信息科学技术学术著作丛书

量子计算数论

Quantum Computational Number Theory

〔英〕颜松远（Song Y. Yan） 著
段乾恒 王 洪 马 智 穆 清 译

科学出版社

信息科学技术学术著作丛书

量子计算数论

Quantum Computational Number Theory

〔英〕颜松远(Song Y. Yan) 著

段乾恒 王 洪 马 智 穆 清 译

科 学 出 版 社

北 京

图字：01-2019-0297

内 容 简 介

本书全面介绍了针对整数分解问题、离散对数问题及椭圆曲线离散对数问题的经典及量子算法。同时对经典计算和量子计算中的基本概念及结论进行了介绍，并简单讨论了一些针对其他数论问题和代数问题的量子算法，完备地描述相关数论问题及其密码应用，简明扼要地讨论了对应经典算法。在量子算法的描述过程中，系统性强、实例清晰、深入浅出。

本书可作为对量子算法、计算数论、抗量子计算密码感兴趣的计算机学者、数学家、电气工程师及物理学者的参考书，也可作为量子计算数论领域高年级本科生或低年级研究生的教材。

First published in English under the title
Quantum Computational Number Theory
by Song Y. Yan
Copyright © Springer International Publishing Switzerland, 2015
This edition has been translated and published under licence from
Springer Nature Switzerland AG.

图书在版编目(CIP)数据

量子计算数论 /（英）颜松远著；段乾恒等译. —北京：科学出版社，2020.4

（信息科学技术学术著作丛书）

书名原文：Quantum Computational Number Theory

ISBN 978-7-03-064840-2

Ⅰ. ①量… Ⅱ. ①颜… ②段… Ⅲ. ①数论－应用－密码学－研究 Ⅳ. ①TN918.1

中国版本图书馆CIP数据核字(2020)第064547号

责任编辑：牛宇锋 纪四稳 / 责任校对：王萌萌
责任印制：吴兆东 / 封面设计：陈 敬

科学出版社出版
北京东黄城根北街16号
邮政编码：100717
http://www.sciencep.com

北京中石油彩色印刷有限责任公司 印刷

科学出版社发行 各地新华书店经销

*

2020年4月第 一 版 开本：720×1000 1/16
2020年4月第一次印刷 印张：15 3/4
字数：297 000

定价：120.00元

（如有印装质量问题，我社负责调换）

此为试读，需要完整PDF请访问：www.ertongbook.com

《信息科学技术学术著作丛书》序

21 世纪是信息科学技术发生深刻变革的时代，一场以网络科学、高性能计算和仿真、智能科学、计算思维为特征的信息科学革命正在兴起。信息科学技术正在逐步融入各个应用领域并与生物、纳米、认知等交织在一起，悄然改变着我们的生活方式。信息科学技术已经成为人类社会进步过程中发展最快、交叉渗透性最强、应用面最广的关键技术。

如何进一步推动我国信息科学技术的研究与发展；如何将信息技术发展的新理论、新方法与研究成果转化为社会发展的推动力；如何抓住信息技术深刻发展变革的机遇，提升我国自主创新和可持续发展的能力？这些问题的解答都离不开我国科技工作者和工程技术人员的求索和艰辛付出。为这些科技工作者和工程技术人员提供一个良好的出版环境和平台，将这些科技成就迅速转化为智力成果，将对我国信息科学技术的发展起到重要的推动作用。

《信息科学技术学术著作丛书》是科学出版社在广泛征求专家意见的基础上，经过长期考察、反复论证之后组织出版的。这套丛书旨在传播网络科学和未来网络技术，微电子、光电子和量子信息技术、超级计算机、软件和信息存储技术、数据知识化和基于知识处理的未来信息服务业、低成本信息化和用信息技术提升传统产业，智能与认知科学、生物信息学、社会信息学等前沿交叉科学，信息科学基础理论，信息安全等几个未来信息科学技术重点发展领域的优秀科研成果。丛书力争起点高、内容新、导向性强，具有一定的原创性，体现出科学出版社“高层次、高质量、高水平”的特色和“严肃、严密、严格”的优良作风。

