

梅森素数的一些注记

石永进¹, 成启明²

1. 中国地质大学资源学院, 武汉 430074
2. 新加坡国立大学理学院, 新加坡 119077, 新加坡

摘要 梅森素数历来是数论研究的重要内容,也是当今科学探索的热点和难点之一;而卢卡斯-雷默测试是迄今为止判断梅森数素性最快最有效的工具;周氏猜测是关于梅森素数分布的著名难题。本文首先介绍与梅森素数研究有关的3个重要问题;然后通过对卢卡斯-雷默测试递归数列的研究,揭示了其衍生数列的一个特殊性质,提出相关的猜想;得出卢卡斯-雷默测试的一个关联等式,由该等式与周氏猜测的密切关系,提出相关的猜想;提出了广义卢卡斯-雷默测试的存在性问题,并提出了相关的猜想。结果表明,采用不同的方法对解决梅森素数的有关问题会有所启发和帮助。

关键词 梅森素数;卢卡斯-雷默测试;周氏猜测;牛顿迭代法

中图分类号 O156

文献标识码 A

文章编号 1000-7857(2010)06-0025-04

Some Notes on Mersenne Primes

SHI Yongjin¹, CHENG Qiming²

1. Faculty of Resources, China University of Geosciences, Wuhan 430074, China
2. Faculty of Science, National University of Singapore, Singapore 119077, Singapore

Abstract A Mersenne prime is a Mersenne number that is a prime. It is known that if 2^p-1 is a prime, p will also be a prime, therefore, it makes no difference which definition of Mersenne number is used. The Mersenne prime has long fascinated both amateur and professional mathematicians. It is always an important topic in the number theory and also one of today's hot and difficult scientific problems. Mersenne primes, as usually the largest known primes, are both rare and beautiful. As of January 2010, only 47 Mersenne primes are known. Lucas-Lehmer test is the fastest and most effective tool for determining the primality of Mersenne numbers. Zhou conjecture is the well-known problem of the distribution of Mersenne primes. This paper first discusses three important problems related with Mersenne primes. Then from the recursive sequence of Lucas-Lehmer test, a special nature of the derivative series is shown, a related guess is made; a correlation equation of Lucas-Lehmer test is obtained, the relevant guess is made from the type of the close relationship between the speculation and Zhou conjecture; and the problem of existence of the generalized Lucas-Lehmer test is formulated, together with a related guess. The results show a good prospect in the studies of Mersenne primes.

Keywords Mersenne primes; Lucas-Lehmer test; Zhou conjecture; Newton iteration

0 引言

2009年4月,挪威计算机专家 O. Strindmo 通过参加一个名为“因特网梅森素数大搜索(GIMPS)”的国际合作项目,发现了第47个梅森素数 $2^{42643801}-1$,它有12837064位数,如果用5号字将这个巨数连续写下来,其长度超过50km。专家认为这一重大发现是数论研究和计算技术中最重要的成果之一。

目前,世界上有170多个国家和地区超过18万人参加了GIMPS项目,并动用近40万台计算机联网来进行大规模的网格计算,以探寻新的梅森素数。

公元前300多年,古希腊数学家欧几里德用反证法证明了素数有无穷多个,并提出了少量素数可写成 2^p-1 (指数 p 为素数)的形式。此后许多数学家,包括费马、笛卡尔、莱布尼

收稿日期: 2010-01-07

作者简介: 石永进,研究方向为数论,电子信箱: shi_yongjin@163.com;成启明(通信作者),教授,研究方向为数论与网格技术,电子信箱: qm_cheng@hotmail.com

