number theory conversion ... product of prime factors. Two l... setting up RSA system (the open key ... Shamir, Adleman). In modern computer ... ple use viewpoints of computing to research mathe... system number theory, which forms currently important branch computation number theory. The important component in computation number theory is discrimination of prime numbers. It is not difficult to make out that discrimination of prime numbers is most valuable to computer science.

素数及其快速判定的新方法与应用

潘树明 著

金工业出版社

SUSHU

素数及其快速判定的新方法与应用

潘树明　著

北　京
冶 金 工 业 出 版 社
2002

内 容 简 介

本书在阐述素数的基本理论和基本概念的基础上，介绍了快速判定素数的新定理、新方法及其应用，用这种新方法比传统方法提高判定效率 7～10 倍。此外，本书还介绍了素数性质、奇偶数性质的 22 个定理、双生素数性质的 37 个猜想及 10 个素数猜想。书后附有 300000 以内的素数表。

本书可供数学爱好者阅读，也可供从事数学、计算机工作的人员参考。

Synopsis

Based on the basic theories and concepts of prime numbers, puts forward new theorems, new methods and their application on discrimination of prime numbers increasing discrimination efficiency by 7-10 times, provides 22 theorems on properties of prime numbers and odd and even numbers, 37 conjectures on properties of twin prime numbers, and 10 conjectures on prime numbers. The appendix includes the prime numbers less than 300,000.

This book is applicable for math enthusiast, and it also can be a reference for the people in the field of mathematics and computer.

图书在版编目(CIP)数据

素数及其快速判定的新方法与应用/潘树明著. —北京：冶金工业出版社，2002.8

ISBN 7-5024-3062-8

Ⅰ.素… Ⅱ.潘… Ⅲ.素数—研究 Ⅳ.0156.2

中国版本图书馆 CIP 数据核字(2002)第 050256 号

出版人 曹胜利（北京沙滩嵩祝院北巷 39 号，邮编 100009）
责任编辑 刘小峰 美术编辑 李 心 责任校对 侯 瑚 责任印制 牛晓波
北京鑫正大印刷有限公司印刷；冶金工业出版社发行；各地新华书店经销
2002 年 8 月第 1 版，2002 年 8 月第 1 次印刷
850mm×1168mm 1/32；4.75 印张；128 千字；142 页；1－2500 册
15.00 元
冶金工业出版社发行部 电话：(010)64044283 传真：(010)64027893
冶金书店 地址：北京东四西大街 46 号(100711) 电话：(010)65289081
（本社图书如有印装质量问题，本社发行部负责退换）

前　言

在大于 1 的整数中，除 1 和其本身之外，不被任何数除尽的数称为素数。素数在数论中占有特殊的地位。任何数都可以用素数的乘积表示，所以素数是数中的“原子”，是构成自然数的基本元素。掌握了任何一个数的素因子分解，数学家就获得了有关这个数的信息。人们一直把素数判定取得的结果看成是人们的重要精神财富。在试验新计算机的效率和硬件性能时，用素数构成多位数，以便为材料加密。在现代数学应用中，例如编码时，就需要讨论某些类别有限域及其上的多项式。这些有限域就是由素数 P 做成的 $Z/PZ=\{\overline{0},\overline{1},\cdots,\overline{P-1}\}$，这就要求我们必须去寻找素数、判定素数。

素数判定从古至今一直受到人们重视，是因为素数判定这个问题具有很大的理论价值和实用价值。

本书中所列出的作者多年来研究的素数判定的新定理、新方法比一般常用的筛选法可提高计算速度 7～10 倍，具有准确、效率高的特点。利用这些定理可以引出一个双生素数定理：“大于 5 的两个差为 2 的相邻双生素数有无限多个，而且每对双生素数之间相差之数为 6 的倍数。”

数学家卡尔·弗里德列希·高斯（Karl Friedrich Gauss）曾经说过：“高等算术中一些最美丽的定理具有这样的特性：它们极易从经验事实中归纳出来，但是证明却隐藏很深，只有高人一等的研究者才能把它们挖掘出来。正是出于这种原因，赋予高等算术以神奇魅力，使之成为第一流数学家们最喜爱的科学。至于它远远凌驾于数学的其他分支之上的无限丰富性，就更不必提了。”

本书也将作者与数学家廖震合作多年研究出的素数性质、奇偶数性质 22 个定理及推论刊出。如能为初等数论内容起到添砖加瓦的作用，作者将感到十分荣幸。

在数学中，数论是最美的一个分支，从古至今，一直受到专家和数学爱好者的偏爱，而双生素数是美中之美的数。本书也给出了作者对双生素数性值的37个猜想和10个素数猜想。数学猜想是数学发展的一个重要思维方式。它具有创新性，尽管这种猜想目标很具体，且正确与否有待于人们去证明。