希望这套丛书的出版，能为我国信息科学技术的发展、创新和突破带来一些启迪和帮助。同时，欢迎广大读者提出好的建议，以促进和完善丛书的出版工作。

中国工程院院士

原中国科学院计算技术研究所所长

李国杰

译者前言

数论的研究与应用具有悠久的历史，量子计算的研究则起源于20世纪80年代。量子计算的研究促使量子计算数论成为新的学科交叉点。鉴于数论问题在密码学领域的广泛应用，量子计算也备受关注。

国内外出版的量子计算或数论相关专著很多，但是较少从量子计算与数论结合的角度去讲述。颜松远教授所著的 *Quantum Computational Number Theory* 一书丰富了这一交叉领域的研究，是一本很有特色的专著，其特点如下：

(1)重点突出，内容新颖。本书以整数分解、离散对数等几个经典的数论问题为核心，首先对相关经典算法进行适当阐述，然后重点介绍量子算法在求解相关问题时的优势，充分体现了量子计算在数论问题求解中的应用。

(2)逻辑清晰，深入浅出。本书将叙述的严谨性和内容的广度、深度进行了有机结合，语言描述浅显易懂而不失严谨，逻辑推理严密。在量子算法的介绍中，剥离不必要的物理细节，重点介绍典型量子算法的数学思想及其在数论问题中的应用；此外，着重阐述算法的核心思路与流程，省去了部分不必要的数学证明细节。

(3)选材精良，可拓展性强。本书介绍了几个核心数论问题的求解，同时给出了丰富的拓展学习素材，对更多数论问题在量子计算模型下的求解进行了思路性的阐述，便于读者进行更深入的研究。

本书主要从数学角度出发，对于缺乏较深物理知识储备但是想学习量子计算与算法的相关读者具有较好的参考价值；尤其对于研究量子算法在数学问题中应用的相关读者，本书是值得精读的入门书籍。

译者经过一年的努力完成了本书的翻译，其中，段乾恒博士、王洪博士、马智教授、穆清讲师翻译了本书的主要章节，费洋扬博士协助完成了全书的统稿和校对，在此表示衷心感谢。

本书的翻译工作得到国家自然科学基金项目(61501514、61472446、61701539)和“十三五”国家密码发展基金项目(mmjj20180107、mmjj20180212)的支持，在此一并表示感谢。

由于作者水平有限，翻译过程中不足之处在所难免，敬请广大读者批评指正。

译　者

2020年1月

原书前言

想象力比知识更重要，因为知识是有限的，而想象力包围着整个世界。

阿尔伯特·爱因斯坦(Albert Einstein 1879—1955)

1921 年诺贝尔物理学奖获得者

量子计算数论是一个全新的交叉学科，涵盖了数论、计算理论和量子计算等学科，旨在利用量子计算技术解决数论和密码学中难以用经典计算机解决的计算难题。确切地说，最广为人知的 Shor 算法就是为了解决整数分解问题、破解 RSA 公钥密码体制而提出的。

本书共 6 章。第 1 章介绍计算数论、量子计算数论的基本概念。第 2 章介绍经典计算和量子计算中的基本概念及结论。第 3～5 章分别介绍整数分解问题(IFP)、离散对数问题(DLP)以及基于椭圆曲线离散对数问题(ECDLP)的经典及量子算法。目前尚无针对 IFP、DLP、ECDLP 的有效经典算法，因此只要设计合理并能够得到妥善应用，所有基于 IFP、DLP、ECDLP 的经典密码体制都是安全的。然而，如果能够建造实用的量子计算机，那么本书介绍的量子算法就能用来破解所有基于 IFP、DLP、ECDLP 的经典密码体制。当然，不能期望量子算法抑或量子计算机能够破解所有的密码体制，一方面，这是因为量子计算机并不是一款“更快”的经典计算机，而是一种具有截然不同计算方式的计算机；另一方面，对于一些计算难题如 IFP、DLP，利用量子算法可以实现指数加速(更一般的说法是超多项式加速)，但是对于诸如 NP 完全问题的其他问题，如旅行商问题(TSP)，利用目前的量子算法根本不能实现加速。因此，可能存在一些量子计算机也无法破解的密码体制，这种类型的密码体制称为抗量子密码体制。第 6 章介绍一些针对其他数论问题和代数问题的量子算法。

