国家出版基金资助项目

现代数学中的著名定理纵横谈丛书

丛书主编　王梓坤

THUE THEOREM—DISCRIMINANT OF PRIME NATURE AND DECOMPOSITION OF LARGE NUMBERS

Thue定理
—素数判定与大数分解

孙琦　旷京华　编著

哈爾濱工業大學出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS

国家出版基金项目
NATIONAL PUBLICATION FOUNDATION

现代数学中的著名定理纵横谈丛书
丛书主编　王梓坤

THUE THEOREM—DISCRIMINANT OF PRIME
NATURE AND DECOMPOSITION OF LARGE NUMBERS

Thue定理
——素数判定与大数分解

孙琦　旷京华　编著

哈爾濱工業大學出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS

内容简介

本书完整地介绍了素数判定问题的全部历史和理论，阐明了它在纯数学研究和应用数学研究中的地位，及其在当代科学中的实用价值(如在密码学中的作用). 全书内容丰富，论述严整.

本书适合大学师生及数学爱好者参考阅读.

图书在版编目(CIP)数据

Thue 定理：素数判定与大数分解/孙琦，旷京华编著. —哈尔滨：哈尔滨工业大学出版社，2018.5
(现代数学中的著名定理纵横谈丛书)
ISBN 978－7－5603－7360－7

Ⅰ.①T… Ⅱ.①孙… ②旷… Ⅲ.①素数－研究 Ⅳ.①O156.2

中国版本图书馆 CIP 数据核字(2018)第 090762 号

策划编辑 刘培杰 张永芹
责任编辑 张永芹 杜莹雪
封面设计 孙茵艾
出版发行 哈尔滨工业大学出版社
社 址 哈尔滨市南岗区复华四道街 10 号 邮编 150006
传 真 0451－86414749
网 址 http://hitpress.hit.edu.cn
印 刷 黑龙江艺德印刷有限责任公司
开 本 787mm×960mm 1/16 印张 5.5 字数 62 千字
版 次 2018 年 5 月第 1 版 2018 年 5 月第 1 次印刷
书 号 ISBN 978－7－5603－7360－7
定 价 68.00 元

代序

读书的乐趣

你最喜爱什么——书籍.

你经常去哪里——书店.

你最大的乐趣是什么——读书.

这是友人提出的问题和我的回答.真的,我这一辈子算是和书籍,特别是好书结下了不解之缘.有人说,读书要费那么大的劲,又发不了财,读它做什么?我却至今不悔,不仅不悔,反而情趣越来越浓.想当年,我也曾爱打球,也曾爱下棋,对操琴也有兴趣,还登台伴奏过.但后来却都一一断交,“终身不复鼓琴”.那原因便是怕花费时间,玩物丧志,误了我的大事——求学.这当然过激了一些.剩下来唯有读书一事,自幼至今,无日少废,谓之书痴也可,谓之书橱也可,管它呢,人各有志,不可相强.我的一生大志,便是教书,而当教师,不多读书是不行的.

读好书是一种乐趣,一种情操;一种向全世界古往今来的伟人和名人求

教的方法，一种和他们展开讨论的方式；一封出席各种活动、体验各种生活、结识各种人物的邀请信；一张迈进科学宫殿和未知世界的入场券；一股改造自己、丰富自己的强大力量. 书籍是全人类有史以来共同创造的财富，是永不枯竭的智慧的源泉. 失意时读书，可以使人重整旗鼓；得意时读书，可以使人头脑清醒；疑难时读书，可以得到解答或启示；年轻人读书，可明奋进之道；年老人读书，能知健神之理. 浩浩乎！洋洋乎！如临大海，或波涛汹涌，或清风微拂，取之不尽，用之不竭. 吾于读书，无疑义矣，三日不读，则头脑麻木，心摇摇无主.