兹、哥德巴赫、欧拉、高斯、图灵等都研究过这种特殊形式的素数,而 17 世纪的法国数学家梅森(M. Mersenne)是其中成果最为卓著的一位。由于梅森学识渊博、贡献良多,并是法兰西科学院的奠基人和当时欧洲科学界的中心人物,为了纪念他,数学界将 2^p-1 型的数称为“梅森数”,并以 M_p 记之;如果 M_p 为素数,则称之为“梅森素数”^[1]。2300 多年来,人类仅发现 47 个梅森素数,由于这种素数珍奇而迷人,因此被人们称为“数海明珠”。梅森素数是数论研究中的重要内容,也是当今科学探索的热点和难点之一^[2]。本文对梅森素数的 3 个相关问题进行探究。

1 与梅森素数研究有关的 3 个重要问题

1.1 卢卡斯-雷默测试

法国数学家卢卡斯(E. Lucas)在研究著名的斐波那契数列时,发现它与梅森素数的惊人联系,并于 1877 年提出了一个用以判别 M_p 是否为素数的重要定理——卢卡斯定理^[1]。这一定理为梅森素数的研究提供了强有力的工具。

1930 年,美国数学家雷默(D. Lehmer)改进了卢卡斯的工作,给出一个针对 M_p 的新素性测试方法,即卢卡斯-雷默测试^[1]:对于所有大于 1 的奇数 p , M_p 是素数,当且仅当 M_p 整除 S_{p-2} ,其中 S_k 由 $S_{k+1}=S_k^2-2, S_0=4$ 递归定义。例如,取 $p=5$,有数列 $S_k:4,14,194,37634$,因为 $M_5=31$ 整除 $S_3=37634$,所以 $M_5=31$ 是一个素数。此方法尤其适合于计算机运算,因为 $M_p=2^p-1$ 的运算在二进制下可以简单地用计算机特别擅长的移位和加法操作来实现。

1.2 周氏猜测

人们在寻找梅森素数的同时,也进行着梅森素数分布规律的研究。由于梅森素数在正整数中的分布是时疏时密极不规则的,加上人们尚未知梅森素数是否有无穷个,因此研究梅森素数的分布规律似乎比寻找新的梅森素数更为困难。英、法、德、美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,与实际情况的接近程度均难如人意。

中国数学家及语言学家周海中运用联系观察法和不完全归纳法,于 1992 年首次给出了梅森素数分布的精确表达式:当 $2^{2^n} < p < 2^{2^{n+1}}$ ($n=0,1,2,\dots$) 时,梅森数 M_p 中有 $2^{n+1}-1$ 个是素数^[3];并且给出推论:当 $p < 2^{2^{n+1}}$ ($n=0,1,2,\dots$) 时,梅森素数的个数为 $2^{n+2}-n-2$ 。这一形式优美简洁的表达式加深了人们对梅森素数重要性质的了解,为探寻新的梅森素数提供了方便^[4],被国际上命名为“周氏猜测”。有关专家认为,这一成果是梅森素数研究中的一重大突破^[5]。值得一提的是,周氏猜测至今尚未被解决,已成为著名的数学难题。

1.3 牛顿迭代法

牛顿迭代法^[6]是一种近似求解方程的方法,用函数 $f(x)$ 的泰勒级数的前几项来寻找方程 $f(x)=0$ 的根。该方法是求方程根的重要方法之一,其最大优点是在方程 $f(x)=0$ 的单根附近

具有平方收敛,也广泛用于计算机编程中。具体地,对于 $\sqrt{n}$ 的牛顿迭代, x_k 表示 $\sqrt{n}$ 第 k 次迭代的近似值(k 充分大),由 $x_{k+1}=\frac{1}{2}(x_k+\frac{n}{x_k}), x_0=1$ 递归定义; k 越大,所得 $\sqrt{n}$ 的近似值就越精确;当 $k \rightarrow +\infty$ 时, x_k 就趋向其真实值。