本书可以视为作者所著 *Quantum Attacks on Public-Key Cryptosystems* 的更新版，不同的是本书更加侧重于介绍基于 IFP、DLP、ECDLP 的公钥密码体制及相应的量子攻击算法。本书可以作为对量子计算数论感兴趣的计算机学者、数学家、电气工程师及物理学者的参考书，也可作为量子计算数论领域高年级本科生或低年级研究生的教材。

本书写作时正值作者在武汉大学计算机学院做特聘教授，书中相关内容的研究在过去十年中先后获得了皇家工程学院、伦敦皇家学会、麻省理工学院、哈佛大学及武汉大学软件工程国家重点实验室基金(SKLSE-2015-A-02)的资助，在此表示感谢，尤其感谢作者的博士研究生王亚辉为本书提供的算例及对本书初稿的校对。

颜松远

2015 年 8 月于中国武汉

缩 略 语

AES	advanced encryption standard	高级加密标准
BPP	bounded-error probabilistic polynomial time	多项式时间的概率图灵机以错误概率 1/3 接受的语言类
BQP	bounded-error quantum polynomial time	多项式时间的量子图灵机以错误概率 1/3 接受的语言类
BSD	Birch-Swinnerton-Dyer	波奇-斯温纳顿-戴雅
CCITT	Consultative Committee on International Telephone and Telegraph	国际电报电话咨询委员会
CHREM	Chinese remainder theorem	中国剩余定理
CFRAC	continued fraction factorization	连分数分解(算法)
CWI	Centrum Wiskunde & Informatica	(荷兰国家)数学和计算机科学研究院
DES	data encryption standard	数据加密标准
DLP	discrete logarithm problem	离散对数问题
DHM	Diffie-Hellman-Merkle	迪菲-赫尔曼-默克尔
DSA	digital signature algorithm	数字签名算法
DSS	digital signature standard	数字签名标准
DTM	deterministic Turing machine	确定型图灵机
ECC	elliptic curve cryptography	椭圆曲线密码体制
ECDLP	elliptic curve discrete logarithm problem	椭圆曲线离散对数问题
ECDSA	elliptic curve digital signature algorithm	椭圆曲线数字签名算法
ECDSS	elliptic curve digital signature standard	椭圆曲线数字签名标准
ECM	elliptic curve method	椭圆曲线因式分解方法
ERH	extended Riemann hypothesis	广义黎曼猜想
EXP	exponential time	指数时间
FFS	function field sieve	函数域筛法

FFT	fast Fourier transform	快速傅里叶变换
GNFS	general number field sieve	通用型数域筛法
GRH	generalized Riemann hypothesis	广义黎曼假设
HPP	Hamilton path problem	哈密顿路径问题
HSP	hidden subgroup problem	隐子群问题
IFP	integer factorization problem	整数分解问题
IP	interactive proof	交互式证明(问题集合)
ISO	International Organization for Standardization	国际标准化组织
LLL	Lenstra-Lenstra-Lovasz	格基归约化(算法)
LP	logarithm problem	对数问题
MPRFP	modular polynomial root finding problem	多项式同余方程的根式解问题
MPQS	multiple polynomial quadratic sieve	多个多项式的二次筛法
NDTM	non-deterministic Turing machine	非确定型图灵机
NFS	number field sieve	数域筛法
NP	non-deterministic polynomial	非确定性多项式(时间复杂度问题)
NPC	NP complete	NP 完全问题
NPH	NP hard	NP 难(问题)
NPS	NP-space	NP 空间(复杂度)
P	polynomial	多项式(时间可解问题)
PFP	prime factorization problem	素因数分解问题
PS	P-space	P 空间
PSC	P-space complete	P 空间完全(问题)
PSH	P-space hard	P 空间难(问题)
PTM	probabilistic Turing machine	概率图灵机
PTP	primality testing problem	素性测试问题
QFT	quantum Fourier transform	量子傅里叶变换

