文章编号: 1672 - 058X(2009)05 - 0443 - 03

有关梅森素数的预测

张 四 保
(喀什师范学院 数学系,新疆 喀什 844007)

摘　要:梅森素数是一种特殊的素数,探究梅森素数的分布规律历来是数论研究的热点与难点;对梅森素数的分布规律作了简略研究,同时也对梅森素数研究的前景进行了展望。

关键词:素数;梅森素数;梅森素数预测
中图分类号: O156　　文献标志码: A

梅森素数是指形如 $2^p - 1$的素数,其中的 p为素数。因 17世纪法国数学家、法兰西科学院奠基人梅森(M. Mersenne)最早深入而系统地研究 $2^p - 1$型的数而得名,并以 M_p 记之。2300多年来,人类仅仅找到了46个梅森素数,由于这种素数珍奇而迷人,因此被人们称为"数学宝山上的璀璨明珠"。

人们一直都在探寻梅森素数的分布规律,但是,要想找到较为一个理想、满意的分布规律可能要比发现单个的梅森素数更为困难。因为从目前已知的梅森素数来看,这种特殊的素数在正整数中的分布是时疏时密极不规则的。数学家们在长期的摸索中,提出了一些猜想。英国数学家 Shank、法国数学家 Bertrand、印度数学家 Ramanujan、美国数学家吉里斯 Gillies和德国数学家 Brillhart等都曾分别给出过关于梅森素数分布的猜测,但他们的猜测有一个共同点,就是都以近似表达式给出,与实际情况的接近程度均难如人意[1]。

中国数学家及语言学家周海中[2]对梅森素数研究多年,他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 $2^{2^n} < p < 2^{2^{n+1}}$ $(n = 0, 1, 2, \cdots)$时,梅森素数的个数为 $2^{n+1} - 1$;并且据此给出了推论:当 $p < 2^{2^{n+1}}$时,梅森素数的个数为 $2^{n+2} - n - 2$。这一形式优美的表达式加深了人们对梅森素数重要性质的了解,为人们探寻新的梅森素数提供了方便。后来,这一科学猜测被国际数学界命名为"周氏猜测"。有关专家认为,这一成果是梅森素数研究中的一项重大突破。

下一个梅森素数在哪,这是数学家及数学爱好者所关注的问题。为了回答这一问题,先假定 M_n 为第 n个梅森素数,下面给出了 $\log_2(\log_2 M_n)$对应于 n的图(图 1):

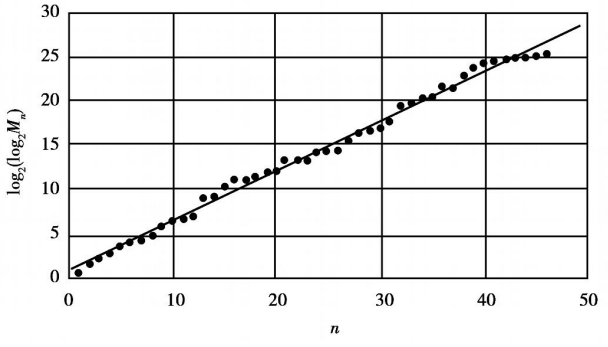


图 1　对应于第 n个梅森素数的 $\log_2(\log_2 M_n)$的值

图 1中的直线是线性回归线方程 $y = 0.562\,3x + 0.825\,5$,其相关系数为 $R^2 = 0.993\,6$。这是一个令人惊

收稿日期: 2009 - 03 - 18;修回日期: 2009 - 04 - 20。
作者简介:张四保 (1978 -),男,江西峡江人,硕士,从事数论研究。

讶的线性图表。1964年, Gillies[3]针对当时的梅森素数数据,提出了一个猜想,暗示图 1的直线斜率为 1/2,但很不幸的是他的启发式违背了素数定理。1980年, Lenstra和 Pomerance[4]各自独立地推测出在小于 x的范围内梅森素数的个数为 $(e^{\gamma}/\log 2)\log\log x$,其中 γ是 Euler常数。几年后 Wagstaff[5]针对该猜想,从 3方面加以说明:

