Mersenne prime

From Wikipedia, the free encyclopedia

In mathematics, a **Mersenne prime** is a prime number that is one less than a power of two. That is, it is a prime number that can be written in the form $M_n = 2^n - 1$ for some integer n. They are named after Marin Mersenne, a French Minim friar, who studied them in the early 17th century. The first four Mersenne primes (sequence A000668 in OEIS) are 3, 7, 31, and 127.

Mersenne prime

Named after	Marin Mersenne
Publication year	1536[1]
Author of publication	Regius, H.
Number of known terms	49
Conjectured number of terms	Infinite
Subsequence of	Mersenne numbers
First terms	3, 7, 31, 127
Largest known term	$2^{74,207,281} - 1$ (January 2016)
OEIS index	A000668 (https://oeis.org/A000668)

If n is a composite number then so is $2^n - 1$. ($2^{ab} - 1$ is divisible by both $2^a - 1$ and $2^b - 1$.) The definition is therefore unchanged when written $M_p = 2^p - 1$ where p is assumed prime.

More generally, numbers of the form $M_n = 2^n - 1$ without the primality requirement are called **Mersenne numbers**. Mersenne numbers are sometimes defined to have the additional requirement that n be prime, equivalently that they be pernicious Mersenne numbers, namely those pernicious numbers whose binary representation contains no zeros. The smallest composite pernicious Mersenne number is $2^{11} - 1 = 2047 = 23 \times 89$.

Mersenne primes M_p are also noteworthy due to their connection to perfect numbers.

As of January 2016, 49 Mersenne primes are known. The largest known prime number $2^{74,207,281} - 1$ is a Mersenne prime.[2][3]

Since 1997, all newly found Mersenne primes have been discovered by the “Great Internet Mersenne Prime Search” (GIMPS), a distributed computing project on the Internet.

Contents

About Mersenne primes

Unsolved problem in mathematics:

? *Are there infinitely many Mersenne primes?*
(more unsolved problems in mathematics)

Many fundamental questions about Mersenne primes remain unresolved. It is not even known whether the set of Mersenne primes is finite or infinite. The Lenstra–Pomerance–Wagstaff conjecture asserts that there are infinitely many Mersenne primes and predicts their order of growth. It is also not known whether infinitely many Mersenne numbers with prime exponents are composite, although this would follow from widely believed conjectures about prime numbers, for example, the infinitude of Sophie Germain primes congruent to 3 (mod 4), for these primes p, $2p + 1$ (which is also prime) will divide M_p, e.g., $23|M_{11}$, $47|M_{23}$, $167|M_{83}$, $263|M_{131}$, $359|M_{179}$, $383|M_{191}$, $479|M_{239}$, and $503|M_{251}$. (sequence A002515 in OEIS)

The first four Mersenne primes are

$M_2 = 3$, $M_3 = 7$, $M_5 = 31$ and $M_7 = 127$.

A basic theorem about Mersenne numbers states that if M_p is prime, then the exponent p must also be prime. This follows from the identity

$$\begin{aligned}2^{ab}-1&=(2^a-1)\cdot\left(1+2^a+2^{2a}+2^{3a}+\cdots+2^{(b-1)a}\right)\\&=(2^b-1)\cdot\left(1+2^b+2^{2b}+2^{3b}+\cdots+2^{(a-1)b}\right).\end{aligned}$$

This rules out primality for Mersenne numbers with composite exponent, such as $M_4 = 2^4 - 1 = 15 = 3 \times 5 = (2^2 - 1) \times (1 + 2^2)$.

Though the above examples might suggest that M_p is prime for all primes p, this is not the case, and the smallest counterexample is the Mersenne number

$$M_{11} = 2^{11} - 1 = 2047 = 23 \times 89.$$

The evidence at hand does suggest that a randomly selected Mersenne number is much more likely to be prime than an arbitrary randomly selected integer of similar size. Nonetheless, prime M_p appear to grow increasingly sparse as p increases. In fact, of the 2,007,537 prime numbers p up to 32,582,657,[4] M_p is prime for only 44 of them.

The lack of any simple test to determine whether a given Mersenne number is prime makes the search for Mersenne primes a difficult task, since Mersenne numbers grow very rapidly. The Lucas–Lehmer primality test (LLT) is an efficient primality test that greatly aids this task. The search for the largest known prime has somewhat of a cult following. Consequently, a lot of computer power has been expended searching for new Mersenne primes, much of which is now done using distributed computing.

Mersenne primes are used in pseudorandom number generators such as the Mersenne twister, Park–Miller random number generator, Generalized Shift Register and Fibonacci RNG.

Perfect numbers

Mersenne primes M_p are also noteworthy due to their connection to perfect numbers. In the 4th century BC, Euclid proved that if $2^p - 1$ is prime, then $2^{p-1}(2^p - 1)$ is a perfect number. This number, also expressible as $M_p(M_p + 1) / 2$, is the M_p-th triangular number and the 2^{p-1}-th hexagonal number. In the 18th century, Leonhard Euler proved that, conversely, all even perfect numbers have this form.[5] This is known as the Euclid–Euler theorem. It is unknown whether there are any odd perfect numbers.

History

Mersenne primes take their name from the 17th-century French scholar Marin Mersenne, who compiled what was supposed to be a list of Mersenne primes with exponents up to 257, as follows:

```
2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257
```

His list was completely accurate until 31, but then becomes largely incorrect, as Mersenne mistakenly included M_{67} and M_{257} (which are composite), and omitted M_{61}, M_{89}, and M_{107} (which are prime). Mersenne gave little indication how he came up with his list.[6] (sequence A109461 in OEIS)

2	**3**	**5**	**7**	11	**13**	**17**	**19**
23	29	**31**	37	41	43	47	53
59	**61**	**67**	71	73	79	83	**89**
97	101	103	**107**	109	113	**127**	131
137	139	149	151	157	163	167	173
179	181	191	193	197	199	211	223
227	229	233	239	241	251	**257**	263
269	271	277	281	283	293	307	311

The first 64 prime exponents with those corresponding to Mersenne primes shaded in cyan and in bold, and those thought to do so by Mersenne in red and bold.

Édouard Lucas proved in 1876 that M_{127} is indeed prime, as Mersenne claimed. This was the largest known prime number for 75 years, and the largest ever found by hand. M_{61} was determined to be prime in 1883 by Ivan Mikheevich Pervushin, though Mersenne claimed it was composite, and for this reason it is sometimes called Pervushin's number. This was the second-largest known prime number, and it remained so until 1911. Lucas had shown another error in Mersenne's list in 1876. Without finding a factor, Lucas demonstrated that M_{67} is actually composite. No factor was found until a famous talk by Cole in 1903.[7] Without speaking a word, he went to a blackboard and raised 2 to the 67th power, then subtracted one. On the other side of the board, he multiplied

193,707,721 × 761,838,257,287 and got the same number, then returned to his seat (to applause) without speaking.[8] He later said that the result had taken him "three years of Sundays" to find.[9] A correct list of all Mersenne primes in this number range was completed and rigorously verified only about three centuries after Mersenne published his list.

