姜发启／著

全球范围内第一次发现了**初等形式的、超越费马小定理的、无伪质数的**判别质数通用公式。
详细介绍了对**判别质数通用公式**（即充要条件）的成功证明。

判别质数通用公式首发现

◎超越费马小定理◎

中国水利水电出版社
www.waterpub.com.cn

判别质数通用公式首发现
——超越费马小定理

姜发启　著

中国水利水电出版社
www.waterpub.com.cn

内 容 提 要

本书是全球范围内唯一敢称首次发现判别质数通用公式的圣书；主要介绍发现者（即作者）通过十几年对质数的探索而首发现的、初等形式的、超越费马小定理的、无伪质数的、判别质数的通用公式，也是判别质数的充要条件；首次揭示不用计算，而用“排列图表法”排寻质数的新方法，特别是用“AB 图表法”排寻质数的方法；详细介绍了对判别质数通用公式的成功证明；以大量篇幅介绍了判别质数通用公式的应用和系列衍生公式，特别是产生孪生质数的条件和判别差公式、偶数二数和“p+p”与“p+p+2”是孪生质数对以及奇数三数和“p+p+p”与“p+p+p+2”是孪生质数对的条件公式；首次提出用偶数二数和“p+p”的“产质率”与奇数三数和“p+p+p”的“产质率”尝试对哥德巴赫猜想的证明等，是对人类探索质数奥秘的重要贡献！

本书可供从事探究数论、质数研究、寻找最大质数（如梅森质数、孪生质数对、X^2+1 及 X^2-1 型质数等）的数学科研专业人员及数学业余爱好者等学习和参考，可供研究和寻找各种质数的人们直接应用和开发编程化应用，开发编程化应用可以结合本书所讲的“关于应用型质数判别公式的分步计算法”。

图书在版编目（CIP）数据

判别质数通用公式首发现 ：超越费马小定理 / 姜发启著. -- 北京 ：中国水利水电出版社，2015.2
ISBN 978-7-5170-2901-4

Ⅰ. ①判… Ⅱ. ①姜… Ⅲ. ①质数－研究 Ⅳ. ①O122

中国版本图书馆CIP数据核字(2015)第020961号

策划编辑：周春元　　责任编辑：宋俊娥　　加工编辑：宋　杨

书　　名	判别质数通用公式首发现——超越费马小定理
作　　者	姜发启　著
出版发行	中国水利水电出版社 （北京市海淀区玉渊潭南路 1 号 D 座　100038） 网址：www.waterpub.com.cn E-mail：mchannel@263.net（万水） sales@waterpub.com.cn 电话：（010）68367658（发行部）、82562819（万水）
经　　售	北京科水图书销售中心（零售） 电话：（010）88383994、63202643、68545874 全国各地新华书店和相关出版物销售网点
排　　版	北京万水电子信息有限公司
印　　刷	三河市铭浩彩色印装有限公司
规　　格	184mm×260mm　16 开本　17.5 印张　437 千字
版　　次	2015 年 3 月第 1 版　2015 年 3 月第 1 次印刷
印　　数	0001—2000 册
定　　价	58.00 元

序　　言

由于质数在自然数列中的分布及其出现的间隔具有不确定性：

关于对质数的表达，能否用初等函数的形式给出或表达？

关于对质数的判定，能否用一个简单的、初等形式的通用公式来判别？

是许多年来数学家们一直尝试并努力追寻的愿望（或理想），然而进展总是不得如愿以偿，所以就出现各种退一步的说法，例如：

- 找到一个或多个公式，来表达或判定出某范围内的一部分质数；
- 或使所有企图寻找表达或判定质数统一公式的尝试都无果而终；
- 或给出某范围内的有限个某种形式的关于质数的通项公式；
- 或由许多数学家或数学业余爱好者贡献了很多的在某些小范围内或指定条件下的表示一些质数的表达式；
- 或者因存在有许多的伪质数而半途而废或暂时搁置。

如梅森质数、费马小定理、欧拉公式、第 n 个质数 P_n 的表达式、小于 25 的奇质数公式、小于 49 的奇质数公式、由第 n 个质数 P_n 的表达式得到的无数个 P_n 质数通项公式……因为这些公式大都会从某个数（或自变量）开始失效或者说产生了伪质数。

虽然已存在诸如用计算机编程对数的素性检验法、AKS 质数测试算法、应用费马小定理对数的素性检验与质数快速检验法、ARCL 检验法等诸多质数检验方法，但是都不能解决自然数是质是合的通用性判别问题。

