Mersenne Primes:
Development through History,
Ongoing Work,
and a New Conjecture

Stephan Thomas Lavavej
Advisor: M. Foster
Thornton High School 0677
November 23, 1999
3997 Words

Stephan Thomas Lavavej

Abstract

The study of Mersenne numbers (numbers expressible as $2^N - 1$) is an important topic in number theory. Thus, the question "what has been discovered about Mersenne numbers, what work is now being done, and is there a way to predict what the N^{th} Mersenne prime is?" is investigated here.

Early work on Mersenne numbers focused on perfect numbers; each Mersenne prime corresponds with exactly one even perfect number. Mathematicians, over the millennia, discovered effective methods to determine whether a given Mersenne number is composite. Mersenne numbers with composite exponents are always composite. Theorems were proven about Mersenne numbers' potential factors: they must be expressible as $2kN + 1$ and congruent to ± 1, modulo 8. An incredibly powerful primality test for Mersenne numbers was found: the Lucas-Lehmer test. Unlike probabilistic primality tests, a Mersenne number is prime if and only if it passes the Lucas-Lehmer test.

Combined with Fast Fourier Transforms, the Lucas-Lehmer test is ideally suited to be performed by binary computers. Initially, supercomputers haphazardly searched for Mersenne primes. However, the Lucas-Lehmer test also happens to be suited for distributed computing. This, along with the Internet, makes an organized, coordinated worldwide search on thousands of personal computers possible: The Great Internet Mersenne Prime Search.

Previous conjectures by Gillies, Wagstaff, and others are investigated here, and empirical support is shown for a new conjecture:

$$¿ \quad M(x) \approx e^{\gamma} \log_2 x - 2^{1/e^{\gamma}} \quad ?$$

$M(x)$ is the number of primes $P \leq x$ for which $2^P - 1$ is prime. This new conjecture may be used to more accurately predict what the N^{th} Mersenne prime is.

Despite the amount of knowledge already gathered and ongoing efforts, unresolved questions about Mersenne numbers still exist. There are indications that an undiscovered Mersenne prime between $2^{3021377} - 1$ and $2^{6972593} - 1$ exists. Clearly, Mersenne numbers will remain a topic of interest in number theory for a long time to come.

Acknowledgements

Thanks to G. Woltman and S. Kurowski for sparking this journey, to Wolfram Research and Texas Instruments for producing their excellent mathematical tools, and special thanks to A. Lee for help in debugging this paper.

Table of Contents

Introduction

From Number Theory to Mersenne Primes

Throughout history, people have been fascinated by the properties of integers. Since Pythagoras's time, these properties have been explored and discovered, and this field of mathematics has been named number theory. A significant part of number theory deals with divisibility, factoring, and prime numbers. Prime numbers, of course, are numbers that have no factors except themselves and one. Primes are more than just oddities: they have become extremely important in cryptography, because it is difficult to factor a large composite number into two primes. In fact, for general numbers a few hundred decimal digits long, factoring is nearly impossible; this gave rise to the RSA cryptosystem. However, prime numbers do not arise from a specific equation. There is no known formula which, given N, can return the N^{th} prime number without laboriously testing numbers for primality from two onwards, but many results have been discovered that describe in a more general way the distribution of primes. Over two millennia ago, Euclid showed that there are infinitely many prime numbers. Other mathematicians have found approximations to the N^{th} prime number, given N. There is something intriguing about the fact that the size of the N^{th} prime can be estimated well by the simple formula N ln N. Number theory is filled with simple, beautiful results such as this. Curious mathematicians have explored prime numbers' properties and have named specific types of them. In addition to "general" primes, like 137, there are more specialized types. For example, Sophie Germain primes are primes N for which 2N + 1 is prime. Pierre de Fermat investigated numbers of the form $2^{(2^N)} + 1$, now called "Fermat numbers". For values of N from 0 to 4, inclusive, the corresponding Fermat number is prime, and thus Fermat conjectured that **all** Fermat numbers were prime (Ore 74). However, $2^{(2^5)} + 1$ was eventually found to be composite, as well as many other Fermat numbers. As no more Fermat primes have been found, this area has become a dead-end. The only interesting work remaining is factoring very large Fermat numbers and attempting to show that the number of Fermat primes is finite. Yet another type has a similar structure to Fermat numbers: numbers of the form $2^N - 1$ are called Mersenne numbers, and several exponents N produce prime Mersenne numbers (Mersenne primes). Unlike Fermat primes, there *seems* to be an infinite number of Mersenne primes, and hence much work has been done with Mersenne numbers. Thus, a question arises: what has been discovered about Mersenne numbers, what work is now being done in this area, and is there a way to predict what the N^{th} Mersenne prime is? Discoveries about Mersenne numbers started over two millennia ago, and with the assistance of powerful electronic digital computers and an algorithm about a century old, Mersenne numbers can quickly be tested for primality. In addition, there appears to be a way to predict statistically what the N^{th} Mersenne prime is.

The Mersenne Primes

To this date, only 38 Mersenne primes have been discovered. Table 1 lists the known Mersenne primes' exponents.

TABLE 1
Mersenne Primes and Related Facts

Order by Size	Exponent in $2^N - 1$	Year Found	Discoverer(s)	Tool Used in Primality Test
1st	2	Antiquity	[Not Applicable]	Hand
2nd	3	Antiquity	[Not Applicable]	Hand
3rd	5	Antiquity	[Not Applicable]	Hand
4th	7	Antiquity	[Not Applicable]	Hand
5th	13	1456	Anonymous	Hand
6th	17	1588	Cataldi	Hand
7th	19	1588	Cataldi	Hand
8th	31	1772	Euler	Hand
9th	61	1883	Pervushin	Hand
10th	89	1911	Powers	Hand
11th	107	1914	Powers	Hand
12th	127	1876	Lucas	Hand
13th	521	1952	Robinson	SWAC
14th	607	1952	Robinson	SWAC
15th	1279	1952	Robinson	SWAC
16th	2203	1952	Robinson	SWAC
17th	2281	1952	Robinson	SWAC
18th	3217	1957	Riesel	BESK
19th	4253	1961	Hurwitz	IBM 7090
20th	4423	1961	Hurwitz	IBM 7090
21st	9689	1963	Gillies	ILLIAC II
22nd	9941	1963	Gillies	ILLIAC II
23rd	11213	1963	Gillies	ILLIAC II
24th	19937	1971	Tuckerman	IBM 360/91
25th	21701	1978	Noll & Nickel	Cyber-174
26th	23209	1979	Noll	Cyber-174
27th	44497	1979	Nelson & Slowinski	Cray-1
28th	86243	1982	Slowinski	Cray-1S
29th	110503	1988	Colquitt & Welsh	NEC SX-2
30th	132049	1983	Slowinski	Cray-XMP
31st	216091	1985	Slowinski	Cray-XMP
32nd	756839	1992	Slowinski & Gage	Cray-2
33rd	859433	1994	Slowinski & Gage	Cray-C916
34th	1257787	1996	Slowinski & Gage	Cray-T94
35th	1398269	1996	Armengaud, Woltman, et al. (GIMPS)	Pentium PC
36th*	2976221	1997	Spence, Woltman, et al. (GIMPS)	Pentium PC
37th*	3021377	1998	Clarkson, Woltman, Kurowski, et al. (GIMPS/PrimeNet)	Pentium PC
38th**? **	6972593	1999	Hajratwala, Woltman, Kurowski, et al. (GIMPS/PrimeNet)	Pentium PC

(Williams 336 and http://www.utm.edu/research/primes/mersenne.shtml)

* All Mersenne numbers with exponents under 3021377 have been tested for primality once, but not all have been double-checked. For the purposes of this paper, it will be assumed that the 36th and 37th largest Mersenne primes are $2^{2976221} - 1$ and $2^{3021377} - 1$, respectively.

** Not all Mersenne numbers with exponents under 6972593 have been tested for primality once. For the purposes of this paper, $2^{6972593} - 1$ will not be considered the 38th Mersenne prime in order of size unless otherwise noted.

