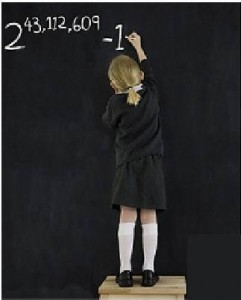
**[梅森素数 - 千年不休的探寻之旅](http://songshuhui.net/archives/12950.html" \t "_blank)**

from [科学松鼠会](http://www.google.com/reader/view/feed/http%3A%2F%2Fsongshuhui.net%2F%3Ffeed%3Drss2) by luscky

Shared by [苏鹏俊](http://www.google.com/reader/view/user/02100361832756711639/state/com.google/broadcast" \t "_blank)

**还记得年少时的梦吗？**

还记得你小学时背诵的素数表吗？那时候它还叫做质数表“2、3、5、7……”如今你是否已经真正理解了老师说过的话：这些只能被1和本身整除的数，具有着无穷的魅力。

还记得你中学时计算的2的整数幂吗？计算机时代，作为二进制的体现，它们正大行其道。“2、4、8、16、32、64、128、256……”十多年来，电脑内存的容量正是经历了这些熟悉的数字，直到现在的2048M（2G）以及更多。

现在，让我们从这些2的整数幂中挑出以素数为指数的，再把它减1，试试看会发现什么？22－1＝3、23－1＝7、25－1＝31、27－1＝127……

嗯，你的心是不是激动起来了？一个伟大的发现似乎就在眼前……

别急别急，你的发现很妙，只是有些儿惋惜……你已经迟到了二千年。

在2300多年前，古希腊的数学家，那位写出不朽的《几何原本》的欧几里得在证明了素数有无穷多个之后，就顺便指出：有许多素数可以写成2P－1的形式，其中指数P也是素数。很容易想到，刚才你所发现的22－1、23－1、25－1、27－1正是其中排列最前的4个！

当P＝11、13、17、19、23……的时候，2P－1还是素数吗？到底有多少这种2P－1型的素数呢？在计算能力低下的公元前，这个关于素数的探寻之旅就已经吸引了无数的人。

人们唯独对素数如此着迷不是没有理由的，它有着许多简单而又美丽的猜想，有的已经成为定理，而有的则至今还没有答案。例如著名的哥德巴赫猜想，让人 们苦苦追索：是否任何一个大于或等于6的偶数，都可以表示为两个奇素数的和？再比如孪生素数问题所提出的：象5和7、41和43这样相差2的素数，到底有 多少对呢？

在数学史上起个大早的古希腊人还有许多关于素数的发现，完美数就是其中之一。毕达哥拉斯学派指出，如果一个数的所有因数（包括1但不包括它本身）的 和正好等于它本身，则这个数就叫做完美数。很容易找到，6＝1＋2＋3是第一个完美数，28＝1＋2＋4＋7＋14则是第二个完美数。他们认为，上帝用6 天创造了世界，因此6是最理想和完美的数字，而和6具有相同性质的数都堪称完美数。

欧几里得在《几何原本》中证明了如果2P－1是一个素数，那么2P－1（2P－1）一定是一个完美数（你会发现，当P分别等于2、3时，它就对应着前两个完美数6、28）。

再后来，欧拉进一步证明，每一个偶完美数也必定是欧几里得所给出的形式。（不要问我奇完美数呢？就连它是否存在，本身也是无数个关于素数的难题中至今未解的一个。）

很容易看到，找到了2P－1形式的素数，也就发现了新的完美数。

形如2P－1的素数还长期占据了人们寻找到的最大素数的光荣榜（仅在1989年后被39158×2216193－1夺走三年），因为判断这样一个数是素数的方法比判断一个差不多大小的其他类型数是素数的方法要简单得多。

对2P－1型素数的搜寻之旅就这样出发了，先后投入这个漫漫长途的就有数学大师费马、笛卡尔、莱布尼兹、哥德巴赫、欧拉、高斯、哈代、图灵……这一个个闪光的名字正如暗夜前行的火炬手，照亮了人类通往未知的道路。

**历史的天空闪烁几颗星**

让我们将坐上时间机器，回到过去，重新浏览这来路风光吧。

1456年，又一个没有留下姓名的人发现了第5个2P－1型的素数：213－1。若是你就降生在那个年代，或许这次发现的光荣将归属于你。只是，你更有可能犯下和当时的人们一样的错误，以为对于所有的素数P，2P－1都是素数。要知道，这个错误是近百年之后，直到1536年，才由雷吉乌斯(Hudalricus Regius)打破的。他指出，211-1＝2047＝23×89，不是素数。