本人十几年来，利用业余时间探究自然数是不是质数的判别公式，通过对多项式理论、质数相关理论、数学数论、算术理论基础知识等相关数学理论深入仔细地学习，随时关注在此方面的国际新进展和科研动向，同时通过对多项式展开式的三角形分支理论、多项式分支中隐藏的精美图案，使用 AB 图表排寻质数法、数位压缩理论、自然数的个位数运算法则、自然数的倒数 1/n 的循环节理论、自然数的四类分类法以及存在有伪质数的许多质数判别公式等进行大量的计算、列表、分析、探究、专研后，终于找到（发现）了初等形式的质数判别通用公式。并在质数判别通用公式的基础上递推和衍生出：

1、孪生质数的判别差△n 通用公式和产生孪生质数应具备的条件；

2、判别是否为梅森质数的通用公式；

3、判别形如X^2+1 质数的通用公式；

4、判别形如X^2-1 质数的通用公式；

5、判别奇质数的通用公式；

6、判别第四类数是否为质数的 8 个通用公式；

7、证明偶数哥德巴赫猜想“$n=n_1+n_2$=质+质”的条件公式；

8、证明奇数哥德巴赫猜想“$n=n_1+n_2+n_3$=质+质+质”的条件公式等。

还发现了不用计算而用 AB 图表法排寻质数的各种方法：

1、用 AB 图表法排寻质数；

2、用 a+b=n 图表法排寻质数；

3、用 a-b=n 图表法排寻质数；

4、用 a*b/n 图表法排寻质数；

5、用“第一步踏空”图表法排寻质数。

在“第一步踏空”图表法的基础上总结出：

1、自然数的三角形倍数表；

2、奇数的三角形倍数表；

3、第三、第四类数的三角形倍数表；

4、第四类数的三角形倍数表；

5、质数的质数倍三角形表。

不用计算而用 AB 图表排寻质数的各种方法是寻找质数的一种新方法，也可以说用 AB 图表排寻质数法是继筛法之后的一种创新方法。如果说过去对质数的判别、寻找和检验有筛法、查表法、用计算机编程对数的素性检验法、AKS 质数测试算法、应用费马小定理对数的素性检验与质数快速检验法、ARCL 检验法等诸多的质数检验方法等，则现在还增添了用 AB 图表法排寻质数法及用初等形式的质数判别通用公式判别法。

本书重点介绍：

- 初等形式的质数判别通用公式；
- 用 AB 图表排寻质数法；
- 判别孪生质数的通用公式和具备的条件；
- 证明（试证明）哥德巴赫猜想的公式和条件。

本人所发现的初等形式的质数判别通用公式具有通用性，当 n 的定义域为 2～+∞时，不会产生伪质数。

如果说 ARCL 质数检验法改观了费马小定理的逆命题不成立——像 341 这样的数称为伪质数的情况；则本人发现的质数判别通用公式是对费马小定理的直接挑战，因为质数判别通用公式不会产生伪质数。

判别孪生质数的通用公式和孪生质数具备的条件，证明（试证明）哥德巴赫猜想的公式和条件等，则是质数判别通用公式的具体应用。如寻找总结出了判别孪生质数的判别差公式；找到了偶数二数和“质+质”孪生链的断链条件、偶数二数和“质+质”孪生链的周期性、奇数三数和“质+质+质”孪生链的周期性；产生偶数二数和“质+质”孪生链的条件及判别公式、产生奇数三数和“质+质+质”孪生链的条件及判别公式等。

本书除了重点介绍和证明质数判别通用公式之外，还利用了大量篇幅重点尝试利用质数判别通用公式等方法或途径对偶数和奇数哥德巴赫猜想进行试证明。

用 AB 图排寻质数法的特点是不用计算，只用两种状态（即 A、B 两种状态）进行排列，可以排列出所有的质数（只是排列图为无限大），也不会出现一个伪质数的情况。

判别孪生质数的通用公式和具备的条件是在初等形式的质数判别通用公式的基础上递推出的。

除初等形式的质数判别通用公式之外，还有应用型的质数判别公式，应用型的质数判别公式是仅当 n=4 时出现了一个伪质数，在某些情况下，它比通用型公式的使用则较为方便和适用。

本书可供从事探究数论、质数研究、寻找最大质数（如梅森质数、孪生质数对、X^2+1 及 X^2-1 型质数等）的数学科研人员及数学业余爱好者等学习和参考。

质数判别通用公式、质数判别应用型公式及在此基础之上递推和衍生出的针对某种质数判别的具体质数判别公式，可供研究和寻找各种质数的人们直接应用和开发编程化应用，开发编程化应用可以结合本书所讲的“关于应用型质数判别公式的分步计算法”。

