TURING 图灵数学·统计学丛书23

An Introduction to the Theory of Numbers

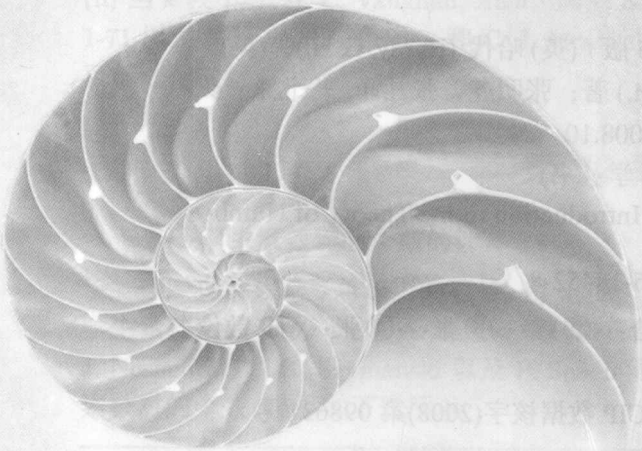
数论导引

（第5版）

[英] G. H. Hardy　E. M. Wright　著
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23



An Introduction to the Theory of Numbers

数论导引

（第5版）

[英] G. H. Hardy　E. M. Wright　著
张明尧　张　凡　译

人民邮电出版社
北　京

图书在版编目(CIP)数据

数论导引：第5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，2008.10

(图灵数学·统计学丛书)

书名原文：An Introduction to the Theory of Numbers

ISBN 978-7-115-18452-8

Ⅰ.数… Ⅱ.①哈…②赖…③张…④张… Ⅲ.数论 Ⅳ.O156

中国版本图书馆 CIP 数据核字(2008)第 098631 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

数论导引(第5版)

◆ 著　[英] G. H. Hardy　E. M. Wright

译　张明尧　张　凡

责任编辑　张继发

◆ 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

北京隆昌伟业印刷有限公司印刷

◆ 开本：700×1000　1/16

印张：29.75

字数：617 千字　2008 年 10 月第 1 版

印数：1–3 000 册　2008 年 10 月北京第 1 次印刷

著作权合同登记号　图字：01-2007-4237 号

ISBN 978-7-115-18452-8/O1

定价：69.00 元

读者服务热线：(010)88593802　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《数论导引》一书初版于 1938 年, 是作者多年在英国牛津大学、剑桥大学、阿伯丁大学以及其他大学所作的若干数论讲座讲义的汇编. 现在出版的中文译本是以原英文书第 5 版为蓝本翻译的.

到今年, 原书初版已整整 70 年了. 在这 70 年中, 数论本身已经有了长足的进展, 它的理论、方法都有了巨大的发展和进步, 人们在对解析数论、代数数论、超越数论以及计算数论等许多重要问题的研究中取得了令人瞩目的重大成果, 完整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). 从这个意义上说, Hardy 和 Wright 的《数论导引》一书的某些内容已落后于我们时代的发展, 这是任何经典著作都无法避免的. 然而, 鉴于这部书仅仅是有关数论基础知识的一个导引性著作, 它的所有的基本内容并没有过时, 更由于作者引人入胜、深入浅出的写作风格, 所以本书历经 70 年的考验, 至今仍然是为数不多的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》).

这部书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的、希望学习数论的学生以及对数论感兴趣的数学工作者编写的. 全书共分 24 章, 分别介绍了素数理论、数的几何、同余式理论、二次剩余和二次互倒律、连分数、用有理数逼近无理数、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. 在每一章的最后, 都有一个关于本章内容的附注, 介绍相关问题的起源、历史发展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, 译者编写了一个简短的补遗予以介绍. 我当初正是靠着这本著作的指引, 才找到了研究的乐趣, 并最终走上了学习和研究数论的人生道路. 希望这本书的中文版能对年轻的数论爱好者也有相当的帮助和教益.

最后, 要感谢我的夫人盛筱平女士, 她的关爱和帮助大大减轻了我们在翻译这部名著时的负担和困难. 同时也要感谢人民邮电出版社图灵公司的诸位领导和编辑, 他们的努力工作和协作精神使得这部著作的中文版得以顺利出版.

张明尧

2008 年 3 月 4 日于上海

第 5 版前言

这一版的主要改变是每一章后面的附注. 我力求为那些希望深入研讨某个特定论题的读者提供最新的参考文献, 并在附注及正文中对当前的知识状况都作比较精确的阐述. 为此我参考了像 *Zentralblatt* 和 *Mathematical Reviews* 这样的一些极具价值的出版物. 而且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, 并回答了我的问题. 特别感谢 J. W. S. Cassels 教授和 H. Halberstam 教授, 他们应我的要求, 为我提供了众多宝贵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, 我尽可能地保持了原书的页码不作任何调整. 因此, 尽管我补充了一个很短的附录, 介绍素数论某些方面的最新进展, 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

本书是最近 10 年间由我们在若干所大学的讲座逐渐完善而形成的. 它与许多由讲座形成的书很相似的是, 这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详尽的介绍, 只不过作为一个或者一系列的导引来轮流阐述几乎所有这些方面的内容. 我们对诸多论题中的每一个都有所涉及, 虽然人们通常并不把它们合起来放在单独的一本书之中. 我们同时也探讨某些并不总是被视为数论的内容, 例如像第 12 章至第 15 章属于数的 "代数的" 理论, 第 19 章至第 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 章讲述的是通常归属于 "数的几何" 或者 "Diophantus 逼近" 这一范畴的内容. 我们所规划的内容极其丰富, 但少有深度. 因为在四五百页的篇幅里完全不可能对这么多论题中的任何一个进行深入的研究.