潜能需要激发

我和书籍结缘，开始于一次非常偶然的机会. 大概是八九岁吧，家里穷得揭不开锅，我每天从早到晚都要去田园里帮工. 一天，偶然从旧木柜阴湿的角落里，找到一本蜡光纸的小书，自然很破了. 屋内光线暗淡，又是黄昏时分，只好拿到大门外去看. 封面已经脱落，扉页上写的是《薛仁贵征东》. 管它呢，且往下看. 第一回的标题已忘记，只是那首开卷诗不知为什么至今仍记忆犹新：

日出遥遥一点红，飘飘四海影无踪.

三岁孩童千两价，保主跨海去征东.

第一句指山东，二、三两句分别点出薛仁贵（雪、人贵）. 那时识字很少，半看半猜，居然引起了我极大的兴趣，同时也教我认识了许多生字. 这是我有生以来独立看的第一本书. 尝到甜头以后，我便千方百计去找书，向小朋友借，到亲友家找，居然断断续续看了《薛丁山征西》《彭公案》《二度梅》等，樊梨花便成了我心

中的女英雄.我真入迷了.从此,放牛也罢,车水也罢,我总要带一本书,还练出了边走田间小路边读书的本领,读得津津有味,不知人间别有他事.

当我们安静下来回想往事时,往往会发现一些偶然的小事却影响了自己的一生.如果不是找到那本《薛仁贵征东》,我的好学心也许激发不起来.我这一生,也许会走另一条路.人的潜能,好比一座汽油库,星星之火,可以使它雷声隆隆、光照天地;但若少了这粒火星,它便会成为一潭死水,永归沉寂.

抄,总抄得起

好不容易上了中学,做完功课还有点时间,便常光顾图书馆.好书借了实在舍不得还,但买不到也买不起,便下决心动手抄书.抄,总抄得起.我抄过林语堂写的《高级英文法》,抄过英文的《英文典大全》,还抄过《孙子兵法》,这本书实在爱得狠了,竟一口气抄了两份.人们虽知抄书之苦,未知抄书之益,抄完毫末俱见,一览无余,胜读十遍.

始于精于一,返于精于博

关于康有为的教学法,他的弟子梁启超说:"康先生之教,专标专精、涉猎二条,无专精则不能成,无涉猎则不能通也."可见康有为强烈要求学生把专精和广博(即"涉猎")相结合.

在先后次序上,我认为要从精于一开始.首先应集中精力学好专业,并在专业的科研中做出成绩,然后逐步扩大领域,力求多方面的精.年轻时,我曾精读杜布(J. L. Doob)的《随机过程论》,哈尔莫斯(P. R. Halmos)的《测度论》等世界数学名著,使我终身受益.简言之,即"始于精于一,返于精于博".正如中国革命一

样，必须先有一块根据地，站稳后再开创几块，最后连成一片.

丰富我文采，澡雪我精神

辛苦了一周，人相当疲劳了，每到星期六，我便到旧书店走走，这已成为生活中的一部分，多年如此. 一次，偶然看到一套《纲鉴易知录》，编者之一便是选编《古文观止》的吴楚材. 这部书提纲挈领地讲中国历史，上自盘古氏，直到明末，记事简明，文字古雅，又富于故事性，便把这部书从头到尾读了一遍. 从此启发了我读史书的兴趣.

我爱读中国的古典小说，例如《三国演义》和《东周列国志》. 我常对人说，这两部书简直是世界上政治阴谋诡计大全. 即以近年来极时髦的人质问题（伊朗人质、劫机人质等），这些书中早就有了，秦始皇的父亲便是受害者，堪称“人质之父”.

《庄子》超尘绝俗，不屑于名利. 其中“秋水”“解牛”诸篇，诚绝唱也.《论语》束身严谨，勇于面世，“己所不欲，勿施于人”，有长者之风. 司马迁的《报任少卿书》，读之我心两伤，既伤少卿，又伤司马；我不知道少卿是否收到这封信，希望有人做点研究. 我也爱读鲁迅的杂文，果戈理、梅里美的小说. 我非常敬重文天祥、秋瑾的人品，常记他们的诗句：“人生自古谁无死，留取丹心照汗青”“休言女子非英物，夜夜龙泉壁上鸣”. 唐诗、宋词、《西厢记》《牡丹亭》，丰富我文采，澡雪我精神，其中精粹，实是人间神品.