本书难免存在叙述不完美和表达不理想的地方，或表达抽象、不尽人意的情况，敬请广大读者用力斧正。

特别感谢周春元等编辑对本书出版从始至终的理解和支持！

作者

2014 年 10 月于青海格尔木

目　　录

第一篇

质数判别通用公式

第一章　质数的基本概念、性质与探研进展状况

第一节　质数的基本概念与性质

一、质数的基本概念

1. 质数与合数

①**质数的定义**：一个大于 1 的整数，如果只能被 1 和它本身整除，就称为**质数**，也称为**素数**。例如 2、3、5、7、11、13……是质数[注[1]]。也可以说比 1 大但不是合数的整数称为质数[注[15]]。

②**合数的定义**：一个大于 1 的整数，除了能被 1 和它本身整除之外，如果还能被其他自然数整除，就称为**合数**。例如 4、6、8、9、10、12……是合数[注[1]]。也可以说比 1 大但不是质数的整数称为合数[注[15]]。合数集合本书中以粗体 **H** 或 **h** 表示。

③**1 和 0 既非质数也非合数**[注[1]]。如果 1 被认为是质数，那么质数与合数定义的严格阐述和规定就不得不取消或增加定义或规定中的一些限制条件[注[15]]，0 由于可以被任何数整除（其结果一定等于 0），所以它不符合质数的定义。

2. 质数的个数、大小与表示

①**最小的质数**：最小的质数是2。

②**质数的个数**：质数有无限多个。

③**最大的质数**：因为质数有无限多个，所以不存在最大的质数。

④**质数的表示**：质数集合通常表示成粗体 **P** 或 **p**。

⑤**通常所说的质数**：在数学领域内，凡提到质数时，通常是指正的质数。

二、关于质数的重要性质

（1）**互质定理**：一个质数如果不能整除一个自然数，那么它就与这个自然数互质[注[1]]。可以理解为它们的最大公约数是 1。

（2）**能被整除定理**：如果几个自然数的积能被一个质数整除，那么这几个数里至少有一个数能被这个质数整除[注[1]]。反之，可以理解为：如果几个自然数的积不能被一个质数整除，那么这几个数里没有一个数能被这个质数整除。

（3）**质数定理**：大于 1 的任何整数，至少有一个约数是质数[注[1]]。可以归纳为：合数的约数至少有两个是质数（两个相同或两个不相同），质数的质约数就是它本身。

（4）**分解质因数定理**：任何一个大于 1 的整数都可以分解质因数[注[1]]。可以归纳为：合数的质因数至少有两个（两个相同或两个不相同），质数的质因数就是它本身。

（5）**算术基本定理**：一个大于 1 的整数，如果不管质因数的次序，那么对它分解质因数的结果是唯一的[注[1]]。

三、质数的分类

（1）**偶质数**：就是个位数是偶数的质数。2 是唯一的一个偶质数，也是最小的质数。

（2）**奇质数**：就是个位数是奇数的质数，如 3、5、7、11、19 等。3 是最小的奇质数。

（3）**个位数是 5 的奇质数**：唯一的一个个位数是 5 的奇质数是 5。

（4）**个位数是 1、3、7、9 的奇质数**：除 2 和 5 外，其他奇质数的个位数是 1、3、7、9，这一类质数的数量最多，并且它们的 **1/P** 均是无限循环小数。

（5）**特殊质数**：在质数中，2 和 5 是两个特殊质数，因为 2 和 5 除其个位数的唯一性特征之外，它两个还能除尽所有的大于 0 的自然数，即 1/2=0.5 和 1/5=0.2 分别是 2 和 5 能除尽所有大于 0 的自然数的系数，0.5 和 0.2 是有限小数，而其余质数 **P** 的 **1/P** 均是无限循环小数，如 1/3=0.33333333333333333……，1/7=0.142857142857142857……。

（6）**孪生质数**：一般情况下，在自然数列中，**孪生质数就是指差为 2 的奇质数对**，例如 11 和 13 是一对孪生质数，17 和 19 是一对孪生质数等。

（7）**龙凤质数**：在自然数列中，2 和 3 是唯一的一对龙凤质数，龙凤质数没有孪生核。

（8）**三胞胎质数**：在自然数列中，3、5、7 是唯一的一组三胞胎质数。三胞胎质数有两个孪生核，即 4 和 6。本书后面的章节中将其称为（3、5、7）质数链或孪生质数链。

（9）**四胞胎质数**：在自然数列中，2、3、5、7 是唯一的一组四胞胎质数。

（10）**独质数**：也称为**孤质数**，是指一个质数加或减 2 后均不是质数的质数。如 23、37、47、53、67、79、83、97 等，它们加减 2 后均为合数。23 是最小的独质数。

