颜松远 著
杨思熳 刘 巍 齐璐璐 陶红伟 译

# 计算数论（第2版）

# Number Theory for Computing

2nd Edition

清华大学出版社

颜松远 著
杨思熳 刘 巍 齐璐璐 陶红伟 译

# 计算数论（第2版）

# Number Theory for Computing

## 2nd Edition

清华大学出版社
北京

## 内 容 简 介

本书是德国施普林格出版社出版的 *Number Theory for Computing* (2nd Edition)的译作. 作者长期从事计算数论与计算复杂性理论的研究,擅长于从数论和计算机科学的结合上研究数论算法和密码算法的复杂性以及难解性. 本书是一本学术专著,主要内容包括初等数论、计算数论、计算与密码学中的数论,叙述清楚易懂,适合作为数学专业和计算机专业的研究生或高年级本科生的教材.



**图书在版编目(CIP)数据**

计算数论: 2 版 / (英) 颜松远著; 杨思熳等译. —北京: 清华大学出版社, 2008.11
书名原文: Number Theory for Computing, 2nd Edition
ISBN 978-7-302-18310-5

Ⅰ. 计… Ⅱ. ①颜… ②杨… Ⅲ. 计算—数论 Ⅳ. O156

中国版本图书馆 CIP 数据核字(2008)第 117041 号

**责任编辑**: 张瑞庆 张为民
**责任校对**: 焦丽丽
**责任印制**: 杨 艳

**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
**社 总 机**: 010-62770175 **邮 购**: 010-62786544
**投稿与读者服务**: 010-62776969, c-service@tup.tsinghua.edu.cn
**质 量 反 馈**: 010-62772015, zhiliang@tup.tsinghua.edu.cn
**印 刷 者**: 清华大学印刷厂
**装 订 者**: 北京市密云县京文制本装订厂
**经 销**: 全国新华书店
**开 本**: 185×230 **印 张**: 23.75 **字 数**: 486 千字
**版 次**: 2008 年 11 月第 1 版 **印 次**: 2008 年 11 月第 1 次印刷
**印 数**: 1～3000
**定 价**: 35.00 元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题,请与清华大学出版社出版部联系调换. 联系电话: 010-62770177 转 3103 产品编号: 023095-01

# 王元院士关于本书的介绍

颜松远教授著“Number Theory for Computing”(Springer,2nd Edition,译为计算数论)是一本很好的书,现在介绍如下:

1. 全书包括三部分:(1)“初等数论”.这部分的内容是熟知的,但该书很重视计算和实例,其中关于素数分布(1.5 节)与椭圆曲线的算术理论(1.7 节)是一般初等数论书很少写或不写的.(2)“计算或算法数论”.作者首先讲述了计算复杂性问题,然后讲到整数的素性检验、因子分解及离散对数计算.前两个问题虽然在小学就讲到过,但当整数略大,就无法实际计算了.作者介绍了一些实际算法及计算复杂性研究,这部分还包括较新近的“量子数论计算”.(3)“计算与密码学中的应用数论”.这部分内容很丰富,包括数的剩余系计算与表示、随机数的生成以及很多密码学特别是公钥密码及信息安全方面的一些著名方法的介绍.这些内容在通常的数论书中很少涉及.

2. 本书不同于通常按“定义、定理、证明”的顺序写法,而是按“定义、定理、算法、例子”这一顺序写法,读者在看完例子之后再回去看算法,更能一目了然.

3. 本书给出了一些重要数学家的照片与简历,能增加阅读兴趣.每章都提出进一步学习的重要参考文献,可供进一步研究与学习.

关于“计算数论”这个重要领域,国内还未开展研究.该书讲述清楚易懂,既是一本专著,又是一本很好的科普读物,对这一领域的普及与研究工作的推动将会起到很好的作用.自从 2000 年由世界著名出版社 Springer 出版后,2002 年即出版了其第二版,可见该书在国外是很受欢迎的.可以预料,该书中文译本的出版,对国内的读者会有很大的帮助.