本书有很大的漏洞, 任何一位专家学者都能立即看得出来. 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, 而且常见的书中对此都有充分的讨论. 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的东西可以添加.

我们经常根据个人兴趣来决定写作计划, 我们选取某些论题, 很少是因为它们的重要性 (尽管它们中大多数都很重要), 而是因为它们很合我们的心意, 也因为其他的作者给我们留下了写作的空间. 我们的本意是写一本有趣的书, 一本与众不同的书. 或许我们已经取得了成功, 而成功的代价是书中有不少怪异之处; 或许我们已经失败了, 但是我们很难完全失败, 因为所研究的论题如此引人入胜, 除非我们实在无能才会使它变得乏味.

本书是为从事数学工作的人写的, 但并不要求读者具有任何高深的数学知识或者技巧. 前 18 章只需要读者具备中学程度的数学知识, 任何一个聪明的大学生都会发现本书浅显易懂. 后 6 章要困难一些, 需要读者有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内容.

本书书名与 L. E. Dickson 教授的一本非常有名的书同名 (但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, 但是有人提出用这个书名可能会误导读者.

有若干位朋友在本书的出版过程中给予了帮助. H. Heilbronn 博士阅读了全部手稿以及清样, 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. 他们还检查了每一章后面的附注中的大部分参考文献. H. Davenport 博士和 R. Rado 博士也阅读了本书的部分内容, 特

别是最后一章, 由于他们以及 Heilbronn 博士的建议, 与初稿相比几乎有了全新的面貌.

我们还从参考书目所列举的其他图书 (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, 我们与所有热衷于学习数论的学生一样, 无论如何感谢他都是毫不过分的.

G. H. H.
E. M. W.
1938 年 8 月于英国牛津

关于记号的说明

我们从形式逻辑中借用 4 个符号, 它们是

$$\rightarrow,\ \equiv,\ \exists,\ \in .$$

“$\rightarrow$” 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”, 或者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 “$=$”(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

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

的含义是 “存在一个 l 使得 (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

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

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”.

一个定理的编号上加星号 (例如, 定理 15*) 表明该定理的证明较有难度, 不适合放在本书中. 那些未加星号但也未加以证明的定理可以利用本书中的类似方法予以证明.

目　录

第1章 素 数 (1)

1.1 整 除 性

数

$$\cdots, -3, -2, -1, 0, 1, 2, \cdots$$

称为**有理整数**(rational integer), 或简称为**整数**(integer). 数

$$0, 1, 2, 3, \cdots$$

称为**非负整数**(non-negative integer). 数 $1, 2, 3, \cdots$ 称为**正整数**(positive integer). 正整数构成算术的主要对象, 但它基本上常被视为整数或者某个更大范围内的数的一个子集.

以后我们用字母

$$a, b, \cdots, n, p, \cdots, x, y, \cdots$$

表示整数, 它们有时 (但并不总是如此) 会服从某些进一步的限制条件, 比如正数或非负数这样的限制. 我们也常用 "数" 来指代 "整数"(或表示 "正整数" 等), 在正文中的含义明确无误时, 我们考虑的就仅仅是这种特殊类型的数.

称一个整数 a 能被另一个整数 $b(b \neq 0)$**整除**(divisible), 如果存在第 3 个整数 c 使得

$$a = bc.$$

如果 a 和 b 都是正数, c 必为正数. 用记号

$$b|a$$

来表示 a 被 b 整除, 或 b 是 a 的一个**因子**(divisor). 于是有

$$1|a, \quad a|a,$$

且对每个不为零的数 b 均有 $b|0$. 有时也用

$$b \nmid a$$

来表示与 $b|a$ 相反的含义. 显然有

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

$$b|a \rightarrow bc|ac \text{ (如果 } c \neq 0),$$

以及

$$c|a, c|b \rightarrow c|(ma + nb) \text{ (对任何整数 } m \text{ 和 } n).$$

1.2 素 数

在 1.2 节到 2.9 节中, 我们考虑的数一般都是正整数.[①] 正整数中有一个特别重要的子集, 即素数集合. 数 p 称为*素数*(prime), 如果

(i) $p > 1$,

(ii) p 没有除了 1 和 p 以外的正因子.

例如, 37 是一个素数. 要特别注意 1 不算作素数. 在第 1 章以及第 2 章里, 我们始终用字母 p 表示素数.[②]

大于 1 且不是素数的数称为*合数*(composite).

