登记号 图字：01-2010-3989 号

ISBN 978-7-115-23203-8

定价：69.00 元

读者服务热线：(010)51095186 印装质量热线：(010) 67129223

反盗版热线：(010)67171154

版权声明

译　者　序

Hardy 和 Wright 的这本书[①] 初版于 1938 年, 是作者多年间在英国牛津大学、剑桥大学、阿伯丁大学以及其他大学所作的若干数论讲座的讲稿汇编. 这本中文版是以原书英文第 6 版作为蓝本翻译的.

2008 年, 这本书问世整整 70 年了. 在这 70 多年中, 数论这个数学分支已经有了长足的进展, 它的理论和方法都有了巨大的发展和进步, 并且人们在解析数论、代数数论、超越数论以及计算数论等所有重要分支的许多重大问题的研究中取得了令人瞩目的成果, 全部或者部分解决了一批著名的数论难题 (例如关于超越数的 Hilbert 第七问题、Waring 问题、Gauss 关于二次域的类数猜想、Goldbach 猜想和孪生素数猜想、Fermat 大定理、Riemann 猜想和广义 Riemann 猜想, 等等等等). 从这个意义上说, Hardy 和 Wright 这本书中的某些内容随着原著作者的去世, 早已落后于当代数学科学的发展, 这是任何经典著作都无法避免的窘境. 然而, 鉴于这部书是有关数论基础知识的导引性著作, 它所讲述的基本内容都没有过时, 更由于作者引人入胜、深入浅出的书写风格, 使得本书历经 70 余年的考验, 至今仍然是为数不多且具有重要参考价值的数论初等教程之一. (另一部出版较早且值得一提的数论初等教程是已故中国数学家华罗庚先生的名著《数论导引》.)

原著者 G. H. Hardy 是 20 世纪在英国乃至全世界享有盛誉的数学家, 他单独或者与他人合作出版过多部数学史上不朽的经典著作, 发表过许多重要的研究论文. 他的许多著作至今仍极有参考价值. 此外, 他还在数学的众多分支, 特别是数论这个分支的研究中, 取得过超出当代数学家的杰出成就. 例如, 他和印度数学家 S. A. Ramanujan 等人所创立的圆法在解决许多解析数论重大难题的过程中成为不可或缺的方法之一, 他的数学理论和思想至今仍是当代数学家们研究的对象和源泉. 此外, Hardy 对于中国数学界的影响也远不止于他的著作和研究. 众所周知, 由于美国著名数学家、控制论创始人、也曾是 Hardy 学生的 N. Wiener 的推荐, 正值青年的华罗庚于 1936 年受到 Hardy 的邀请到剑桥大学作访问学者. 华罗庚在剑桥大学得到以 Hardy 为核心的数学研究集体中许多年轻数学家的帮助, 在与他们的交流中获益匪浅. 在留学期间, 他至少在国际一流期刊发表了 15 篇论文, 这对他本人后来研究工作的深入和发展显然有巨大的作用和影响. 这一事实表明: Hardy 本人对于华罗庚个人一生的学术成就以及华罗庚归国后对于培养整整一代新中国数学家所作的贡献都有着重大而直接的影响. 从这个意义上说, 我们中国数学界今天无论怎样感谢 Hardy 都不为过.

