研 究 生 数 学 丛 书 9
Mathematics Series for Graduate Students

素数论

Les Nombres Premiers

GÉRALD TENENBAUM
MICHEL MENDÈS FRANCE 合著

姚家燕 翻译
文志英 审校

清华大学出版社 Springer

研 究 生 数 学 丛 书 9
Mathematics Series for Graduate Students

素数论

Les Nombres Premiers

GÉRALD TENENBAUM
MICHEL MENDÈS FRANCE 合著

姚家燕 翻译
文志英 审校

清华大学出版社
北京

Springer

GÉRALD TENENBAUM, MICHEL MENDÈS FRANCE
Les nombres premiers
ISBN 2-13-048399-2

图书在版编目（CIP）数据

素数论 /（法）戴南勃姆（Tenenbaum, G.），（法）孟戴斯－弗朗斯（Mendès France, M.）著；姚家燕译. —北京：清华大学出版社，2007.10
（研究生数学丛书）
ISBN 978-7-302-15332-0

Ⅰ. 素…　Ⅱ. ①戴…　②孟…　③姚…　Ⅲ. 素数－研究生－教材　Ⅳ. O156.2

中国版本图书馆 CIP 数据核字（2007）第 079551 号

责任编辑：陈朝晖
责任校对：赵丽敏
责任印制：王秀菊
出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　**邮　　编**：100084
c-service@tup.tsinghua.edu.cn
社 总 机：010-62770175　**邮购热线**：010-62786544
投稿咨询：010-62772015　**客户服务**：010-62776969
印 装 者：北京市清华园胶印厂
经　　销：全国新华书店
开　　本：170×230　**印　张**：8　**字　数**：122 千字
版　　次：2007 年 10 月第 1 版　　**印　　次**：2007 年 10 月第1 次印刷
印　　数：1～3000
定　　价：23.00 元

编审委员会

研究生数学丛书 Mathematics Series for Graduate Students

1. 连续介质力学中的数学模型
(Mathematical Modeling in Continuum Mechanics)

2. 应用密码学
(Applied Cryptography)

3. Introduction to Malliavin Calculus
(Malliavin 随机变分引论)

4. 纠错码的代数理论
(Algebraic Theory of Error-Correcting Codes)

5. 抽象代数基础
(Basic Algebra)

6. Algebraic Geometry
(代数几何)

7. 反问题
(Inverse Problem)

8. 泛函分析——理论和应用
(Analyse Fonctionnelle —— Théorie et applications)

9. 素数论
(Les nombres premiers)

总 序

数学是一门在非常广泛的意义下研究自然和社会现象中的数量关系和空间形式的科学. 长期以来，在人们认识世界和改造世界的过程中，数学作为一种精确的语言和一个有力的工具一直发挥着重要的作用. 在现代，数学科学已构成包括纯粹数学及应用数学内涵的众多分支学科和许多新兴交叉学科的庞大的科学体系. 作为各门科学的重要基础，作为“四化”建设的重要武器，作为人类文明的重要支柱，数学科学在很多重要的领域中已起着关键性甚至决定性的作用，数学技术已成为高技术的突出标志和重要组成部分. 数学的影响和作用已深入到各行各业，可以说无处不在. 马克思当年的预言：“一门科学只有当它成功地运用了数学之后，才算达到了真正完善的地步”，正在不断得到证实. 在这样的背景下，数学科学的重要性已得到空前广泛的认同. 在研究生（不限于数学专业的研究生）的培养中，重视数学基础的训练，强调数学思想的熏陶，也已成为一种必然的趋势. 但是，国内研究生数学教材及参考读物的实际情况，无论从品种、数量及质量各方面来看，都远远不能适应这个形势，甚至也远远落后于本科生的数学教材. 这已成为制约提高研究生培养质量的一个重要瓶颈. 清华大学出版社和施普林格出版社(Springer-Verlag)合作，倡议出版这一套《研究生数学丛书》(Mathematics Series for Graduate Students)，可望改善这方面的状况，为我国的研究生打好数学基础、提高数学素质起到积极的作用.