Development through History

Early History – Euclid

While work today focuses on Mersenne numbers, two millennia ago they were merely a footnote in the work done on perfect numbers (numbers whose set of all divisors, excluding the number itself, add up to the number itself). The Pythagorean mathematicians, who were fascinated with numbers for numerological and mystical reasons, first studied perfect numbers (http://www-history.mcs.st-andrews.ac.uk/history/HistTopics/Prime_numbers.html). The first four perfect numbers, known since antiquity, are 6, 28, 496, and 8128. Euclid proved that when $2^N - 1$ is prime, $2^{(N-1)}(2^N - 1)$ is a (necessarily even) perfect number (Dickson 3). Thus, every Mersenne prime produces a perfect number. Apparently, Euclid was the first to define "prime number", and possibly the definition arose from this proof (Shanks 3). However, other mathematicians at the time stated things later proven incorrect about perfect numbers. Nichomachus erroneously stated that perfect numbers end alternately (when they are ordered by size) in 6 and 8, and other mathematicians believed this as well (Dickson 3). Though the pattern of ending digits 6, 8, 6, 8 seen in the first four perfect numbers does not hold, all perfect numbers do end in 6 or 8 (Griffin 37), which can be proven using an important fact about Mersenne numbers. Namely, when N is composite, $2^N - 1$ is composite (Hardy & Wright 15) (Proof 1 in Appendix III). This fact is a **great** advantage in the search for Mersenne primes, as the number of exponents that must be considered is significantly reduced when only prime exponents must be tested. With Proof 1, the proof that perfect numbers of the form $2^{(N-1)}(2^N - 1)$ end in 6 or 8 follows easily (Proof 2 in Appendix III).

After the Dark Ages – Fermat and Mersenne

Though many incorrect statements were made about perfect numbers after Euclid's time, little else was discovered during the Dark Ages about perfect and Mersenne numbers (http://www-history.mcs.st-andrews.ac.uk/history/HistTopics/Prime_numbers.html). Work on perfect and Mersenne numbers began again around the 16^{th} century. Though many thought that $2^N - 1$ was prime for all prime N, in 1536, Hudalricus Regius showed that $2^{11} - 1 = 2047 = 23 \cdot 89$ (http://www.utm.edu/research/primes/mersenne.shtml). In 1603, Pietro Cataldi had proven $2^{13} - 1$, $2^{17} - 1$, and $2^{19} - 1$ to be prime by the laborious process of trial division (trying every prime under the number's square root as a possible divisor) (Ore 73). Though Cataldi stated that $2^{23} - 1$, $2^{29} - 1$, $2^{31} - 1$, and $2^{37} - 1$ were prime (http://www.utm.edu/research/primes/mersenne.shtml), and was only correct for $2^{31} - 1$, he did prove that perfect numbers of Euclid's form end in 6 or 8, as Proof 2 shows (Dickson 10). Pierre de Fermat corresponded (as did other mathematicians) with the French monk Marin Mersenne about mathematics. In a letter to Mersenne written in June 1640, Fermat stated that he had proven three propositions: that $2^N - 1$ is composite when N is composite (Proof 1 shows this but may not use Fermat's exact approach), that $2^N - 2$ is divisible by 2N when N is prime, and that $2^N - 1$ is only divisible by primes of the form $2kN + 1$, where k is an arbitrary integer (Dickson 12) (Proof 3 in Appendix III shows the latter).

Proof 3, as with Proof 1, is highly useful in the search for Mersenne primes, as the number of possible factors a Mersenne number may have is reduced and trial division is made easier. Though testing a gigantic number like $2^{6972593} - 1$ by trial division, even with the help of Proof 3, is clearly infeasible, trial division was used to find some small Mersenne primes, as Euler did. Although numbers of the form $2^N - 1$ had been investigated before the 17th century, they are named for Marin Mersenne because he discussed them in his work Cogita physico-mathematica and stated conjectures about the numbers' occurrence (Ore 71). One of his most famous conjectures was that $2^N - 1$ is prime for N = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, and 257, and is composite for all other integers $2 \leq N \leq 257$ (http://www.utm.edu/research/primes/mersenne.shtml). Mersenne's conjecture was not completely correct, but his name is still attached to the numbers. A symbol based on Mersenne's name has also come into use. Mersenne numbers (of form $2^N - 1$) are often represented by M_N, and these two notations will be used interchangeably here. Occasionally, M(N) is used to represent $2^N - 1$, but it also infrequently refers to the N^{th} Mersenne number in order of size. In this paper, M(x) has a different meaning, which will be discussed below.

Additional Factor Restrictions – Euler

Leonhard Euler, like Fermat, also made important discoveries about Mersenne numbers. Euler was able to further restrict the set of possible divisors of Mersenne numbers; possible factors must be congruent to ±1, modulo 8 (Proof 4 in Appendix III).

In 1752, Euler was unsure of M_{31}'s primality, but in 1771, Euler proved that M_{31} is prime, using what he discovered about the structure of the possible factors of Mersenne numbers (Williams 38). He did this by systematically testing prime numbers of the form 248N + 1 and 248N + 63 below 46339 as possible factors of M_{31} (Dickson 19). While knowledge about Mersenne primes was clearly increasing (the 7th Mersenne prime, M_{19}, had been discovered almost two centuries before Euler found the 8th), it quickly becomes infeasible to primality test larger Mersenne numbers using trial division. Though there are only 84 prime numbers of the form 248N + 1 or 248N + 63 below 46339, as compared to the **4791** odd primes of general form below 46339 (which made Euler's work much easier), even the reduced set of possible factors grows too large as M_N increases.

Besides the further factor limitations, Euler also proved the converse to Euclid's theorem that every Mersenne prime produces an even perfect number: all even perfect numbers are produced by Mersenne primes (Proof 5 in Appendix III). After Euler proved the converse of Euclid's theorem, the search for perfect numbers became completely equivalent to the search for Mersenne primes (it is unknown if odd perfect numbers exist). In Euclid's time, perfect numbers were heavily investigated and Mersenne numbers were largely disregarded, but in modern times the situation has reversed.

The Test – Lucas

Édouard Lucas made an important discovery in 1876 concerning Mersenne

numbers, and in the process set a record that may never be broken again. While studying Fibonacci numbers, he discovered the following theorem:

Theorem 1: Let U_N be the N^{th} Fibonacci number ($U_1 = U_2 = 1$, $U_{K+1} = U_K + U_{K-1}$). If $N \equiv \pm 3 \pmod{10}$ and N is a proper (now called primitive) divisor of U_{N+1}, then N is prime. If $N \equiv \pm 1 \pmod{10}$ and N is a proper divisor of U_{N-1}, then N is prime (Williams 56).

While Lucas later provided incorrect proofs of this theorem, Carmichael eventually proved the theorem in 1913 (Williams 57). In an 1876 communication, Lucas stated, along with the previous theorem, "Furthermore, it is important to remark that [Theorem 1] allows us to determine whether a number is prime… without making the use of a table of prime numbers. It is with the aid of this theorem that I think I have proved that the number $A = 2^{127} - 1$ is prime… Indeed, the number A is of the form $10P - 3$ and I have verified that U_K is never divisible by A for $K = 2^N$ except for N = 127" (Williams 57). Before Lucas's discovery, there was no way to test **any** number of general form, much less Mersenne numbers, for primality using many trial divisions (Williams 57). The exact manner in which Lucas arrived at his discovery is uncertain, but he may have been aware of a more specific result than Theorem 1 (Proof 6 in Appendix III).

Proof 6 reveals that $2^{127} - 1$ can be proven prime by showing that $2^{127} - 1$ divides $V_{2^{126}}$ (Williams 58). The following small proof, from Hugh C. Williams, shows how Lucas actually computed this. Let $R_K = V_{2^K}$. It is simple to show: $V_{2N} = (V_N)^2 - 2(-1)^N$. Thus $R_0 = 1$, $R_1 = 3$, and $R_{K+1} = (R_K)^2 - 2$ (for $K \geq 1$). Hence Lucas had to demonstrate that $R_{126} \equiv 0$, modulo $2^{127} - 1$ (Williams 58). Interestingly, to do this computation, Lucas did not use written arithmetic; he moved counters on a 127 x 127 chessboard (Williams 60). Though this method did not leave any written work, making errors difficult to detect, Lucas said that with training one could become quick at manipulating the counters to do the computation. Nevertheless, it is estimated that Lucas spent 170 to 300 hours proving M_{127}'s primality, which may be why he performed the computation only once in his lifetime (Williams 60).

Lucas proved M_{127}'s primality in 1876, and while other Mersenne primes smaller than it were discovered later, the next larger Mersenne prime was discovered in 1952 with computer assistance. Because untested Mersenne numbers are now **much** too large to test by hand (and testing general numbers is much slower than testing Mersenne numbers) the 12^{th} Mersenne prime M_{127} will, in all likelihood, stand forever as the largest number to have been proven prime using an entirely manual method.

The Revised Test and Binary Computers

After Lucas originated the theory, D. H. Lehmer simplified the primality test Lucas used, producing the Lucas-Lehmer (LL) test.