王元

2007 年 5 月 25 日

# 英文原著者中文译文版序言

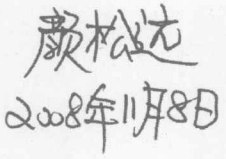
很高兴我的《计算数论》一书的中文译文，能在上海华东师范大学数学系杨思熳教授及其研究团体和清华大学出版社张瑞庆副教授、张为民编辑的共同努力下与我们国内的读者见面.

这本书开始写作于1989年，当时一边教学，一边研究，一边写作，整整写了十年，于1999年完成，2000年4月出第1版，2002年4月出第2版，随后又曾多次重印. 该书还被译成包括波兰文在内的多种文字. 美国数学学会的《数学评论》和美国计算机学会的《计算评论》等多家权威评论刊物都对该书有高度的评价. 在国内，我国著名数学家王元院士、万哲先院士、王梓坤院士和朱尧辰教授等都对该书有很高的评价，尤其是王元院士还在2007年5月身体康复中热情向国内读者介绍该书，万哲先院士曾邀请作者在2008年6月于北京举办《计算数论》讲座. 相信这本书能对我国计算数论与应用的研究起到一定的推动作用. 有关该书的一些修订进展情况，读者可从如下网页上找到：

http://www.springer.com/computer/foundations/book/978-3-540-43072-8

http://math.mit.edu/~syan

非常欢迎国内读者能将您的意见和建议来信告诉我们，以便在再版时能修正和改进. 来信可发电子邮件给 songyuanyan@hotmail.com. 谢谢！



2008年11月8日

# 第 2 版前言

在越来越多的计算数论书籍中，这是一本优秀的、实时性的著作. 它把基本理论、补充这些理论的大量例子，以及使得许多巧妙算法得到进一步发展的那些计算视角很好地融合在一起. 尤其要提到的是，作者对那些当代数论的奠基人，从欧几里得开始的几代贡献者的历史评价和传记进行了精心的收集和剪裁. 这可以让读者对数学的这一丰富而充满挑战性的分支学科的历史有一个不错的了解.

本书共分为三大章. 第 1 章是对初等数论的全面介绍，可作为入门教材. 它涵盖了大部分入门课程的内容，包括可除性、丢番图方程、算术函数、素数分布、同余及椭圆曲线，这些是数论的基本内容. 纳入对椭圆曲线的介绍使得该书更具实时性，受到人们的欢迎.

第 2 章先对计算的复杂性理论作了初步的详细讨论，对人们感兴趣的标准问题的许多著名算法的概况进一步展开，包括素性检测、素因子分解和离散对数等. 这一章中还有一节对量子计算及其相关数论作了令人愉快的介绍.

最后一章介绍了数论的一个为人们所熟悉的重要应用：信息安全与密码学. 这一章还对数论算法在有效算术进程和公钥密码的设计、数字签名及量子密码学的应用作了全面的回顾.

该书可用作研究生一年级的两类课程：第一类课程是数论问题的算法（基于第 1、2 章），第二类课程是数论在计算机算法和信息安全的应用. 书中还包含了大量不同难易程度的练习. 本书也可用作专业人士的指导用书，是该领域出版物中一个令人愉悦且受到欢迎的补充.

# 第1版前言

数学家们研究的不是实物，而是实物之间的关系；只要关系不变，他们就不关心实物被其他实物所替代. 实物并不重要，只有结构才能吸引他们.

亨利·庞加莱(1854—1912)

建议从事因子分解算法的计算机科学家完善他们的数论知识.