QIP	quantum interactive proof	量子交互式证明(问题集合)
QP	quantum polynomial	量子多项式(时间可解问题)
QR	quadratic residue	平方剩余
QRP	quadratic residuosity problem	平方剩余问题
QS	quadratic sieve	二次筛法
QTM	quantum Turing machine	量子图灵机
RSA	Rivest-Shamir-Adleman	李维斯特-萨莫尔-阿德曼
RFP	root finding problem	求根问题
RP	randomize polynominal	随机多项式(复杂度)
SAT	satisfiability problem	可满足性问题
SNFS	special NFS	特殊型数域筛法
SQRTP	square root problem	二次同余方程求解问题
SQUFOF	Shanks' square form factorization method	平方形式分解算法
SVP	shortest vector problem	最短向量问题
SWIFT	Society for Worldwide Interbank Financial Telecommunications	环球同业银行金融电讯协会
TSP	traveling salesman problem	旅行商问题
TQFT	topological quantum field theory	拓扑量子场论
ZPP	zero-error probabilistic polynomial	零错误概率多项式(时间复杂度问题)
ZQP	zero-error quantum polynomial	量子零错误多项式(时间复杂度问题)

此为试读,需要完整PDF请访问: www.ertongbook.com

作 者 简 介

颜松远博士写作本书时为武汉大学特聘教授，在英国约克大学数学系获得数论博士学位，先后在英国以及北美的多所大学做博士后研究，包括约克大学、剑桥大学、阿斯顿大学、考文垂大学、罗格斯大学、哥伦比亚大学、多伦多大学、麻省理工学院和哈佛大学等。主要研究领域有计算数论、计算复杂度理论、算法的设计与分析、密码学、信息安全和网络安全等。并在相关研究领域出版了多本广受欢迎的教材，包括：

(1) *Perfect, Amicable and Sociable Numbers: A Computational Approach*, World Scientific, 1996.

(2) *Number Theory for Computing*, Springer, First Edition, 2000; Second Edition, 2002; Polish Translation, 2006 (Polish Scientific Publishers PWN); Chinese Translation, 2007 (Tsinghua University Press).

(3) *Primality Testing and Integer Factorization in Public-Key Cryptography*, Springer, First Edition, 2004; Second Edition, 2009.

(4) *Cryptanalytic Attacks on RSA*, Springer, 2008; Russian Translation, 2010 (Russian Scientific Publishers).

(5) *Computational Number Theory and Modern Cryptography*, Wiley, 2012.

(6) *Quantum Attacks on Public-Key Cryptosystems*, Springer, 2013.

目　录

第1章 绪 论

上帝用漂亮的数学创造了世界。

保罗·狄拉克(Paul Dirac 1902—1984)

1933年诺贝尔物理学奖获得者

数论是数学中最古老的一门学科。传统上，数论又称为数学学科中最纯粹的分支。就像分析方法和代数方法在解析数论和代数数论中起着重要的作用一样，随着现代计算机的发明，计算科学在数论研究中扮演着越来越重要的角色，由此导致计算数论以致量子计算数论的诞生。本章介绍数论中的一些基本思想、概念以及数论、计算数论、量子计算数论中的一些开放问题，尤为重要的是，本章将回答以下三个问题：

