The Search for Mersenne Primes

The history of the search for Mersenne primes can be divided into the eras before and after the advent of computers. In precomputer days, the search was littered with errors and unsubstantiated claims, many turning out to be false. By 1588, Pietro Cataldi had verified that M_{17} and M_{19} were primes, but he also stated, without any justification, that M_p was prime for $p = 23, 29, 31$, and 37 (of these, only M_{31} is prime). In his *Cogitata Physica-Mathematica,* published in 1644, Mersenne claimed (without providing a justification) that M_p is prime for $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127$, and 257, and for no other prime p with $p < 257$. In 1772, Euler showed that M_{31} was prime, using trial division by all primes up to 46,339, which is the largest prime not exceeding the square root of M_{31}. In 1811, the English mathematician Peter Barlow wrote in his *Theory of Numbers* that M_{31} would be the greatest Mersenne prime ever found—he thought that no one would ever attempt to find a larger Mersenne prime because they are "merely curious, without being useful." This turned out to be a terrible prediction; not only was Barlow wrong about people finding new Mersenne primes, but he was wrong about their utility, as our subsequent comments will show.

In 1876, Lucas used the test that he had developed to show that M_{67} was composite without finding a factorization; it took an additional twenty-seven years for M_{67} to be factored. The American mathematician Frank Cole devoted 20 years of Sunday afternoon computations to discover that $M_{67} = 193{,}707{,}721 \cdot 761{,}838{,}257{,}287$. When he presented this result at a meeting of the American Mathematical Society in 1903, writing the factorization on a blackboard and not saying a word, the audience gave him a standing ovation, as they understood how much work had been required to find this factorization. The numbers M_{61}, M_{89}, M_{107}, and M_{127} were shown to be prime between 1876 and 1914. But it was not until 1947 that the primality of M_p for all primes p not exceeding 257 was tested, with the help of mechanical calculating machines. When this work was done, it was seen that Mersenne had made exactly five mistakes. He was wrong when he stated that M_{67} and M_{257} are primes, and he failed to include the Mersenne primes M_{61}, M_{89}, and M_{107} in his list.

As we have seen, only twelve Mersenne primes were known before the advent of modern computers, the last of which was discovered in 1914. But since the invention of computers, new Mersenne primes have been found at a fairly steady rate, averaging about one new Mersenne prime every two years since 1950. The first five Mersenne primes found with the help of a computer were the 13th through the 17th Mersenne primes. All five were found in 1952 by Raphael Robinson, using SWAC (the National Bureau of Standards Western Automatic Computer) with the help of D.H. and Emma Lehmer. The thirteenth and fourteenth Mersenne primes were found the first day SWAC was used to run the Lucas-Lehmer test, and the other three were found in the following nine months. Compared to computers today, SWAC was primitive. Its total memory was 1152 bytes, and half of this was used for the commands that ran the program. It is interesting to note that Robinson's program to implement the Lucas-Lehmer test was the first program he ever wrote.

Riesel found the eighteenth Mersenne prime using the Swedish BESK computer, Hurwitz found the nineteenth and twentieth Mersenne primes using the IBM 7090, and

FROM "ELEMENTARY NUMBER THEORY AND ITS APPLICATIONS" BY KENNETH ROSEN

Gillies found the twenty-first, twenty-second, and twenty-third Mersenne primes using the ILLIAC 2. Tuckerman found the twenty-fourth Mersenne prime using the IBM 360.

The twenty-fifth and twenty-sixth Mersenne primes were found by high school students Laura Nickel and Landon Noll using idle time on the Cyber 174 computer at California State Unversity, Hayward. Nickel and Noll, who were eighteen years old at the time, were also studying number theory with D.H. Lehmer and CSU professor Dan Jurca. Their discoveries were announced on the nightly news shows of major networks around the world. Nickel and Noll discovered the twenty-fifth Mersenne prime together, while only Noll went on to discover the twenty-sixth Mersenne prime by himself.

David Slowinski, working with several different collaborators, discovered the nth Mersenne prime for $n = 27$, 28, 30, 31, 32, 33, and 34 between 1979 and 1996. For example, Slowinski and Gage found the Mersenne prime $M_{1,257,787}$, a number with 378,632 digits, in 1996. The proof that this number is prime took approximately six hours on a Cray supercomputer. The Mersenne prime that Slowinski missed, the twenty-ninth, was found by Colquitt and Welsh in 1988 using a NEC SX-2 computer. You may wonder how Slowinski overlooked this prime. The reason is that he did not check whether M_p is prime for consecutive primes, but instead jumped around following hunches about the distribution of Mersenne primes, just as many researchers have done.

The Internet is another factor accelerating the discovery of Mersenne primes. Many people are cooperating to find new Mersenne primes as part of the Great Internet Mersenne Prime Search (GIMPS), founded by George Woltman in 1996. Approximately 700 billion floating point operations per second (0.7 Teraflops) are devoted to GIMPS on PrimeNet, the network linking the distributed computers in GIMPS into one virtual supercomputer. This virtual supercomputer is now the equivalent of more than a dozen of the largest supercomputers in the world, even though most of the individual computers used are Pentium PCs.

The four largest Mersenne primes known, the thirty-fourth through the thirty-eighth, were all found as part of the GIMPS project, with $M_{1,398,269}$ and $M_{2,976,221}$ discovered to be prime in 1996 and 1997, respectively. The Mersenne prime $M_{2,976,221}$ was shown to be prime using a 100 MHz Pentium computer using about fifteen days of CPU time. In January 1998, $M_{3,021,377}$, a number with 909,526 decimal digits, was found to be prime by GIMPS. The lucky person who made this discovery, Roland Clarkson, was a nineteen-year-old student at California State University, Dominguez Hills, at the time. He used a 200 MHz Pentium computer, taking the equivalent of about a week of full-time CPU processing, to find this prime. The largest Mersenne prime known at the time this book was written, $M_{6,972,593}$, a number with 2,098,960 decimal digits, was found in June 1999 by Nayan Hajratwala, a GIMPS participant, using a 350 MHz Pentium computer, using the equivalent of about three weeks of uninterrupted processing. (See Table 7.3 for a list of all the currently known Mersenne primes, along with information about their discovery.)