Searching for Mersenne primes

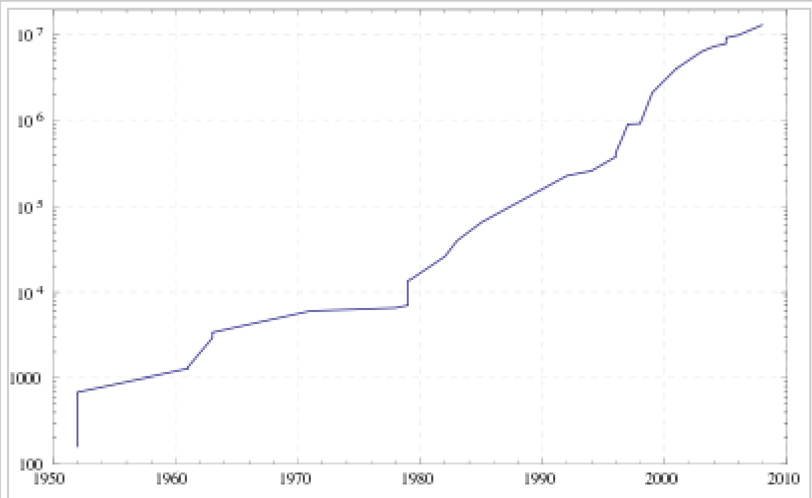
Fast algorithms for finding Mersenne primes are available, and as of 2016 the eleven largest known prime numbers are Mersenne primes.

The first four Mersenne primes $M_2 = 3$, $M_3 = 7$, $M_5 = 31$ and $M_7 = 127$ were known in antiquity. The fifth, $M_{13} = 8191$, was discovered anonymously before 1461; the next two (M_{17} and M_{19}) were found by Cataldi in 1588. After nearly two centuries, M_{31} was verified to be prime by Euler in 1772. The next (in historical, not numerical order) was M_{127}, found by Lucas in 1876, then M_{61} by Pervushin in 1883. Two more (M_{89} and M_{107}) were found early in the 20th century, by Powers in 1911 and 1914, respectively.

The best method presently known for testing the primality of Mersenne numbers is the Lucas–Lehmer primality test. Specifically, it can be shown that for prime $p > 2$, $M_p = 2^p - 1$ is prime if and only if M_p divides S_{p-2}, *where* $S_0 = 4$ *and, for* $k > 0$,

$$S_k = (S_{k-1})^2 - 2$$

The search for Mersenne primes was revolutionized by the introduction of the electronic digital computer. Alan Turing searched for them on the Manchester Mark 1 in 1949,[10] but the first successful identification of a Mersenne prime, M_{521}, by this means was achieved at 10:00 pm on January 30, 1952 using the U.S. National Bureau of Standards Western Automatic Computer (SWAC) at the Institute for Numerical Analysis at the University of California, Los Angeles, under the direction of Lehmer, with a computer search program written and run by Prof. R. M. Robinson. It was the first Mersenne prime to be identified in thirty-eight years; the next one, M_{607}, was found by the computer a little less than two hours later. Three more — M_{1279}, M_{2203}, M_{2281} — were found by the same program in the next several months. M_{4253} is the first Mersenne prime that is titanic, M_{44497} is the first gigantic, and $M_{6,972,593}$ was the first megaprime to be discovered, being a prime with at least 1,000,000 digits.[11] All three were the first known prime of any kind of that size.



Graph of number of digits in largest known Mersenne prime by year – electronic era. Note that the vertical scale, the number of digits, is a double logarithmic scale of the value of the prime.

In September 2008, mathematicians at UCLA participating in GIMPS won part of a $100,000 prize from the Electronic Frontier Foundation for their discovery of a very nearly 13-million-digit Mersenne prime. The prize, finally confirmed in October 2009, is for the first known prime with at least 10 million digits. The prime was found on a Dell OptiPlex 745 on August 23, 2008. This is the eighth Mersenne prime discovered at UCLA.[12]

On April 12, 2009, a GIMPS server log reported that a 47th Mersenne prime had possibly been found. This report was apparently overlooked until June 4, 2009. The find was verified on June 12, 2009. The prime is $2^{42,643,801} - 1$. Although it is chronologically the 47th Mersenne prime to be discovered, it is smaller than the largest known at the time, which was the 45th to be discovered.

On January 25, 2013, Curtis Cooper, a mathematician at the University of Central Missouri, discovered a 48th Mersenne prime, $2^{57,885,161} - 1$ (a number with 17,425,170 digits), as a result of a search executed by a GIMPS server network.[13] This was the third Mersenne prime discovered by Dr. Cooper and his team in the past seven years.

On January 19, 2016, Cooper also published about his discovery of a 49th Mersenne prime, $2^{74,207,281} - 1$ (a number with 22,338,618 digits), as a result of a search executed by a GIMPS server network.[2] This was the fourth Mersenne prime discovered by Dr. Cooper and his team in the past ten years.