(1)何谓数论？

(2)何谓计算数论？

(3)何谓量子计算数论？

1.1 数论的概念

数论是关于整数的理论，主要研究整数集合

$$\mathbb{Z}=\{\cdots,-3,-2,-1,0,1,2,3,\cdots\}$$

的性质，尤其是正整数集合

$$\mathbb{Z}^{+}=\{1,2,3,\cdots\}$$

的性质。例如，由整除的性质可知，所有的正整数都可以归为以下三类中的一种：

(1)1；

(2)素数，即2,3,5,7,11,13,17,19,23,…；

(3)合数，即4,6,8,9,10,12,14,15,16,18,20,21,22,…。

由素数的定义可知，对于大于1的正整数n，如果其正因数仅有1及其自身，则称为素数，否则称为合数。1既不是合数也不是素数。素数在数论研究中发挥着重要的作用，因为任意大于1的正整数n都可以分解为标准形式：

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

其中，$p_1 < p_2 < \cdots < p_k$ 且它们都为素数；α_1、α_2、…、α_k 为正整数。尽管人们对素数定理已经研究了 2000 多年，但是关于素数的分布依然有很多开放问题。下面介绍几种素数研究中最有趣的问题。

1. *素数的分布*

欧几里得(Euclid)2000 年前在其著作《几何原本》中证明：素数有无穷多个，即素数序列

$$2,3,5,7,11,13,17,19,\cdots$$

是无穷的。例如，2、3、5 是最初的三个素数，$2^{57885161}-1$ 是已知的最大素数(截至 2015 年 8 月)，这个数有 17425170 位，发现于 2013 年 1 月 25 日。若用 $\pi(x)$ 表示不大于 x 的素数的个数(表 1.1 给出了 x 较大时 $\pi(x)$ 的一些数值)，则欧几里得定理关于素数有无穷多个的论述可以表示为

$$\text{当 } x \to \infty \text{ 时，} \quad \pi(x) \to \infty$$

对素数分布的一个更好的论述来自素数定理，该定理指出

$$\pi(x) \sim x/\log x$$

或者说

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1$$

需要注意的是，这里是自然对数，即以 e=2.7182818…为底。然而，若黎曼(Riemann)猜想[1]是正确的，则需要将素数定理

$$\pi(x) = \int_2^x \frac{\mathrm{d}t}{\log t} + O\left(x\mathrm{e}^{-c\sqrt{\log x}}\right)$$

修正为

$$\pi(x) = \int_2^x \frac{\mathrm{d}t}{\log t} + O\left(\sqrt{x}\log x\right)$$

表 1.1 x 较大时的 $\pi(x)$ 值

x	$\pi(x)$	$\pi(x)-x/\log x$
10	4	−0.3
10^2	25	3.3
10^3	168	23
10^4	1229	143
10^5	9592	906
10^6	78498	6116
10^7	664579	44158
10^8	5761455	332774
10^9	50847534	2592592
10^{10}	455052511	20758029
10^{11}	4118054813	169923159
10^{12}	37607912018	1416705193
10^{13}	346065536839	11992858452
10^{14}	3204941750802	102838308636
10^{15}	29844570422669	891604962452
10^{16}	279238341033925	7804289844393
10^{17}	2623557157654233	68883734693281
10^{18}	24739954287740860	612483070893536
10^{19}	234057667276344607	5481624169369960
10^{20}	2220819602560918840	49347193044659701
10^{21}	21127269486018731928	446579871578168707
10^{22}	201467286689315906290	4060704006019620994
10^{23}	1925320391606803968923	37083513766578631309
10^{24}	18435599767349200867866	339996354713708049069
10^{25}	176846309399143769411680	3128516637843038351228
10^{26}	1699246750872437141327603	28883358936853188823261

当然，我们不清楚黎曼猜想是否正确。黎曼猜想的正确与否是数学中一个最

此为试读，需要完整PDF请访问：www.ertongbook.com