Theorem 2 (the Lucas-Lehmer test): $2^N - 1$ is prime if and only if $S_{N-2} \equiv 0 \pmod{2^N - 1}$, where $S_0 = 4$ and $S_{K+1} = (S_K)^2 - 2$ (http://www.utm.edu/research/primes/notes/proofs/LucasLehmer.html)

The Lucas-Lehmer test happens to be ideally suited for binary computers, as the computation of S_K does not involve division (which binary computers do slowly) and can be done using only multiplication and addition (which binary computers do quickly). As a bonus, taking each S_K modulo M_N is ridiculously easy in binary because M_N is a string of 1s in binary. The N least significant bits of S_K are removed and stored as a new number (call it A). The remaining bits of S_K are shifted down, so that the N+1 bit of the original S_K is now the least significant bit. Call this new number B. A and B are added (call it C). If $C > M_N$, the process is repeated until it is under M_N. If $C = M_N$ then C is set to 0, and finally C is returned. As the LL test is done modulo M_N, the S_K that must be stored stays small throughout the test. Unfortunately, the sequence of S values must be recomputed for each exponent N that is tested. If the modulo M_N operation is not performed at every cycle of computing S_K, the estimated number of elementary particles in the observable universe soon becomes insufficient to store the value of S (http://www.tasam.com/~lrwiman/faq-mers).

Ongoing Work

The FFT Speedup and the Era of Supercomputers

Recently, the use of Fast Fourier Transformations (FFTs) has sped up the computation of the Lucas-Lehmer test. Using FFTs, the squaring operation done while calculating S_K is quicker, and the time taken to square larger numbers does not grow as quickly with the size of the number as for the "standard" multiplication process. In fact, multiplication of two N bit numbers can be done, via FFT, in O(N log N log log N) operations, while "ordinary" multiplication takes $O(N^2)$ operations (Williams 331). The FFT also easily performs the modulo M_N operation. Although LL testing has superseded factoring as a method of primality testing Mersenne numbers, the advances made centuries ago in factoring are still utilized today. While Mersenne numbers are not **completely** factorized, some factoring is done to eliminate Mersenne numbers with small factors. This can save time as compared to a full LL test. Of course, if no small factors are found in a Mersenne number, a LL test must be performed to test for primality.

Very large Mersenne primes have been found by using the Lucas-Lehmer test in combination with quick factoring techniques. In 1914, manual methods, for the last time, found a Mersenne prime. In 1952, Raphael Robinson wrote a program for LL testing on the Standards Western Automatic Computer, and it ran the first time he tried it on January 30. On that day, M_{521} and M_{607} were discovered. Incredibly, on June 25, October 7, and October 9 of the same year, M_{1279}, M_{2203}, and M_{2281} were respectively discovered (http://www.utm.edu/research/primes/notes/by_year.html). More Mersenne prime discoveries followed as supercomputers increased in speed. In 1961, A. Hurwitz found two Mersenne primes using the IBM 7090 computer. Because of the way the printed output was stacked, he learned of M_{4423} seconds before M_{4253} (http://www.utm.edu/research/primes/by_year.html). However, the increasing speed of

supercomputers created a problem. No organized search for Mersenne primes existed, and this led to confusion among researchers as to which Mersenne number exponents had been tested (Williams 337). In fact, in 1988 Colquitt and Welsh found M_{110503}, which had been overlooked between the previous discoveries of M_{86243} and M_{132049} (Williams 336-337). The advent of networking has now provided a solution.

Distributed Computing and the Era of Personal Computers

In January 1996, George Woltman started the Great Internet Mersenne Prime Search, GIMPS (http://www.mersenne.org/prime.htm). The GIMPS is classified as "distributed computing", and does not utilize a massively parallel supercomputer. Woltman wrote a program, Prime95, that runs Lucas-Lehmer tests (using Crandall and Fagin's DWT algorithm to speed up multiplication) on personal computers (PCs) and placed it on the Internet. Anyone could download the program and run it on a PC. Initially, Woltman personally assigned Mersenne number exponents to each participant and gathered the results via electronic mail. As the project grew (it has approximately 15,000 participants at this time), it became increasingly harder for Woltman to handle the electronic mail. Luckily, by 1997, Scott Kurowski had organized PrimeNet, a central Internet-based server that automatically assigns "work" for the participants' computers to do and collects results. In 1998, this was made an official part of Prime95 (http://www.mersenne.org/prime.htm). The coordinated project has solved the problem inherent in supercomputer searches; at this time, GIMPS has tested and double-checked in an orderly fashion all Mersenne numbers with exponents below 2,032,200, and has tested all exponents below 4,159,700 at least once. In fact, the GIMPS has found all four most recently discovered Mersenne primes, second only to Robinson's five discoveries (Slowinski has been in different teams) (http://www.mersenne.org/6972593.htm). Just as the LL test is suited to binary computers, searching for Mersenne primes is suited for distributed computing. There are many exponents that must be tested, so a PC can take a few at a time. The central server needs only to transmit the exponents to each PC and to collect the last few bits of the final Lucas-Lehmer S value, the residue (generally, 64 bits is enough to ensure that two residues are identical for double-checking). Each PC, once assigned work to do, is kept busy for weeks. Therefore, the data that must be sent over the Internet is minimal, and the numbers can be encoded as plain text. While many distributed computing projects now exist, GIMPS is the only search for Mersenne primes. The "virtual machine" produced by over 26,000 PCs working together executes over 950,000,000,000 floating point operations per second, and the project is growing at a steady rate as both new participants join and existing participants upgrade their personal computers (http://entropia.com/primenet/). See Appendix IV for a list of GIMPS's achievements. See Appendix V for a history of PrimeNet.

A New Conjecture

Previous Mersenne Conjectures – Gillies and Wagstaff

A systematic search for Mersenne primes is very useful, but by its nature it does not utilize any predictions as to what the next Mersenne prime might be. After all, the N^{th} general prime can be predicted, given N. Over time, mathematicians have formulated

conjectures about Mersenne primes' distribution. Richard K. Guy's definition of M(x) is used here: M(x) is the number of primes $P \leq x$ for which $2^P - 1$ is prime (Guy 8). Note that this is not S. Wagstaff's definition, which is the number of Mersenne primes $\leq x$ (Wagstaff 388). In 1964, D. B. Gillies conjectured that:

Conjecture 1:

¿ $M(x) \sim c \ln x$?

Where c is a constant (Guy 8). Wagstaff, H.W. Lenstra, and Carl Pomerance went further and conjectured that:

Conjecture 2:

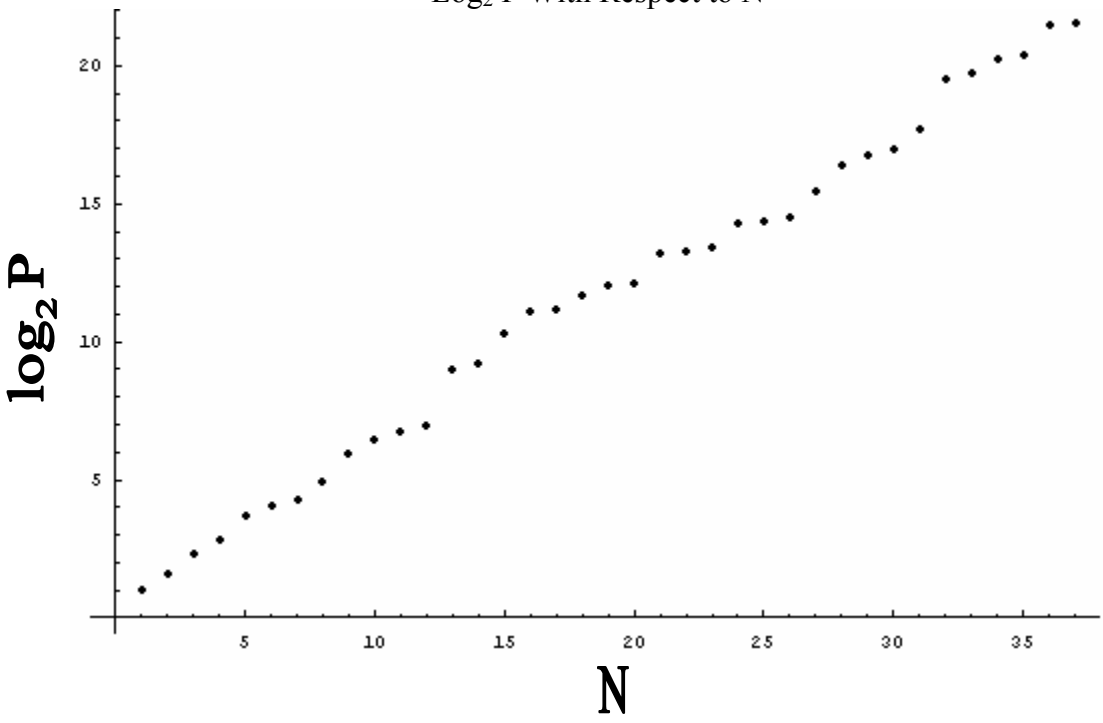
¿ $M(x) \sim e^{\gamma} \log_2 x$?