2 问题与讨论

2.1 卢卡斯-雷默测试衍生数列的一个性质

若以 $S_1=4$,由 $S_{k+1}=S_k^2-2$ 得^[7]

$$S_k=3(2S_1S_2 \cdots S_{k-2})^2+2 \quad (k=3,4,\dots)$$

以 $S_0=4$,则上式应调整为

$$S_k=3(2S_0S_1 \cdots S_{k-2})^2+2 \quad (k=2,3,\dots)$$

即

$$S_k=12(S_0S_1 \cdots S_{k-2})^2+2 \quad (k=2,3,\dots)$$

设 $S_i(i=0,1,2,\dots,k-2)$ 的任意大于 2 的约数为 d ,显然 $12(S_0S_1S_2 \cdots S_{k-2})^2$ 能被 d 整除,由于 2 不能被 d 整除,因此 S_k 不能被 d 整除,则 S_k 与 $S_i(i=0,1,2,\dots,k-2)$ 除 1 和 2 外没有其他的公约数,同理,由 $S_k=S_{k-1}^2-2$ 可证得 S_k 与 S_{k-1} 除 1 和 2 外没有其他的公约数。

由上可知, S_k 与 $S_i(i=0,1,2,\dots,k-1)$ 除 1 和 2 外没有其他的公约数,反过来也就是说, S_k 与 $S_i(i=k+1,k+2,\dots)$ 除 1 和 2 外没有其他的公约数,则卢卡斯-雷默测试递归数列 $S_0, S_1, S_2, \dots$ 任意两项除 1 和 2 外没有其他的公约数。又因为 $S_2/2=6(S_0S_1S_2 \cdots S_{k-2})^2+1(k=2,3,\dots)$,所以 $S_k/2(k=2,3,\dots)$ 为奇数, $S_1/2=7$ 为奇数, $S_0/2=2$ 与所有奇数互质,因此有如下结论: $S_0/2, S_1/2, S_2/2, \dots$ 两两互质。

由以上结论及卢卡斯-雷默测试递归数列的衍生数列 $S_0/2, S_1/2, S_2/2, \dots$ 前面若干项,本文猜想: $S_k/2(k=0,1,2,\dots)$ 没有平方因数。如果此猜想成立,就揭示了该衍生数列的特殊性质,对梅森素数的研究具有启发意义。

2.2 卢卡斯-雷默测试的一个关联等式与周氏猜测的关系

以 $x_0=1$,由牛顿迭代法的递归公式

$$x_{k+1}=\frac{1}{2}\left(x_k+\frac{n}{x_k}\right) \quad (k=0,1,2,\dots)$$

得到等式^[6]

$$x_k=\sqrt{n}\left[1+\frac{2}{\left(\frac{1+\sqrt{n}}{1-\sqrt{n}}\right)^{2^k}-1}\right] \\ =\frac{\left[\left(\frac{1+\sqrt{n}}{1-\sqrt{n}}\right)^{2^k}+(1-\sqrt{n})^{2^k}\right]/2}{\left[\left(\frac{1+\sqrt{n}}{1-\sqrt{n}}\right)^{2^k}-(1-\sqrt{n})^{2^k}\right]/2\sqrt{n}}$$

当 $n=3$ 时,有

$$x_k=\frac{\left[\left(\frac{1+\sqrt{3}}{1-\sqrt{3}}\right)^{2^k}+(1-\sqrt{3})^{2^k}\right]/2}{\left[\left(\frac{1+\sqrt{3}}{1-\sqrt{3}}\right)^{2^k}-(1-\sqrt{3})^{2^k}\right]/2\sqrt{3}} \quad (1)$$

若以 $x_1=1, S_1=4$,由 $x_{k+1}=\frac{1}{2}\left(x_k+\frac{3}{x_k}\right), S_{k+1}=S_k^2-2$ 得^[7]

$$x_k = \frac{(S_{k-1}/2) \cdot 2^{2^{k-2}}}{(S_1 S_2 \cdots S_{k-2}) \cdot 2^{2^{k-2}}} \quad (k=3, 4, \cdots) \quad (2)$$