不过你的莽撞完全可以得到谅解，在黑暗中寻找的数学家正如年轻人一样，犯下的错误连上帝都会原谅。第一个对这种类型的素数进行整理的皮特罗•卡塔尔 迪(Pietro Cataldi)在他在1603年宣布的结果中就言之凿凿地说：对于p=17，19，23，29，31和37，2P－1是素数。只可惜，37年后，他的六个结果就被推翻了两个，费尔马使用著名的小费尔马（不是那个更著名的大费尔马定理）证明了卡塔尔迪关于P＝23和37的结论是错误的。

不知道下面的事实会不会让你联想到“屋漏偏逢连夜雨”呢？大约一百年后，1738年，欧拉证明了卡塔尔迪的结果中P＝29也是错误的。幸好，欧拉又证明了P＝31的结论是对的。

虽然，卡塔尔迪的六个结果“阵亡”了一半，但考虑到他是用手工计算取得结论的，而费尔马和欧拉则是使用了在他们那时最先进的数学知识，避免了许多复 杂的计算和因此可能造成的错误，因此我们仍然要对卡塔尔迪致敬。他也由此光荣地占据了第六个和第七个的发现者之位，在他之前的，都是无名氏。



卡塔尔迪的成功，说明了整理和预测是正确道路。继他之后，集研究成果大成的，是17世纪法国著名的数学家和修道士马林•梅森（Marin Mersenne,1588-1648）。

梅森热心于宗教，但更喜爱数学；他是一个交往广泛、热情诚挚的人，更是一座“科学信息交换站”。为什么呢？那时候，学术刊物、国际会议甚至科研机构 都还没有诞生。“及时雨”般的梅森是欧洲众多科学家之间联系的桥梁，大家把研究成果寄给他，然后再由他转告给更多的人。费马、笛卡尔等数学家每周在他家聚 会，讨论问题，就这样慢慢形成的”梅森学院”，后来有了一个更响亮的名字——法兰西科学院。

1644年，梅森在欧几里得、费马等人的有关研究的基础上对2P－1作了大量的计算、验证工作，并于1644年在他的《物理数学随感》一书中断言：对于P＝2、3、5、7、13、17、19、31、67、127、257时，2P－1是素数；而对于P等于其他所有小于257的数时，2P－1是合数。这里前7个数（即2，3，5，7，13，17和19）是在前人的工作已经证实的部分。而后面的4个数（即31，67，127和257）属于被猜测的部分。不过，人们对他的断言深信不疑，连大数学家莱布尼兹和哥德巴赫都认为它是对的。

梅森的工作极大地激发了人们研究2P－1型素数的热情，成为素数研究的一个转折点和里程碑。为了纪念他，数学界就把这种数称为“梅森数”，并以Mp记之（其中M为梅森姓名的首字母），即Mp=2P－1。如果梅森数为素数，则称之为“梅森素数”（即2P－1型素数）。

对梅森素数的验证，需要进行艰巨的计算，即使是”猜测”部分中最小的M31=231－1=2147483647，也是一个 10位数。而梅森自己则承认：“一个人，使用一般的验证方法，要检验一个15位或20位的数字是否为素数，即使终生的时间也是不够的。”年迈力衰的他四年 之后就去世了，最终并没有任何一个梅森素数的发现权归属于他，但考虑到他已经享有了“冠名权”，就把荣誉分给那些在漫漫长途上跋涉的发现者们吧！

**那些手扛肩挑的年代**

手算笔录的时代，每前进一步，都显得格外艰难。1772年，在卡塔尔迪提出近200年之后，瑞士数学家欧拉证明了M31确实是一个素数，这是人们找 到的第8个梅森素数，它共有10位数，堪称当时世界上已知的最大素数，欧拉也因此成为第二个在发现者名单上留名的人。让人惊叹的是，这是在他双目失明的情 况下，靠心算完成的。这种超人般的毅力与技巧让欧拉获得了“数学英雄”的美誉。法国大数学家拉普拉斯（P.Laplace）说的话，或许可以代表我们的心 声：“读读欧拉，他是我们每一个人的老师。”

100年后，法国数学家鲁卡斯提出了一个用来判别Mp是否是素数的重要定理——鲁卡斯定理，这为梅森素数的研究提供了有力的工具。1883年，数学 家波佛辛（Pervushin）利用鲁卡斯定理证明了M61也是素数–这是梅森漏掉了的。梅森还漏掉另外两个素数：M89和M107，它们分别在1911 年与1914年被数学家鲍尔斯（Powers）发现。

还记得梅森预测的四个素数吗？其中M31已经为欧拉证明，M127则在鲁卡斯提出定理时顺带证明，虽然中间漏掉了3个，但至少还有另外两个：M67和M257是不是素数呢……

M67的证明又是一个精彩的故事。

1903年，数学家柯尔在美国数学学会的大会上作了一个报告。他先是专注地在黑板上算出267－1，接着又算出193707721×761838257287，两个算式结果完全相同！换句话说，他成功地把267－1分解为两个素数相乘的形式，从而证明了M67是个合数。

