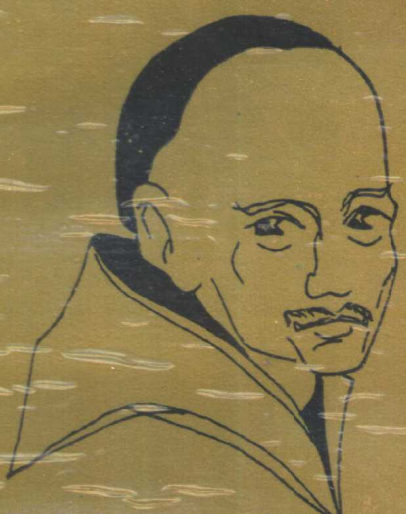
世界数学名题欣赏



素数判定与大数分解

辽宁教育出版社

世界数学名题欣赏丛书

素数判定与大数分解

孙　琦
旷京华　编著

辽宁教育出版社
1987年·沈阳

素数判定与大数分解

孙琦　旷京华　编著

辽宁教育出版社出版　辽宁省新华书店发行
（沈阳市南京街6段1里2号）　大连印刷工业总厂印刷

字数：52,000　开本：787×1092 1/32　印张：3 1/4　插页：4
印数：1—4,086
1987年10月第1版　1987年10月第1次印刷

责任编辑：俞晓群　谭坚　　责任校对：周广东
封面设计：安今生　　插　　图：安　迪

统一书号：7371·506　　定价：1.00元
ISBN 7—5382—0180—7

内 容 简 介

本书是”世界数学名题欣赏丛书“之一。素数判定与大数分解问题在数论中占有重要地位，远古时代人们就十分重视它的研究。近年来，由于计算机科学的发展，使这一古老的问题焕发了青春，形成了数论中的新分支——计算数论。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。

Summary

This book is one of a Series of World Famous Mathematics Appreciat ion. 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 subst antial content and the exposition is inneat 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《算术探讨》（《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作为算术中最重要最有用的问题之一。"我国的《易经》中也对这个问题作了研究。

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，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：$2^{131}-1$是否素数？由23个1组成的数是否素数？怎么分解

31487694841572361？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$Z/pZ=\{\overline{0},\overline{1},\cdots,\overline{p-1}\}$，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) 和鲁梅利 (Rumely) 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。首先，要具体建立一个 RSA 体制就需要两个大素数，因而就涉及到寻找大素数的问题；而RSA体制的破译之可能性就依赖于分解一个大数可能性。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？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*：“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，…，n－1去试除，来判定 n 是否素数，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。在本世纪四十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

* 可参看：管梅谷，组合最优化介绍，数理化信息，1，73—80。

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。到六十年代末期，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。而到七十年代末，数论学家和计算机专家们已深入地研究了这个问题，得到许多实际有效的方法。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。

我们写这个小册子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，如第二章第七节，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。作为“世界数学名题欣赏丛书”中的一本，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，本书的缺点和错误一定不少，我们期待着读者的批评指正。

作　者

1987年4月

作者简介

孙琦（左），1937年生于浙江省吴兴县，1961年毕业于四川大学数学系，现为四川大学数学系教授、数学研究所数论研究室主任、《数学学报》编委、四川省数学会副秘书长。已发表学术论文50余篇，出版著作五种。主要研究方向为数论中的不定方程和应用数论。

旷京华，1963年生于江西，1982年毕业于江西大学数学系，继续读研究生于四川大学数学系，现在美国明尼苏达大学数学系攻读数学。主要研究方向是与数论有关的分支。

世界数学名题欣赏丛书

费马猜想
黎曼猜想
连续统假设
希尔伯特第十问题
欧几里得第五公设
哥德尔不完全性定理
不动点定理
无处可微的连续函数
科克曼女生问题
斐波那契数列
哥德巴赫猜想
置换多项式及其应用
素数判定与大数分解
货郎担问题

目　录

Catalogue

一　数论中的基本算法