根据数学这门科学的特点，同时考虑到研究生学习数学的基本要求和特有方式，这套以面向研究生（包括高年级本科生、硕士及博士研究生）的数学教材或参考读物，将力求体现以下的一些原则：

- 主题具有理论或（和）应用方面的重要性；
- 在重点介绍基础性内容的前提下，兼顾学科前沿的重要发展趋势和研究成果；
- 在讲授数学内容的同时，充分体现数学的思想方法和精神实质；
- 少而精，在较小的篇幅中展现基本的内容；
- 有相当好的可读性，适宜读者自学；
- 附有习题、思考题及参考资料目录，书末有索引，方便读者深入学习与思考.

为了有利于体现这些原则，本丛书将采取相当灵活的体例及风格：内容可以是纯粹数学、应用数学或数学与其他学科的交叉；可以是较系统地介绍某一个分支的教材，或是介绍某一前沿分支状况的综述，也可以是课外参考书；可以是原著，也可以是译著；可以是国内作者，也可以是国外作者；可以用中文编写，也可以用英文编写，等等.

要实现本丛书的目标和宗旨，任重而道远，但千里之行，始于足下.在学界同仁和广大读者的支持和帮助下，让我们共同努力.

李大潜

2003 年 9 月于上海

中文版前言

面对让人感到惊讶(或许是反感?)的风险，我们坚持认为数学著作也应该是文学作品.在数学变得极为尖端复杂这一现实情况下，描述那些计算通常比实施它们更有助于分享知识. 从这个角度而言，文笔是科学论文的一个基本要素，无论它是乏味的还是充满诗意的，是简洁的还是典雅的.

因此，将一本数学书从一种语言翻译成另外一种语言并不是一件简单的事情.翻译者会基于他自己的风格和意愿来重新组织原文. 于是从某种意义上讲，他就成了作者. 我们的翻译者是数学工作者姚家燕，他完成了一项极具华彩的工作：我们的中国朋友向我们肯定了这点，而我们知道他们是真诚的. 他在完成这项工作期间曾得到了两位同行的帮助,他们是北京的文志英教授和法国南锡的吴杰研究员. 我们谨向他们表示最热忱的感谢!

这是我们继法文版和英文版之后所出的第三个版本. 在此，我们仅更新了那些在前面版本出版之后获得了巨大进展的论题,而没有增加任何新的概念. 参考文献也更新了.

热哈尔德·戴南勃姆

米歇尔·孟戴斯-弗朗斯

2005 年 11 月分别于南锡和波尔多

译者的话

素数论

《素数论》是法国大学出版社出版的大型丛书《知否？》(也译为《我知道什么？》)中的第 571 卷. 该丛书是法国科普著作方面的杰出代表, 迄今已出版三千七百多卷, 覆盖了几乎所有的领域, 成为法国大众文化修养的一部分. 每卷的篇幅都是 128 页, 均为所涉及领域内的顶尖专家撰写, 书名永远不变, 但内容却会围绕主题随着学科前沿的变化和需要而不断更新. 本书的法文版是最新的第三版, 在 1997 年出版后即大受欢迎, 并在 1999 年被授予 Paul Doistau-Émile Blutet 奖. 随后在 2000 年出了第二版, 同年由美国数学学会出了英文版.

本书介绍现代解析素数论, 同其前两版相比, 在内容上更深也更为现代. 本书从数论的某些经典论题入手, 而以讨论一些著名的猜想作为结束, 其目的是想让读者对素数理论有一个初步的了解, 并以此为依托来解释为什么如此高度有序的素数序列会蕴涵着大量的令人惊叹的随机性. 事实上, 将概率的思想引入素数论是上世纪末素数研究中的一个值得注意的动向, 而本书正是介绍该发展动向的一本极好的入门书. 整本书语言通俗朴素, 行文流畅, 特别适合高年级本科生或研究生阅读.

在翻译本书的各个不同阶段, 林莉女士和田庆生博士在语言修饰方面给予了本人许多指导和帮助. 文志英教授仔细审校了全文并提出了许多建设性意见. 吴杰研究员, 曲彦博士, 胡慧硕士, 以及陈修梅硕士通读了全文并给出了许多有益建议. 两位原著作者也提供了不少帮助. 在此对他(她)们一并表示最诚挚的谢意! 最后还要感谢法国大学出版社的 Marion Colas 女士以及清华大学出版社的陈朝晖先生, 没有两位不懈的努力和卓有成效的工作, 本书的中文版可能永远也不会问世!