Where γ is Euler's constant (Guy 8). Wagstaff noted that this implies that e^{γ} Mersenne primes exist with exponent P between x and 2x (Wagstaff 388). Ideally, for prime M_X, a conjectured equation for M(x) should return an integer equal to the Mersenne prime's order by size. For example, M(1398269) should equal 35, because there are 35 primes $P \leq 1398269$ for which M_P is prime (i.e. $M_{1398269}$ is the 35^{th} Mersenne prime). Conjecture 2 returns 36.361. This suggests that a way to predict M(x) more accurately exists.

The New Empirical Evidence

Using the first 37 Mersenne primes, the author performed a series of calculations that suggests a new conjecture. (See note about $M_{6972593}$ under Table 1.) Appendix I contains the relevant data used to create the following graphs. The Mersenne primes, in a list P, were numbered according to size, producing the list N. Then, $\log_2$ P w.r.t. (with respect to) N was plotted, producing Graph 1.

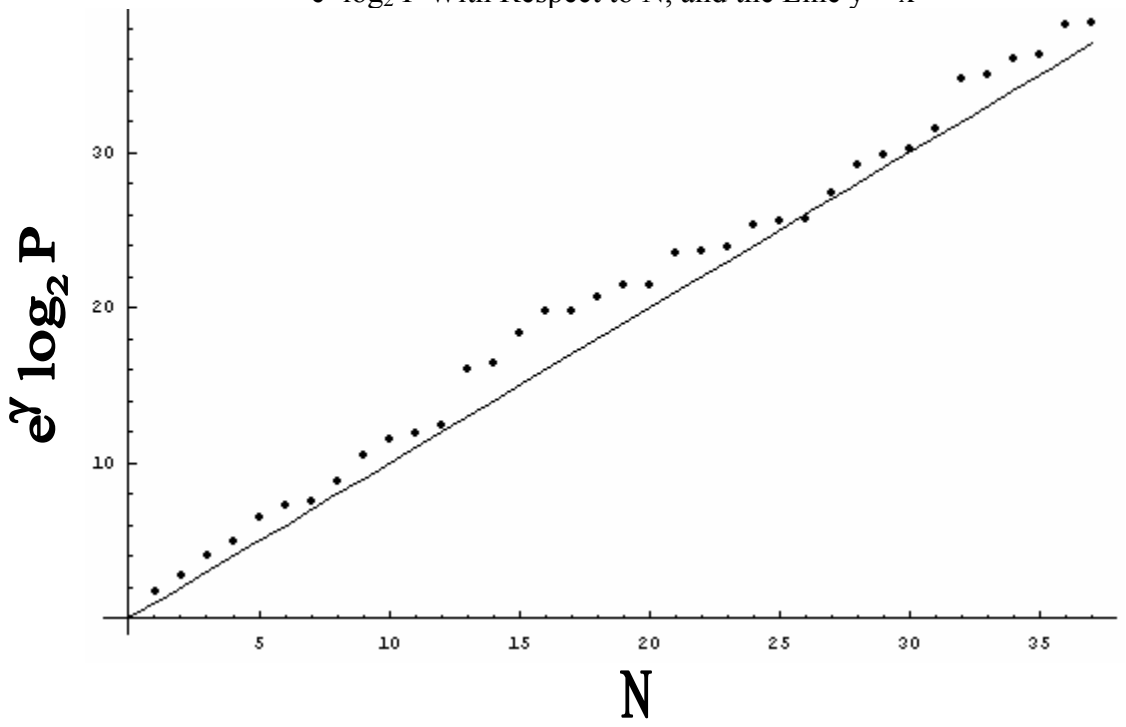
GRAPH 1
Log_2 P With Respect to N



Chris Caldwell said of a similar graph: "One can not miss that this graph is amazingly linear" (http://www.utm.edu/research/primes/notes/faq/NextMersenne.html). This suggests conjectures by itself, such as the one that Gillies made.

Then, $e^{\gamma} \log_2 P$ w.r.t. N was plotted in Graph 2, along with the line y = x. This line represents Conjecture 2; if all Mersenne prime exponents followed Conjecture 2 precisely, $e^{\gamma} \log_2$ (exponent) would equal 1, 2, 3… for each exponent in turn (Conjecture 2 relates N and P). Hence, Graph 2 is a measure of how well Conjecture 2 applies to the actual Mersenne prime exponents.

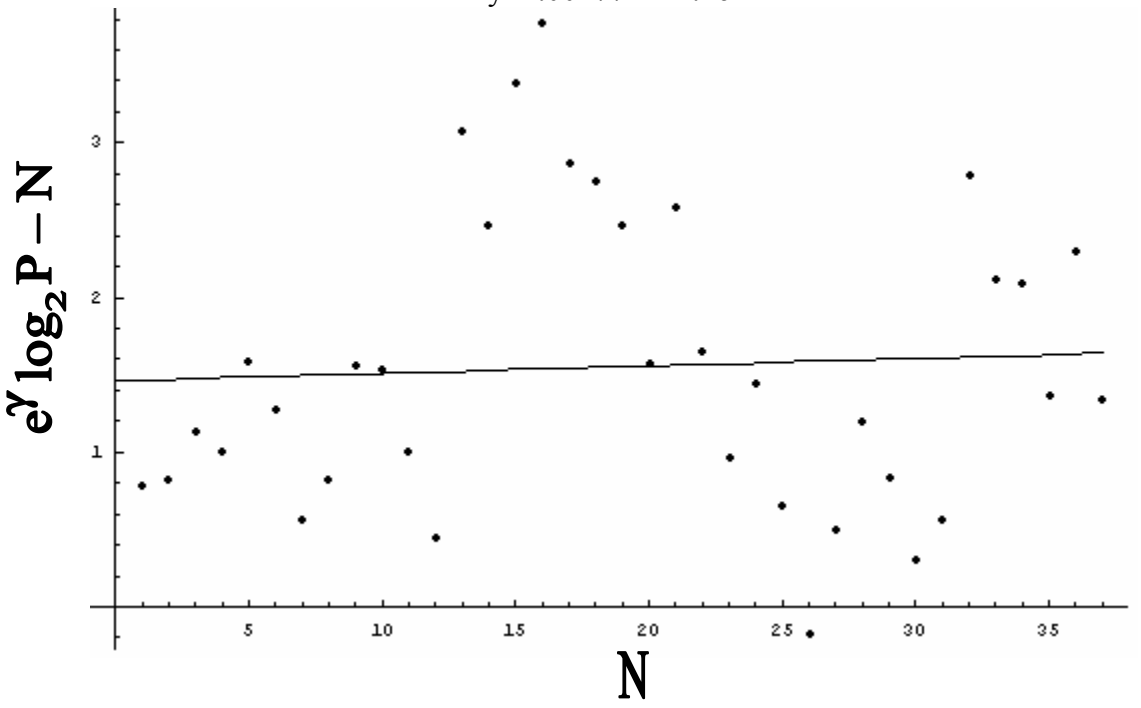
GRAPH 2
$e^{\gamma} \log_2 P$ With Respect to N, and the Line y = x



It is apparent from Graph 2 that Conjecture 2 seems slightly strange. For all but one given N, Conjecture 2 underestimates the actual value of $e^{\gamma} \log_2 P$.

Therefore, $e^{\gamma} \log_2 P - N$ w.r.t. N was plotted in Graph 3, along with a linear regression line of the data. This graph represents how inaccurate Conjecture 2 is when applied to real Mersenne prime exponents. If Conjecture 2 predicted that M(3021377) = 37, then $e^{\gamma} \log_2 3021377 - 37$ would equal 0. Graph 3 clearly shows that it does not.