按照 Hardy 本人的建议, 这部《哈代数论》既不是数论的系统教科书, 也不是一本数论的通俗读物. 它是为具有大学数学系一年级以上水平且希望学习数论的学生,

① 本版书名为《哈代数论 (第 6 版)》, 上一版书名为《数论导引 (第 5 版)》, 二者有所不同. —— 编者注

以及感兴趣的数学家编写的. 上一版共 24 章, 经修订, 本版著者英国牛津大学教授 D. R. Heath-Brown 以及美国布朗大学教授 J. H. Silverman 新增一章专门介绍椭圆曲线理论. 现在, 这本第 6 版共 25 章, 分别介绍了素数理论、数的几何、同余式理论、二次剩余和二次互反律、连分数、有理数逼近无理数、二次域、不定方程、算术函数、数的分划、一致分布以及椭圆曲线等方面的基本概念、初等理论和方法以及相关的问题. 在每一章的末尾, 都有一个关于本章内容的附注, 介绍相关问题的起源、发展历史以及相应的参考资料等. 为了使读者了解书中所涉及的某些重要的数论问题的最新进展 (到 2010 年 3 月 5 日止), 我们编写了一个简短的附录作为补遗予以介绍. 希望这本中文版的出版能对中国未来的年轻数论爱好者有相当的帮助和教益. 译者中的一位年长者 —— 一个在差不多四十年前黑暗的 "文化大革命" 时期生活在充满阶级斗争氛围中看不到前途和光明、由于无法实现自己的人生价值而在痛苦中挣扎的青年, 正是靠着这本著作和其他数学著作的指引, 才找到了思想的乐趣, 摆脱了人生的苦恼, 最终走上了学习和研究数论的人生旅程.

在第 6 版的翻译过程中, 我们将发现的一些问题提交给参与英文第 6 版编著工作的几位作者, 得到了他们的大力帮助. 例如, George E. Andrews 给我来信解答了有关第 19 章附注中的一处疑问; Joseph H. Silverman 的来信肯定了我在新增的第 25 章及其附注中发现的所有涉及数学以及英文方面的错误 (读者通过将英文第 6 版与中文译本对照, 即可发现这些错误之处), 他还给我指出了第 25 章中某些需要更改的地方 (指的是根据他的建议在中文译本中取消了定理 478~481 这四处的星号).

对于上述各位以及为这部中文译本付出辛勤劳动的北京图灵文化发展有限公司的诸位编辑, 谨此表示我衷心的感谢!

张明尧

2010 年 3 月 4 日于上海

序

我非常幸运地受教于一位研究过数论的中学数学老师. 在他的建议下, 我搞到一本绝妙的书 ——Hardy 与 Wright 合著的第 4 版 *An Introduction to the Theory of Numbers*. 这本书与 Davenport 的 *The Higher Arithmetic* 一起, 成为引导我进入这一领域的我最喜爱的书籍. 通过搜寻这部教程的书页来寻找有关 Fermat 问题的线索 (我已经对此问题着迷), 我第一次领教了数论真正的广博无垠. 这部书仅有中间的四章是有关二次域和 Diophantus 方程的, 其他的大多数材料对我来说都是全新的, 如 Diophantus 几何、圆整数、Dirichlet 定理、连分数、四元数、互倒律, 等等等等, 这一目录可以一直写下去.

这部书已经成为进入这一领域的不同分支进行探索的起点. 对我来说, 首要的一步是要找到更多的有关代数数论的知识, 特别是关于 Kummer 理论. 在我学习过一些复分析之前, 偏重解析数论的部分对我始终没有同样的吸引力, 也未能真正激发我的想象力. 只有在那以后我才深知 zeta 函数的威力. 然而, 每当我被一门新的理论强烈吸引时, 这本书总会作为我回顾思考的起点, 即便有时在许多年之后也依然如此. 这本书的成功之处, 部分在于它包罗万象的注释与参考文献, 它们为缺少经验的数学工作者标示出研究方向. 本书的这一部分由 Roger Heath-Brown 作了更新和扩充, 从而使得 21 世纪的学生们仍能从更加新近的发现以及教材中获益. 这是按照他对 Titchmarsh 所著*The Theory of the Riemann Zeta Functions* 一书所作的绝妙评注之风格进行的. 这对于新的读者有无法估量的帮助, 即便对在年轻时已经读过这本书的人来说亦会带来莫大的愉悦, 颇有点类似聆听往昔的校友讲述人生经历.

增加的最后一章给出了有关椭圆曲线理论的介绍. 虽然这一理论在原先的版本中并未予以描述 (除了在 13.6 节的附注中简单提及之外), 但是已经证明: 这一理论在 Diophantus 方程, 尤其是在 Fermat 方程的研究中起着决定性的作用. 一方面由于 Birch 与 Swinnerton-Dyer 的猜想, 另一方面由于它与 Fermat 方程的异乎寻常的联系, 这一理论已经成了数论学者生活的中心. 它甚至在有效求解著名的 Gauss 类数问题中也起着核心作用. 当此书写成时, 所有这一切看起来似乎都还是荒诞不经得不可能发生的. 于是由 Joe Silverman 来对这一理论作一个明白易懂的介绍作为这部新版著作的结尾是恰如其分的. 当然, 这仅仅是对这一理论的浮光掠影般的简介, 读者若要解读这一理论的诸多奥秘, 即便无需耗费一生最好的时光, 也必定要奉献出许多的时间.