谨将此书献给 Paul Erdös 以表达我们深切的怀念. 1996 年 9 月, 就在本书法文版第一版完成之际, 他离开了人世. 对我们来说, 他是位叔叔 (朋友们也正是这样称呼他的) 和导师. 一代数学巨匠就这样走了, 但他的影响将永世长存.

法文版前言

《知否?》这一丛书的第 571 卷已有一段历史. 其第一版可追溯到 1953 年. 作者是对分析、概率和数学物理产生过不可磨灭影响的杰出数学家Émile Borel. 他的一些开创性工作涉及概率论在数论中的应用, 但可惜这部分内容未能在其《素数论》中提及. 利用随机来研究必然性确实有令人震惊的地方, 然而这却是本世纪整个数学特别是数论最深刻的成果之一.

Jean Itard 在 1969 年接替Émile Borel 撰写了新的《素数论》. 他在书中用了大量的篇幅来讨论数论中的代数方法. 这无疑使新版的《素数论》更易于为初学者接受.

我们决定采取与两位前任截然不同的做法来进行一场也许是野心勃勃的赌博: 介绍现代解析素数理论.

一个世纪以来, 在对是否有许多素数、它们是如何分布的等古老问题进行解答的过程中, 素数论获得了史无前例的发展, 而这尤其要归功于该理论与概率论之间的相互融合与渗透. 素数表显示了素数的混沌特性, 而其表面的无序性最终却与一些, 比如说源于物理现象的经典随机模型相吻合. 这本小册子的目的也正在于此: 描述, 然后试着理解为什么像素数这样高度确定的序列能够包含着那样的随机性.

我们来对这一点作进一步的讨论. 完全随机即混沌具有无穷大的复杂度; 另一方面, 整数的复杂度显然是随其大小的增加而增大: 整数 $2^{6972593}-1$ 是素数吗[1)] ? 在无穷远处, 整数序列表现出随机的性状, 因而素数序列也蕴涵着随机性. 如何对这一现象进行分析解释是解析数论的前沿研究课题.

[1)] Hajratwala, Woltman 和 Kurowski 在 1999 年对此给了一个肯定的回答.

物理学家和哲学家们仍在争论假想的“隐变量”. 哥本哈根学派同 Niels Bohr 一道捍卫亚原子世界为随机规律所主宰的观点. 至于 Einstein, 他则向往一个借助于亚亚原子并完全属于决定论的解释. 素数序列能否作为模型来为其想法服务呢? Einstein 认为上帝不是掷骰子的, 而就在同时, 杰出的数论专家 Mark Kac 却公开宣称素数与掷硬币猜正反面的游戏暗暗吻合.

自从 Legendre 和 Gauss 猜测素数满足一个和谐的分布规律, 即第 n 个素数近似地等于 $n\log n$ [1], 有序/无序的辨证关系就一直吸引着数论学家们的注意力. 这样一个随机中的规则性不应该让人吃惊：什么能比抛掷硬币所出现的结果更难以预料呢？然而控制事件的概率恒等于 $\frac{1}{2}$ 却是一个绝对刚性的规律.

我们决定依托历史沿革及哲学思想的演变来描述这些现象, 也就是说侧重于基本概念来介绍素数理论. 第 1、第 2 和第 4 章主要涉及正则性方面的结果, 而第 3 章则着重讨论素数分布的随机性. 在第 5 章, 我们将描述那些构成本理论骨架的主要猜想. 人们最终将会明白随机与必然的区别只是表面的: 二者互相解释说明并协调地统一起来共同生成素数的内在结构.

任何选择都必然有其局限性: 我们所采用的叙述方式也有其危险和缺陷. 故意地 (某些人会说是令人反感地) 与此类著作的百年传统相决裂. 我们既不提供素数表[2]也不给出二次互反律最让我们喜爱的证明. 更为严重的是, 我们也没有讨论交换代数中有关素数的各种深刻推广: 数域中的素理想, 环或有限域上的既约多项式等. 关于这些, 读者可查阅已有的法文经典著作[3]. 我们也几乎完全忽略了素数的“因子”性质, 而这却正是数论中的概率方法所优先考察研究的地方[4]. 最后, 我们也只是 (在第 1 章第 3 节) 很简单扼要地讨论了该理论中的密码学和算法. 在最近几年里, 它们令人瞩目的应用已广

---

[1] 该猜想于 1896 年由 Jacques Hadamard 和 Charles de La Vallée-Poussin 所独立证明, 距今约 100 多年.