本书中也给出了30万以内的素数，以便于研究和使用者查找。

本书在编写过程中，由潘锋工程师承担了全部中译英工作和打字工作。在此对廖震、潘锋、李总成先生的帮助表示衷心感谢。

尽管书中内容不太完善，作者借ICM－2002国际数学大会之机将此书献给广大数学家及数学爱好者。由于水平所限和时间仓促，不足之处难免，欢迎批评指正。

潘树明

2002年6月

Preface

Prime number is the number which can not be divided by any number except for 1 and itself. Prime numbers play important role in number theory. Any number can be expressed as the product of prime numbers, so prime numbers are 'atoms' of numbers – basic elements of natural numbers. Once grasping prime factor explosion for a number, mathematicians obtain information about this number. People always regard the result of discrimination of prime numbers as important spirit treasure. During efficiency and hardware testing of a new computer, multi – digit number is made of prime numbers to encrypt confidential materials. The more important usage is in modern application mathematics, for example, certain limited regions are required to be discussed in encoding. These limited regions are $Z/PZ = \{\bar{0}, \bar{1}, \cdots \overline{P-1}\}$ made up of prime number P, which asks us to look for prime numbers and discriminate prime numbers.

Discrimination of prime numbers has been all along thought highly of, for it has great theoretical and practical value.

This book lists new theorems and methods on discrimination of prime numbers being studied for many years by the author, which can increase computation speed by 7 – 10 times comparing with normal filters and so are accurate and efficient. With these theorems, there comes out a twin prime numbers theorem: "there are infinite neighboring twin prime numbers larger than 5 in which the difference of the two numbers is 2, and the difference of every pair of twin prime numbers is a multiple of 6."

Mathematician Karl Friedrich Gauss has ever stated: "some

beautiful theorems in higher arithmetic have such attributes: they are easy concluded from experiences but deeply concealed for proving. Only super mathematicians can dig them out. Just for this reason, higher arithmetic has amazing charm and becomes the favorite of excellent mathematicians. Even no need to comment on its infinite abundance beyond other branches of mathematics."

This book also lists 22 theorem and deductions on properties of prime numbers and odd and even numbers being studied by Pan Shuming and Mathematician Liaozhen for many years. If they can be supplement for number theory, the author will be greatly honored.

In mathematics, number theory is the most beautiful branch and twin prime numbers are beautiful－in－beautiful. This book also lists 37 conjectures of twin prime numbers and 10 conjectures on prime numbers made out by the author. Conjectures in mathematics are an important thinking method. It has innovation, though this kind of conjectures have concrete targets and are under proving.

This book also provides prime numbers less than 300,000 for researchers' and users' convenience.

During the writing, Mr. Pan Feng took on the whole translation and typing job. The author are greatly grateful to Mr. Liao Zhen, Pan Feng and Li Zongcheng here. The author would like to present this book to mathematicians during ICM－2002. Because of ability limit and time shortage, there may be inevitable deficiencies. If you have any comments and suggestions, please let the author know.

Pan Shuming
June, 2002

目　录

Catalogue

1 素数判定的新定理、新方法

本章提出了素数判定的新定理、新方法。用本章提出的新定理、新方法可提高运算速度，并引出大于 5 的双生素数有无限多个，每对双生素数之间相差之数为 6 的倍数。本章提出的定理及方法在计算机科学、研究 RSA 密钥码体制中、大素数寻找、计算数论中有广泛的应用。

在历史上，素数曾吸引了大批数学家：高斯(Gauss)、费马(Fermat)、欧拉(Euler)、勒让德(Legendre)花费大量的精力和时间研究它。高斯在他的《算术讨论》(*Disquistiones Arithmeticae*)中曾这样写到："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是算术中最重要、最有用的问题之一。"中国的《易经》一书也对这个重要问题做了研究。

将合数分解成素因子的乘积是算术基本定理的构造性方面之需要。在快速数论变换中研讨的 Z/nZ 的乘法群的构造就依赖于将 n 分解为素因子的乘积。要具体建立 RSA 体制(鲁梅利(Rumely)、沙米尔(Shamir)、埃德勒曼(Adleman) 三人发明的公开密钥码体制)就需要两个大素数，就必须寻找大素数问题。在现代计算机科学发展中，人们用计算的观点研讨数学分支理论体系——数论，形成了当前重要的分支——计算数论。计算数论中重要组成部分就是素数判别。不难看出，素数判定对计算机科学来说是有十分重要价值的。