(1) 小于等于 x的范围内梅森素数的个数为 $(e^{\gamma}/\log 2)\log\log x$,其中 γ是 Euler常数;

(2) 在 x与 $2x$之间梅森素数的个数预计为 e^{γ};

(3) 2^p-1是素数的概率大约为 $(e^{\gamma}\log ap)/(p\log 2)$,其中当 $p\equiv 3 \pmod 8$时, $a=2$;当 $p\equiv 3 \pmod 8$时, $a=6$。

这就意味着连续两个梅森素数的指数 p的几何平均比例从 2提升到 $1/e^{\gamma}$或 1.475 76。而 Eberhart和他之后的许多人根据有限的数据都认为其值为 3/2,但很少有其他论据支持这一观点。

将 Lenstra和 Pomerance的推测与图 1对照:如果推测是正确的,那么 $\log_2(\log_2 M_n)$的分布就是一个泊松过程,那得到直线的斜率大概为 $1/e^{\gamma}=0.561\cdots$。通过现在已知的 46个梅森素数,可以得到回归线的斜率为 0.562 3,相关系数 $R^2=0.993\ 6$。

泊松过程的间隔值累积分布是一个指数分布,尤其是间隔的概率密度函数 $f(t)$和间隔长度概率 $p(t)$。

$$f(t)=\lambda e^{-\lambda t}\frac{(\lambda t)^{n-1}}{(n-1)!};\quad p(t)=1-e^{-\lambda t}\sum_{j=0}^{n-1}\frac{(\lambda t)^j}{j!}$$

其中参数 $t=\log_2(\log_2 M_n)$。

下面来检验预测的泊松分布的间隔与已知的梅森素数的实际间隔,这里将以图的形式给出,即图 2。

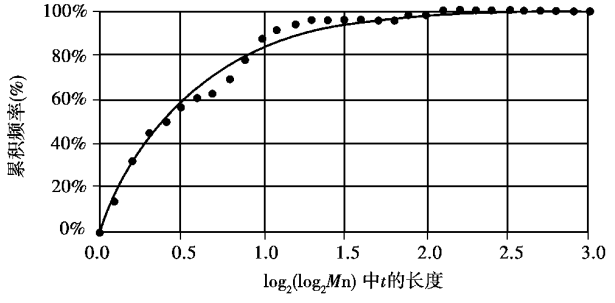


图 2 $\log_2(\log_2 M_n)$中间隔的累积频率

要找到下一个梅森素数,首先要给出梅森素数的指数 p。由于一个梅森素数的指数 p_i与其下一个梅森素数的指数 P_{i+1}之间的关系大致是: $p_{i+1}=1.475\ 76p_i$[6]。但它们之间的这种关系并非稳定,其间隔有时很大,有时很小。目前只知道 46个梅森素数,假设已被发现的 46个梅森素数已确定其位次,即在 $2\le p\le 43\ 112\ 609$范围内,没有其他的梅森素数存在,则只需考虑 p的预计间隔,如图 3所示。