Andrew. J. Wiles

2008 年 1 月

前 言

这部第 6 版包含了大为扩展的章后附注. 自从上一次改版以来, 数论又有了许多令人欢欣鼓舞的进展, 现将这些进展写进了附注之中. 希望它们能为感兴趣的读者提供一条通向现代研究领域的大道. 某些章节的附注是在其他作者不遗余力的帮助下完成的. D. Masser 教授更新了第 4 章和第 11 章附注中的材料, G. E. Andrews 教授则对第 19 章附注作了同样的工作. T. D. Wooley 教授将大量新材料添加进了第 21 章附注之中, 第 24 章附注中类似的评述则是由 R. Hans-Gill 教授承担的. 对于他们各位给予的帮助, 谨此表示我们衷心的感谢.

此外, 我们增加了全新的一章讲述椭圆曲线. 这部分内容在较早的版本中没有提及, 现在它已经成为数论中一个占据中心地位的课题, 因而我们认为单辟一章对它进行详细阐释是值得的. 这部分材料与书中讨论 Diophantus 方程的原有章节有本质的联系.

最后, 我们还纠正了第 5 版中相当数量的印刷错误. 有大量的来信指出了其中的印刷错误或者数学上的错误, 我们感谢每一位来信提供帮助者.

对此书出一部新版本的建议最初是由 John Maitland Wright 教授以及 John Coates 教授提出的. 对于他们的热情支持, 谨此表示我们诚挚的谢意.

D. R. Heath-Brown

J. H. Silverman

2007 年 9 月

第5版前言

这一版的主要改变是每一章后面的附注. 我力求为那些希望进一步研讨某个特定论题的读者提供最新的参考文献, 并在附注及正文中都对当前的知识状况作比较精确的阐述. 为此我还参考了 *Zentralblatt* 和 *Mathematical Reviews* 这样一些极具价值的出版物. 除此以外, 我也在与一些人的通信中受益匪浅, 他们提供了修改的建议, 或者回答了我的问题. 我特别感谢 J. W. S. Cassels 教授和 H. Halberstam 教授, 他们两位都应我的要求, 向我提供了众多极有价值的建议以及参考文献.

书中的定理 445 有一个新的、更为清晰的证明, 关于处理无理性的 Theodorus 方法, 有一处说明谈及了我的观念转变. 为了方便读者利用这一版作为参考书, 我尽可能保持了原书的页码不改变. 基于这个原因, 尽管我补充了一个很短的附录, 来介绍素数论的某些方面最新的进展, 但却并没有把这些材料加到正文中相应的地方去.

E. M. Wright

1978 年 10 月于英国阿伯丁

第1版前言

本书是根据最近十年间在若干所大学的讲座内容逐渐累积而形成的, 与许多由讲座形成的书很相似, 本书没有确定的内容规划.

从任何意义上讲, 本书都不是一本系统的数论专著 (专家学者只要看一看本书的目录就会明白这一点). 它甚至并不包括数论诸多理论中任何一个方面的完整合理的介绍, 只不过作为导引来轮流阐释几乎所有这些方面的内容. 我们对若干个论题中的每一个都作一些介绍, 虽然人们通常并不把它们合起来放在单独的一本书之中. 同时, 我们也对某些并不总是被视为数论的内容作了一些探讨, 例如第 12 到 15 章属于数的 "代数的" 理论; 第 19 到第 21 章属于数的 "加性的" 理论; 第 22 章属于 "解析的" 理论; 而第 3 章、第 11 章、第 23 章以及第 24 章处理的内容通常是归属在 "数的几何" 或者 "Diophantine 逼近" 这一范畴. 我们所规划的内容极其丰富, 但少有深度, 因为在区区四五百页的篇幅里完全不可能对这么多问题中的任何一个论题加以深入研究.

本书有很大的漏洞, 任何一位专家学者都能轻易指出来. 最显而易见的一个问题是对于二次型的理论没有任何介绍. 这个理论比数论的任何其他部分都有更为系统的发展, 而且在常见的书中对此都有完善的讨论. 我们不得不略去某些东西, 因为我们对那部分理论的现存结果没有什么新鲜内容可以添加.