Why do people look for Mersenne primes? Many people are devoted to the quest for new Mersenne primes. Why do they spend so much time and energy on this task? There are many reasons. The discovery of a new Mersenne prime brings fame and notoriety.

Number	p	Decimal digits in M_p	Date of discovery	Discoverer(s)	Computer used
1	2	1	ancient times		
2	3	1	ancient times		
3	5	2	ancient times		
4	7	3	ancient times		
5	13	4	1456	anonymous	
6	17	6	1588	Cataldi	
7	19	6	1588	Cataldi	
8	31	10	1772	Euler	
9	61	19	1883	Pervushin	
10	89	27	1911	Powers	
11	107	33	1914	Powers	
12	127	39	1876	Lucas	
13	521	157	1952	Robinson	SWAC
14	607	183	1952	Robinson	SWAC
15	1279	386	1952	Robinson	SWAC
16	2203	664	1952	Robinson	SWAC
17	2281	687	1952	Robinson	SWAC
18	3217	969	1957	Riesel	BESK
19	4253	1281	1961	Hurwitz	IBM 7090
20	4423	1332	1961	Hurwitz	IBM 7090
21	9689	2917	1963	Gillies	ILLIAC 2
22	9941	2993	1963	Gillies	ILLIAC 2
23	11,213	3376	1963	Gillies	ILLIAC 2
24	19,937	6002	1971	Tuckerman	IBM 360/91
25	21,701	6533	1978	Noll, Nickel	Cyber 174
26	23,209	6987	1979	Noll	Cyber 174
27	44,497	13,395	1979	Nelson, Slowinski	Cray 1
28	86,243	25,962	1983	Slowinski	Cray 1
29	110,503	33,265	1988	Colquitt, Welsh	NEC SX-2
30	132,049	39,751	1983	Slowinski	Cray X-MP
31	216,091	65,050	1985	Slowinski	Cray X-MP
32	756,839	227,832	1992	Slowinski, Gage	Cray 2
33	859,433	258,716	1994	Slowinski, Gage	Cray 2
34	1,257,787	378,632	1996	Slowinski, Gage	Cray T94
35	1,398,269	420,921	1996	Armendgaud, Woltman (GIMPS)	90 MHz Pentium
36	2,976,221	895,952	1997	Spence, Woltman (GIMPS)	100 MHz Pentium
37	3,021,377	909,526	1998	Clarkson, Woltman, Kurowski (GIMPS, PrimeNet)	200 MHz Pentium
38	6,972,593	2,098,960	1999	Hajratwala, Woltman, Kurowksi (GIMPS, PrimeNet)	350 MHz Pentium

Table 7.3 *The known mersenne primes.*

Some people may be motivated by the recent cash prizes being offered for finding new Mersenne primes; other people like to contribute to team efforts. By joining GIMPS and PrimeNet, anyone can begin making useful contributions to the search for new Mersenne primes. The quest for new Mersenne primes has sparked the development of new theoretical results, and this has motivated many people; others are interested in the distribution of primes and want evidence to use as the basis for conjectures. Many people have used software for the Lucas-Lehmer test to check out new hardware platforms, as these programs are CPU and computer bus intensive. For example, the Intel Pentium II chip was tested using GIMPS software. Some people would rather have their computer look for Mersenne primes during idle time, than run a screen-saver. For these and other reasons, many people look for Mersenne primes.

If you catch the bug and become interested in the search for Mersenne primes, you should investigate the GIMPS Web site, as well as several other relevant Web sites (links for these can be found in Appendix D and on the Web site for this book). At the GIMPS site, you can obtain a program for running the Lucas-Lehmer test, and learn how to join PrimeNet. The GIMPS program for running the Lucas-Lehmer test has been optimized in many ways, so that it runs much more efficiently than a naive implementation of the test. You can reserve a particular range of exponents to check. If history is a guide, it should not be too much longer before the world's record for Mersenne (and all) primes is smashed. If you join GIMPS, you may be the lucky one to break this record!

Odd Perfect Numbers

We have reduced the study of even perfect numbers to the study of Mersenne primes. But are there odd perfect numbers? The answer is still unknown. It is possible to demonstrate that if they exist, odd perfect numbers must have certain properties (see Exercises 32–36 for example). Furthermore, it is known that there are no odd perfect numbers less than 10^{300}; an odd perfect number must have at least eight different prime divisors and at least twenty-nine prime divisors counting multiplicities; and the largest prime factor of the number must be at least 10^{20}. A discussion of odd perfect numbers may be found in [Gu94] or [Ri96], and information about recent results may be found in [BrCote93], [Co87], and [Ha83].

A Prime Jackpot. When Nayan Hajratwala found the Mersenne prime $2^{6,972,593} - 1$, he was the first person to find a prime with more than one million decimal digits. This made him eligible for a prize of $50,000 from the Electronic Frontier Foundation (EFF), an organization devoted to protecting the health and growth of the Internet. You still have a chance to collect a prize from the EFF by finding large primes. They offer $100,000 for the first person who finds a prime with ten million digits, a prize that most likely will be claimed within the next few years. Prizes of $150,000 and $250,000 are offered for the first person to find a prime with one hundred million and one billion decimal digits, respectively. An anonymous donor has funded these prizes to spur cooperative work on scientific problems that involve massive computation.