读了邓拓的《燕山夜话》，既叹服其广博，也使我动了写《科学发现纵横谈》的心. 不料这本小册子竟给我招来了上千封鼓励信. 以后人们便写出了许许多多

的“纵横谈”.

从学生时代起,我就喜读方法论方面的论著.我想,做什么事情都要讲究方法,追求效率、效果和效益,方法好能事半而功倍.我很留心一些著名科学家、文学家写的心得体会和经验.我曾惊讶为什么巴尔扎克在51年短短的一生中能写出上百本书,并从他的传记中去寻找答案.文史哲和科学的海洋无边无际,先哲们的明智之光沐浴着人们的心灵,我衷心感谢他们的恩惠.

读书的另一面

以上我谈了读书的好处,现在要回过头来说说事情的另一面.

读书要选择.世上有各种各样的书:有的不值一看,有的只值看20分钟,有的可看5年,有的可保存一辈子,有的将永远不朽.即使是不朽的超级名著,由于我们的精力与时间有限,也必须加以选择.决不要看坏书,对一般书,要学会速读.

读书要多思考.应该想想,作者说得对吗?完全吗?适合今天的情况吗?从书本中迅速获得效果的好办法是有的放矢地读书,带着问题去读,或偏重某一方面去读.这时我们的思维处于主动寻找的地位,就像猎人追找猎物一样主动,很快就能找到答案,或者发现书中的问题.

有的书浏览即止,有的要读出声来,有的要心头记住,有的要笔头记录.对重要的专业书或名著,要勤做笔记,“不动笔墨不读书”.动脑加动手,手脑并用,既可加深理解,又可避忘备查,特别是自己的灵感,更要及时抓住.清代章学诚在《文史通义》中说:“札记之功必不可少,如不札记,则无穷妙绪如雨珠落大海矣.”

许多大事业、大作品，都是长期积累和短期突击相结合的产物. 涓涓不息，将成江河；无此涓涓，何来江河？

爱好读书是许多伟人的共同特性，不仅学者专家如此，一些大政治家、大军事家也如此. 曹操、康熙、拿破仑、毛泽东都是手不释卷，嗜书如命的人. 他们的巨大成就与毕生刻苦自学密切相关.

王梓坤

Summary

Decidability of prime number and the problem of decomposition of large numbers hold an important place in number theory. From ancient times people paid great attention to its research. Because of the development of computer science recently the old problem forms a new branch of number theory—computation of number theory. The book completely introduces the whole history and theories of the problem of decidability of prime number, and expounds its position in the research of pure mathematics, applied mathematics, and practical value in modern science(e. g. the use in Cryptography). The book has substantial content and the exposition is in neat formation.

序 言

数论中一个最基本、最古老而当前仍然受到人们重视的问题就是判别给定的整数是否为素数(简称为素数判别或素性判别)和将大合数分解成素因子乘积(简称为大数分解).在历史上,这个问题曾经吸引了包括费马(Fermat)、欧拉(Euler)、勒让德(Legendre)和高斯(Gauss)在内的大批数学家,他们花费了大量的时间和精力去研究这个问题.高斯在其著名的《算术探索》(《Disquisitiones Arithmeticae》)中称道:"把素数同合数鉴别开来及将合数分解成素因子乘积被认为是算术中最重要和最有用的问题之一."我国的《易经》中也对这个问题做了研究.

素数判别和大数分解这个问题具有很大的理论价值.因为素数在数论中占有特殊的地位,所以鉴别它们则成为最基本的问题,而把合数分解成素因子的乘积是算术基本定理的构造性方面的需要.人类总是有兴趣问如下的问题:$2^{131}-1$是否为素数?由23个1组成的数是否为素数?怎么分解31 487 694 841 572 361?对素数判别和大数分解的研究必然会丰富人类的精神财富.更重要的是,素数判别和大数分解具有很大的应用价值.在编码中,需要讨论某类有限域及其上的多项式,这类有限域就是由素数p所作成的$Z/pZ=\{\bar{0},\bar{1},\cdots,\overline{p-1}\}$,这就要求我们去寻找素数、判别素数.在快速数论变换中,要讨论Z/nZ上的卷积运算,就要知道Z/nZ的乘法群的构造,而这就依赖于将n分