计算数论中提出：是否存在判别素数的多项式方法，是当前悬而未决的难题之一。

对于素数判定，从古至今，曾提出了许多方法，但仍认为"试除法"是最简单的素数判别法。和其相关的埃拿托申斯(Eratosthenes)筛选法对制作素数表起了重大的作用。当今，人们多么希望尽早找到一种素数判别的多项式算法，然而这尚需进一步去研

究。在尚未找到素数判别多项式法之前，能否找到比“试除法”更简便的计算快速的运算方法、素数判别的新定理、新方法？本章就是针对这一问题，为解决这一问题寻找到一个比“试除法”更简便、计算速度提高几倍的素数判定新定理、新方法。

1.1 素数判定的新定理

定理：$n\in\mathbf{N}$，$f(n)=6n\pm1$ 数列自然数中划去能被小于 $\sqrt{f(n)}$ 的素数整除之数，添上 2 和 3 两个数，即为全部素数。

证明：设数列 5，7，11，13，17，19，…，n

$$P_0=5,\ P_1=7,\ P_3=11,\cdots,\ P_r\leqslant\sqrt{n}<P_{r+1}$$

将数列中依次划去：

$$\begin{aligned}&5P_0,\ 7P_0,\ 11P_0,\ 13P_0,\cdots\\&5P_1,\ 7P_1,\ 11P_1,\ 13P_1,\cdots\\&5P_2,\ 7P_2,\ 11P_2,\ 13P_2,\cdots\\&\cdots\\&5P_r,\ 7P_r,\ 11P_r,\ 13P_r,\cdots\end{aligned}\qquad(1\text{-}1)$$

此后所剩下的数，都不能被 P_0，P_1，…，P_r 各素数所整除。假设所剩下的数中有其复合数：

$$Q=d\times P_m$$

其中，Q 为 n 内的数，P_m 为不同于 P_0，P_1，…，P_r 的素因数，d 和 P_m 都是大于 1 的整数，故 $Q=d\times P_m\leqslant n$。由于 $n\in\mathbf{N}$，又小于 $\sqrt{Q}$ 的整数都除不尽，所以 $d>\sqrt{Q}$，$P_m>\sqrt{Q}$，而得 $d\times P_m>\sqrt{Q}\times\sqrt{Q}=Q$，这与 $d\times P_m=Q$ 是相矛盾的。所以如果 $n\in\mathbf{N}$，而小于 $\sqrt{Q}$ 的整数都除尽，则 Q 不是素数。由上所述，Q 是复合数，则 Q 一定有 $n\in\mathbf{N}$ 而小于 $\sqrt{Q}$ 的因数。由于 $n\in\mathbf{N}$，则 Q 的大于 1 的最小因数一定是素数，所以 $f(n)=6n\pm1$ 中将式 1-1 中划去之后所剩下的数都不能被 P_0，P_1，…，P_r 各素数所整除，因此 Q 必定是素数，应有下式：

$$Q < \sqrt{n} < P_{r+1}$$

d 是 $r+1$ 个中某一个素数，必在式 1-1 中被划除，故 n 内所剩之数均为素数，故式 1-1 可简化为：

$$P_0^2,\ 5P_0,\ 7P_0,\ 11P_0,\cdots$$

$$P_1^2,\ 7P_1,\ 11P_1,\ 13P_1,\cdots$$

$$P_2^2,\ 11P_2,\ 17P_2,\ 19P_2,\cdots$$

$$\cdots$$

定理证毕。

1.2 比较

例：判定 100 内的素数，逐一列出。

解：运用前述定理 $f(n) = 6(n) \pm 1$，列出 $n = 1, 2, 3, \cdots$，16 时的数，即：5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47, 49, 53, 55, 59, 61, 65, 67, 71, 73, 77, 79, 83, 85, 89, 91, 95, 97，共 32 个。

$\sqrt{100}$ 内大于 5 的素数为 5, 7。

将 100 内的复合数逐次划去：

划去被 5 整除的数(5 除外)，即：

25, 35, 55, 65, 85, 95。

划去被 7 整除的数(7 除外)，即：

49, 77, 91。

再根据定理，将 2、3 两个素数放入，得出 100 以内的全部素数是：

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97，共 25 个。

为了对比说明本定理的优点，用现在应用的一般方法(非本文定理方法)判定 $n = 100$ 内的素数有哪些。

列出：(1 除外)从 2, 3, 4, 5, …, 99, 100 数列将 100 内复合数逐次一一划去，即将 100 内能被 2, 3, 5, 7 整除的数划去。