我们经常根据个人的兴趣来决定写作计划, 选取某些论题, 很少是因为这些问题的重要性 (尽管其中大多数问题都很重要), 而是因为它们很合我们的心意, 也因为其他作者给我们留下了写作的空间. 我们最初的目的是写一本有趣的书, 一本独具匠心的书. 或许我们已经取得了成功, 成功的代价是书中有太多的怪异之处; 或许我们已经失败了, 但是我们不会彻底失败, 因为所研究的论题是如此的引人入胜, 故而只有非同一般的无能才会使得它变得枯燥乏味.

这本书是为从事数学工作的人写的, 并不要求读者具备任何高深的数学知识或者技巧. 在前 18 章里我们只需要读者具备中学程度的数学知识, 任何聪明的大学生都会发现本书易于读懂. 后 6 章要难一些, 需要读者具备稍微多一点的预备知识, 但也绝不超出比较简单的大学课程的内容.

本书书名与 L. E. Dickson 教授的一本非常有名的书同名 (而本书与他的书几乎没有共同之处). 有一段时期我们打算更名为 *An introduction to arithmetic* (算术导引), 这是一个更为新颖且在某些方面来说也更加合适的书名, 但是有人指出用这个书名可能会使人对书的内容产生误解.

有多位朋友在本书的准备过程中给予了帮助. H. Heibronn 博士阅读了全部手稿以及印刷文本, 他的批评和建议使本书有了许多重要的改进, 其中最重要的一些已在

正文中予以致谢. H. S. A. Potter 博士和 S. Wylie 博士阅读了书中的证明, 并帮助我们去掉了许多错误以及含糊不清之处. 他们还对每一章后面附注中的大部分参考文献进行了检查. H. Davenport 博士和 R. Rado 博士也阅读了本书的一部分内容, 特别是最后一章, 这一章由于他们以及 Heibronn 博士的建议, 与原稿相比几乎焕然一新.

我们还从参考目录中所列举的其他书籍中 (特别是从 Landau 和 Perron 的著作中) 不受限制地借用了许多东西. 特别是对于 Landau, 我们与数论方面所有求上进的学生一样, 无论如何感谢他都是应该的.

G. H. H.

E. M. W

1938 年 8 月于牛津

关于记号的说明

我们从形式逻辑中借用 4 个符号, 它们分别是

$$\rightarrow, \equiv, \exists \text{ 和 } \in .$$

$\rightarrow$ 读作 "蕴含". 于是

$$l|m \rightarrow l|n$$

的含义是 "'l 是 m 的因子' 蕴含 'l 是 n 的因子'", 或者 "如果 l 整除 m, 那么 l 整除 n". 而

$$b|a.\, c|b \rightarrow c|a$$

的含义是 "如果 b 整除 a 且 c 整除 b, 那么 c 整除 a".

$\equiv$ 读作 "等价于". 于是

$$m|(ka - ka') \equiv m_1|(a - a')$$

的含义是 "'m 整除 $ka - ka'$' 这一结论等价于 'm_1 整除 $a - a'$ 这一结论", 也就是说其中任何一个结论都蕴含另一个结论.

这两个符号必须和符号 "$\rightarrow$"(趋向于) 以及符号 "$\equiv$" (同余于) 仔细区别开来. 这些符号的不同含义之间不大可能会产生任何误解, 因为 "$\rightarrow$" (蕴含) 和 "$\equiv$" (等价于) 总是指**命题**之间的关系.

$\exists$ 读作 "有 (存在) 一个". 于是

$$\exists l.\, 1 < l < m.\, l|m$$

的含义是 "存在一个 l 使得有 (1) $1 < l < m$ 和 (2) $l|m$ 成立".

$\in$ 表达的是一个集合的元素和这个集合之间的关系. 于是

$$m \in S, n \in S \rightarrow (m \pm n) \in S$$

的含义是 "如果 m 和 n 都是 S 的元素, 那么 $m + n$ 和 $m - n$ 也都是 S 的元素".

定理的编号上加星号 (例如定理 15*) 表明该定理的证明过于困难, 不适合放在本书中. 那些未加星号但未加以证明的定理可以利用与本书中所用的类似的方法予以证明.