解成素因子的乘积.下面介绍的RSA公开密钥码体制更加说明了这个问题的两个方面在实际应用中的作用.1977年,艾德利曼(Adleman)、希爱默(Shamir)和李维斯特(Rivest)发明了一个公开密钥码体制.在这个密码体制中,对电文的加密过程是公开的,但是你仅知道加密过程而未被告知解密过程,则不可能对电文进行解密.他们的体制就是依靠这样一个事实:我们能够很容易地将两个大素数(譬如两个百位素数)乘起来;反过来,要分解一不大整数(譬如200位)则几乎不可能.(关于RSA体制的详细介绍,请参阅文献[1]).因此RSA体制就与素数判别和大数分解有密切联系.要具体建立一个RSA体制就需要两个大素数,因而就涉及寻找大素数的问题;而RSA体制的破译的可能性就依赖于分解一个大数的可能性.于是,RSA体制的建立与破译就等价于素数判别与大数分解问题.近年来,由于计算机科学的发展,人们对许多数学分支的理论体系重新用计算的观点来讨论.从计算的观点来讨论数论问题形成了当前很活跃的分支——计算数论,而素数判别和大数分解成为这一分支的重要组成部分.在这一部分里提出了两个重要的、悬而未决的问题:是否存在判别素数的多项式算法?是否存在分解大整数的多项式算法?现已知道"分解整数"这个问题是一个NP完全问题,因此对上面第二个问题的讨论是解决计算机科学中的难题[①]:"NP完全问题是否一定是多项式算法可解的?"的一个突破口.因此,素数判别和大数分解对计算机科学来说也是很有价值

① 可参看:管梅谷,组合最优化介绍,数理化信息,1,73-80.

的.

最直接的素数判别和大数分解方法就是试除法，即对整数 n，用 $2,\cdots,n-1$ 去试除，来判定 n 是否为素数，分解式如何. 这个方法是最简单的一个方法，古希腊时就被人们所知，但这个方法对较大的数(20 位左右)就要耗费很多时间. 在 20 世纪 40 年代电子计算机出现之前，尽管产生了许多素数判别和大数分解方法，但因为用手算，速度太慢，很多方法在实用中即使对十几位的数也需要好几天，而对更大的数就无能为力了. 随着计算机的出现及发展，人们开始用这个有力的工具来研究素数判别和大数分解. 到 20 世纪 60 年代末期，已产生了许多新方法，历史上的许多方法也得到了应用，使得对四十几位数的素数判别可以很快得到结果. 而到 20 世纪 70 年代末，数论学家和计算机专家们已深入地研究了这个问题，并得到许多实际而有效的方法. 用这些方法在较好的计算机上判别一个 100 位数是否为素数只需不到一分钟；分解 70 位左右的整数也是日常工作了. 这些成果已引起人们的普遍关注，在这个领域中的研究空前活跃. 虽然离问题的彻底解决还很远，但在本领域中已取得了一个又一个的突破，在这方面的研究必有光辉的前景.

我们写这本书的目的是要介绍素数判别和大数分解的发展历史、一般理论、各种方法及最新成果，是想让许多非专业的读者了解这个方向的内容和进展情况. 当然，只有在这些定理的证明较为初等而又不太长时，我们才给出其证明. 因为这个方向与计算机科学的密切关系，我们还要结合计算量来介绍一些数论中常用的基本算法.

除了极个别内容，如 2.7 节，本书的绝大部分内容只需要某些初等数论的知识，它们可以在任何一本介绍初等数论的书中都能找到，如文献[1]．对于广义黎曼猜想，我们写了一则简短的附录．如果读者在欣赏之余，还打算进一步学习和探讨的话，那么，后面所列的文章和书目可供参考．

限于水平，本书的缺点和疏漏一定不少，我们期待着读者的批评与指正．

作　者

Catalogue

目 录