以 $x_0=1, S_0=4$, 则式(2)调整为

$$x_k = \frac{(S_{k-1}/2) \cdot 2^{2^{k-1}}}{(S_0 S_1 S_2 \cdots S_{k-2}) \cdot 2^{2^{k-1}}} \quad (k=2, 3, \cdots) \quad (3)$$

观察式(1)和式(3), 本文猜想以下等式成立:

$$\left[(1+\sqrt{3})^{2^k} + (1-\sqrt{3})^{2^k} \right] / 2 = (S_{k-1}/2) \cdot 2^{2^{k-1}} \quad (k=2, 3, \cdots) \quad (4)$$

证明 当 $k=2$ 时, 式(4)显然成立。

假设当 $k=n$ 时, 式(4)成立, 即

$$\left[(1+\sqrt{3})^{2^n} + (1-\sqrt{3})^{2^n} \right] / 2 = (S_{n-1}/2) \cdot 2^{2^{n-1}}$$

又

$$x_n = \frac{\left[(1+\sqrt{3})^{2^n} + (1-\sqrt{3})^{2^n} \right] / 2}{\left[(1+\sqrt{3})^{2^n} - (1-\sqrt{3})^{2^n} \right] / 2\sqrt{3}}$$

$$x_n = \frac{(S_{n-1}/2) \cdot 2^{2^{n-1}}}{(S_0 S_1 S_2 \cdots S_{n-2}) \cdot 2^{2^{n-1}}}$$

则有

$$\left[(1+\sqrt{3})^{2^n} - (1-\sqrt{3})^{2^n} \right] / 2\sqrt{3} = (S_0 S_1 S_2 \cdots S_{n-2}) \cdot 2^{2^{n-1}}$$

令

$$\left[(1+\sqrt{3})^{2^n} + (1-\sqrt{3})^{2^n} \right] / 2 = (S_{n-1}/2) \cdot 2^{2^{n-1}} = a_n$$

$$\left[(1+\sqrt{3})^{2^n} - (1-\sqrt{3})^{2^n} \right] / 2\sqrt{3} = (S_0 S_1 S_2 \cdots S_{n-2}) \cdot 2^{2^{n-1}} = b_n$$

则有

$$x_n = \frac{a_n}{b_n}$$

由 $x_{k+1} = \frac{1}{2} \left(x_k + \frac{3}{x_k} \right)$ 得

$$x_{n+1} = \frac{a_n^2 + 3b_n^2}{2a_nb_n}$$

$$2a_nb_n = 2(S_{n-1}/2) \cdot 2^{2^{n-1}} \cdot (S_0 S_1 S_2 \cdots S_{n-2}) \cdot 2^{2^{n-1}} = (S_0 S_1 S_2 \cdots S_{n-1}) \cdot 2^{2^n}$$

又

$$x_{n+1} = \frac{(S_n/2) \cdot 2^{2^n}}{(S_0 S_1 S_2 \cdots S_{n-1}) \cdot 2^{2^n}}$$

则有

$$(S_n/2) \cdot 2^{2^n} = a_n^2 + 3b_n^2$$

$$= \left\{ \left[(1+\sqrt{3})^{2^n} + (1-\sqrt{3})^{2^n} \right] / 2 \right\}^2 +$$

$$3 \left\{ \left[(1+\sqrt{3})^{2^n} - (1-\sqrt{3})^{2^n} \right] / 2\sqrt{3} \right\}^2$$

$$= \left[(1+\sqrt{3})^{2^{n+1}} + (1-\sqrt{3})^{2^{n+1}} \right] / 2$$

即当 $k=n+1$ 时, 式(4)也成立。

因此, 当 $k=2, 3, \cdots$ 时, 式(4)成立。

证毕。

根据等式(4), 有

$$(1+\sqrt{3})^{2^k} + (1-\sqrt{3})^{2^k} = S_{k-1} \cdot 2^{2^{k-1}} \quad (k=2, 3, \cdots)$$