目　　录

第 1 章　素数 (1) ···· 1
- 1.1 整除性 ···· 1
- 1.2 素数 ···· 2
- 1.3 算术基本定理的表述 ···· 3
- 1.4 素数序列 ···· 3
- 1.5 关于素数的某些问题 ···· 5
- 1.6 若干记号 ···· 6
- 1.7 对数函数 ···· 8
- 1.8 素数定理的表述 ···· 8
- 本章附注 ···· 10

第 2 章　素数 (2) ···· 12
- 2.1 Euclid 第二定理的第一个证明 ···· 12
- 2.2 Euclid 方法的更进一步的推论 ···· 12
- 2.3 某种算术级数中的素数 ···· 13
- 2.4 Euclid 定理的第二个证明 ···· 14
- 2.5 Fermat 数和 Mersenne 数 ···· 15
- 2.6 Euclid 定理的第三个证明 ···· 16
- 2.7 关于素数公式的进一步结果 ···· 17
- 2.8 关于素数的未解决的问题 ···· 19
- 2.9 整数模 ···· 19
- 2.10 算术基本定理的证明 ···· 21
- 2.11 基本定理的另一个证明 ···· 21
- 本章附注 ···· 21

第 3 章　Farey 数列和 Minkowski 定理 ···· 24
- 3.1 Farey 数列的定义和最简单的性质 ···· 24
- 3.2 两个特征性质的等价性 ···· 25
- 3.3 定理 28 和定理 29 的第一个证明 ···· 25
- 3.4 定理 28 和定理 29 的第二个证明 ···· 26
- 3.5 整数格点 ···· 27
- 3.6 基本格的某些简单性质 ···· 28
- 3.7 定理 28 和定理 29 的第三个证明 ···· 29
- 3.8 连续统的 Farey 分割 ···· 30
- 3.9 Minkowski 的一个定理 ···· 31
- 3.10 Minkowski 定理的证明 ···· 32
- 3.11 定理 37 的进一步拓展 ···· 34
- 本章附注 ···· 36

第 4 章　无理数 ···· 38
- 4.1 概论 ···· 38
- 4.2 已知的无理数 ···· 38
- 4.3 Pythagoras 定理及其推广 ···· 39
- 4.4 基本定理在定理 43~45 证明中的应用 ···· 41
- 4.5 历史杂谈 ···· 41
- 4.6 $\sqrt{5}$ 无理性的几何证明 ···· 43
- 4.7 更多的无理数 ···· 44
- 本章附注 ···· 46

第 5 章　同余和剩余 ···· 47
- 5.1 最大公约数和最小公倍数 ···· 47
- 5.2 同余和剩余类 ···· 48
- 5.3 同余式的初等性质 ···· 49
- 5.4 线性同余式 ···· 49
- 5.5 Euler 函数 $\phi(m)$ ···· 51
- 5.6 定理 59 和定理 61 对三角和的应用 ···· 53
- 5.7 一个一般性的原理 ···· 56
- 5.8 正十七边形的构造 ···· 57
- 本章附注 ···· 61