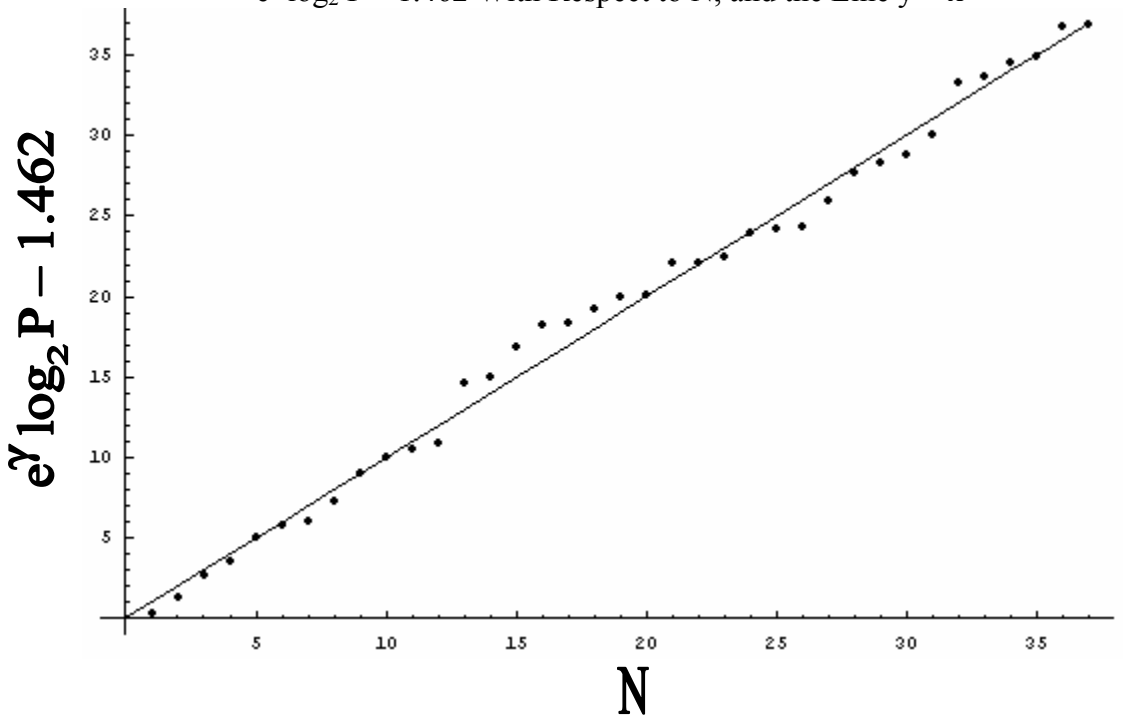
GRAPH 3
$e^{\gamma} \log_2 P - N$ With Respect to N, and the Resulting Linear Regression Line
$y = .00477x + 1.462$



Graph 3 is **very** strange. Save for one exponent, all of these calculated "errors" were positive, and often disturbingly large. The linear regression line $y = .00477x + 1.462$ was found (see Appendix II for all regression calculations). Apparently there is a consistent error (1.462) in Conjecture 2 that varies little as the Mersenne primes grow (hence the coefficient .00477). The author went back and applied a correction to Graph 2, which better fit $y = x$. $e^{\gamma} \log_2 P - 1.462$ w.r.t. N was plotted in Graph 4, along with the line $y = x$.

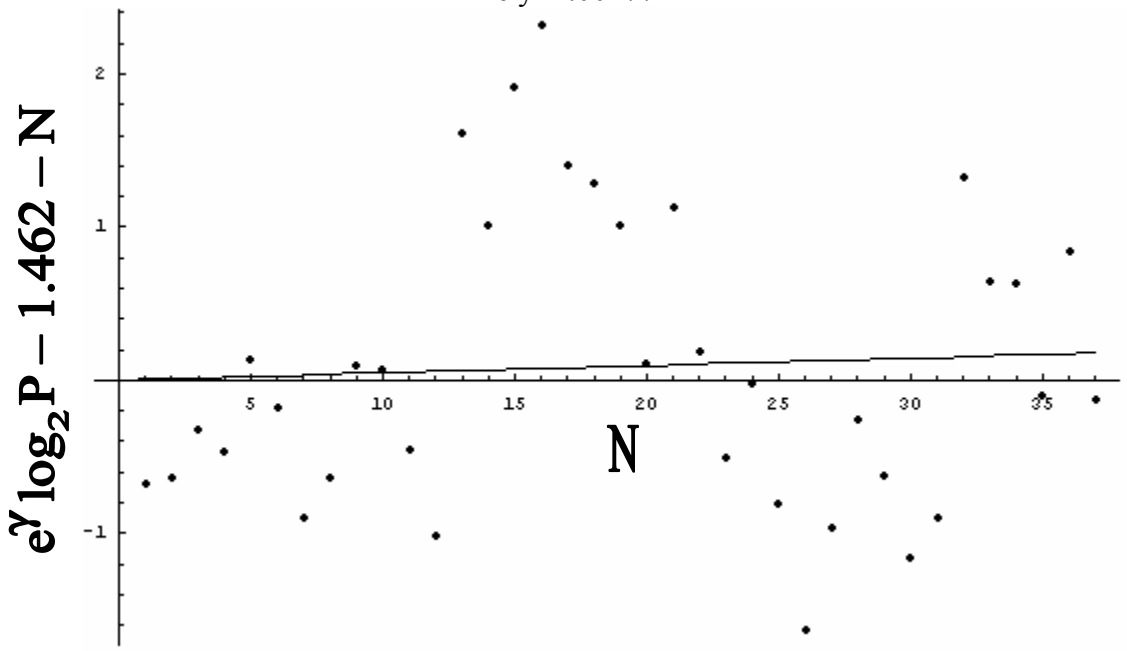
GRAPH 4

$e^{\gamma} \log_2 P - 1.462$ With Respect to N, and the Line y = x



Graph 4 with the "correction" of –1.462 appears to fit the actual data better than the uncorrected Graph 2. $e^{\gamma} \log_2 P - 1.462 - N$ w.r.t. N was plotted in Graph 5, along with a linear regression line.

GRAPH 5
$e^{\gamma} \log_2 P - 1.462 - N$ With Respect to N, and the Resulting Linear Regression Line y = .00477x



The calculated "errors" in Graph 5 are more evenly distributed around 0.

The New Conjecture

These graphs provide empirical support for a new conjecture. At the very least:

Conjecture 3 (Weak Form):
¿ $M(x) \sim e^{\gamma} \log_2 x + C$?

Of course, an appropriate C must be found. The first 37 Mersenne primes suggest that C = –1.462. Perhaps C is actually equal to –1.5. However, Manfred Schroeder noted that Conjecture 2 implies that the geometric mean of two successive Mersenne prime exponents is $2^{1/e^{\gamma}} = 1.47576\ldots$ (Schroeder 31). Schroeder remarks that this may have led to the Erhardt Conjecture that the average ratio of successive exponents is 1.5 (Schroeder 31). Interestingly, the aforementioned 1.462 is extremely close to $2^{1/e^{\gamma}}$. Thus, the author was led to conjecture a value for C.

Conjecture 4 (Strong Form):
¿ $M(x) \sim e^{\gamma} \log_2 x - 2^{1/e^{\gamma}}$?

It should be noted that these results do not change the validity of Conjecture 2, as it is an asymptotic estimate of M(x), which is not affected by the addition of a constant. However, the empirical evidence indicates that Conjecture 4 is more useful in predicting

the N^{th} Mersenne prime. In fact, Conjecture 4 may be a good **approximation** of M(x), rather than just an asymptotic estimate.

Conjecture 5 (Approximation Form):

¿ $M(x) \approx e^{\gamma} \log_2 x - 2^{1/e^{\gamma}}$?

Conjecture 5 may be used to predict the N^{th} Mersenne prime M_P, given N.

$$M(P) \approx N$$
$$e^{\gamma} \log_2 P - 2^{1/e^{\gamma}} \approx N$$
$$e^{\gamma} \log_2 P \approx N + 2^{1/e^{\gamma}}$$
$$\log_2 P \approx (N + 2^{1/e^{\gamma}})/e^{\gamma}$$
$$P \approx 2^{(N + 2^{1/e^{\gamma}})/e^{\gamma}}$$

Using this, one may predict the exponents of undiscovered Mersenne primes. A short selection of predictions:

TABLE 2
Expected Values for Exponents of the N^{th} Mersenne Prime, Calculated From Conjecture 5

N (In Order of Size)	Exponent P in $2^P - 1$
38	4,699,385
39	6,935,171
40	10,234,658
41	15,103,913
42	22,289,772
43	32,894,385
44	48,544,264
45	71,639,751
50	501,458,270
55	3,510,067,986
60	24,569,496,568
65	171,979,620,925

Note: Commas are used in only this table to enhance the readability of large numbers.