Theorems about Mersenne numbers

1. If a and p are natural numbers such that $a^p - 1$ is prime, then $a = 2$ or $p = 1$.
   - **Proof**: $a \equiv 1 \pmod{a-1}$. Then $a^p \equiv 1 \pmod{a-1}$, so $a^p - 1 \equiv 0 \pmod{a-1}$. Thus $a - 1 \mid a^p - 1$. However, $a^p - 1$ is prime, so $a - 1 = a^p - 1$ or $a - 1 = \pm 1$. In the former case, $a = a^p$, hence $a = 0,1$ (which is a contradiction, as neither -1 nor 0 is prime) or $p = 1$. In the latter case, $a = 2$ or $a = 0$. If $a = 0$, however, $0^p - 1 = 0 - 1 = -1$ which is not prime. Therefore, $a = 2$.
2. If $2^p - 1$ is prime, then p is prime.
   - **Proof**: suppose that p is composite, hence can be written $p = a\ b$ with a and $b > 1$. Then $2^p - 1 = 2^{ab} - 1 = (2^a)^b - 1 = (2^a - 1)[(2^a)^{b-1} + (2^a)^{b-2} + \ldots + 2^a + 1]$ so $2^p - 1$ is composite contradicting our assumption that $2^p - 1$ is prime.
3. If p is an odd prime, then every prime q that divides $2^p - 1$ must be 1 plus a multiple of $2p$. This holds even when $2^p - 1$ is prime.
   - **Examples**: Example I: $2^5 - 1 = 31$ is prime, and $31 = 1 + 3 \times (2 \times 5)$. Example II: $2^{11} - 1 = 23 \times 89$, where $23 = 1 + (2 \times 11)$, and $89 = 1 + 4 \times (2 \times 11)$.
   - **Proof**: By Fermat's little theorem, q is a factor of $2^{q-1} - 1$. Since q is a factor of $2^p - 1$, for all positive integers c, q is also a factor of $2^{pc} - 1$. Since p is prime and q is not a factor of $2^1 - 1$, p is also the smallest positive integer x such that q is a factor of $2^x - 1$. As a result, for all positive integers x, q is a factor of $2^x - 1$ if and only if p is a factor of x. Therefore, since q is a factor of $2^{q-1} - 1$, p is a factor of $q - 1$ so $q \equiv 1 \pmod{p}$. Furthermore, since q is a factor of $2^p - 1$, which is odd, q is odd. Therefore, $q \equiv 1 \pmod{2p}$.
   - **Note**: This fact provides a proof of the infinitude of primes distinct from Euclid's theorem: for every odd prime p, all primes dividing $2^p - 1$ are larger than p; thus there are always larger primes than any particular prime.
4. If p is an odd prime, then every prime q that divides $2^p - 1$ is congruent to $\pm 1 \pmod{8}$.
   - **Proof**: $2^{p+1} \equiv 2 \pmod{q}$, so $2^{(p+1)/2}$ is a square root of 2 mod q. By quadratic reciprocity, every prime modulo which the number 2 has a square root is congruent to $\pm 1 \pmod{8}$.
5. A Mersenne prime cannot be a Wieferich prime.
   - **Proof**: We show if $p = 2^m - 1$ is a Mersenne prime, then the congruence $2^p - 1 \equiv 1 \pmod{p^2}$ does not hold. By Fermat's Little theorem, $m \mid p - 1$. Now write, $p - 1 = m\lambda$. If the given congruence is satisfied, then $p^2 \mid 2^{m\lambda} - 1$,therefore $0 \equiv (2^{m\lambda} - 1) / (2^m - 1) = 1 + 2^m + 2^{2m} + ... + 2^{\lambda - 1m} \equiv -\lambda \bmod (2^m - 1)$. Hence $2^m - 1 \mid \lambda$,and therefore $\lambda \geq 2^m - 1$. This leads to $p - 1 \geq m(2^m - 1)$, which is impossible since $m \geq 2$.
6. If m and n are natural numbers then m and n are coprime if and only if 2^m-1 and 2^n-1 are coprime. Consequently a prime number divides at most one prime-exponent Mersenne number,[14] so in other words the set of pernicious Mersenne numbers is pairwise coprime.
7. If p and $2p + 1$ are both prime (meaning that p is a Sophie Germain prime), and p is congruent to

3 (mod 4), then $2p + 1$ divides $2^p - 1$.[15]

- **Example**: 11 and 23 are both prime, and $11 = 2 \times 4 + 3$, so 23 divides $2^{11} - 1$.
- **Proof**: Let q be $2p + 1$. By Fermat's Little theorem, $2^{2p} \equiv 1 \pmod q$, so either $2^p \equiv 1 \pmod q$ or $2^p \equiv -1 \pmod q$. Supposing latter true, then $2^{p+1} = (2^{(p+1)/2})^2 \equiv -2 \pmod q$, so -2 would be a quadratic residue mod q. However, since p is congruent to 3 (mod 4), q is congruent to 7 (mod 8) and therefore 2 is a quadratic residue mod q. Also since q is congruent to 3 (mod 4), -1 is a quadratic nonresidue mod q, so -2 is the product of a residue and a nonresidue and hence it is a nonresidue, which is a contradiction. Hence, the former congruence must be true and $2p + 1$ divides M_p.

8. All composite divisors of prime-exponent Mersenne numbers pass the Fermat primality test for the base 2.
9. The number of digits in the decimal representation of M_n equals $\lfloor n \times \log_{10} 2 \rfloor + 1$, where $\lfloor x \rfloor$ denotes the floor function.

List of known Mersenne primes

The table below lists all known Mersenne primes (sequence A000043 (p) and A000668 (M_p) in OEIS):

#	p	M_p	M_p digits	Discovered	Discoverer	Method used
1	2	3	1	c. 430 BC	Ancient Greek mathematicians[16]	
2	3	7	1	c. 430 BC	Ancient Greek mathematicians[16]	
3	5	31	2	c. 300 BC	Ancient Greek mathematicians[17]	
4	7	127	3	c. 300 BC	Ancient Greek mathematicians[17]	
5	13	8191	4	1456	Anonymous[18][19]	Trial division
6	17	131071	6	1588[20]	Pietro Cataldi	Trial division[21]
7	19	524287	6	1588	Pietro Cataldi	Trial division[22]
8	31	2147483647	10	1772	Leonhard Euler[23][24]	Enhanced trial division[25]
9	61	2305843009213693951	19	1883 November[26]	I. M. Pervushin	Lucas sequences
10	89	618970019642...137449562111	27	1911 June[27]	Ralph Ernest Powers	Lucas sequences
11	107	162259276829...578010288127	33	1914 June 1[28][29][30]	Ralph Ernest Powers[31]	Lucas sequences
12	127	170141183460...715884105727	39	1876 January 10[32]	Édouard Lucas	Lucas sequences
13	521	686479766013...291115057151	157	1952 January 30[33]	Raphael M. Robinson	LLT / SWAC
14	607	531137992816...219031728127	183	1952 January 30[33]	Raphael M. Robinson	LLT / SWAC
15	1,279	104079321946...703168729087	386	1952 June 25[34]	Raphael M. Robinson	LLT / SWAC
16	2,203	147597991521...686697771007	664	1952 October 7[35]	Raphael M. Robinson	LLT / SWAC
17	2,281	446087557183...418132836351	687	1952 October 9[35]	Raphael M. Robinson	LLT / SWAC
18	3,217	259117086013...362909315071	969	1957 September 8[36]	Hans Riesel	LLT / BESK
19	4,253	190797007524...815350484991	1,281	1961 November 3[37][38]	Alexander Hurwitz	LLT / IBM 7090
20	4,423	285542542228...902608580607	1,332	1961 November 3[37][38]	Alexander Hurwitz	LLT / IBM 7090