第 6 章 Fermat 定理及其推论 ···· 63
6.1 Fermat 定理 ···· 63
6.2 二项系数的某些性质 ···· 63
6.3 定理 72 的第二个证明 ···· 65
6.4 定理 22 的证明 ···· 66
6.5 二次剩余 ···· 67
6.6 定理 79 的特例：Wilson 定理 ···· 68
6.7 二次剩余和非剩余的初等性质 ···· 69
6.8 $a \pmod{m}$ 的阶 ···· 71
6.9 Fermat 定理的逆定理 ···· 71
6.10 $2^{p-1}-1$ 能否被 p^2 整除 ···· 73
6.11 Gauss 引理和 2 的二次特征 ···· 73
6.12 二次互倒律 ···· 76
6.13 二次互倒律的证明 ···· 78
6.14 素数的判定 ···· 79
6.15 Mersenne 数的因子; Euler 的一个定理 ···· 80
本章附注 ···· 81
第 7 章 同余式的一般性质 ···· 83
7.1 同余式的根 ···· 83
7.2 整多项式和恒等同余式 ···· 83
7.3 多项式 $(\mathrm{mod}\ m)$ 的整除性 ···· 84
7.4 素数模同余式的根 ···· 85
7.5 一般定理的某些应用 ···· 86
7.6 Fermat 定理和 Wilson 定理的 Lagrange 证明 ···· 88
7.7 $\left[\frac{1}{2}(p-1)\right]!$ 的剩余 ···· 89
7.8 Wolstenholme 的一个定理 ···· 90
7.9 von Staudt 定理 ···· 92
7.10 von Staudt 定理的证明 ···· 93
本章附注 ···· 95
第 8 章 复合模的同余式 ···· 96
8.1 线性同余式 ···· 96
8.2 高次同余式 ···· 98
8.3 素数幂模的同余式 ···· 98
8.4 例子 ···· 99
8.5 Bauer 的恒等同余式 ···· 101
8.6 Bauer 的同余式：$p=2$ 的情形 ···· 102
8.7 Leudesdorf 的一个定理 ···· 103
8.8 Bauer 定理的进一步的推论 ···· 105
8.9 2^{p-1} 和 $(p-1)!$ 关于模 p^2 的同余式 ···· 107
本章附注 ···· 109
第 9 章 用十进制小数表示数 ···· 110
9.1 与给定的数相伴的十进制小数 ···· 110
9.2 有限小数和循环小数 ···· 112
9.3 用其他进位制表示数 ···· 114
9.4 用小数定义无理数 ···· 115
9.5 整除性判别法 ···· 116
9.6 有最大周期的十进制小数 ···· 117
9.7 Bachet 的称重问题 ···· 118
9.8 Nim 博弈 ···· 120
9.9 缺失数字的整数 ···· 122
9.10 测度为零的集合 ···· 123
9.11 缺失数字的十进制小数 ···· 124
9.12 正规数 ···· 126
9.13 几乎所有的数都是正规数的证明 ···· 127
本章附注 ···· 130
第 10 章 连分数 ···· 132
10.1 有限连分数 ···· 132
10.2 连分数的渐近分数 ···· 133
10.3 有正的商的连分数 ···· 134
10.4 简单连分数 ···· 135
10.5 用简单连分数表示不可约有理分数 ···· 136
10.6 连分数算法和 Euclid 算法 ···· 138
10.7 连分数与其渐近分数的差 ···· 140
10.8 无限简单连分数 ···· 141

10.9　用无限连分数表示无理数 ···· 142
10.10　一个引理 ···················· 144
10.11　等价的数 ···················· 145
10.12　周期连分数 ·················· 147
10.13　某些特殊的二次根式 ········· 149
10.14　Fibonacci 数列和 Lucas 数列 ······················· 151
10.15　用渐近分数作逼近 ··········· 154
本章附注 ························· 157
第 11 章　用有理数逼近无理数 ···· 158
11.1　问题的表述 ·················· 158
11.2　问题的推广 ·················· 159
11.3　Dirichlet 的一个论证方法 ···· 160
11.4　逼近的阶 ···················· 161
11.5　代数数和超越数 ············· 162
11.6　超越数的存在性 ············· 163
11.7　Liouville 定理和超越数的构造 ······················· 164
11.8　对任意无理数的最佳逼近的度量 ······················· 166
11.9　有关连分数的渐近分数的另一个定理 ···················· 168
11.10　具有有界商的连分数 ········· 169
11.11　有关逼近的进一步定理 ······· 172
11.12　联立逼近 ···················· 173
11.13　e 的超越性 ·················· 174
11.14　π 的超越性 ·················· 177
本章附注 ························· 180
第 12 章　$k(1)$, $k(\mathrm{i})$, $k(\rho)$ 中的算术基本定理 ·········· 182
12.1　代数数和代数整数 ··········· 182
12.2　有理整数、Gauss 整数和 $k(\rho)$ 中的整数 ···················· 182
12.3　Euclid 算法 ·················· 183
12.4　Euclid 算法对 $k(1)$ 中的基本定理的应用 ················· 184
12.5　关于 Euclid 算法和基本定理的历史注释 ················ 185
12.6　Gauss 整数的性质 ··········· 186
12.7　$k(\mathrm{i})$ 中的素元 ·············· 187
12.8　$k(\mathrm{i})$ 中的算术基本定理 ······ 189
12.9　$k(\rho)$ 中的整数 ··············· 191
本章附注 ························· 193
第 13 章　某些 Diophantus 方程 ···················· 194
13.1　Fermat 大定理 ·············· 194
13.2　方程 $x^2+y^2=z^2$ ··········· 194
13.3　方程 $x^4+y^4=z^4$ ··········· 195
13.4　方程 $x^3+y^3=z^3$ ··········· 196
13.5　方程 $x^3+y^3=3z^3$ ·········· 199
13.6　用有理数的三次幂之和表示有理数 ···················· 201
13.7　方程 $x^3+y^3+z^3=t^3$ ······· 203
本章附注 ························· 205
第 14 章　二次域 (1) ·············· 208
14.1　代数数域 ···················· 208
14.2　代数数和代数整数; 本原多项式 ························ 209
14.3　一般的二次域 $k(\sqrt{m})$ ········ 210
14.4　单位和素元 ·················· 211
14.5　$k(\sqrt{2})$ 中的单位 ············· 212
14.6　基本定理不成立的数域 ······· 214
14.7　复 Euclid 域 ················· 215
14.8　实 Euclid 域 ················· 217
14.9　实 Euclid 域 (续) ············ 219
本章附注 ························· 220
第 15 章　二次域 (2) ·············· 222
15.1　$k(\mathrm{i})$ 中的素元 ·············· 222
15.2　$k(\mathrm{i})$ 中的 Fermat 定理 ······· 223
15.3　$k(\rho)$ 中的素元 ·············· 224
15.4　$k(\sqrt{2})$ 和 $k(\sqrt{5})$ 中的素元 ···· 225
15.5　Mersenne 数 M_{4n+3} 的素性的 Lucas 判别法 ··············· 227