（11）**(6n+1)与(6n-1)型质数**：除质数 2、3 之外，其他质数均可以分类为(6n+1)与(6n-1)型两种类型，(6n-1)型质数如：5、11、17、23、29 等，(6n+1)型质数如 7、13、19、31、37、43 等。

在孪生质数对中，(6n-1)型质数是孪生质数（除 2 与 3 之外）的小的弟弟数，如 5、11、17、29 等，(6n+1)型质数是孪生质数（除 2 与 3 之外）的大的哥哥数，如 7、13、19、31、43 等，(6n+1)型独质数，如 37、67、79 等，(6n-1)型独质数，如 23、53、83 等。

（12）**梅森质数**：满足 $M_p=2^p-1$，且当 p 为质数时，M_p 也是质数，则 M_p 就称为梅森质数。如 p=2 时，$M_p=3$，3 是梅森质数；p=3 时，$M_p=7$，7 是梅森质数；p=7 时，$M_p=127$，127 是梅森质数等[注【17】]。

（13）**其他各种形式的质数**：人们在研究质数时，还定义有各种形式的质数，如形如(X^2+1)和(X^2-1)的质数[注【7】]、五角星质数[注【6】]等，在此不详列。

四、有关质数的重要概念

（1）**孪生质数的核**：孪生质数的核是指孪生的两个奇质数之间的偶数，也称孪生核。如：4 是孪生质数对 3 与 5 的核，6 是孪生质数对 5 与 7 的核。孪生质数的核也称为中心点。

（2）**质数的间隔**：在自然数列中，相邻的两个质数之间的算术差称为质数的间隔。只有龙凤质数对 2 与 3 的间隔是 1，其他的两个相邻质数的间隔均是偶数，而所有两个孪生的奇质数对之间的间隔均是 2。按照统计及理论分析，大于 2 的奇质数之间的间隔为 2n。因为质数有无限多个，所以不存在最大的质数间隔。

（3）**质数的长链**[注【16】]（或称链节）：从某个质数（或从 1 或合数开始也可以）开始，按照某种规律而连续递增出来的有限数列的数如果均是质数（如果是从 1 或合数开始，则除去 1

或这个合数，但之后的有限个数均是质数），则就把这种现象称为质数的长链。如：从质数 5 开始，2+3*1=5，5 是质数；接下来：2+3*3=11，11 是质数；2+3*5=17，17 是质数；2+3*7=23，23 是质数；2+3*9=29，29 是质数；2+3*11=35，35 不是质数；到 35 处，质数的链就中断了，所以从 5 到 29 的质数长链中，有 5、11、17、23、29 共 5 个质数，这个质数长链的通式是：2+3(2n-1)。

第二节　质数的归属范畴与研究质数的意义

一、质数归属于数论的研究范畴

质数是属于数学领域的哪个范畴或者说学科分支呢？请看数学家与数学专业人士下面的一些论述：

1. 数论的四个部分

数论形成了一门独立的学科后，随着数学其他分支的发展，研究数论的方法也在不断发展。如果按照研究方法来说，数论可以分成**初等数论、解析数论、代数数论和几何数论**四个部分[注[5]]。

①**初等数论**是数论中不求助于其他数学学科的帮助，而只依靠初等的方法来研究**整数性质**的分支。比如中国古代有名的“**中国剩余定理**”，就是初等数论中很重要的内容[注[5]]。由于质数是归属于整数的范畴，**所以说研究质数与初等数论有关。**

②**解析数论**是使用数学分析作为工具来解决数论问题的分支。数学分析是以函数作为研究对象，在极限概念的基础上建立起来的数学学科。用数学分析来解决数论问题是由大数学家欧拉奠基的，俄国数学家车比雪夫等也对它的发展做出过重要贡献。**解析数论是解决数论中艰深问题的强有力的工具。**比如，对于“**质数有无限多个**”这个命题，欧拉给出了解析方法的证明，其中利用了数学分析中有关**无穷级数**的若干知识。二十世纪三十年代，苏联数学家维诺格拉多夫创造性地提出了“三角和方法”，这个方法对于解决某些数论难题有着重要的作用。我国数学家陈景润在解决“哥德巴赫猜想”问题中也使用的是解析数论的方法[注[5]]。**所以说研究质数与解析数论有关。**

③**代数数论**是把整数的概念推广到代数整数的一个分支。数学家把整数概念推广到一般代数数域上去，相应地也建立了**素整数、可除性**等概念[注[5]]。**所以说研究质数与代数数论有关。**

④**几何数论**是由德国数学家、物理学家闵可夫斯基等人开创和奠基的。几何数论研究的基本对象是“空间格网”。什么是空间格网呢？在给定的直角坐标系上，**坐标全是整数的点，称为整点，当然也包括了质数的整点。**全部整点构成的组就称为空间格网。空间格网对几何学和结晶学有着重大的意义。由于几何数论涉及的问题比较复杂，必须具有相当的**数学基础**才能深入研究[注[5]]。**所以说研究质数与几何数论也有关系。**