It should be noted that at one time, it was known to the general public that a Mersenne prime with exponent P between 6 and 7 million had been found, while the exponent's exact identity remained unknown. The author predicted from Conjecture 5 that this exponent was near 6.9 million, which turned out to be remarkably close (it was 6972593). However, Conjecture 5 forced the prediction of an undiscovered Mersenne prime between $M_{3021377}$ and $M_{6972593}$. This, along with the fact that not all Mersenne primes in that range have been tested for primality, is the reason why $M_{6972593}$ has not been considered here.

Conclusion

From the Past to the Future

Just five centuries ago, it was still thought that $2^N - 1$ was prime for all prime N. In this short period of time (as compared with all of history), mathematics has realized that very few Mersenne numbers are prime, and has devised powerful methods for searching for these rarities. Tremendous numbers of potential factors may be discarded without worry, thanks to the work of mathematicians such as Fermat and Euler. Work in the 19^{th} century led to the incredibly fast Lucas-Lehmer primality test for Mersenne numbers, which happens to be optimally suited for the binary computers that people are now fond of using. In fact, the LL test is easily distributed to thousands of personal computers. With the LL test and the Internet's help, the search for Mersenne primes is now more comprehensive and organized than haphazard supercomputer searches have been in the past. Recently, conjectures by Gillies, Wagstaff, et al. have indicated that there may be an underlying pattern to the Mersenne primes' distribution. However, the field of Mersenne numbers is far from being completely explored. There are still unproven conjectures and open problems, some of which have existed for millennia. Questions such as "Is the number of Mersenne primes infinite?", "If P is prime, is $2^P - 1$ always squarefree?", and even "Are there an infinite number of composite Mersenne numbers with prime exponents?" remain unresolved. Mathematicians are currently seeking proofs of the various conjectures regarding Mersenne primes. It is unknown whether there are heuristic (rather than simply empirical) arguments that support Conjectures 4 and 5. There may even be an **undiscovered** Mersenne prime between $M_{3021377}$ and $M_{6972593}$. It would be only the fourth missing Mersenne prime ever recovered, and would provide further support for the author's conjecture.

Bibliography

Caldwell, Chris K. "Mersenne Primes: History, Theorems and Lists." Prime Pages (1999). Online. Internet. Accessed November 22, 1999. Available HTTP: http://www.utm.edu/research/primes/mersenne.shtml

Caldwell, Chris K. "The Largest Known Prime by Year: A Brief History." Prime Pages (1999). Online. Internet. Accessed November 22, 1999. Available HTTP: http://www.utm.edu/research/primes/notes/by_year.html

Caldwell, Chris K. "Where is the next larger Mersenne prime?" Prime Pages (1999). Online. Internet. Accessed November 22, 1999. Available HTTP: http://www.utm.edu/research/primes/notes/faq/NextMersenne.html

Caldwell, Chris K. "Lucas-Lehmer Theorem." Prime Pages (1999). Online. Internet. Accessed November 22, 1999. Available HTTP: http://www.utm.edu/research/primes/notes/proofs/LucasLehmer.html

Caldwell, Chris K. "Modular restrictions on Mersenne divisors." Prime Pages (1999). Online. Internet. Accessed November 22, 1999. Available HTTP: http://www.utm.edu/research/primes/notes/proofs/MerDiv.html

Caldwell, Chris K. "Prime-square Mersenne divisors are Wieferich." Prime Pages (1999). Online. Internet. Accessed November 22, 1999. Available HTTP: http://www.utm.edu/research/primes/notes/proofs/SquareMerDiv.html

Dickson, Leonard Eugene. History of the Theory of Numbers. Vol. 1. New York: Chelsea Publishing Company, 1966.

Griffin, Harriet. Elementary Theory of Numbers. New York: McGraw-Hill Book Company, Inc., 1954.

Guy, Richard K. Unsolved Problems in Number Theory. 2nd ed. New York: Springer-Verlag, 1994.

Hardy, G. H., and Wright, E. M. An Introduction to the Theory of Numbers. 5th ed. New York: Oxford University Press Inc., 1996.

Kurowski, Scott. "Current Internet PrimeNet Server World Test Status." Entropia.com (November 22, 1999). Online. Internet. Accessed November 22, 1999. Available HTTP: http://entropia.com/primenet/

O'Connor, John J., and Robertson, Edmund F. "Prime numbers." The MacTutor History of Mathematics Archive (December 1996). Online. Internet. Accessed November 22, 1999. Available HTTP: http://www-history.mcs.st-andrews.ac.uk/history/HistTopics/Prime_numbers.html

Ore, Oystein. Number Theory and Its History. New York: Dover Publications, Inc., 1988.

Schroeder, Manfred R. "Where Is the Next Mersenne Prime Hiding?" Mathematical Intelligencer 5.3 (1983): 31-33.

Shanks, Daniel. Solved and Unsolved Problems in Number Theory. Vol. 1. Washington: Spartan Books, 1962.

Wagstaff, Samuel S., Jr. "Divisors of Mersenne Numbers." Mathematics of Computation 40.161 (1983): 385-397.

Williams, Hugh C. Édouard Lucas and Primality Testing. New York: John Wiley & Sons, Inc., 1998.

Wiman, Lucas, et al. "The Mersenne Prime Mailing List FAQ." Mersenne FAQ (1999). Online. Internet. Accessed November 22, 1999. Available HTTP:

http://www.tasam.com/~lrwiman/faq-mers

Woltman, George. "38th Mersenne Prime Discovered." Mersenne.org (June 30, 1999). Online. Internet. Accessed November 22, 1999. Available HTTP: http://www.mersenne.org/6972593.htm

Woltman, George. "Mersenne Prime Search." Mersenne.org (October 4, 1999). Online. Internet. Accessed November 22, 1999. Available HTTP: http://www.mersenne.org/prime.htm

Woltman, George. "Mersenne Search Status." Mersenne.org (November 17, 1999). Online. Internet. Accessed November 22, 1999. Available HTTP: http://www.mersenne.org/status.htm

Appendix I
Data Used in Graphs

TABLE 3
Data Used For All Graphs, Including List of Exponents P for Which M_P is Prime in Order of Size

N (Rank of P by Size)	P (Exponent in $2^P - 1$)	Log_2 P	$e^\gamma \log_2 P$	$e^\gamma \log_2 P - N$	$e^\gamma \log_2 P - 1.462$	$e^\gamma \log_2 P - 1.462 - N$
1	2	1.000	1.781	0.781	0.319	**–0.681**
2	3	1.585	2.823	0.823	1.361	**–0.639**
3	5	2.322	4.136	1.136	2.674	**–0.326**
4	7	2.807	5.000	1.000	3.538	**–0.462**
5	13	3.700	6.591	1.591	5.129	0.129
6	17	4.087	7.280	1.280	5.818	**–0.182**
7	19	4.248	7.566	0.566	6.104	**–0.896**
8	31	4.954	8.824	0.824	7.362	**–0.638**
9	61	5.931	10.563	1.563	9.101	0.101
10	89	6.476	11.534	1.534	10.072	0.072
11	107	6.741	12.007	1.007	10.545	**–0.455**
12	127	6.989	12.447	0.447	10.985	**–1.015**
13	521	9.025	16.074	3.074	14.612	1.612
14	607	9.246	16.467	2.467	15.005	1.005
15	1279	10.321	18.382	3.382	16.920	1.920
16	2203	11.105	19.779	3.779	18.317	2.317
17	2281	11.155	19.869	2.869	18.407	1.407
18	3217	11.652	20.752	2.752	19.290	1.290
19	4253	12.054	21.470	2.470	20.008	1.008
20	4423	12.111	21.570	1.570	20.108	0.108
21	9689	13.242	23.585	2.585	22.123	1.123
22	9941	13.279	23.651	1.651	22.189	0.189
23	11213	13.453	23.961	0.961	22.499	**–0.501**
24	19937	14.283	25.439	1.439	23.977	**–0.023**
25	21701	14.405	25.657	0.657	24.195	**–0.805**
26	23209	14.502	25.830	**–0.170**	24.368	**–1.632**
27	44497	15.441	27.502	0.502	26.040	**–0.960**
28	86243	16.396	29.203	1.203	27.741	**–0.259**
39	110503	16.754	29.840	0.840	28.378	**–0.622**
30	132049	17.011	30.297	0.297	28.835	**–1.165**
31	216091	17.721	31.563	0.563	30.101	**–0.899**
32	756839	19.530	34.784	2.784	33.322	1.322
33	859433	19.713	35.110	2.110	33.648	0.648
34	1257787	20.262	36.089	2.089	34.627	0.627
35	1398269	20.415	36.361	1.361	34.899	**–0.101**
36	2976221	21.505	38.302	2.302	36.840	0.840
37	3021377	21.527	38.341	1.341	36.879	**–0.121**