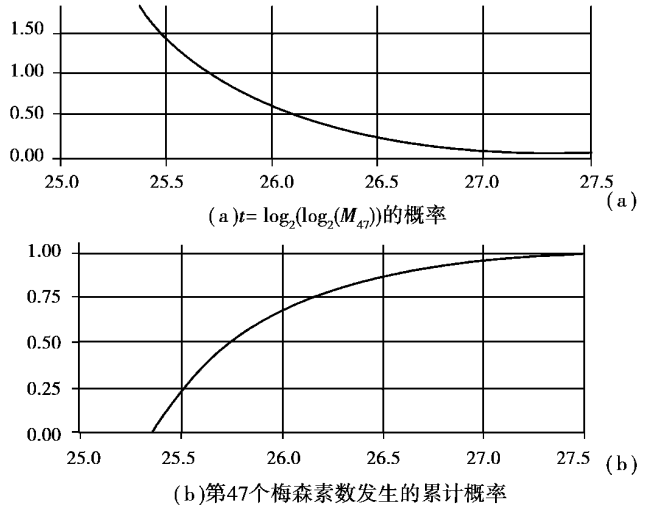
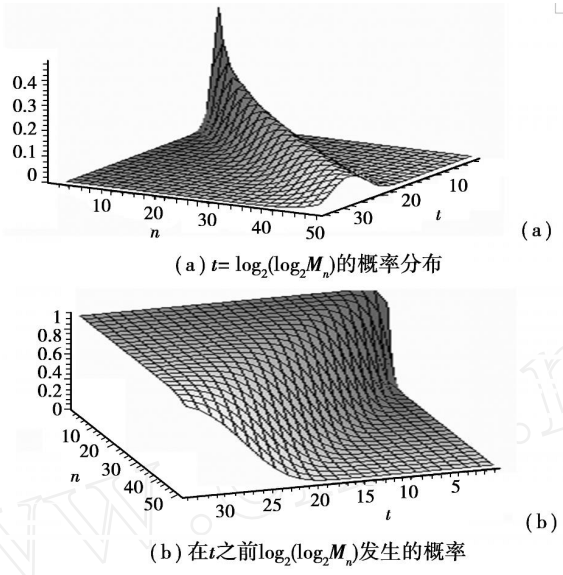


图 3 在第 39-46个梅森素数之间没有梅森素数的情况下 $t=\log_2(\log_2 M_{47})$的预测值

假定不知前 46个梅森素数的情况,以图的形式给出预测到第 50个梅森素数的概率密度图和 $t = \log_2(\log_2 M_n)$图,其中 $n = 50$(图 4)。



(a) $t = \log_2(\log_2 M_n)$的概率分布

(b) 在t之前$\log_2(\log_2 M_n)$发生的概率

图 4　直到第 50个梅森素数的预测图

探究梅森素数在当代具有十分丰富的理论意义和实用价值,它是发现已知最大素数的最有效途径。它推动了数学皇后 ——数论的研究,也促进了计算数学、程序设计技术、网格技术以及密码技术的发展。探究梅森素数的方法还可用来测试计算机硬件运算是否正确。因此,科学家们认为,对于梅森素数的探究能力如何,已在某种意义上标志着一个国家的科技水平。英国顶尖科学家 M. Sautoy甚至认为它是标志科学发展的里程碑,而梅森素数分布的研究对梅森素数的研究至关重要。

参考文献:

[1] 李明达. 梅森素数:数学宝库中的明珠 [J]. 科学:中文版, 2000, 262(6): 62-63

[2] 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

[3] GILLIES D B. Three new Mersenne primes and a statistical theory[J]. Math. Comp, 1964(18): 93-95

[4] POMERANCE C. Recent developments in primality testing[J]. Math. Intelligencer, 1980/81, 3(3): 97-105

[5] WAGSTAFF S. Divisors of Mersenne numbers[J]. Math. Comp., 1983, 40: 385-397

[6] 张四保. 梅森素数研究综述 [J]. 科技导报, 2008, 26(18): 88-92

Prediction on Mersenne primes

ZHANG Si-bao

(Department of Mathematics, Kashgar Teachers College, Xinjiang Kashgar 844007, China)

Abstract: Mersenne prime is a special kind of primes. The study of Mersenne prime has effectivily been a hot and difficult point in mathematical researches. In this paper, the distribution of Mersenne primes is studied roughly. At the same time, future prospect of the research on Mersenne primes is presented.

Key words: prime number; Mersenne prime; prediction of Mersenne primes

责任编辑:李翠薇