15.6 关于二次域的算术的一般性注释 …… 229
15.7 二次域中的理想 …… 230
15.8 其他的域 …… 233
本章附注 …… 234

第 16 章 算术函数 $\phi(n)$, $\mu(n)$, $d(n)$, $\sigma(n)$, $r(n)$ …… 235
16.1 函数 $\phi(n)$ …… 235
16.2 定理 63 的进一步证明 …… 236
16.3 Möbius 函数 …… 236
16.4 Möbius 反转公式 …… 237
16.5 进一步的反转公式 …… 238
16.6 Ramanujan 和的估计 …… 239
16.7 函数 $\mathrm{d}(n)$ 和 $\sigma_k(n)$ …… 241
16.8 完全数 …… 241
16.9 函数 $r(n)$ …… 242
16.10 $r(n)$ 公式的证明 …… 244
本章附注 …… 245

第 17 章 算术函数的生成函数 …… 246
17.1 由 Dirichlet 级数生成算术函数 …… 246
17.2 ζ 函数 …… 247
17.3 $\zeta(s)$ 在 $s \to 1$ 时的性状 …… 248
17.4 Dirichlet 级数的乘法 …… 249
17.5 某些特殊算术函数的生成函数 …… 251
17.6 Möbius 公式的解析说明 …… 253
17.7 函数 $\Lambda(n)$ …… 255
17.8 生成函数的进一步的例子 …… 257
17.9 $r(n)$ 的生成函数 …… 258
17.10 其他类型的生成函数 …… 259
本章附注 …… 261

第 18 章 算术函数的阶 …… 263
18.1 $\mathrm{d}(n)$ 的阶 …… 263
18.2 $\mathrm{d}(n)$ 的平均阶 …… 266
18.3 $\sigma(n)$ 的阶 …… 268
18.4 $\phi(n)$ 的阶 …… 269
18.5 $\phi(n)$ 的平均阶 …… 271
18.6 无平方因子数的个数 …… 272
18.7 $r(n)$ 的阶 …… 273
本章附注 …… 274