2. 质数在数学的数论研究中有着非常重要的地位——质数是数论的皇冠

质数在数学的数论研究中有着非常重要的地位，而数论在数学中的地位是独特的。高斯曾经说过“**数学是科学的皇后，数论是数学中的皇冠**”。还有“**质数是数论的皇冠**”的说法。因此，数学家都喜欢把数论中一些悬而未决的疑难问题，称为“皇冠上的明珠”，以鼓励人们去“摘取”，如**费马大定理、孪生质数问题、哥德巴赫猜想、圆内整点问题、完全数问题**等，它们都是数论中最为显要的几颗“明珠”[注[5]]。

二、研究质数的意义

1. 对数论的研究中实际也包括了对质数的研究

数论是一门高度抽象的数学学科，对数论的研究中实际也包括了对质数的研究。长期以来，数论的发展处于纯理论的研究状态，它对数学理论的发展起到了积极的作用。但对于大多数人来讲并不清楚它的实际意义。

由于近代计算机科学和应用数学的发展，数论得到了广泛的应用。比如在计算方法、代数编码、组合论等方面都广泛使用了初等数论范围内的许多研究成果注【5】。

2. 我国数论的研究发展情况

在我国近代，数论也是发展最早的数学分支之一。

从二十世纪三十年代开始，华罗庚、闵嗣鹤、柯召等第一流的数论专家在解析数论、刁藩都方程、一致分布等方面都有过重要的贡献。其中华罗庚教授在**三角和估值、堆砌质数论**方面的研究是享有盛名的。

1949 年以后，**我国数论的研究得到了更大的发展，**特别是在“筛法”和对“哥德巴赫猜想”的证明方面的研究，**已取得世界领先的优秀成绩。**陈景润在 1966 年证明“哥德巴赫猜想”的**“一个大偶数可以表示为一个质数和一个不超过两个质数的乘积之和”**后，在国际数学界引起了强烈的反响，盛赞陈景润的论文是解析数学的名作，是筛法的光辉顶点。至今，这仍是“哥德巴赫猜想”证明的最好结果注【5】。

3. 数论被冠以“数学皇后”的原因

数学的“大家庭”中包含着各式各样的“成员”。以研究数（特别是自然数）的规律的数论就是众多“成员”之一。对于数学家来说，它如同**“数学王子”**高斯所认为的那样，是整个数学王国中的“数学皇后”。那么究竟是什么原因，使数论赢得了这一美誉呢？注【13】

第一，这一迷人的数学领域产生了许多富于刺激性的难题，丰富而辉煌，堪称数学家的金矿。正如希尔伯特所说：“只要一个科学分支能提出大量的问题，它就充满着生命力，而问题缺乏则预示着它将会独立发展，或衰亡或中止。”**数论就是一个包含着大量尚未解决的问题的数学领域，这就向一代一代的数学家提出了挑战。**高斯曾把数论描绘成“一座仓库，贮藏着用之不尽的，能引起人们兴趣的真理”注【13】。

第二，它的一个真正诱惑是：有时所研究的一些问题简单得甚至连小学生都能看懂；然而，却使**一代又一代世界一流数学家为它的证明付出了巨大并艰苦的努力。**如著名的费马大定理就曾困惑了世间智者 360 余年，到 1995 年才最终获得解决。而诸多的这类至今尚未解决的问题在数论中比比皆是，如哥德巴赫猜想、奇完全数存在性、**孪生质数对**问题等。问题表述的简单与解答的极端复杂，作为这一数学分支看似反常的特点吸引着无数的数学专家与业余爱好者为之奋斗注【13】。

第三，人们为了解决这些问题使用了很多极其复杂的手段。在现今的数论进展中，代数、实与复分析、几何，甚至概率论的方法，都做出了至关重要的贡献。这些不同数学方法的深刻的相互影响，使人们清楚地看到了一个惊人的事实，从而也让我们几乎不可避免地会产生一种玄秘的感觉。有些结论的陈述，仅仅牵涉到一些关于自然数的最简单的概念，如**质数，**然而要证明这些结论，却非得用到分析、代数几何之类的复杂工具不可，尽管光看假设条件或结论是怎么也想不到会要这样的大动干戈。哥德巴赫猜想就是一个极好的例证。国内著名的数论专