[2] 台式计算机可以很容易地弥补这个缺陷.

[3] 例如可参见: P. Samuel, *Théorie algébrique des nombres,* Hermann, 1967; Z. I. Borevitch & I. R. Chafarevitch, *Théorie des nombres,* Gauthier-Villars, 1967; J.-P. Serre, *Corps locaux,* Hermann, 1968. 以上三书均有英文版.

[4] 这个观点在最近出版的一些著作中得到了展开和详细讨论, 尤其可见: P. D. T. A. Elliott, *Probabilistic number theory* (2 vol.), Springer-Verlag, 1979-1980; R. R. Hall & G. Tenenbaum, *Divisors,* Cambridge University Press, 1988.

为大众媒体所了解[1].

整个科学以及它所包含的数学已构成大众文化修养的一个不断增长壮大的组成部分. 再说, 也不缺乏讨论素数那些惊人性质的"有趣且令人愉快"[2]的著作. 事实上, 它们当中的一些还相当优秀[3]. 因此在这本科普著作中, 我们选择了与时下流行观点不同的做法而特意将目标瞄得稍高一些. 我们清醒地明白某些论述可能会看起来有些难 —— 实际上它们也确实很难. 我们有时会选择一个简短的计算 (对于数学工作者们来说, 简短的计算相当于图解说明) 而不是一些长的解释. 文体也有意弄得有些言简意赅, 甚至时不时地做一些影射暗示. 对我们来说, 为了突出一些要点, 这样做是非常必要的. 因此我们希望书中的一些局部完整的证明能够满足那些勤奋刻苦有韧性的读者的好奇心 —— 也正是出于这个考虑, 我们才撰写了基本上可以单独阅读的第 4 章. 但我们也鼓励没有时间或不太愿意进入细节的读者以"对角线"的方式来阅读这本小书. 事实上只有定义是重要的. 一旦理解了这些定义以及它们之间互相关联的内在逻辑/音乐关系, 剩下的只是一些饶舌的闲话.

我们反对学究式的分析性阅读, 即只在消化理解第 n 行后才读第 $n+1$ 行的阅读方式. 我们建议读者沿着贯穿全文的主线, 如级进滑奏的音乐那样进行综合性阅读 (正是由于本书叙述的相对紧凑性才使得这种阅读方式成为可能).

在综合阅读结束后, 什么也不能阻止大家手拿算笔回过头来验证那些严格甚至是困难的证明 (读者将明白, 为取得更大进步, 这样做其实是非常必要的). 所有的努力都将证明是值得的.

因此本书并不容易, 但我们仍希望能够透过其神秘色彩为大家带来一股悠悠的诗意. 梦幻源于复杂. 关于这一点, Stéphane Mallarmé 和 Umberto Eco 都不会同我们唱反调.

在撰写这本小册子的各个不同阶段, 我们得到了大量的、各种形式的友好帮助. 在这里谨向 Jean-Paul Allouche, Jean-Philippe Anker, Michel Balazard,

---

1) 若想对此有更多了解, 可参见: G. Robin, *Algorithmique et cryptographie*, SMAI, coll. 《Ellipses》, 1991.

2) 根据 Bachet 的说法 (1612).

3) 由 P. Ribenboim 所撰写的内容完整、阐述透彻的书*Nombres premiers: mystères et records*, PUF, 1994, 就属于这类著作.

Daniel Barlet, Régis de La Bretèche, Éric Charpentier, Hédi Daboussi, Cécile Dartyge, Jean-Marc Deshouillers, Jean-Claude Fort, Andrew Granville, Jerzy Kaczorowski, Bernard Landreau, Pierre Marchand, Gérard Mathieu, Jean-Louis Nicolas, Emmanuel Pedon, Patrick Sargos, Jacques Sicherman, André Stef, 吴杰和 Paul Zimmermann 表达我们最特别的谢意.

热哈尔德·戴南勃姆
米歇尔·孟戴斯-弗朗斯

1996 年 9 月分别于南锡和波尔多

记号与约定

我们在这里指出整本书中都会用到的主要记号与约定. 至于那些只在某一章节出现的, 我们将在它们出现的地方给出定义.