报告中，他一言未发，却赢得了现场听众的起立鼓掌，更成了数学史上的佳话。阅读这段历史，我们懂得了什么叫做“事实胜于雄辩”。记者好奇地问他是怎 样得到这么精彩的发现的，柯尔回答“三年里的全部星期天”。他后来当选为美国数学协会的会长，去世后，该协会专门设立了“柯尔奖”，用于奖励作出杰出贡献 的数学家。

1922年，数学家克莱契克验证了M257并不是素数，而是合数（但他没有给出这一合数的因子，直到20世纪80年代人们才知道它有3个素因子）。

于是乎，梅森的四个猜测获得了两正确、三遗漏和两错误的成绩，但这无损于他的光荣。在千年的探寻之旅中，伟大如欧拉也会犯错误，他在1750年宣布说找到了梅森的“遗漏”：M41和M47也是素数，但最终上M41和M47都不是素数。

直到1947年，对于p<=257的梅森素数Mp的正确结果才被确定，也就是当p=2，3，5，7，13，17，19，31，61，89，107和127时，Mp是素数。现在这个表已经被反复验证，一定不会有错误了。

我们看到，在手工计算的时代，人们一共找到了12个梅森素数。

**计算机！计算机！**

1930年，美国数学家雷默改进了鲁卡斯的工作，给出了一个新的测试方法，即鲁卡斯－雷默方法。很快地，计算机时代到来了，这一方法发挥了重要的作 用。1952年，数学家鲁滨逊（Robinson）等人将鲁卡斯－雷默方法编译成计算机程序，使用SWAC型计算机在短短几小时之内，就发现了第13个、 第14个，并在当年总共找到了5个梅森素数：M521、M607、M1279、M2203和M2281。

其后，M3217在1957年被黎塞尔（Riesel）证明是素数；M4253和M4423在1961年被赫维兹（Hurwitz）证明是素数。

1963年，美国数学家吉里斯（Gillies）证明M9689和M9941是素数，这已经是第21和22个梅森素数。1963年9月6日晚上8 点，当吉里斯通过大型计算机找到第23个梅森素数M11213时，美国广播公司（ABC）中断了正常的节目播放，第一时间发布了这一重要消息，发现这一素 数的美国伊利诺伊大学数学系全体师生更是激动地把所有从系里发出的信件都敲上了“211213－1是个素数”的邮戳。



1971年3月4日晚，美国哥伦比亚广播公司（CBS）中断了正常节目播放，发布了布萊恩特•塔克曼（Bryant Tuckerman）使用IBM360-91型计算机找到新的梅森素数M19937的消息。而到1978年10月，世界几乎所有的大新闻机构（包括我国的 新华社）都报道了以下消息：两名年仅18岁的美国高中生诺尔（Noll）和尼科尔（ Nickel）使用CYBER174型计算机找到了第25个梅森素数：M21701。

超级计算机的引入加快了梅森素数的寻找脚步，但随着素数P值的增大，每一个梅森素数的产生都更加艰难，各国科学家及业余研究者们之间的竞争变得越来 越激烈。在1979年2月23日，当美国克雷研究公司的计算机专家史洛温斯基和纳尔逊正兴致冲冲地宣布他们找到第26个梅森数M23209时，有人浇来一 盆冷水：两星期前美国加州的高中生诺尔就已经给出了同样结果。心有不甘的他们又花了一个半月的时间“卧薪尝胆”，使用Cray－1型计算机找到了第27个 梅森素数M44497，这件事成了当时不少报纸的头版新闻。

为了与美国人较量，英国的哈威尔实验室也专门成立了一个研究小组来寻找更大的梅森素数。他们用了两年时间，花了12万英镑的经费，于1992年3月 25日找到了新的梅森素数M756839。但到了1994年1月14日，史洛温斯基等人为美国再次夺回发现“已知最大素数”的桂冠——这一梅森素数是 M859433。史洛温斯基本人一共发现了7个梅森素数，他因此被人们称为“素数大王”。

数学研究的深入更重于计算能力的提升，在搜寻梅森素数的同时，对梅森素数的分布规律的研究也在进行着，英、法、印、美、德等国的数学家都曾分别给出 过关于梅森素数分布规律的猜测，但这些猜测都以近似表达式给出，而与实际情况的接近程度均难如人意。中国数学家和语言学家周海中则是这方面研究的领先者， 他运用联系观察法和不完全归纳法，于1992年首先给出了梅森素数分布的精确表达式。著名的《科学美国人》杂志有一篇文章指出：这一成果为人们探究梅森素 数提供了方便，是素数研究的一项重大突破。后来这项重要成果被国际上命名为“周氏猜测”。  
伴随数学理论的改善，为了寻找梅森素数而使用的计算机也越来越强大，包括了著名的IBM360型计算机，和超级计算机Cray系列。1996年发现的 M1257787是迄今为止最后一个由超级计算机发现的梅森素数，数学家使用了Cray T94，这也是人类发现的第34个梅森素数。