21	9,689	478220278805...826225754111	2,917	1963 May 11[39]	Donald B. Gillies	LLT / ILLIAC II
22	9,941	346088282490...883789463551	2,993	1963 May 16[39]	Donald B. Gillies	LLT / ILLIAC II
23	11,213	281411201369...087696392191	3,376	1963 June 2[39]	Donald B. Gillies	LLT / ILLIAC II
24	19,937	431542479738...030968041471	6,002	1971 March 4[40]	Bryant Tuckerman	LLT / IBM 360/91
25	21,701	448679166119...353511882751	6,533	1978 October 30[41]	Landon Curt Noll & Laura Nickel	LLT / CDC Cyber 174
26	23,209	402874115778...523779264511	6,987	1979 February 9[42]	Landon Curt Noll	LLT / CDC Cyber 174
27	44,497	854509824303...961011228671	13,395	1979 April 8[43][44]	Harry L. Nelson & David Slowinski	LLT / Cray 1
28	86,243	536927995502...709433438207	25,962	1982 September 25	David Slowinski	LLT / Cray 1
29	110,503	521928313341...083465515007	33,265	1988 January 29[45][46]	Walter Colquitt & Luke Welsh	LLT / NEC SX-2[47]
30	132,049	512740276269...455730061311	39,751	1983 September 19[48]	David Slowinski	LLT / Cray X-MP
31	216,091	746093103064...103815528447	65,050	1985 September 1[49][50]	David Slowinski	LLT / Cray X-MP/24
32	756,839	174135906820...328544677887	227,832	1992 February 17	David Slowinski & Paul Gage	LLT / Harwell Lab's Cray-2[51]
33	859,433	129498125604...243500142591	258,716	1994 January 4[52][53][54]	David Slowinski & Paul Gage	LLT / Cray C90
34	1,257,787	412245773621...976089366527	378,632	1996 September 3[55]	David Slowinski & Paul Gage[56]	LLT / Cray T94
35	1,398,269	814717564412...868451315711	420,921	1996 November 13	GIMPS / Joel Armengaud[57]	LLT / Prime95 on 90 MHz Pentium PC
36	2,976,221	623340076248...743729201151	895,932	1997 August 24	GIMPS / Gordon Spence[58]	LLT / Prime95 on 100 MHz Pentium PC

37	3,021,377	127411683030...973024694271	909,526	1998 January 27	GIMPS / Roland Clarkson[59]	LLT / Prime95 on 200 MHz Pentium PC
38	6,972,593	437075744127...142924193791	2,098,960	1999 June 1	GIMPS / Nayan Hajratwala[60]	LLT / Prime95 on 350 MHz Pentium II IBM Aptiva
39	13,466,917	924947738006...470256259071	4,053,946	2001 November 14	GIMPS / Michael Cameron[61]	LLT / Prime95 on 800 MHz Athlon T-Bird
40	20,996,011	125976895450...762855682047	6,320,430	2003 November 17	GIMPS / Michael Shafer[62]	LLT / Prime95 on 2 GHz Dell Dimension
41	24,036,583	299410429404...882733969407	7,235,733	2004 May 15	GIMPS / Josh Findley[63]	LLT / Prime95 on 2.4 GHz Pentium 4 PC
42	25,964,951	122164630061...280577077247	7,816,230	2005 February 18	GIMPS / Martin Nowak[64]	LLT / Prime95 on 2.4 GHz Pentium 4 PC
43	30,402,457	315416475618...411652943871	9,152,052	2005 December 15	GIMPS / Curtis Cooper & Steven Boone[65]	LLT / Prime95 on 2 GHz Pentium 4 PC
44	32,582,657	124575026015...154053967871	9,808,358	2006 September 4	GIMPS / Curtis Cooper & Steven Boone[66]	LLT / Prime95 on 3 GHz Pentium 4 PC
45[n 1]	37,156,667	202254406890...022308220927	11,185,272	2008 September 6	GIMPS / Hans-Michael Elvenich[67]	LLT / Prime95 on 2.83 GHz Core 2 Duo PC
				2009 April	GIMPS / Odd M.	LLT / Prime95

46[n 1]	42,643,801	169873516452...765562314751	12,837,064	12[n 2]	Strindmo[68][n 3]	on 3 GHz Core 2 PC
47[n 1]	43,112,609	316470269330...166697152511	12,978,189	2008 August 23	GIMPS / Edson Smith[67]	LLT / Prime95 on Dell Optiplex 745
48[n 1]	57,885,161	581887266232...071724285951	17,425,170	2013 January 25	GIMPS / Curtis Cooper[69]	LLT / Prime95 on 3 GHz Intel Core2 Duo E8400[70]
49[n 1]	74,207,281	300376418084...391086436351	22,338,618	2015 September 17[n 4]	GIMPS / Curtis Cooper[2]	LLT / Prime95 on Intel I7-4790 CPU

1. It is not verified whether any undiscovered Mersenne primes exist between the 44th ($M_{32,582,657}$) and the 49th ($M_{74,207,281}$) on this chart; the ranking is therefore provisional.
2. $M_{42,643,801}$ was first found by a machine on April 12, 2009; however, no human took notice of this fact until June 4. Thus, either April 12 or June 4 may be considered the 'discovery' date.
3. Strindmo also uses the alias Stig M. Valstad.
4. $M_{74,207,281}$ was first found by a machine on September 17, 2015; however, no human took notice of this fact until January 7, 2016. Thus, either date may be considered the 'discovery' date. GIMPS considers the January 2016 date to be the official one.

All Mersenne numbers below the 48th Mersenne prime ($M_{57,885,161}$) have been tested at least once but some have not been double-checked. Primes are not always discovered in increasing order. For example, the 29th Mersenne prime was discovered *after* the 30th and the 31st. Similarly, $M_{43,112,609}$ was followed by two smaller Mersenne primes, first 2 weeks later and then 8 months later.[71]

The largest known Mersenne prime ($2^{74,207,281} - 1$) is also the largest known prime number.[2] To help visualize its size, displaying the number in base 10 would require 5,957 pages with 75 digits per line and 50 lines per page. $M_{43,112,609}$ was the first discovered prime number with more than 10 million decimal digits.

In modern times, the largest known prime has almost always been a Mersenne prime.[72]

Factorization of composite Mersenne numbers

The factors of a prime number are by definition one, and the number itself - this section is about composite numbers. Mersenne numbers are very good test cases for the special number field sieve algorithm, so often the largest number factorized with this algorithm has been a Mersenne number. As of October 2014, $2^{1,193} - 1$ is the record-holder,[73] using a variant on the special number field sieve allowing the factorisation of several numbers at once. See integer factorization records for links to more information. The special number field sieve can factorize numbers with more than one large factor. If a number has only one very large factor then other algorithms can factorize larger numbers by first finding small factors and then making a primality test on the cofactor. As of January 2015, the largest factorization with probable prime factors allowed is $2^{3,464,473} - 1 = 604,874,508,299,177 \times q$, where q is a 1,042,896-digit probable prime.[74]

(sequence A244453 in OEIS) (or A089162 with both prime and composite Mersenne numbers) (for the primes p, see A054723)