字母 $\mathbb{N}$ 表示自然数集 $\{1, 2, \cdots\}$, 而 $\mathscr{P}$ 表示素数集. 整数集, 实数集和复数集分别用 $\mathbb{Z}$, $\mathbb{R}$ 和 $\mathbb{C}$ 来表示. 字母 p, 不管带或不带下标, 总是表示 $\mathscr{P}$ 中元素. 我们用 $a \mid b$ (相应地, $a \nmid b$) 来表示 a 整除 b (相应地, a 不整除 b), 而 $p^\nu \parallel a$ 意味着 $p^\nu \mid a$ 且 $p^{\nu+1} \nmid a$.

两整数 a, b 的最大公约数记为 (a, b). 当 $(a, b) = 1$ 时, 我们称 a 与 b 互素.

有限集 A 的元素个数可根据情况记为 $|A|$ 或者 $\sum_{a\in A} 1$. 对于整数 $a \in \mathbb{N}$, 我们用 $P^+(a)$ (相应地, $P^-(a)$) 来表示它的最大素因子 (相应地, 最小素因子), 其中约定 $P^+(1) = 1$, $P^-(1) = \infty$.

自然对数记作 $\log$ [1]. 它的迭代函数 $\log\log$, $\log\log\log$ 等记为 $\log_2$, $\log_3$ 等. 欧拉常数 γ 被定义为极限

$$\gamma = \lim_{N\to\infty} \Big(\sum_{n\leqslant N} 1/n - \log N \Big).$$

因此 $\gamma \approx 0.577215664$. 须注意的是, 我们在第 2 章中会采用习惯做法, 也用 γ 来表示 Riemann zeta 函数一般非平凡零点的虚部.

实数 x 的整数部分与小数部分分别记为 $[x]$ 和 $\{x\}$. 因此

$$[5/3] = 1, \quad \{-3.15\} = 0.85.$$

符号 $:=$ 表示等式的左边由其右边来定义.

---

[1] 因此在 $a \geqslant 1$ 时, $\log a$ 就是由数轴 $x = 1$, $x = a$, $y = 0$ 与曲线 $y = 1/x$ 所围成的区域的面积. 当 a 变得 "很大" 时, 我们有 $\log a \sim \sum_{n\leqslant a} 1/n$.

对数积分函数被定义为

$$\mathrm{li}(x) := \int_2^x \frac{\mathrm{d}t}{\log t} \qquad (x \geqslant 2).$$

当字母 s 表示一个复数时, 我们通过关系式 $s = \sigma + i\tau$ 来隐含地定义其实部和虚部.

对于给定的实变量或复变量函数 f, g, 我们将不加区别地使用 Landau 记号 $f = O(g)$ 或 Vinogradov 记号 $f \ll g$ 来表示存在一个正常数 C 使得在 f 与 g 的公共定义域内有 $|f| \leqslant Cg$. 有时常数 C 会依赖于某一参数 α, 这时我们记 $f = O_\alpha(g)$ 或 $f \ll_\alpha g$. Landau 记号 $f = o(g)$ 习惯上表示 $\lim f/g = 0$ [1].

在集合 A 上为 1, 而在它的余集上为 0 的函数被称为该集合的*示性函数*. 最后, 我们用 $\mathscr{C}^k[a, b]$ 来表示在区间 $[a, b]$ 上 k 次连续可导的函数所构成的函数空间.

另外, 我们还经常利用下面的技巧来估计函数 $f \in \mathscr{C}^1[1, x]$ 被一些系数 $a_n \in \mathbb{C}$ 在其整点加权平均后所得到的和式:

$$\begin{aligned}\sum_{1\leqslant n\leqslant x} a_n f(n) &= \sum_{1\leqslant n\leqslant x} a_n \Big\{ f(x) - \int_n^x f'(t)\,\mathrm{d}t \Big\} \\ &= f(x) \sum_{1\leqslant n\leqslant x} a_n - \int_1^x f'(t) \Big\{ \sum_{1\leqslant n\leqslant t} a_n \Big\} \mathrm{d}t.\end{aligned}$$

[1] 因此 $O(1)$ 表示一个有界量而 $o(1)$ 为一个趋向于 0 的量.

目　录

素数论