伊恩·斯图尔特

《用几何方法快速寻找因子》

《自然》，325卷，1987年1月15日，199页

在数学中，数论主要是研究全体整数性质的理论，特别是正整数. 例如，2000多年前，欧几里得在他的《几何原本》中就证明了存在无穷多个素数. 这门学科因其很少在其他领域中有所应用，而长期被人们认为是最纯的一门数学分支. 但是，近几年来，人们对数论中的一些主要问题的研究兴趣有了明显的提高，正是由于它们在其他领域的重要性以及诸多应用，特别是在计算和信息技术领域. 今天，数论已经应用在众多领域，诸如，物理，化学，声学，生物，计算，编码与密码，数字通信系统，平面设计，甚至音乐和商业领域①. 特别地，同余理论已经应用在制作万年历，安排循环联赛，连接电话电缆，设计用来存储计算机文件的系统方法，制作魔方，生成随机数，提出高安全度和可信度的加密方案，甚至用于设计高速(剩余)计算机. 特别值得一提的是，计算机本质上是有限机器：它们有有限的存储空间，只能处理一些有限长的数，只能进行有限步的计算. 由于这些限制的存在，同余算术在计算机硬件和软件的设计上特别有用.

本书将带领读者进行这样一次旅程，从初等数论开始，历经算法数论与计算数论，最终以计算科学上的应用数论结束. 本书分为三部分：

---

① 弗雷德·古特尔于1994年6月20日发表在《国际商业周刊》62～64页的一篇文章中写到：数论，曾经的一门研究用各种方法巧妙处理整数时各种情况的深奥的学问，如今正成为一门可以帮助解决许多复杂的商业问题的充满生命力的实践科学.

(1) 初等数论,

(2) 计算数论/算法数论,

(3) 计算/密码学中的应用数论.

第一部分主要是关于整除理论,同余理论,连分数,丢番图方程以及椭圆曲线的基本概念和结果.这一部分的新颖之处在于它包含了椭圆曲线的叙述,这在初等数论书中通常是不会涉及的.第二部分给出了算法和复杂度的简要介绍,并且介绍了一些在计算数论中重要和应用广泛的算法,特别是用于素性检测,整数因子分解,离散对数以及椭圆曲线离散对数的算法.这一部分的主要特色是其中有一节介绍了用于整数因子分解和离散对数的量子算法,这在目前的关于计算/算法数论的其他书籍中是不容易找到的.这部分以介绍用于计算 $\pi(x)$,寻找亲和数对,证明哥德巴赫猜想,以及寻找完全数和亲和数的算法结束.本书的第三部分讨论了初等数论和计算数论在计算以及信息技术方面的一些新的应用,特别是密码学和信息安全上的应用:它覆盖的题材相当广泛,有安全通讯,信息系统安全,计算机构造,设计,检错与纠错,Hash 函数的设计,以及随机数的生成等等.在整本书中,按照"定义-定理-算法-例题"的模式呈现材料,而不是按照传统的哈代-怀特的"定义-定量-证明"的模式[100],虽然我们的确给出了大部分定理的证明.我们相信这是将数学知道展现给计算专业人员的最适当的方式.就像 Donald Knuth[121] 在 1974 年所指出的:"人们常常说,除非一个人能将某事教给其他人,他才算是真正地了解了这件事.实际上,直到一个人可以将某事教授给计算机,他才算是真正地了解了这件事."因此,作者强烈建议读者在计算机上执行本书中介绍的所有算法和方法,利用诸如 maple 的数学系统(计算机代数)以更好地理解算法和方法背后的思想.在某些小节后附有少量习题,值得读者全部尝试.

本书试图做到自包含,而不要求具有初等数论和抽象代数的知识,当然熟悉大学一年级数学有助于阅读本书.本书可作为本科或研究生阶段开设的用于计算或密码学的数论或数学课程的教科书,也可作为这一领域研究员的基本参考用书.