#	p	Factorization of M_p
1	11	23 × 89
2	23	47 × 178481
3	29	233 × 1103 × 2089
4	37	223 × 616318177
5	41	13367 × 164511353
6	43	431 × 9719 × 2099863
7	47	2351 × 4513 × 13264529
8	53	6361 × 69431 × 20394401
9	59	179951 × 3203431780337 (13 digits)
10	67	193707721 × 761838257287 (12 digits)
11	71	228479 × 48544121 × 212885833
12	73	439 × 2298041 × 9361973132609 (13 digits)
13	79	2687 × 202029703 × 1113491139767 (13 digits)
14	83	167 × 57912614113275649087721 (23 digits)
15	97	11447 × 13842607235828485645766393 (26 digits)
16	101	7432339208719 (13 digits) × 341117531003194129 (18 digits)
17	103	2550183799 × 3976656429941438590393 (22 digits)
18	109	745988807 × 870035986098720987332873 (24 digits)
19	113	3391 × 23279 × 65993 × 1868569 × 1066818132868207 (16 digits)
20	131	263 × 10350794431055162386718619237468234569 (38 digits)
...	...	...
23	149	86656268566282183151 (20 digits) × 8235109336690846723986161 (25 digits)
...	...	...
43	257	535006138814359 (15 digits) × 1155685395246619182673033 (25 digits) × 374550598501810936581776630096313181393 (39 digits)
...	...	...
86	523	160188778313...217468039063 (69 digits) × 171417691861...101859504089 (90 digits)
...	...	...
119	751	227640245125...672549806487 (66 digits) × 649350031993...523089149897 (67 digits) × 801306808403...587821853073 (94 digits)
...	...	...
164	1061	468172263510...207943564433 (143 digits) × 527739642811...707148303247 (177 digits)
...	...	...
172	1109	30963501968569 (14 digits) × 85608965982066833903 (20 digits) × 246160192118...804809798519 (146 digits) × 106580571390...112526589967 (156 digits)
...	...	...
182	1193	121687 × 852273262013...757462472729 (104 digits) × 129706511503...433815839617 (251 digits)
...	...	...

Mersenne primitive part

The primitive part of Mersenne number M_n is Φ_n (2), the n-th cyclotomic polynomial at 2, they are

1, 3, 7, 5, 31, 3, 127, 17, 73, 11, 2047, 13, 8191, 43, 151, 257, 131071, 57, 524287, 205, 2359, 683, 8388607, 241, 1082401, 2731, 262657, 3277, 536870911, 331, ... (sequence A019320 in OEIS)

Besides, if we notice those prime factors, and delete "old prime factors", for example, 3 divides the 2nd, 6th, 18th, 54th, 162nd, ... terms of this sequence, we only allow the 2nd term divided by 3, if we do, they are

1, 3, 7, 5, 31, 1, 127, 17, 73, 11, 2047, 13, 8191, 43, 151, 257, 131071, 19, 524287, 41, 337, 683, 8388607, 241, 1082401, 2731, 262657, 3277, 536870911, 331, ... (sequence A064078 in OEIS)

The numbers n which $\Phi_n(2)$ is prime are

2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 14, 15, 16, 17, 19, 22, 24, 26, 27, 30, 31, 32, 33, 34, 38, 40, 42, 46, 49, 56, 61, 62, 65, 69, 77, 78, 80, 85, 86, 89, 90, 93, 98, 107, 120, 122, 126, 127, 129, 133, 145, 150, ... (sequence A072226 in OEIS)

The numbers n which 2^n - 1 has an only primitive prime factor are

2, 3, 4, 5, 7, 8, 9, 10, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 24, 26, 27, 30, 31, 32, 33, 34, 38, 40, 42, 46, 49, 54, 56, 61, 62, 65, 69, 77, 78, 80, 85, 86, 89, 90, 93, 98, 107, 120, 122, 126, 127, 129, 133, 145, 147, 150, ... (sequence A161508 in OEIS) (Differ from last sequence, this sequence does not have the term 6, but has the terms 18, 20, 21, 54, 147, 342, 602, and 889, and it is conjectured that no others)

Mersenne numbers in nature and elsewhere

In computer science, unsigned n-bit integers can be used to express numbers up to M_n. Signed (n + 1)-bit integers can express values between $-(M_n + 1)$ and M_n, using the two's complement representation.

In the mathematical problem Tower of Hanoi, solving a puzzle with an n-disc tower requires M_n steps, assuming no mistakes are made.[75]

The asteroid with minor planet number 8191 is named 8191 Mersenne after Marin Mersenne, because 8191 is a Mersenne prime (3 Juno, 7 Iris, 31 Euphrosyne and 127 Johanna having been discovered and named during the 19th century).[76]

Mersenne–Fermat primes

A **Mersenne–Fermat number** is defined as $\frac{2^{p^r}-1}{2^{p^{r-1}}-1}$, with p prime, r natural number, and can be written as **MF(*p*, *r*)**, when r = 1, it is a Mersenne number, and when p = 2, it is a Fermat number, the only known Mersenne–Fermat prime with $r > 1$ are

MF(2, 2), MF(3, 2), MF(7, 2), MF(59, 2), MF(2, 3), MF(3, 3), MF(2, 4), and MF(2, 5).[77]

In fact, MF(p, r) = Φ_{p^r} (2), where Φ is the cyclotomic polynomial.

Generalizations

It is natural to try to generalize primes of the form $2^n - 1$ to primes of the form $b^n - 1$ for $b \neq 2$ (and $n > 1$). However (see also theorems above), $b^n - 1$ is always divisible by $b - 1$, so unless $b - 1$ is a unit, the former is not a prime. There are two ways to deal with that:

Complex numbers

In the ring of integers (on real numbers), if $b-1$ is a unit, then b is either 2 or 0. But 2^n-1 are the usual Mersenne primes, and the formula 0^n-1 does not lead to anything interesting. Thus, we can regard a ring of "integers" on complex numbers instead of real numbers, like Gaussian integers and Eisenstein integers.

Gaussian Mersenne primes

If we regard the ring of Gaussian integers, we get the case $b=1+i$ and $b=1-i$, and can ask (WLOG) for what n the number

$$(1+i)^n-1$$

is a *Gaussian prime* which will then be called a **Gaussian Mersenne prime**.[78]

$(1+i)^n-1$ is a Gaussian prime for exponents n:

> 2, 3, 5, 7, 11, 19, 29, 47, 73, 79, 113, 151, 157, 163, 167, 239, 241, 283, 353, 367, 379, 457, 997, 1367, 3041, 10141, 14699, 27529, 49207, 77291, 85237, 106693, 160423, 203789, 364289, 991961, 1203793, 1667321, 3704053, 4792057, ... (sequence A057429 in OEIS)

This sequence is in many ways similar to the list of exponents of ordinary Mersenne primes.

The norms (i.e. squares of absolute values) of these Gaussian primes are rational primes:

> 5, 13, 41, 113, 2113, 525313, 536903681, 140737471578113, ... (sequence A182300 in OEIS).