Note: **Bold** entries are used in this table to clearly set apart negative numbers.
Here and in all other appearances, γ is Euler's gamma (.5772156649…) and e is the base of natural logarithms (2.718281828…)

Appendix II
Linear Regression Line Calculations

From information in the CRC Standard Mathematical Tables and Formulae, 30th edition, if X and Y are two lists of data which each contain Q elements, then the linear regression line $y = Ax + B$ can be calculated if A and B are found.

$$A = (Q \cdot \sum XY - \sum X \cdot \sum Y) / (Q \cdot \sum X^2 - (\sum X)^2)$$
$$B = (\sum X^2 \cdot \sum Y - \sum X \cdot \sum XY) / (Q \cdot \sum X^2 - (\sum X)^2)$$

For the first calculation, $Q = 37$, $X = N$, and $Y = e^{\gamma} \log_2 P - N$.

TABLE 4

Data Used in Linear Regression Line Calculation for N and $e^{\gamma} \log_2 P - N$ in Graph 3

X	Y	X^2	XY
1	0.781	1	0.781
2	0.823	4	1.646
3	1.136	9	3.408
4	1.000	16	4.000
5	1.591	25	7.955
6	1.280	36	7.680
7	0.566	49	3.962
8	0.824	64	6.592
9	1.563	81	14.067
10	1.534	100	15.340
11	1.007	121	11.077
12	0.447	144	5.364
13	3.074	169	39.962
14	2.467	196	34.538
15	3.382	225	50.730
16	3.779	256	60.464
17	2.869	289	48.773
18	2.752	324	49.536
19	2.470	361	46.930
20	1.570	400	31.400
21	2.585	441	54.285
22	1.651	484	36.322
23	0.961	529	22.103
24	1.439	576	34.536
25	0.657	625	16.425
26	–0.170	676	–4.420
27	0.502	729	13.554
28	1.203	784	33.684
39	0.840	841	24.360
30	0.297	900	8.910
31	0.563	961	17.453
32	2.784	1024	89.088
33	2.110	1089	69.630
34	2.089	1156	71.026
35	1.361	1225	47.635
36	2.302	1296	82.872
37	1.341	1369	49.617
$\sum X$	$\sum Y$	$\sum X^2$	$\sum XY$
703	57.430	17575	1111.285

Hence, for Graph 3:

$A = (37 \cdot 1111.285 – 703 \cdot 57.430) / (37 \cdot 17575 – 703^2) = .00477$
$B = (17575 \cdot 57.430 – 703 \cdot 1111.285) / (37 \cdot 17575 – 703^2) = 1.462$

The linear regression line between N and $e^\gamma \log_2 P – N$ is thus $y = .00477x + 1.462$.

For the second calculation, $Q = 37$, $X = N$, and $Y = e^\gamma \log_2 P – 1.462 – N$.

TABLE 5
Data Used in Linear Regression Line Calculation for N and $e^{\gamma} \log_2 P - 1.462 - N$ in Graph 5

X	Y	X^2	XY
1	–0.681	1	–0.681
2	–0.639	4	–1.278
3	–0.326	9	–0.978
4	–0.462	16	–1.848
5	0.129	25	0.645
6	–0.182	36	–1.092
7	–0.896	49	–6.272
8	–0.638	64	–5.104
9	0.101	81	0.909
10	0.072	100	0.720
11	–0.455	121	–5.005
12	–1.015	144	–12.180
13	1.612	169	20.956
14	1.005	196	14.070
15	1.920	225	28.800
16	2.317	256	37.072
17	1.407	289	23.919
18	1.290	324	23.220
19	1.008	361	19.152
20	0.108	400	2.160
21	1.123	441	23.583
22	0.189	484	4.158
23	–0.501	529	–11.523
24	–0.023	576	–0.552
25	–0.805	625	–20.125
26	–1.632	676	–42.432
27	–0.960	729	–25.920
28	–0.259	784	–7.252
39	–0.622	841	–18.038
30	–1.165	900	–34.950
31	–0.899	961	–27.869
32	1.322	1024	42.304
33	0.648	1089	21.384
34	0.627	1156	21.318
35	–0.101	1225	–3.535
36	0.840	1296	30.24
37	–0.121	1369	–4.477
$\sum X$	$\sum Y$	$\sum X^2$	$\sum XY$
703	3.336	17575	83.499

Hence, for Graph 5:

$A = (37 \cdot 83.499 – 703 \cdot 3.336) / (37 \cdot 17575 – 703^2) = .00477$
$B = (17575 \cdot 3.336 – 703 \cdot 83.499) / (37 \cdot 17575 – 703^2) = 0.000$

The linear regression line between N and $e^{\gamma} \log_2 P – 1.462 – N$ is thus $y = .00477x$.

Appendix III
Proofs

Proof 1: Numbers of the form $2^N - 1$ with composite N are composite (Hardy & Wright 15).

N is composite and hence may be factored into two integers R, S (both greater than 1) such that $R \cdot S = N$. If $2^{RS} - 1$ is divisible by $2^R - 1$, then $2^{RS} - 1$ modulo $2^R - 1$ will be congruent to 0, because of the basic laws of modular arithmetic. Thus, we wish to verify that the following equation does, indeed, hold:

$$2^{RS} - 1 \equiv 0 \pmod{2^R - 1}$$
$$2^{RS} \equiv 1 \pmod{2^R - 1}$$

Because R and S are both integers greater than 1, the last equation is simply:

$$2^R \cdot 2^R \cdot 2^R \cdot \ldots \cdot 2^R \cdot 2^R \equiv 1 \pmod{2^R - 1}$$

2^R, of course, appears on the previous equation's left-hand-side S number of times. However, 2^R taken modulo $2^R - 1$ is 1. Obviously:

$$1 \cdot 1 \cdot 1 \cdot \ldots \cdot 1 \cdot 1 \equiv 1 \pmod{2^R - 1}$$

This equation is true; hence $2^{RS} - 1$ is divisible by $2^R - 1$. QED

Proof 2: All perfect numbers of the form $2^{(N-1)}(2^N - 1)$ are congruent to 6 or 8 modulo 10 (Griffin 37).

Numbers of the form $2^{(N-1)}$ as N increases by 1, when taken modulo 10, give rise to the pattern 2, 4, 8, 6, 2, 4, 8, 6…. (Each number in the pattern, when doubled modulo 10, gives rise to the next.) Similarly, numbers of the form $2^N - 1$ as N increases by 1, when taken modulo 10, give rise to the pattern 3, 7, 5, 1, 3, 7, 5, 1…. Because these patterns have the same period, for the same N, $2^{(N-1)}(2^N - 1)$ modulo 10 can only take the values $2 \cdot 3$, $4 \cdot 7$, $8 \cdot 5$, or $6 \cdot 1$. Since the period is an even number (4), for odd N, the number $2^{(N-1)} \cdot (2^N - 1)$ modulo 10 can only be $4 \cdot 7$ or $6 \cdot 1$. Thus, for Mersenne primes, which always have a prime exponent N in $2^N - 1$, the corresponding perfect number is congruent to 8 or 6 modulo 10 because all primes are either odd or 2. For 2, it may be verified by hand that $2^{(2-1)}(2^2 - 1)$ is 6. QED

Proof 3: Numbers of the form $2^N - 1$ are only divisible by numbers of the form $2kN + 1$, where k is an arbitrary integer (Shanks 19).

If Q divides $2^N - 1$, then $2^N \equiv 1 \pmod{Q}$ and the order of 2 (mod Q) divides the prime N, so it must be N. By Fermat's Little Theorem the order of 2 also divides $Q - 1$, so $Q - 1 = 2kN$. Hence, $Q = 2kN + 1$ (http://www.utm.edu/research/primes/notes/proofs/MerDiv.html). QED

Proof 4: Numbers of the form $2^N - 1$ are only divisible by numbers congruent to 1 or 7, modulo 8 (Shanks 26).