梅森素数的探寻之旅似乎正变得离普通人越来越远，直到GIMPS时代的到来……

**草根英雄，人人参与**

网格(Grid)这一崭新技术的出现使梅森素数的搜寻如虎添翼，也使它重新走到了“人人参与”的大众时代。1996年初，美国数学家和程序设计师沃 特曼(G.Woltman)编制了一个梅森素数的计算程序，并把它放在网页上供数学家和数学爱好者免费使用，这就是闻名世界的“因特网梅森素数大搜寻 ”（GIMPS）项目，是全世界第一个基于互联网的分布式计算项目。

该项目利用大量普通计算机的闲置时间来获得相当于超级计算机的运算能力，只要你去GIMPS的主页下载为一个名为Prime95的免费程序，就可以立即参加GIMPS项目，一起踏上持续了千年的梅森素数探寻之旅。

12年来，人们通过GIMPS项目找到了12个梅森素数，其发现者来自美国、英国、法国、德国和加拿大。目前，世界上有160多个国家和地区近16 万人参加了这一项目，并动用了30多万台计算机联网来进行网格计算。该项目的计算能力已超过当今世界上任何一台最先进的超级矢量计算机的计算能力，运算速 度超过每秒350万亿次！

为了激励人们寻找梅森素数，1999年3月，设在美国的电子新领域基金会（EFF）向全世界宣布了为通过GIMPS项目来探寻梅森素数而设立的奖 金。它规定向第一个找到超过一百万位的素数的个人或机构颁发五万美元的奖金。后面的奖金依次为：超过一千万位，十万美元；超过一亿位，十五万美元；超过十 亿位，二十五万美元。

1999年6月1日，住在美国密歇根州普利茅茨的那扬•哈吉拉特瓦拉（Nayan Hajratwala）先生找到了第38个梅森素数：26972593－1， 这也是我们知道的第一个位数超过一百万位的素数。如果把它写下来的话，共有两百零九万八千九百六十位数字。因此，哈吉拉特瓦拉先生获得了五万美元的奖励。 而他所做的，就是从互联网上下载了一个程序，这个程序在他不使用他的奔腾II350型计算机时悄悄地运行。在经过111天的计算后，这个素数被发现了。

听起来非常诱人，但你也要知道，通过参加GIMPS计划来获得奖金的希望是相当小的。哈吉拉特瓦拉使用的计算机是当时21000台计算机中的一台。 每一个参与者都在验证分配给他的不同梅森数，当然其中绝大多数都不是素数——只有大约三万分之一的可能性碰到一个素数。所以，绝大多数研究者参与该项目并 不是为了金钱，而是出于乐趣、荣誉感和探索精神。

成功者就在眼前，去年8月23日，美国加州大学洛杉矶分校数学系计算中心的雇员史密斯，通过GIMPS项目发现了第46个梅森素数243112609－1， 这个发现被著名的美国《时代》周刊评为“2008年度50项最佳发明”之一。该素数是目前已知的最大素数，它有12978189位数，如果用普通字号将这 个巨数连续写下来，其长度可超过50公里！由于史密斯发现的梅森素数已超过1000万位，他将有资格获得EFF颁发的10万美元大奖。虽然说史密斯是私自 利用中心内的75台计算机参加GIMPS的，但由于为学校争了光，他受到了校方的表彰。

但在你心动之前，不妨也听听另一个人的故事。美国一家电话公司发现计算机经常出错，本来只需要5秒钟就可以接通的电话号码，需要5分钟才能接通。最 终查出原来是雇员福雷斯特偷偷地使用公司内的2585台计算机参加GIMPS，福雷斯特承认了自己“被GIMPS项目引诱”，他最后被公司解雇，并被罚款 一万美元，这只能说是工作与私事没有分开，令人叹息。

**最后的话**

素数的研究曾经在人类很长的历史时期没有实际用处，直到二次世界大战之后，才在密码学中得到了重要的应用。对于梅森素数的寻找之旅已经历经千年，人 们一共才找到46个梅森素数，在数学家的眼里，它们的价值远胜于钻石，而对它的研究，促进了计算技术、程序设计技术、密码技术、分布式计算技术的发展。让 我们谨记梅森素数最早的研究者欧几里得的教诲：当一个人问他”几何学有什么用”的时候，他对侍者说：“给他拿三个硬币吧，他想从几何学中得到好处。”

不是三枚硬币，也不是百万美元，激励着人类不断地向前探寻的，是好奇心、求知欲和荣誉感。

**（已刊载于《中国教师报》）**