Eisenstein Mersenne primes

We can also regard the ring of Eisenstein integers, we get the case $b=1+\omega$ and $b=1-\omega$, and can ask for what n the number

$$(1-\omega)^n-1$$

is an *Eisenstein prime* which will then be called a **Eisenstein Mersenne prime**.

$(1-\omega)^n-1$ is an Eisenstein prime for exponents n:

> 2, 5, 7, 11, 17, 19, 79, 163, 193, 239, 317, 353, 659, 709, 1049, 1103, 1759, 2029, 5153, 7541, 9049, 10453, 23743, 255361, 534827, 2237561, ... (sequence A066408 in OEIS)

The norms (i.e. squares of absolute values) of these Eisenstein primes are rational primes:

> 7, 271, 2269, 176419, 129159847, 1162320517, ... (sequence A066413 in OEIS)

Divide an integer

Repunit primes

The other way to deal with the fact that b^n-1 is always divisible by $b-1$, it is to simply take out this factor and ask which n makes

$$\frac{b^n-1}{b-1}$$

to be prime. (The integer b can be either positive or negative). If for example we take $b = 10$, we get n values of 2, 19, 23, 317, 1031, 49081, 86453, 109297, 270343, ... (sequence A004023 in OEIS), corresponding to primes 11, 1111111111111111111, 11111111111111111111111, ... (sequence A004022 in OEIS). These primes are called **repunit primes**. Another example is when we take $b = -12$, we get n values of 2, 5, 11, 109, 193, 1483, 11353, 21419, 21911, 24071, 106859, 139739, ... (sequence A057178 in OEIS), corresponding to primes -11, 19141, 57154490053, ... It is a conjecture that for every integer b which is not a perfect power, there are infinitely many n values such that $\frac{b^n - 1}{b - 1}$ is prime. (since when b is a perfect power, it can be shown that there is at most one n value such that $\frac{b^n - 1}{b - 1}$ is prime)

Least n such that $\frac{b^n - 1}{b - 1}$ is prime are (start with $b = 2$)

> 2, 3, 2, 3, 2, 5, 3, 0, 2, 17, 2, 5, 3, 3, 2, 3, 2, 19, 3, 3, 2, 5, 3, 0, 7, 3, 2, 5, 2, 7, 0, 3, 13, 313, 2, 13, 3, 349, 2, 3, 2, 5, 5, 19, 2, 127, 19, 0, 3, 4229, 2, 11, 3, 17, 7, 3, 2, 3, 2, 7, 3, 5, 0, 19, 2, 19, 5, 3, 2, 3, 2, ... (sequence A084740 in OEIS)

For negative base b, they are (start with $b = -2$)

> 3, 2, 2, 5, 2, 3, 2, 3, 5, 5, 2, 3, 2, 3, 3, 7, 2, 17, 2, 3, 3, 11, 2, 3, 11, 0, 3, 7, 2, 109, 2, 5, 3, 11, 31, 5, 2, 3, 53, 17, 2, 5, 2, 103, 7, 5, 2, 7, 1153, 3, 7, 21943, 2, 3, 37, 53, 3, 17, 2, 7, 2, 3, 0, 19, 7, 3, 2, 11, 3, 5, 2, ... (sequence A084742 in OEIS) (notice this OEIS sequence does not allow $n = 2$)

Least base b such that $\frac{b^{\text{prime}(n)} - 1}{b - 1}$ is prime are

> 2, 2, 2, 2, 5, 2, 2, 2, 10, 6, 2, 61, 14, 15, 5, 24, 19, 2, 46, 3, 11, 22, 41, 2, 12, 22, 3, 2, 12, 86, 2, 7, 13, 11, 5, 29, 56, 30, 44, 60, 304, 5, 74, 118, 33, 156, 46, 183, 72, 606, 602, 223, 115, 37, 52, 104, 41, 6, 338, 217, ... (sequence A066180 in OEIS)

For negative bases b, they are

> 3, 2, 2, 2, 2, 2, 2, 2, 2, 7, 2, 16, 61, 2, 6, 10, 6, 2, 5, 46, 18, 2, 49, 16, 70, 2, 5, 6, 12, 92, 2, 48, 89, 30, 16, 147, 19, 19, 2, 16, 11, 289, 2, 12, 52, 2, 66, 9, 22, 5, 489, 69, 137, 16, 36, 96, 76, 117, 26, 3, ... (sequence A103795 in OEIS)

Other generalized Mersenne primes

Another generized Mersenne number is

$$\frac{a^n - b^n}{a - b}$$

with a, b any coprime integers, $a > 1$, $-a < b < a$. (Since $a^n - b^n$ is always divisible by $a - b$, the division is necessary for there to be any chance of finding prime numbers. In fact, this number is the same as the Lucas number $U_n(a + b, ab)$, since a and b are the roots of the quadratic equation $x^2 - (a + b)x + ab = 0$, and this number equals 1 when $n = 1$) We can ask which n make this number prime. It can be shown that such n must be primes themselves or equal to 4, and n can be 4 if and only if $a + b = 1$ and $a^2 + b^2$ is prime. (Since $\frac{a^4 - b^4}{a - b} = (a + b)(a^2 + b^2)$. Thus, in this case the pair (a, b) must be $(x + 1, -x)$ and $x^2 + (x + 1)^2$ must be prime. That is, x must in A027861.) It is a conjecture that for any pair (a, b) such that for every natural number $r > 1$, a and b are not both perfect rth powers, and if $b < 0$, the absolute values of a and b are not "one is a fourth power, the other is 4 times a fourth power".

there are infinitely many values of n such that $\frac{a^n - b^n}{a - b}$ is prime. (When a and b are both perfect rth powers for an $r > 1$ or when $b < 0$ and one of their absolute values is a fourth power, the other is 4 times a fourth power, it can be shown that there are at most two n values with this property.) However, this has not been proved for any single value of (a, b).