## 致谢

我在 1990 年开始着手写这本书,当时我是澳大利亚拉筹伯大学数学与信息科学院的一名讲师.我在约克大学完成本书,最终定稿于考文垂大学和阿斯顿大学,均位于英国.我非常感谢拉筹伯大学数学与信息科学院的 Bertram Mond 教授和 John Zeleznikow 博士,约克大学数学系的 Terence Jackson 博士和计算机科学系的 Jim Austin 教授,考文垂大学数学与信息科学院的 Glyn James 教授,Brian Aspinall 先生,Eric Tatham 先生,位于伯明翰的阿斯顿大学计算机科学与应用数学的 David Lowe 教授和 Ted Elsworth 博士,感谢他们富有成果的讨论,友好的鼓励以及慷慨的支持.还要特别感谢施普林格出版社柏林/海德堡的 Hans Wössner 博士,Andrew Ross 先生和施普林格出版社的审稿人,感谢

他们的评论、校正和建议. 在准备本书的漫长过程中，我从以下很多人那里得到帮助，有威斯康星大学麦迪逊分校的 Eric Bach 教授，巴斯大学的 Jim Davenport 教授，卡尔加里大学的 Richard Guy 教授，斯坦福大学的 Martin Hellman 教授，AT&T 贝尔实验室的 David Johnson 博士，俄克拉何马大学的 S. Lakshmivarahan 教授，贝尔通讯研究的 Ajie Lenstra 博士，加州大学伯克利分校的 Hendrik Lenstra Jr. 教授，剑桥大学的 Roger Needham 教授和 Richard Pinch 博士，南太平洋大学(斐济)的 Peter Pleasants 博士，佐治亚大学的 Carl Pomerance 教授，阿姆斯特丹数学与计算机科学中心(CWI)的 Herman te Riele 博士，曼尼托巴大学的 Hugh William 教授. 最后，我要感谢 William Bloodworth 先生(达拉斯，得克萨斯州)，John Cosgrave 博士(圣帕特里克学院，都柏林)，Gavin Doherty 博士(卢瑟福阿普尔顿实验室，牛津郡)，Robert Pargeter 先生(蒂夫顿，德文郡)，Alexandros Papanikolaon 先生(阿斯顿大学，伯明翰)，特别感谢 Richard Brent 教授(牛津大学计算实验室)，Rodney Coleman 先生(法国格勒诺伯第一大学)和 Glyn James 教授(考文垂大学)，感谢他们阅读了本书的不同版本. 正如 Hans Wössner 博士在交流中说的：金无足赤，人无完人. 本书以及作者也不例外. 欢迎读者提出宝贵的意见和建议，以及纠正书中的错误，读者可以通过普通邮件寄给作者或者发送电子邮件到 s. yan@aston. ac. uk.

颜松远

2000 年 2 月于伯明翰

# 译 者 序

颜松远教授的《计算数论》一书在目前众多的密码学相关书籍中是一本有特色的专著. 通过教学实践我觉得该书具有以下独特的优点：一是数学基础部分介绍详尽，对初等数论以及解析数论介绍之完备为其他密码书籍所不如；二是书中例子众多，有助于初学者的理解和演算；三是给出了大量的算法，便于读者编程实现；四是取材新颖，对前沿学科，如量子密码学和计算复杂性问题等有精准的描述；五是对计算数论的历史发展给出了引人入胜的描述. 这是一本适合密码学初学者的书籍，对有经验的研究者也不乏启示. 自2005年以来，该书一直是华东师范大学数学系信息安全专业研究生的指定参考书.

本书的翻译是由杨思熳、刘巍、齐璐璐、陶红伟共同完成的. 其中，刘巍翻译第1章，齐璐璐翻译第2章，陶红伟翻译第3章. 全书的核对和定稿是由杨思熳完成的.

杨思熳

2008年9月于上海

# 符 号 说 明

符号应该与它适用的运算的性质一样简单。

Charles Babbage(1791—1871)