即

$$(1+\sqrt{3})^{2^{k+1}} + (1-\sqrt{3})^{2^{k+1}} = S_k \cdot 2^{2^k} \quad (k=1, 2, \cdots) \quad (5)$$

以 $S_0=4$, 由 $S_{k+1}=S_k^2-2$ 得

$$S_k = (2+\sqrt{3})^{2^k} + (2-\sqrt{3})^{2^k} \quad (k=0, 1, 2, \cdots) \quad (6)$$

由式(5)和式(6)得

$$\frac{(1+\sqrt{3})^{2^{k+1}} + (1-\sqrt{3})^{2^{k+1}}}{(2+\sqrt{3})^{2^k} + (2-\sqrt{3})^{2^k}} = 2^{2^k} \quad (k=1, 2, \cdots) \quad (7)$$

当 $k=0$ 时, 式(7)也成立, 因此有以下等式成立:

$$\frac{(1+\sqrt{3})^{2^{k+1}} + (1-\sqrt{3})^{2^{k+1}}}{(2+\sqrt{3})^{2^k} + (2-\sqrt{3})^{2^k}} = 2^{2^k} \quad (k=0, 1, 2, \cdots) \quad (8)$$

可以看出, 所得 $2^{2^k} (k=0, 1, 2, \cdots)$ 与周氏猜测所阐述的梅森素数分布规律的区间端点完全一致。基于该结论, 本文认为, 等式(8)或许会在解决周氏猜测的研究中发挥重要作用。

2.3 广义卢卡斯-雷默测试的存在性问题

由

$$\left[(1+\sqrt{3})^{2^k} + (1-\sqrt{3})^{2^k} \right] / 2 = (S_{k-1}/2) \cdot 2^{2^{k-1}} = (S_{k-2}^2 - 2) / 2 \cdot 2^{2^{k-1}}$$

得

$$\left[(1+\sqrt{3})^{2^k} + (1-\sqrt{3})^{2^k} \right] / 2 + 2^{2^{k-1}} = 2^{2^{k-1}-1} S_{k-2}^2$$

则有

$$\left[(1+\sqrt{3})^{2^p} + (1-\sqrt{3})^{2^p} \right] / 2 + 2^{2^{p-1}} = 2^{2^{p-1}-1} S_{p-2}^2$$

当 $M_p (p \neq 2)$ 是素数时, M_p 整除 S_{p-2} , 则 M_p 整除 $2^{2^{p-1}-1} S_{p-2}^2$,

$$M_p \text{ 整除 } \left[(1+\sqrt{3})^{2^p} + (1-\sqrt{3})^{2^p} \right] / 2 + 2^{2^{p-1}}.$$

将 $\left[(1+\sqrt{3})^{2^p} + (1-\sqrt{3})^{2^p} \right] / 2 + 2^{2^{p-1}}$ 按二项式展开得

$$1 + C_2^2 \cdot 3 + C_2^4 \cdot 3^2 + \cdots + C_2^{2^{p-2}} \cdot 3^{2^{p-1}-1} + 3^{2^{p-1}} + 2^{2^{p-1}}$$

当 $M_p (p \neq 2)$ 是素数时, 显然 M_p 整除 $C_{2^i}^{2^i} (i=1, 2, \cdots, 2^{p-1}-1)$, 则

$$M_p \text{ 整除 } 1 + 3^{2^{p-1}} + 2^{2^{p-1}}.$$

又 $1 + 3^{2^{p-1}} + 2^{2^{p-1}} = 3 + 3^{2^{p-1}} + 2(2^{2^{p-1}-1} - 1)$, 根据费马小定理, $2^{p-1} \equiv 1 \pmod{p}$, 则 p 整除 $2^{p-1}-1$, 2^{p-1} 整除 $2^{2^{p-1}-1}-1$, 即 M_p 整除 $2^{2^{p-1}-1}-1$, 则 M_p 整除 $3 + 3^{2^{p-1}}, M_p$ 整除 $1 + 3^{2^{p-1}-1}$.