a	b	numbers n such that $\frac{a^n - b^n}{a - b}$ is prime (some large terms are only probable primes, these n are checked up to 100000 for $\lvert b\rvert \leq 5$ or $\lvert b\rvert = a - 1$, 20000 for $5 < \lvert b\rvert < a - 1$)	OEIS sequence
2	1	2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243, 110503, 132049, 216091, 756839, 859433, 1257787, 1398269, 2976221, 3021377, 6972593, 13466917, 20996011, 24036583, 25964951, 30402457, 32582657, ..., 37156667, ..., 42643801, ..., 43112609, ..., 57885161, ...	A000043
2	−1	3, 4, 5, 7, 11, 13, 17, 19, 23, 31, 43, 61, 79, 101, 127, 167, 191, 199, 313, 347, 701, 1709, 2617, 3539, 5807, 10501, 10691, 11279, 12391, 14479, 42737, 83339, 95369, 117239, 127031, 138937, 141079, 267017, 269987, 374321, 986191, 4031399, ..., 13347311, 13372531, ...	A000978
3	2	2, 3, 5, 17, 29, 31, 53, 59, 101, 277, 647, 1061, 2381, 2833, 3613, 3853, 3929, 5297, 7417, 90217, 122219, 173191, 256199, 336353, 485977, 591827, 1059503, ...	A057468
3	1	3, 7, 13, 71, 103, 541, 1091, 1367, 1627, 4177, 9011, 9551, 36913, 43063, 49681, 57917, 483611, 877843, ...	A028491
3	−1	2, 3, 5, 7, 13, 23, 43, 281, 359, 487, 577, 1579, 1663, 1741, 3191, 9209, 11257, 12743, 13093, 17027, 26633, 104243, 134227, 152287, 700897, 1205459, ...	A007658
3	−2	3, 4, 7, 11, 83, 149, 223, 599, 647, 1373, 8423, 149497, 388897, ...	A057469
4	3	2, 3, 7, 17, 59, 283, 311, 383, 499, 521, 541, 599, 1193, 1993, 2671, 7547, 24019, 46301, 48121, 68597, 91283, 131497, 148663, 184463, 341233, ...	A059801
4	1	2 (no others)	
4	−1	2, 3 (no others)	
4	−3	3, 5, 19, 37, 173, 211, 227, 619, 977, 1237, 2437, 5741, 13463, 23929, 81223, 121271, ...	A128066
5	4	3, 43, 59, 191, 223, 349, 563, 709, 743, 1663, 5471, 17707, 19609, 35449, 36697, 45259, 91493, 246497, 265007, 289937, ...	A059802
5	3	13, 19, 23, 31, 47, 127, 223, 281, 2083, 5281, 7411, 7433, 19051, 27239, 35863, 70327, ...	A121877
5	2	2, 5, 7, 13, 19, 37, 59, 67, 79, 307, 331, 599, 1301, 12263, 12589, 18443, 20149, 27983, ...	A082182
5	1	3, 7, 11, 13, 47, 127, 149, 181, 619, 929, 3407, 10949, 13241, 13873, 16519, 201359, 396413, ...	A004061
5	−1	5, 67, 101, 103, 229, 347, 4013, 23297, 30133, 177337, 193939, 266863, 277183, 335429, ...	A057171
5	−2	2, 3, 17, 19, 47, 101, 1709, 2539, 5591, 6037, 8011, 19373, 26489, 27427, ...	A082387
5	−3	2, 3, 5, 7, 17, 19, 109, 509, 661, 709, 1231, 12889, 13043, 26723, 43963, 44789, ...	A122853
5	−4	4, 5, 7, 19, 29, 61, 137, 883, 1381, 1823, 5227, 25561, 29537, 300893, ...	A128335
6	5	2, 5, 11, 13, 23, 61, 83, 421, 1039, 1511, 31237, 60413, 113177, 135647, 258413, ...	A062572
6	1	2, 3, 7, 29, 71, 127, 271, 509, 1049, 6389, 6883, 10613, 19889, 79987, 608099, ...	A004062
6	−1	2, 3, 11, 31, 43, 47, 59, 107, 811, 2819, 4817, 9601, 33581, 38447, 41341, 131891, 196337, ...	A057172
6	−5	3, 4, 5, 17, 397, 409, 643, 1783, 2617, 4583, 8783, ...	A128336
7	6	2, 3, 7, 29, 41, 67, 1327, 1399, 2027, 69371, 86689, 355039, ...	A062573
7	5	3, 5, 7, 113, 397, 577, 7573, 14561, 58543, ...	A128344
7	4	2, 5, 11, 61, 619, 2879, 2957, 24371, 69247, ...	A213073
7	3	3, 7, 19, 109, 131, 607, 863, 2917, 5923, 12421, ...	A128024
7	2	3, 7, 19, 79, 431, 1373, 1801, 2897, 46997, ...	A215487
7	1	5, 13, 131, 149, 1699, 14221, 35201, 126037, 371669, 1264699, ...	A004063

7	−1	3, 17, 23, 29, 47, 61, 1619, 18251, 106187, 201653, ...	A057173
7	−2	2, 5, 23, 73, 101, 401, 419, 457, 811, 1163, 1511, 8011, ...	A125955
7	−3	3, 13, 31, 313, 3709, 7933, 14797, 30689, 38333, ...	A128067
7	−4	2, 3, 5, 19, 41, 47, 8231, 33931, 43781, 50833, 53719, 67211, ...	A218373
7	−5	2, 11, 31, 173, 271, 547, 1823, 2111, 5519, 7793, 22963, 41077, 49739, ...	A128337
7	−6	3, 53, 83, 487, 743, ...	A187805
8	7	7, 11, 17, 29, 31, 79, 113, 131, 139, 4357, 44029, 76213, 83663, 173687, 336419, 615997, ...	A062574
8	5	2, 19, 1021, 5077, 34031, 46099, 65707, ...	A128345
8	3	2, 3, 7, 19, 31, 67, 89, 9227, 43891, ...	A128025
8	1	3 (no others)	
8	−1	2 (no others)	
8	−3	2, 5, 163, 191, 229, 271, 733, 21059, 25237, ...	A128068
8	−5	2, 7, 19, 167, 173, 223, 281, 21647, ...	A128338
8	−7	4, 7, 13, 31, 43, 269, 353, 383, 619, 829, 877, 4957, 5711, 8317, 21739, 24029, 38299, ...	A181141
9	8	2, 7, 29, 31, 67, 149, 401, 2531, 19913, 30773, 53857, 170099, ...	A059803
9	7	3, 5, 7, 4703, 30113, ...	
9	5	3, 11, 17, 173, 839, 971, 40867, 45821, ...	A128346
9	4	2 (no others)	
9	2	2, 3, 5, 13, 29, 37, 1021, 1399, 2137, 4493, 5521, ...	A173718
9	1	(none)	
9	−1	3, 59, 223, 547, 773, 1009, 1823, 3803, 49223, 193247, 703393, ...	A057175
9	−2	2, 3, 7, 127, 283, 883, 1523, 4001, ...	A125956
9	−4	2, 3, 5, 7, 11, 17, 19, 41, 53, 109, 167, 2207, 3623, 5059, 5471, 7949, 21211, 32993, 60251, ...	A211409
9	−5	3, 5, 13, 17, 43, 127, 229, 277, 6043, 11131, 11821, ...	A128339
9	−7	2, 3, 107, 197, 2843, 3571, 4451, ..., 31517, ...	
9	−8	3, 7, 13, 19, 307, 619, 2089, 7297, 75571, 76103, 98897, ...	A187819
10	9	2, 3, 7, 11, 19, 29, 401, 709, 2531, 15787, 66949, 282493, ...	A062576
10	7	2, 31, 103, 617, 10253, 10691, ...	
10	3	2, 3, 5, 37, 599, 38393, 51431, ...	A128026
10	1	2, 19, 23, 317, 1031, 49081, 86453, 109297, 270343, ...	A004023
10	−1	5, 7, 19, 31, 53, 67, 293, 641, 2137, 3011, 268207, ...	A001562
10	−3	2, 3, 19, 31, 101, 139, 167, 1097, 43151, 60703, 90499, ...	A128069
10	−7	2, 3, 5, 11, 19, 1259, 1399, 2539, 2843, 5857, 10589, ...	
10	−9	4, 7, 67, 73, 1091, 1483, 10937, ...	A217095
11	10	3, 5, 19, 311, 317, 1129, 4253, 7699, 18199, 35153, 206081, ...	A062577
11	9	5, 31, 271, 929, 2789, 4153, ...	
11	8	2, 7, 11, 17, 37, 521, 877, 2423, ...	
11	7	5, 19, 67, 107, 593, 757, 1801, 2243, 2383, 6043, 10181, 11383, 15629, ...	
11	6	2, 3, 11, 163, 191, 269, 1381, 1493, ...	
11	5	5, 41, 149, 229, 263, 739, 3457, 20269, 98221, ...	A128347