家曾形容那些试图仅用初等数学或简单的微积分知识就能解决这一猜想的努力是“蹬着自行车上月球”，好比是“拿着锯和刨子造一架航天飞机”，因为他们的工具太原始了，于是再多的努力都是白费。而要解决这一猜想，需要全新的观念与更先进的工具才行。话说回来，人们的确很难解释，人的认知机制为什么非要这么七弯八转兜上一个或数个大圈子，才能在一个假设条件和另一个看上去跟它那么相近的结论之间建立起联系。不过，这种定理陈述的简单性，所用方法的深奥性，却以极其明显的形式体现了数学内部深刻的和谐一致性，从而使数论深深地吸引了世世代代的数学家。希尔伯特把数论看成是“一幢出奇地美丽而又和谐的大厦”，“它有简单的基本定律，它有直截了当的概念，它有纯正的真理”注【13】。

第四，数论的研究课题并不马上招致对科学的应用，然而一部分数学家却因为它脱离实用的“纯正洁白”而着迷。如同1896年鲍尔所说：“这门学科本身是一个特别吸引人、特别雅致的学科，但它的结论没什么实际意义。”确实，如果按通常分法把数学分为“纯粹”数学与“应用”数学的话，数论或许是数学中所能达到的最纯粹的了。费马、欧拉、拉格朗日、勒让德、高斯等都是出自数论“**内在的趣味**”及其“**特有的美**”、“**纯正的洁白**”及其“**特别的雅致与纯粹**”而研究人类知识的这一领域的，他们确实毫不在乎那些优美的定理是否会有什么“有用的”应用。高斯认为“皇后”不愿弄脏她那洁白的双手，而英国数论专家哈代曾为自己所研究的数论问题无用而干杯。尽管数论居于数学中最美妙的思想之列，但在哈代以前却从未被用于任何非常实际的目的。不过，这一现象现在已被改变。如大质数分解问题已与密码破译紧密联系在一起了注【13】。

正是以上这些极为独特的风格带来的迷人魅力终使数论能高居“数学皇后”的宝座之上，并引无数门外汉们与极富才智者一起为之如醉如痴并流连忘返吧注【13】。

4. 数论就是一门研究整数性质的学科

数论这门学科最初是从研究整数开始的，所以原称为整数论。后来整数论又进一步发展，就改称数论了。确切的说，**数论就是一门研究整数性质的学科。**在国外，古希腊时代的数学家对于数论中一个最基本的问题——整除性问题就有系统的研究，关于质数、合数、约数、倍数等一系列概念也已经被提出来并应用了。后来各个时代的数学家也都对整数性质的研究做出过重大的贡献，使数论的基本理论逐步得到完善注【5】。

5. 质数是构成正整数的基本“材料”

在整数性质的研究中，人们发现**质数是构成正整数的基本“材料”**，要深入研究整数的性质，就必须首先从研究**质数的性质**开始。因此关于质数性质的有关问题，一直受到数学家和数学界的关注。如人们对数的素性检验方法及质数表达通式的研究探索，在近几年得到了飞速的发展注【5】。

第三节　质数判别的探研进展状况

一、传统的质数判别方法

传统的质数判别方法（即数的素性检验方法）有查表法、试除法和筛法等。

1. 查表法

判断一个大于 1 的自然数是不是质数，可以查找事先制备好的相应范围的质数表，如果

表内有这个数，它就是质数；如果没有，它就是合数注[1]。

1000 以内的质数表是希腊学者**埃拉托斯特尼**（Eratosthenes）利用筛法首先创造的注[1]。1000 以内的质数共 168 个，见表 1-1-1。

表 1-1-1：1000 以内的质数表

按位数分类	质数	数量
一位数的	2 3 5 7	**4 个**
二位数的	11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97	**21 个**
三位数的	101 103 107 109 113 127 131 137 139 149 151 157 163 167 173 179 181 191 193 197 199 211 223 227 229 233 239 241 251 257 263 269 271 277 281 283 293 307 311 313 317 331 337 347 349 353 359 367 373 379 383 389 397 401 409 419 421 431 433 439 443 449 457 461 463 467 479 487 491 499 503 509 521 523 541 547 557 563 569 571 577 587 593 599 601 607 613 617 619 631 641 643 647 653 659 661 673 677 683 691 701 709 719 727 733 739 743 751 757 761 769 773 787 797 809 811 821 823 827 829 839 853 857 859 863 877 881 883 887 907 911 919 929 937 941 947 953 967 971 977 983 991 997	**143 个**
合计		**168 个**

100000 以内的质数表详见附表 1-1，对 100000 以内质数的情况统计分析详见附表 1-2 及附表 1-3，仅供参考。

2. 试除法

如果没有质数表，或有质数表但欲要判断的自然数超过质数表的范围，可以用试除法进行判断注[1]，这也是过去人们检验一个自然数 n 是否是质数，常用的且最简单的检测方法，能根据数的整除特征直接判断的就不必试除。