From Proof 3, if Q divides $2^N - 1$, $Q = 2kN + 1$, where k is an arbitrary integer. Thus, $Q - 1 = 2kN$. Hence:

$$2^{(Q-1)/2} \equiv 2^{kN} \equiv 1 \pmod{Q}$$

Thus, 2 is a quadratic residue mod Q, and it follows that $Q \equiv \pm 1 \pmod 8$ (http://www.utm.edu/research/primes/notes/proofs/MerDiv.html). QED

Proof 5: All even perfect numbers are of the form $2^{(N-1)}(2^N - 1)$, where $2^N - 1$ is prime (Griffin 36).

Assume that M is a perfect number of the form $2^K Q$, where Q is odd; hence M is even. By letting S represent the sum of all the divisors of Q except Q itself, the following equation holds:

$$2^{K+1}Q = (2^{K+1} - 1)(Q + S)$$

However, $2^{K+1} - 1$ is odd, and hence 2^{K+1} divides $Q + S$. Thus,

$$Q + S = 2^{K+1}N$$

Substituting this into the first equation:

$$Q = (2^{K+1} - 1)N$$

Therefore, N is a divisor of Q. By subtracting Q from Q + S, it is apparent that S = N. Now, suppose that S = N = Q. Then the preceding equation becomes simplified:

$$\begin{aligned} Q &= (2^{K+1} - 1)N \\ Q &= (2^{K+1} - 1)Q \\ 1 &= 2^{K+1} - 1 \\ 2 &= 2^{K+1} \end{aligned}$$

Therefore, K = 0 and hence the "even" perfect number M (of the form $2^K Q$, where is odd) is not even. However, if it is supposed that N is a divisor of Q that is not Q and not 1, then N = S is at least the sum of the divisors N and 1. However, it is impossible that $N \geq N + 1$, so N = 1 and the only divisors of Q are Q and 1. Therefore, Q is a prime number, and since $Q = 2^{K+1} - 1$, the exponent K + 1 is a prime number (from Proof 1). Hence, every even perfect number is of the form $2^{(N-1)}(2^N - 1)$, in which both $2^N - 1$ and N are prime (Griffin 36). QED

Proof 6: Let $V_N = U_{2N} / U_N$. Let P be an odd prime and suppose P divides V_{2^N}. Therefore $P \equiv \pm 1 \pmod{2^{N+1}}$ (Williams 58).

Since P divides V_{2^N}, by Theorem 1, P does not divide U_{2^N}. Hence, P divides $U_{2^{N+1}}$ but P does not divide U_{2^M} for $M \leq N$. Thus, P is a proper divisor of $U_{2^{N+1}}$ (Williams 58). QED

Appendix IV
Great Internet Mersenne Prime Search Milestones

Current Search Status:

All exponents below 2,032,200 have been tested and double-checked.
All exponents below 4,159,700 have been tested at least once.
Exponents left until $M_{2976221}$ is proven to be the 36th Mersenne prime: 880
Exponents left until $M_{3021377}$ is proven to be the 37th Mersenne prime: 968
Exponents below 6,972,593 not yet tested at least once: 4691

GIMPS, GIMPS/PrimeNet Milestones:

October 16, 1999:	All exponents less than 2,000,000 double-checked.
August 19, 1999:	All exponents less than 4,000,000 tested at least once.
June 1, 1999:	**Prime $M_{6972593}$ is discovered.**
December 26, 1998:	All Mersenne numbers less than a million digits tested at least once.
December 18, 1998:	*Double-checking proves $M_{1398269}$ is the 35th Mersenne prime.*
September 26, 1998:	All exponents below 3,021,377 tested at least once.
September 19, 1998:	All exponents below 2,976,221 tested at least once.
March 29, 1998:	*Double-checking proves $M_{1257787}$ is the 34th Mersenne prime.*
March 5, 1998:	All exponents below 2,000,000 tested at least once.
January 27, 1998:	**Prime $M_{3021377}$ is discovered.**
January 1998:	PrimeNet begins official operation.
October 30, 1997:	All exponents below 1,000,000 double-checked.
October 11, 1997:	All exponents below 1,398,269 tested at least once.
August 30, 1997:	*Double-checking proves M_{756839} and M_{859433} are the 32nd and 33rd Mersenne primes, respectively.*
August 28, 1997:	All exponents below 1,257,787 tested at least once.
August 24, 1997:	**Prime $M_{2976221}$ is discovered.**
May 26, 1997:	All exponents below 1,000,000 tested at least once.
March 28, 1997:	All exponents below 859,433 tested at least once.
March 1997:	PrimeNet begins operation, unofficially.
January 15, 1997:	All exponents below 756,839 tested at least once.
November 13, 1996:	**Prime $M_{1398269}$ is discovered.**
Third quarter, 1996:	*Double-checking proves M_{216091} is the 31st Mersenne prime.*

(http://www.mersenne.org/status.htm)

Note: Mersenne prime discoveries are highlighted in bold, while double-checking accomplishments are italicized.

Appendix V
History of PrimeNet

Thanks to Scott Kurowski who graciously provided this history of PrimeNet.

Timeline:

* March 1997
Entropia.com selects GIMPS for candidate project; PrimeNet 1.0 prototype built from Duncan Booth's modifications of the MSDN example RPC server implementation. Used built-in hooks in Prime95 v14 APIs for a primenet.dll to get work and return results messages. At this time, George Woltman was not involved.

* April-June 1997
Primenet.dll is modified to provide the equivalent of prime.spl and worktodo.ini support. PrimeNet 2.0 is rewritten, tested with 16 machines, and put onto Entropia.com web site to cultivate testers. By late April, PrimeNet 2.4 started to get used by GIMPS folks around the Internet on their own LANs. A lot of good feedback (credited on the entropia.com website), fixes and features turned it into version 2.6. More than 100 GIMPS users ran their own local PrimeNet servers. The old web site for this is still at:

http://entropia.com/primenet/original-primenet.html
http://entropia.com/primenet/userguide.html
http://entropia.com/primenet/installing.html
http://entropia.com/primenet/tipsnhelp.html
http://entropia.com/primenet/challenge.html

* July 1997
PrimeNet 2.6 was strong enough for an Internet trial using a P166 server. Some 200 machines from several of the top LAN users of the 2.6 version of the server, most notably Intershop Communications, who later became 'netconx' account. 2.6 didn't support user accounts, so all the results were submitted under the userid 'challenge' to GIMPS (to this day, Entropia.com owns this first account ID). George Woltman was now ready to work with us in a concentrated effort to support GIMPS on the Internet.

* August-September 1997
Work continued to add accounting support to the new 2.8 server. Scott Kurowski started designing PrimeNet 3.0 and George started designing Prime95 v15. Unlike v14, v15 integrated a full suite of basic PrimeNet APIs. Support for the public version of PrimeNet 2.6 continued.

* October-November 1997
Testing of PrimeNet 2.8 was underway. In November just before Thanksgiving, PrimeNet 2.8 replaced the 2.6 server on the Internet, taking over the extant 200+ machines running v14, which had grown to about 500 computers. This is why

PrimeNet's statistics charts start on 23 November. Work on PrimeNet 3.0 and Prime95 v15 was also now in full swing.

* December 1997
Final development and testing of PrimeNet 3.0 and Prime95 v15 wrapped up.

* January 1998
On 3 January 1998, PrimeNet 3.0 replaced the 2.8 server on the Internet, v15 released, and GIMPS officially converted to using Entropia.com, Inc.'s PrimeNet. Of course, we got lucky; prime $2^{3021377} - 1$ was found less than a month later!

* February-June 1998
Support for the public version of PrimeNet 2.6 for v14 continued on the web site until more than 99.5% of GIMPS used PrimeNet in June 1998. Entropia.com continued promoting v15 for use on the Internet PrimeNet 3.0 server.

* July-September 1998
Entropia.com software is redesigned for scalability and general-purpose use. Base software system layers are rewritten.

* October-November 1998
PrimeNet 4.0 is redesigned and entirely rewritten to use the new Entropia.com architecture.

* December 1998 - January 1999
PrimeNet 4.0 is tested; final components are written.

* February 1999
PrimeNet 3.0, a P166 server (which by now suffered under the load of over 15,000 computers) is upgraded the 3.0 system to the faster, stronger dual P350 and 4.0 system architecture we have today. There was a lot of cleanup work to complete the transition to 4.0, but by the end of the month, things were running fairly smoothly.

* March-April 1999
EFF.org preparations are completed. EFF announces the Cooperative Computing Awards.

* May 1999
Entropia.com hires KQED for two brief promotional radio ads. A few thousand new GIMPS users sign up.

* June 1999
Prime $2^{6972593} - 1$ is discovered.