| 符 号 | 说 明 |
|---|---|
| $\mathbb{N}$ | 自然数集：$\mathbb{N}=\{1,2,3,\cdots\}$ |
| $\mathbb{Z}$ | 整数集：$\mathbb{Z}=\{0,\pm n : n\in\mathbb{N}\}$ |
| $\mathbb{Z}^+$ | 正整数集：$\mathbb{Z}^+=\mathbb{N}$ |
| $\mathbb{Z}_{>1}$ | 大于 1 的正整数集：$\mathbb{Z}_{>1}=\{n : n\in\mathbb{Z}\text{ 且 }n>1\}$ |
| $\mathbb{Q}$ | 有理数集：$\mathbb{Q}=\left\{\frac{a}{b} : a,b\in\mathbb{Z}\text{ 且 }b\neq 0\right\}$ |
| $\mathbb{R}$ | 实数集：<br>$\mathbb{R}=\{n+0.d_1d_2d_3\cdots : n\in\mathbb{Z},d_i\in\{0,1,\cdots,9\}$且没有 9 的无穷序列出现$\}$ |
| $\mathbb{C}$ | 复数集：$\mathbb{C}=\{a+bi : a,b\in\mathbb{R}\text{ 且 }i=\sqrt{-1}\}$ |
| $\mathbb{Z}/n\mathbb{Z}$ | 或记为$\mathbb{Z}_n$，模 $n$ 的剩余类；一个整数环；若 $n$ 为素数，则为域 |
| $(\mathbb{Z}/n\mathbb{Z})^*$ | 乘法群；这个群由$\mathbb{Z}/n\mathbb{Z}$ 中与 $n$ 互素的元素组成：<br>$(\mathbb{Z}/n\mathbb{Z})^*=\{[a]_n\in\mathbb{Z}/n\mathbb{Z} : \gcd(a,n)=1\}$ |
| $\mathbb{F}_p$ | $p$ 元有限域，其中 $p$ 是素数 |
| $\mathbb{F}_q$ | $q$ 元有限域，其中 $q=p^k$ 是素数的幂次 |
| $\mathcal{K}$ | (任意的)域 |
| $\mathcal{R}$ | 环 |
| $\mathcal{G}$ | 群 |
| $\lvert\mathcal{G}\rvert$ | 群 $\mathcal{G}$ 的阶 |
| $B_n$ | 伯努利数：$\binom{n+1}{1}B_n+\cdots+\binom{n+1}{n}B_1+B_0=0$ |
| $F_n$ | 费马数：$F_n=2^{2^n}+1,n\geqslant 0$ |
| $M_p$ | 梅森素数：当 $p$ 是素数时，$M_p=2^p-1$ 是素数 |
| $\sqrt{x}$ | $x$ 的平方根 |
| $\sqrt[k]{x}$ | $x$ 的 $k$ 次方根 |

续表

| 符　号 | 说　明 |
| --- | --- |
| $\sim$ | 渐近等式 |
| $\approx$ | 近似等式 |
| $\infty$ | 无穷 |
| $\Rightarrow$ | 推出 |
| $\Leftrightarrow$ | 等价 |
| $\square$ | 空白符号;证明结束符 |
| $\sqcup$ | 空格 |
| Prob | 概率测度 |
| $\|S\|$ | 集合 $S$ 的基数 |
| $\in$ | ……的成员 |
| $\subset$ | 真子集 |
| $\subseteq$ | 子集 |
| $\star$, $*$ | 二元运算 |
| $\oplus$ | 二元运算(加法);不可兼的或(XOR) |
| $\odot$ | 二元运算(乘法) |
| $f(x)\sim g(x)$ | $f(x)$与 $g(x)$渐近相等 |
| $(\mathcal{G},*)\cong(\mathcal{H},\star)$ | $(\mathcal{G},*)$与$(\mathcal{H},\star)$同构 |
| $\perp$ | 未定义的 |
| $e_k$ | 密钥 |
| $d_k$ | 解钥 |
| $E_{e_k}(M)$ | 加密过程 $C=E_{e_k}(M)$,其中 $M$ 是明文 |
| $D_{d_k}(C)$ | 解密过程 $M=D_{d_k}(C)$,其中 $C$ 是密文 |
| $f(x)$ | $x$ 的函数 |
| $f^{-1}$ | $f$ 的逆 |
| $\binom{n}{i}$ | 二项式系数 |
| $\int$ | 积分 |
| $\mathrm{Li}(x)$ | 对数积分:$\mathrm{Li}(x)=\int_2^x \frac{\mathrm{d}t}{\ln t}$ |
| $\sum_{i=1}^{n} x_i$ | 和式:$x_1+x_2+\cdots+x_n$ |
| $\prod_{i=1}^{n} x_i$ | 乘积式:$x_1x_2\cdots x_n$ |
| $n!$ | 阶乘:$n(n-1)(n-2)\cdots3\cdot2\cdot1$ |
| $x^k$ | $x$ 的 $k$ 次幂 |
| $kP$ | $kP=\underbrace{P\oplus P\oplus\cdots\oplus P}_{k\text{个直和项}}$,其中 $P$ 是椭圆曲线 $E:y^2=x^3+ax+b$ 上的一个点$(x,y)$ |