第 19 章 分划 …… 276
19.1 加性算术的一般问题 …… 276
19.2 数的分划 …… 276
19.3 $p(n)$ 的生成函数 …… 277
19.4 其他的生成函数 …… 279
19.5 Euler 的两个定理 …… 280
19.6 进一步的代数恒等式 …… 282
19.7 $F(x)$ 的另一个公式 …… 283
19.8 Jacobi 的一个定理 …… 284
19.9 Jacobi 恒等式的特例 …… 286
19.10 定理 353 的应用 …… 288
19.11 定理 358 的初等证明 …… 288
19.12 $p(n)$ 的同余性质 …… 290
19.13 Rogers-Ramanujan 恒等式 …… 292
19.14 定理 362 和定理 363 的证明 …… 294
19.15 Ramanujan 连分数 …… 296
本章附注 …… 297

第 20 章 用两个或四个平方和表示数 …… 300
20.1 Waring 问题：数 $g(k)$ 和 $G(k)$ …… 300
20.2 平方和 …… 301
20.3 定理 366 的第二个证明 …… 302
20.4 定理 366 的第三个和第四个证明 …… 303
20.5 四平方定理 …… 304
20.6 四元数 …… 306
20.7 关于整四元数的预备定理 …… 308
20.8 两个四元数的最高右公因子 …… 309
20.9 素四元数和定理 370 的证明 …… 310

20.10 $g(2)$ 和 $G(2)$ 的值 …… 312
20.11 定理 369 的第三个证明的引理 …… 312
20.12 定理 369 的第三个证明：表法个数 …… 313
20.13 用多个平方和表示数 …… 316
本章附注 …… 317

第 21 章 用立方数以及更高次幂表示数 …… 320
21.1 四次幂 …… 320
21.2 三次幂：$G(3)$ 和 $g(3)$ 的存在性 …… 321
21.3 $g(3)$ 的界 …… 322
21.4 更高次幂 …… 323
21.5 $g(k)$ 的一个下界 …… 324
21.6 $G(k)$ 的下界 …… 324
21.7 受符号影响的和：数 $v(k)$ …… 327
21.8 $v(k)$ 的上界 …… 329
21.9 Prouhet-Tarry 问题：数 $P(k,j)$ …… 330
21.10 对特殊的 k 和 j, $P(k,j)$ 的估计 …… 332
21.11 Diophantus 分析的进一步的问题 …… 334
本章附注 …… 337

第 22 章 素数 (3) …… 343
22.1 函数 $\vartheta(x)$ 和 $\psi(x)$ …… 343
22.2 $\vartheta(x)$ 和 $\psi(x)$ 的阶为 x 的证明 …… 344
22.3 Bertrand 假设和一个关于素数的“公式” …… 346
22.4 定理 7 和定理 9 的证明 …… 348
22.5 两个形式变换 …… 349
22.6 一个重要的和 …… 350
22.7 $\sum p^{-1}$ 与 $\prod(1-p^{-1})$ …… 352
22.8 Mertens 定理 …… 354
22.9 定理 323 和定理 328 的证明 …… 356
22.10 n 的素因子个数 …… 357
22.11 $\omega(n)$ 和 $\Omega(n)$ 的正规阶 …… 358
22.12 关于圆整数的一个注解 …… 361
22.13 $d(n)$ 的正规阶 …… 361
22.14 Selberg 定理 …… 362
22.15 函数 $R(x)$ 和 $V(\xi)$ …… 364
22.16 定理 434、定理 6 和定理 8 证明的完成 …… 367
22.17 定理 335 的证明 …… 369
22.18 k 个素因子的乘积 …… 370
22.19 区间中的素数 …… 372
22.20 关于素数对 $p, p+2$ 的分布的一个猜想 …… 372
本章附注 …… 374

第 23 章 Kronecker 定理 …… 377
23.1 一维的 Kronecker 定理 …… 377
23.2 一维定理的证明 …… 378
23.3 反射光线的问题 …… 380
23.4 一般定理的表述 …… 382
23.5 定理的两种形式 …… 383
23.6 一个例证 …… 384
23.7 Lettenmeyer 给出的定理的证明 …… 385
23.8 Estermann 给出的定理的证明 …… 386
23.9 Bohr 给出的定理的证明 …… 388
23.10 一致分布 …… 390
本章附注 …… 391

第 24 章 数的几何 …… 393
24.1 基本定理的导引和重新表述 …… 393
24.2 简单的应用 …… 394
24.3 定理 448 的算术证明 …… 396
24.4 最好的可能的不等式 …… 397
24.5 关于 $\xi^2+\eta^2$ 的最好可能的不等式 …… 398