划去被 2 整除的数(2 除外,49 个):

4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100。

划去被 3 整除的数(3 除外,16 个):

9, 15, 21, 27, 33, 39, 45, 51, 57, 63, 69, 75, 81, 87, 93, 99。

划去被 5 整除的数(5 除外,6 个):

25, 35, 55, 65, 85, 95。

划去被 7 整除的数(7 除外,3 个):

49, 77, 91。

所剩余的数如下:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97,即为 100 以内的全部素数。用一般方法判定 100 以内素数要划去的次数为:49 + 16 + 6 + 3 = 74(次),而用本定理要划去的次数为:6 + 3 = 9(次),减少了 65 次。

例:判定 200 内的全部素数有哪些?

解:用本文提出的定理的做法。

用 $f(n) = 6n \pm 1$ 列出 $n = 1, 2, \cdots, 33$ 时所有的数:

5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47, 49, 53, 55, 59, 61, 65, 67, 71, 73, 77, 79, 83, 85, 89, 91, 95, 97, 101, 103, 107, 109, 113, 115, 119, 121, 125, 127, 131, 133, 137, 139, 143, 145, 149, 151, 155, 157, 161, 163, 167, 169, 173, 175, 179, 181, 185, 187, 191, 193, 197, 199。

$\sqrt{200}$内大于 5 的素数是:5,7,11,13。

将 200 内复合数逐次划去:

划去被 5 整除的数(5 除外):

25, 35, 55, 65, 85, 95, 115, 125, 145, 155, 175, 185。

划去被 7 整除的数(7 除外):

49, 77, 91, 119, 133, 161。

划去被 11 整除的数(11 除外):121, 143,187。

划去被 13 整除的数(13 除外):169。

再根据本定理,将 2、3 两个素数放入,得出 200 以内全部素数是:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199,共 46 个。

为了对比说明,对此例使用非本文定理的方法判定 $n=200$ 内的素数。具体做法是:

列出(1 除外)2, 3, 4, 5,…,199, 200 数列,将 200 以内复合数逐次一一划去,即将$\sqrt{200}$内能被 2, 3, 5, 7, 11, 13 整除的数划去:

划去被 2 整除的数(2 除外,99 个):

4, 6, 8, 10,…,198, 200

划去被 3 整除的数(3 除外,32 个):

9, 15, 21, 27, 33, 39, 45, 51, 57, 63, 69, 75, 81, 87, 93, 99, 105, 111, 117, 123, 129, 135, 141, 147, 153, 159, 165, 171, 177, 183, 189, 195

划去被 5 整除的数(5 除外,12 个):

25, 35, 55, 65, 85, 95, 115, 125, 145, 155, 175, 185。

划去被 7 整除的数(7 除外,6 个):

49, 77, 91, 119, 133, 161。

划去被 11 整除的数(11 除外,3 个):

121, 143,187。

划去被 13 整除的数(13 除外,1 个):

169。

所剩下的数如下:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199。

用一般方法判定 200 以内素数要划去的次数为:99 + 32 + 12 + 6 + 3 + 1 = 153(次),而用本定理要划去的次数为:12 + 6 + 3 + 1 = 22(次),减少了 153 - 22 = 131 (次)。

表 1-1 用本定理方法和用一般筛选法判定素数划去次数的比较

判 定 方 法	100 内	200 内	1000 内
用一般方法划去次数	74	153	825
用本定理法划去次数	9	22	94

从表 1-1 看出,用本定理给出的素数判定新方法比一般通用的筛素数法减少筛(划去)次数大约 7～10 倍,可以说提高效率或者提高计算速度 7～10 倍。说明用本定理去做"素数判别"具有效率高、速度快 7～10 倍的优点。

1.3 讨论

直观地讲,我们列出以 6 为公差的 6 个数列如下:

第一个数列:2, 8, 14, 20, 26, 32, 38, 44

第二个数列:3, 9, 15, 21, 27, 33, 39, 45

第三个数列:4, 10, 16, 22, 28, 34, 40, 46

第四个数列:6, 12, 18, 24, 30, 36, 42, 48

第五个数列:5, 11, 17, 23, 29, 35, 41, 47

第六个数列:7, 13, 19, 25, 31, 37, 43, 49

本定理给出的素数判定方法,巧妙地运用公差为 6 的上述六个等差级数中的第五个、第六个两个,即素数(补充 2 和 3 两数)集中在第五个、第六个两个数列,在这两个数列中要筛去的数即复合数中均有一个素数因子在其中,例如运用本定理给出的方法求 $f(n)=1000$ 内的素数有哪些? 列出 $6n \pm 1$ 的数列,要筛去被 5