续表

| 符　号 | 说　明 |
| --- | --- |
| $\mathcal{O}_E$ | 某域上椭圆曲线 $E$ 的无穷远点 |
| $e$ | 超越数 $e=\sum_{n\geqslant 0}\frac{1}{n!}\approx 2.7182818$ |
| $\log_b x$ | 以 $b(b\neq 1)$为底 $x$ 的对数：$x=b^{\log_b x}$ |
| $\log x$ | 以 2 为底的对数：$\log_2 x$ |
| $\ln x$ | 自然对数：$\log_e x$ |
| $\exp(x)$ | $x$ 和指数：$e^x=\sum_{n\geqslant 0}\frac{x^n}{n!}$ |
| $a\mid b$ | $a$ 整除 $b$ |
| $a\nmid b$ | $a$ 不整除 $b$ |
| $p^a\parallel n$ | $p^a\mid n$ 但 $p^{a+1}\nmid n$ |
| $\gcd(a,b)$ | $(a,b)$的最大公因子 |
| $\operatorname{lcm}(a,b)$ | $(a,b)$的最小公倍数 |
| $\lfloor x\rfloor$ | 小于等于 $x$ 的最大整数 |
| $\lceil x\rceil$ | 大于等于 $x$ 的最小整数 |
| $x \bmod n$ | 剩余：$x-n\left\lfloor\frac{x}{n}\right\rfloor$ |
| $x=y \bmod n$ | $x$ 等于 $y$ 模 $n$ 的剩余 |
| $x\equiv y(\bmod n)$ | $x$ 与 $y$ 模 $n$ 同余 |
| $x\not\equiv y(\bmod n)$ | $x$ 与 $y$ 模 $n$ 不同余 |
| $[a]_n$ | $a$ 模 $n$ 的剩余类 |
| $+_n$ | 模 $n$ 加法 |
| $-_n$ | 模 $n$ 减法 |
| $\cdot_n$ | 模 $n$ 乘法 |
| $x^k \bmod n$ | $x$ 的 $k$ 次幂模 $n$ |
| $kP \bmod n$ | $kP$ 模 $n$ |
| $\operatorname{ord}_n(a)$ | 整数 $a$ 模 $n$ 的阶；或记为 $\operatorname{ord}(a,n)$ |
| $\operatorname{ind}_{g,n}a$ | 以 $g$ 为底 $a$ 模 $n$ 的指标；当 $n$ 固定时，也记为 $\operatorname{ind}_g a$ |
| $\pi(x)$ | 小于等于 $x$ 的素数的个数：$\pi(x)=\sum_{\substack{p\leqslant x\\ p\text{为素数}}}1$ |
| $\tau(n)$ | $n$ 的正因子的个数：$\tau(n)=\sum_{d\mid n}1$ |
| $\sigma(n)$ | $n$ 的正因子之和：$\sigma(n)=\sum_{d\mid n}d$ |
| $s(n)$ | $n$ 的真因子之和：$s(n)=\sigma(n)-n$ |
| $\varphi(n)$ | 欧拉函数：$\phi(n)=\sum_{\substack{0\leqslant k<n\\ \gcd(k,n)=1}}1$ |