由此得出结论: 若 $M_p (p \neq 2)$ 是素数, 则 M_p 整除 $1 + 3^{2^{p-1}-1}$.

本文猜想: $M_p (p \neq 2)$ 是素数, 当且仅当 M_p 整除 $1 + 3^{2^{p-1}-1}$.

如果以上猜想成立, 本文提出以下问题:

是否存在更多的与卢卡斯-雷默测试原理相同的整除测试方法来检验梅森素数性, 即是否存在广义的卢卡斯-雷默测试? 如果存在的话, 将会对寻找新的梅森素数提供极大的便利。

3 结论

通过本文的研究, 可得出以下结论。

1) 卢卡斯-雷默测试递归数列的衍生数列 $S_0/2, S_1/2, S_2/2, \dots$ 两两互质; 猜想该数列的每一项都没有平方因数。

2) 等式 $\frac{(1+\sqrt{3})^{2^{k+1}} + (1-\sqrt{3})^{2^{k+1}}}{(2+\sqrt{3})^{2^k} + (2-\sqrt{3})^{2^k}} = 2^{2^k} (k=0, 1, 2, \dots)$ 所得 $2^{2^k} (k=0, 1, 2, \dots)$ 与周氏猜测所阐述的梅森素数分布规律的区间端点完全一致。

3) 若 $M_p (p \neq 2)$ 是素数, 则 M_p 整除 $1+3^{2^{p-1}}$; 猜想 $M_p (p \neq 2)$ 是素数, 当且仅当 M_p 整除 $1+3^{2^{p-1}}$, 即存在广义的卢卡斯-雷默测试。

参考文献 (References)

- [1] Rosen K H. Elementary number theory and its applications[M]. Wokingham: Addison-Wesley, 2009.
- [2] 张四保. 梅森素数研究综述[J]. 科技导报, 2008, 26(18): 88-92.
Zhang Sibao. Science & Technology Review, 2008, 26(18): 88-92.
- [3] 周海中. 梅森素数的分布规律 [J]. 中山大学学报: 自然科学版, 1992,

31(4): 121-122.

Zhou Haizhong. Acta Scientiarum Naturalium Universitatis Sunyatseni, 1992, 31(4): 121-122.

- [4] 张景中. “周氏猜测”揭示数学之美[C]//30 年科技成就 100 例. 武汉: 湖北少年儿童出版社, 2008: 8-9.

Zhang Jingzhong. Zhou conjecture reveals the beauty of mathematics[C]// 100 Cases of Scientific and Technological Achievements in 30 Years. Wuhan: Hubei Children's Press, 2008: 8-9.

- [5] 施潇潇, 陈晓东. 基于网格技术的梅森素数搜索 [J]. 世界科技研究与进展, 2008, 30(3): 260-263.

Shi Xiaoxiao, Chen Xiaodong. World Science-Technology R&D, 2008, 30(3): 260-263.

- [6] Weisstein E. Newton's iteration[EB/OL]. [2009-12-06]. <http://mathworld.wolfram.com/NewtonsIteration.html>.

- [7] 石永进. 梅森素数与 $\sqrt{3}$ [J]. 中国科技信息, 2009, 20(22): 44-46.

Shi Yongjin. China Science and Technology Information, 2009, 20(22): 44-46.

(责任编辑 代丽)

第二十五届世界纯电动车、混合动力车和燃料电池车大会暨展览会

时间: 2010年11月5-9日

地点: 广东·深圳

主办单位: 中国电工技术学会
中国汽车工程学会
亚太电动车协会

联系人: 中国电工技术学会
联系电话: 010-68595355, 68594993
传真: 010-68595110
通信地址: 北京市三里河路46号 (100823)

会议网站: <http://www.evs25.org/event/2009ddc/index.html>