试除法，即将该数 n 用小于等于 $n^{1/2}$ 的所有质数去挨个试除，若均不能整除，则 n 为质数。

例如，判断 197 是不是质数，可以用小于 $197^{1/2}$ 的质数 2、3、5、7、11、13、17 去试除，而不必用大于 17 的质数去试除，197 不能被 2、3、5、7、11、13、17 整除，这时就可以断定 197 是质数。

试除法对于比较小的数来说还较适用，但对于比较大的数来说，操作较为困难，因为首先要事先列出小于 $n^{1/2}$ 的所有质数。

3. 筛法

为了列出 1000 以内的质数表，早在公元前三世纪，希腊学者**埃拉托斯特尼**找到了一种寻求质数的方法：即依次写出 2 到 1000 的自然数，第一个数是 2，2 是质数，把它留下，然后把所有 2 的倍数的数划去；2 后面第一个未划去的数是 3，3 是质数，把它留下，再把剩下的数中所有 3 的倍数的数都划去；3 后面第一个未划去的数是 5，5 是质数，把它留下，再把剩下的数中所有 5 的倍数的数都划去……这样继续下去，完成将质数 2、3、5、7、11、13、17、19、23、29、31 的倍数的数划去，划到 37 以前的一个质数 31 为止（因为 31*31=961，即最后划去一个合数是 961，而 29*37=1073>999，31*37=1147>999，37*27=999，3*333=999，999 是被 3 的 333 倍给划去了，而不是被 37 的 27 倍给划去的，所以 37～999 之间的质数也被留下了），就把 1000 以内的合数全给划尽了，最后留下的数就组成了 1000 以内的质数表。

因为希腊人是把数字写在涂了蜡的板上，每要划去一个数，就在涂蜡板上面记一小点，

寻求质数的工作完毕后，这许多的小点就像一个筛子，所以就把**埃拉托斯特尼**寻求质数的方法称为“**埃拉托斯特尼筛**”，简称“筛法”。另一种解释是当时的数字是写在纸草上，每要划去一个数，就把这个数从纸草上挖去，成了一个小洞，寻求质数的工作完毕后，纸草上这许多的小洞就像一个筛子注【1】。

二、质数探研的进展状况

由于质数是构成正整数的基本“材料”，要深入研究整数的性质就必须首先从研究**质数的性质**开始。因此关于质数性质的有关问题一直受到数学家的关注注【5】。

人们对数的素性检验方法及质数表达通式的研究探索，在近几年得到了飞速的发展。但是至今**还没有找到一个数的素性检验方法的通用公式**注【9】**及关于质数表达的通用公式**注【12】。

（一）数的素性检验方法研究进展状况

1. 用计算机编程对数的素性进行检验

过去，要检验一个数 n 是否为质数，最简单的方法是用试除法，用小于 n 的平方根以下的所有质数去除 n，若都除不尽，则 n 就是质数，否则为合数，对于比较小的数这种方法还适用，若用计算机编程对自然数的素性进行检验，对于一个 10 位数，几乎瞬间即可完成，对于一个 20 位数，则需要 2 个小时，对于一个 50 位数就需要一百亿年，令人吃惊的是，要检验一个 100 位数，需要的时间就猛增到 10^{36} 年注【8】。

随着计算机科研进一步大型化及编程的飞速发展，对数的素性检验的时间也大大缩短了。

2. AKS 质数测试算法

2002 年，印度人 M.Agrawal、N.Kayal 及 N.Saxena 提出了AKS 质数测试算法，证明了可以在**多项式时间内**检验一个数是否为质数注【7】。

（1）AKS 质数测试重要性。

AKS 最关键的重要性在于它是：第一个**被发表的一般的**（①）、**多项式的**（②）、**确定性的**（③）、**无仰赖的**（④）质数判定算法。先前的算法至多达到了其中三点，但从未达到全部四点注【11】。

AKS 算法可以被用于检测任何一个**一般的**给定数字是否为质数。很多已知的高速判定算法**仅对**满足特定条件的算法适用。例如，用于梅森质数的**卢卡斯-莱默检验法**仅对**梅森质数**适用，而**Pépin 测试**仅对**费马质数**适用注【14】。

AKS 算法的最长运行时间可以被标识为一个关于目标数字长度的**多项式**。**ECPP**和**APR**能判断一个给定数字是否为质数，但无法对所用输入给出多项式时间范围注【14】。

AKS 算法可以**确定性**地判断一个给定数字是质数或是合数，随机测试演算法，例如米勒-拉宾检验和Baillie-PSW，可以在多项式时间内对给定数字进行校验，但只能给出概率性的结果注【14】。