续表

| 符　号 | 说　明 |
| --- | --- |
| $\lambda(n)$ | Carmichael 函数：若 $n=\prod_{i=1}^{k} p_i^{a_i}$，则 $\lambda(n)=\mathrm{lcm}(\lambda(p_1^{a_1})\lambda(p_2^{a_2}),\cdots,\lambda(p_k^{a_k}))$ |
| $\mu(n)$ | 麦比乌斯函数 |
| $\zeta(s)$ | 黎曼 zeta-函数：$\zeta(s)=\prod_{n=1}^{\infty}\frac{1}{n^s}$，其中 $s$ 是复变量 |
| $\left(\frac{a}{p}\right)$ | 勒让德符号，其中 $p$ 是素数 |
| $\left(\frac{a}{n}\right)$ | 雅可比符号，其中 $n$ 是合数 |
| $Q_n$ | $n$ 的所有二次剩余组成的集合 |
| $\overline{Q}_n$ | $n$ 的所有二次非剩余组成的集合 |
| $J_n$ | $J_n=\left\{a\in(\mathbb{Z}/n\mathbb{Z})^* : \left(\frac{a}{n}\right)=1\right\}$ |
| $\widetilde{Q}_n$ | $n$ 的伪平方组成的集合：$\widetilde{Q}_n=J_n-Q_n$ |
| $K(k)_n$ | $n$ 的所有 $k$ 次剩余组成的集合，其中 $k\geqslant 2$ |
| $\overline{K(k)}_n$ | $n$ 的所有 $k$ 次非剩余组成的集合，其中 $k\geqslant 2$ |
| $[q_0,q_1,q_2,\cdots,q_n]$ | 有限简单连分数 |
| $C_k=\frac{P_k}{Q_k}$ | 连分数的 $k$ 次收敛子 |
| $[q_0,q_1,q_2,\cdots]$ | 无限简单连分数 |
| $[q_0,q_1,\cdots,q_k,\overline{q_{k+1},q_{k+2},\cdots,q_{k+m}}]$ | 循环简单连分数 |
| $\mathcal{P}$ | 在确定的多项式时间内可以解决的问题类 |
| $\mathcal{NP}$ | 在不确定的多项式时间内可以解决的问题类 |
| $\mathcal{RP}$ | 在随机多项式时间内可以解决的带单边错误的问题类 |
| $\mathcal{BPP}$ | 在随机多项式时间内可以解决的带双边错误的问题类 |
| $\mathcal{ZPP}$ | 在随机多项式时间内可以解决的带零错误的问题类 |
| $\mathcal{O}(\cdot)$ | 上界：$f(n)=\mathcal{O}(g(n))$，若存在某一常数 $c$，使得 $f(n)\leqslant c\cdot g(n)$ |
| $\mathcal{O}(\cdot)$ | 不是渐近紧的上界：<br>$f(n)=\mathcal{O}(g(n))$，$\forall c\geqslant 0$，使得 $f(n)\leqslant c\cdot g(n)$ |
| $\Omega(\cdot)$ | 下界：$f(n)=\Omega(g(n))$，若存在某一常数 $c$，使得 $f(n)\geqslant\frac{1}{c}\cdot g(n)$ |
| $\Theta(\cdot)$ | 紧界：$f(n)=\Theta(n)$，若 $f(n)=\mathcal{O}(g(n))$ 且 $f(n)=\Omega(g(n))$ |
| $\mathcal{O}(N^k)$ | 用算术运算度量的多项式时间复杂性，其中 $k>0$ 是常数 |
| $\mathcal{O}((\log N)^k)$ | 用位运算度量的多项式时间复杂性，其中 $k>0$ 是常数 |
| $\mathcal{O}((\log N)^{c\log N})$ | 超多项式时间复杂性，其中 $c$ 是常数 |