下面引入第一个定理:

定理 1 *除了 1 以外的每个正整数都是素数的乘积.*

n 要么是素数 (此时不需要证明了), 要么 n 有大于 1 且小于 n 的因子. 设 m 是这些因子中最小的一个, 那么 m 必为素数, 否则,

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

则

$$l|m \to l|n,$$

这与 m 的定义矛盾.

因此, n 要么是素数, 要么可以被一个小于 n 的素数 (比方说 p_1) 整除. 在后一种情形中, 有

$$n = p_1 n_1, \quad 1 < n_1 < n.$$

这里 n_1 要么是素数 (此种情形证明已经完成), 要么 n_1 可以被一个小于 n_1 的素数 p_2 整除, 此时有

$$n = p_1 n_1 = p_1 p_2 n_2, \quad 1 < n_2 < n_1 < n.$$

重复这个方法, 得到一列递减的数 $n, n_1, \cdots, n_{k-1}, \cdots$, 它们全都大于 1, 对其中每个数都同样有以上两种可能性成立. 但迟早我们必定会接受第一种可能性, 此时得到的 n_{k-1} 已经是一个素数, 比如记之为 p_k, 这样就得到

$$n = p_1 p_2 \cdots p_k. \tag{1.2.1}$$

例如

$$666 = 2 \times 3 \times 3 \times 37.$$

① 偶尔也有例外, 如在 1.7 节中, e^x 是分析中的指数函数.

② 需要注意的是, 如果本书自始至终都严格遵守这个约定会很不方便, 因而有时也不坚持用它表示素数. 例如第 9 章用 p/q 表示典型的有理分数, 其中的 p 并不总是表示素数. 不过 p 是表示素数的 "自然的" 字母, 因此只要方便的话, 我们总用这个字母来表示素数.

如果 $ab=n$, 那么 a 和 b 不可能都大于 $\sqrt{n}$. 于是任何合数 n 必可被一个不超过 $\sqrt{n}$ 的素数 p 整除.

(1.2.1) 式中的素数不一定是互不相同的, 也不一定非要按照某个特定的次序排列. 如果把它们按照递增的顺序排列, 把相同的素数合写成单一的因子, 并适当改变记号, 就得到

$$n=p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}\ (a_1>0,a_2>0,\cdots,p_1<p_2<\cdots). \tag{1.2.2}$$

称 n 被表示成了**标准型**(standard form).

1.3 算术基本定理的表述

在定理 1 的证明中没有证明 (1.2.2) 式是 n 的唯一表示, 换句话说, 除了因子可以重新排列外, (1.2.1) 式是唯一的. 然而考虑几个特殊情形可以立即看出这是正确的.

定理 2(算术基本定理) *n 的标准型是唯一的. 也就是说, 除了因子可以重新排列以外, n 只能用唯一一种方式表示成素数的乘积.*

定理 2 是算术理论体系的基础, 但本章不会用到它, 关于它的证明将在 2.10 节给出. 但是, 证明它是下面较为简单的定理的一个推论还是很方便的.

定理 3(Euclid 第一定理) *如果 p 是素数, 且 $p|ab$, 那么 $p|a$ 或者 $p|b$.*

眼下先将此定理视为已经成立, 由它来推导出定理 2. 这样一来, 定理 2 的证明就简化为证明定理 3, 而定理 3 的证明在 2.10 节中给出.

显然,

$$p|abc\cdots l \to p|a \text{ 或者 } p|b \text{ 或者 } p|c\cdots \text{ 或者 } p|l$$

是定理 3 的一个推论. 特别地, 如果 $a,b,\cdots,l$ 都是素数, 那么 p 是 $a,b,\cdots,l$ 中的一个. 现在假设

$$n=p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}=q_1^{b_1}q_2^{b_2}\cdots q_j^{b_j},$$

其中每个乘积都是标准型中的素数乘积. 从而对每个 i 都有 $p_i|q_1^{b_1}\cdots q_j^{b_j}$, 于是每个 p 都是某个 q. 类似地, 每个 q 都是某个 p. 所以有 $k=j$, 又由于这两个素数集合都是按照递增次序排列, 因此对每个 i 有 $p_i=q_i$.

如果 $a_i>b_i$, 用 $p_i^{b_i}$ 来除即得

$$p_1^{a_1}\cdots p_i^{a_i-b_i}\cdots p_k^{a_k}=p_1^{b_1}\cdots p_{i-1}^{b_{i-1}}p_{i+1}^{b_{i+1}}\cdots p_k^{b_k}.$$

左边可以被 p_i 整除, 然而右边则不能: 这是一对矛盾. 类似地, $b_i>a_i$ 也同样推出矛盾. 由此得出有 $a_i=b_i$. 这就完成了定理 2 的证明.

现在就会清楚为什么不把 1 作为素数. 因为如果把 1 作为素数的话, 定理 2 就不能成立, 这是因为此时可以插入任意多个 1 作为乘积因子.