AKS 算法的正确性是**不仰赖于**任何辅助性未证明的猜想。一个反例是米勒-拉宾检验：该算法可以在多项式时间内对所有输入给出确定性结果，但其正确性却基于**尚未被证明**的**广义黎曼猜想**注【14】。

（2）AKS 质数测试概念。

AKS 质数测试主要是基于以下定理：整数 n（≥2）是质数，当且仅当：

$$(x-a)^n \equiv (x^n-a) \pmod{n} \qquad (1)$$

这个同余多项式对所有与 n互质的整数 a 均成立。这个定理是**费马小定理**的**一般化**，并且可以简单地使用**二项式定理**跟**二项式系数**的特征：

$$\binom{n}{k} \equiv 0 \pmod{n}$$

对任何 $0<k<n$，当且仅当 n 是质数来证明出此定理。

虽然说关系式（1）**基本上构成了整个质数测试，但是验证花费的时间却是对数时间。因此，为了减少计算复杂度，**AKS 改为使用以下的同余多项式：

$$(x-a)^n \equiv (x^n-a) \pmod{n, x^r-1} \quad (2)$$

这个多项式与存在多项式 f 与 g，令：

$$(x-a)^n-(x^n-a) = nf + (x^r-1)g \quad (3)$$

意义是等同的。

这个同余式可以在**多项式时间之内**检查完毕。这里我们要注意**所有的质数必定满足此条件式**（令 g=0 则（3）等于（1），因此符合 n 必定是质数）。**然而，有一些合数也会满足这个条件式。**有关 AKS 正确性的证明包含了推导出存在一个够小的 r 以及一个够小的整数集合 A，令：如果此同余式对所有 A 中的整数都满足，则 n 必定为质数注【14】。

3. *应用费马小定理对数的素性进行检验与质数快速检验法*

我们知道，**费马小定理是现代质数判定方法的基础，**如果该定理的逆命题成立那该多好，只要计算一下 a^p-a 是否能被 p 整除，如能整除，则 p 是质数，否则 p 是合数。遗憾的是这只对 $1<p<341$ 内的数成立，因为 $2^{341}-2$ 能被合数 341 整除，即费马小定理的逆命题不成立。像 341 这样的数称为伪质数，$341=11*31$ 注【9】。

1980 年末，两位欧洲数学家创造了一种检验质数的方法，使得过去需要比宇宙年龄还长的运算时间缩短到一个小时就可以完成，这便是所谓**“质数快速检验法”**。说到这儿，还要从下面的事实谈起注【10】。

1640 年，法国数学家**费尔马**不加证明地提出了下面的定理：若 p 是质数，又 $1<a<(p+1)$，则 $p|(a^p-a)$，这里的“|”表示整除注【10】。

问题反过来又是如何呢？据说早在 **2500 多年以前（即中国的孔子时代）**，我国对此事实就有研究，当时对于 **$p|(2^p-2)$**的情形进行讨论，在验证了某些 p 能整除 2^p-2，得到 p 是质数后断定：若 $p|(2^p-2)$则 p 是质数。然而这个结论并不成立，比如 341=11×31（即 341 是合数），但：

$$2^{341}-2=2(2^{340}-1)=2[(2^{10}-1)(2^{34}+2^{33}+\cdots+1)]$$

注意到 $2^{10}-1=1023$，而 $341|1023$，从而 $341|(2^{341}-2)$，而 341 不是质数。可是，后来人们发现：这种现象并不是很多，即若 $p|(a^p-a)$，则 p 大多为质数，只有极少数情形 p 不是质数，这样的 p 称为假质数（伪质数）。可以证明：假质数有无穷多个（若 n 是奇假质数，则 2^n-1 是一个更大的**奇假质数**。第一个发现**偶假质数**的人是**莱赫麦尔**，他在 1950 年发现 161038 是**偶假质数**，1951 年贝格证明有无穷多个偶假质数），但是**假质数比起真质数来少得可怜，在 10^{10} 以内的数中，假质数只有 14884 个，而真质数却有 455052512 个。**这样人们可以从 n 能否整除 2^n-2 去检验一个数是否为质数。虽然求 2 的**高次幂运算**也不简单，**但由于人们只关心 n 去除 2^n-2 所得的余数，**因而存在着数学方面的捷径，**所需要的只是剔除为数极少的假质数的办法，**这一方法有人已经给出（即剔除为数极少的假质数的办法有人已经给出）注【10】。

本人认为：**虽然假质数比起真质数来少得可怜**（如在 10^{10} 以内的数中，假质数只有 14884 个注【10】），**但是，由于假质数的存在，影响了费马小定理的关于质数检验的唯一性。**