续表

| 符　号 | 说　明 |
| --- | --- |
| $\mathcal{O}(\exp(c\sqrt{\log N\log\log N}))$ | 亚指数复杂性，$\mathcal{O}(\exp(c\sqrt{\log N\log\log N}))=\mathcal{O}(N^{c\sqrt{\log\log N/\log N}})$ |
| $\mathcal{O}(\exp(x))$ | 指数复杂性，有时记为 $\mathcal{O}(e^x)$ |
| $\mathcal{O}(N^\varepsilon)$ | 用位运算度量的指数复杂性：$\mathcal{O}(N^\varepsilon)=\mathcal{O}(2^{\varepsilon\log N})$，其中 $\varepsilon>0$ 是常数 |
| CFRAC | 连分数法(用于因子分解) |
| ECM | 椭圆曲线法(用于因子分解) |
| NFS | 数域筛法(用于因子分解) |
| QS/MPQS | 二次筛法/多重多项式二次筛法(用于因子分解) |
| ECPP | 椭圆曲线素性证明 |
| DES | 数据加密标准 |
| AES | 高级加密标准 |
| DSA | 数字签名算法 |
| DSS | 数字签名标准 |
| RSA | Rivest-Shamir-Adleman |
| WWW | 万维网 |

# 目　录


**第 1 章　初等数论** …… 1

1.1　导言 …… 1

1.1.1　数论概述 …… 1

1.1.2　数论的应用 …… 11

1.1.3　代数初步 …… 12

1.2　可除性理论 …… 18

1.2.1　可除性的基本概念及性质 …… 18

1.2.2　算术基本定理 …… 23

1.2.3　梅森素数与费马数 …… 27

1.2.4　欧几里得算法 …… 35

1.2.5　连分数 …… 38

1.3　丢番图方程 …… 45

1.3.1　丢番图方程的基本概念 …… 45

1.3.2　线性丢番图方程 …… 46

1.3.3　Pell 方程 …… 49

1.4　算术函数 …… 56

1.4.1　可积函数 …… 56

1.4.2　函数 $\tau(n)$、$\sigma(n)$和 $s(n)$ …… 58

1.4.3　完全数、亲和数与多亲数 …… 61

1.4.4　函数 $\phi(n)$、$\lambda(n)$和 $\mu(n)$ …… 69

1.5　素数分布 …… 74

1.5.1　素数分布函数 $\pi(x)$ …… 74

1.5.2　用 $\frac{x}{\ln x}$ 逼近 $\pi(x)$ …… 76

1.5.3　用 $\mathrm{Li}(x)$ 逼近 $\pi(x)$ …… 81

1.5.4　黎曼 $\zeta$-函数 $\zeta(s)$ …… 83

1.5.5　第 $n$ 个素数 …… 90

1.5.6 孪生素数分布 …… 92
1.5.7 素数项算术级数 …… 95
1.6 同余理论 …… 96
1.6.1 同余的基本概念与性质 …… 96
1.6.2 模运算 …… 101
1.6.3 线性同余方程 …… 105
1.6.4 中国剩余定理 …… 111
1.6.5 高阶同余方程 …… 114
1.6.6 勒让德和雅可比符号 …… 119
1.6.7 阶和原根 …… 129
1.6.8 指数和 $k$ 次剩余 …… 134
1.7 椭圆曲线的算术理论 …… 137
1.7.1 椭圆曲线的基本概念 …… 138
1.7.2 椭圆曲线的几何复合定律 …… 139
1.7.3 椭圆曲线的代数计算定律 …… 140
1.7.4 椭圆曲线上的群定律 …… 144
1.7.5 椭圆曲线上点的个数 …… 144
1.8 小结 …… 146
**第2章 计算数论/算法数论** …… 148
2.1 简介 …… 148
2.1.1 计算/算法数论概述 …… 148
2.1.2 计算可行性 …… 151
2.1.3 计算复杂性 …… 154
2.1.4 数论算法的复杂性 …… 160
2.1.5 快速模指数算法 …… 165
2.1.6 椭圆曲线上的快速群运算 …… 167
2.2 素性检测算法 …… 171
2.2.1 确定性的严格素性检测 …… 172
2.2.2 费马的拟素性检测 …… 174
2.2.3 强拟素性检测 …… 176
2.2.4 卢卡斯拟素性检测 …… 181
2.2.5 椭圆曲线检测 …… 187