整除的数可归结为一个公式:$5+5(n\pm1)\times6$,要筛去被 7 整除的可归纳一个公式 $7+30(n-1)$,要筛去的被 13 整除的归纳为 13 乘以 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73 诸素数,要筛去的被 17 整除的归纳为 17 乘以 17, 19, 23, 29, 31, 37,41, 43, 47, 53 诸素数,要筛去的被 23 整除的归纳为 23 乘以 23,29,31,37,41,43 诸素数。要筛去被 29 整除的归纳为 29 乘以 29, 31 两个素数,要筛去被 31 整除的只有一个即 $961=31\times31$,即素数 31^2。

1.4 判定素数应用举例

例:判定 4999 是否素数。

解:$\sqrt{4999}=70.7036$,用本定理给出的公式 $f(n)=6n\pm1$ 列出数列,式中 $n=1, 2, 3,\cdots, 10, 11$,相应的数列为:5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47, 49, 53, 55, 59, 61, 65, 67。

因为 $\sqrt{70.7036}=8.4$,即用小于 8 的素数 5 和 7 整除上数列(2、3 两素数除外)。划去被 5 整除的数:25, 35, 55, 65;划去被 7 整除的数:49。余下的素数为:

5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67。用这些素数除 4999,均不能整除,故 4999 为素数。

例:判定 128431 是否素数。

解:$\sqrt{128431}=258.37$,用本定理给出的公式 $f(n)=6n\pm1$ 列出数列,式中 $n=1, 2, 3,\cdots$,相应的数列为:5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47, 49, 53, 55, 59, 61, 65, 67, 71, 73, 77, 79, 83, 85, 89, 91, 95, 97, 101, 103, 107, 109, 113, 115, 119, 121, 125, 127, 131, 133, 137, 139, 143, 145, 149, 151, 155, 157, 161, 163, 167, 169, 173, 175, 179, 181, 185, 187, 191, 193, 197, 199, 203, 205, 209, 211, 215, 217, 221, 223, 227, 229, 233, 235, 239, 241, 245, 247, 251, 253, 257。

因为$\sqrt{258.37}=16.07$,即用小于 16 的素数 5, 7, 11, 13 去整除上数列。划去被 5 整除的数:25, 35, 55, 65, 85, 95, 115, 125, 145, 155, 175, 185, 205, 215, 235, 245;划去被 7 整除的数:49, 77, 91, 119, 113, 161, 203, 217;划去被 11 整除的数:121, 143, 187, 209, 253;划去被 13 整除的数:169, 221, 247。余下的素数为:5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 115, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257。用这些数除 128431,发现均不能整除,故 128431 是素数。

根据前述定理可以提出一个关于双生素数定理:

大于 5 的两个近邻素数相差 2 的双生素数有无限多个,而且每对双生素数之间相差的数为 6 的倍数。

如:5, 7; 11, 13; 17, 19; 29, 31; 41, 43; 59, 61; 71, 73; 101, 103; 107, 109; 137, 139; 191, 193; 197, 199; 227, 229, …

双生素数 5, 7 和 11, 13 之间 $11-5=6, 13-7=6$;双生素数 11, 13 和 17, 19 之间 $17-11=6, 19-13=6$;双生素数 29, 31 和 41, 43 之间 $41-29=12, 43-31=12$;…

证明:$n\in\mathbf{N}$,$f(n)=6n\pm1$,可写为 $f(n)=5+6(n-1)$ 和 $f(n)=7+6(n-1)$ 两个数列($n=1, 2, \cdots, \infty$),得出两个公差为 6 的等差级数。分别按本定理求出各素数,划掉复合数(含素因子)之后,余下的素数间隔为 6 的倍数;将两个数列合在一起,由于数列 $f(n)=5+6(n-1)$ 和 $f(n)=7+6(n-1)$ 相差为 2,故双生素数相差为 2。

下面再用反证法证明本题:假设双生素数有很多个,共有 n 个,就是 $P_1, P_2, P_3, \cdots, P_n$,其中 $P_1=5, P_2=7, P_3=11, P_4=13, \cdots$。令 $Q=P_1, \cdots, P_{n+1}$,如果 Q 是双生素数,则因 Q 不等于 $P_1, P_2, P_3, \cdots, P_n$ 中的任何一个,故双生素数的个数最少有 n