11	4	3, 5, 11, 17, 71, 89, 827, 22307, 45893, 63521, ...	A216181
11	3	3, 5, 19, 31, 367, 389, 431, 2179, 10667, 13103, 90397, ...	A128027
11	2	2, 5, 11, 13, 331, 599, 18839, 23747, 24371, 29339, 32141, 67421, ...	A210506
11	1	17, 19, 73, 139, 907, 1907, 2029, 4801, 5153, 10867, 20161, 293831, ...	A005808
11	−1	5, 7, 179, 229, 439, 557, 6113, 223999, 327001, ...	A057177
11	−2	3, 5, 17, 67, 83, 101, 1373, 6101, 12119, 61781, ...	A125957
11	−3	3, 103, 271, 523, 23087, 69833, ...	A128070
11	−4	2, 7, 53, 67, 71, 443, 26497, ...	A224501
11	−5	7, 11, 181, 421, 2297, 2797, 4129, 4139, 7151, 29033, ...	A128340
11	−6	2, 5, 7, 107, 383, 17359, 21929, ...	
11	−7	7, 1163, 4007, 10159, ...	
11	−8	2, 3, 13, 31, 59, 131, 223, 227, 1523, ...	
11	−9	2, 3, 17, 41, 43, 59, 83, ...	
11	−10	53, 421, 647, 1601, 35527, ...	A185239
12	11	2, 3, 7, 89, 101, 293, 4463, 70067, ...	A062578
12	7	2, 3, 7, 13, 47, 89, 139, 523, 1051, ...	
12	5	2, 3, 31, 41, 53, 101, 421, 1259, 4721, 45259, ...	A128348
12	1	2, 3, 5, 19, 97, 109, 317, 353, 701, 9739, 14951, 37573, 46889, 769543, ...	A004064
12	−1	2, 5, 11, 109, 193, 1483, 11353, 21419, 21911, 24071, 106859, 139739, ...	A057178
12	−5	2, 3, 5, 13, 347, 977, 1091, 4861, 4967, 34679, ...	A128341
12	−7	2, 3, 7, 67, 79, 167, 953, 1493, 3389, 4871, ...	
12	−11	47, 401, 509, 8609, ...	A213216

(Note: if $b < 0$ and n is even, then the numbers n are not included in the corresponding OEIS sequence)

For more information, see.[79][80][81][82][83][84][85][86]

A conjecture related to the generalized Mersenne primes:[87][88] (the conjecture predicts where is the next generalized Mersenne prime, if the conjecture is true, then there are infinitely many primes for all such (a, b) pairs)

For any integers a, b, which satisfy the conditions:

1. $a > 1, -a < b < a$.
2. a and b are coprime.
3. For every natural number $r > 1$, a and b are not both perfect rth powers. (since when a and b are both perfect rth powers, it can be shown that there are at most two n value such that $\frac{a^n - b^n}{a - b}$ is prime, and these n values are r itself or a root of r, or 2)
4. If $b < 0$, the absolute values of a and b are not "one is a fourth power, the other is 4 times a fourth power". (if so, then the number has aurifeuillean factorization)

has prime numbers of the form

$$R_p(a, b) = \frac{a^p - b^p}{a - b}$$

for prime p, the prime numbers will be distributed near the best fit line

$$Y = G \cdot \log_a(\log_a(R_{(a,b)}(n))) + C$$

where

$$\lim_{n\to\infty} G = \frac{1}{e^\gamma} = 0.561459483566\ldots$$

and there are about

$$(\log_e(N) + m \cdot \log_e(2) \cdot \log_e\left(\log_e(N)) + \frac{1}{\sqrt{N}} - \delta\right) \cdot \frac{e^\gamma}{\log_e(a)}$$

prime numbers of this form less than N.

- e is the base of natural logarithm.
- γ is Euler–Mascheroni constant.
- $\log_a$ is the logarithm in base a.
- $R_{(a,b)}(n)$ is the nth prime number of the form $\frac{a^p - b^p}{a - b}$ for prime p.
- C is a data fit constant which varies with a and b.
- δ is a data fit constant which varies with a and b.
- m is the largest natural number such that a and $-b$ are both 2^{m-1}th powers.

We also have the following three properties:

1. The number of prime numbers of the form $\frac{a^p - b^p}{a - b}$ (with prime p) less than or equal to n is about $e^\gamma \cdot \log_a(\log_a(n))$.
2. The expected number of prime numbers of the form $\frac{a^p - b^p}{a - b}$ with prime p between n and $a \cdot n$ is about e^γ.
3. The probability that number of the form $\frac{a^p - b^p}{a - b}$ is prime (for prime p) is about $\frac{e^\gamma}{p \cdot \log_e(a)}$.

If this conjecture is true, then for all such (a, b) pairs, let q be the nth prime of the form $\frac{a^p - b^p}{a - b}$, the graph "$\log_a(\log_a(q))$ verse n" is almost linear. (See [87])

When $a = b + 1$, it is

$$(b+1)^n - b^n$$

is a difference of two perfect nth powers, and if $a^n - b^n$ is prime, than a must be $b + 1$ or $b - 1$, because it is divisible by $a - b$.

Least n such that $(b + 1)^n - b^n$ is prime are

> 2, 2, 2, 3, 2, 2, 7, 2, 2, 3, 2, 17, 3, 2, 2, 5, 3, 2, 5, 2, 2, 229, 2, 3, 3, 2, 3, 3, 2, 2, 5, 3, 2, 3, 2, 2, 3, 3, 2, 7, 2, 3, 37, 2, 3, 5, 58543, 2, 3, 2, 2, 3, 2, 2, 3, 2, 5, 3, 4663, 54517, 17, 3, 2, 5, 2, 3, 3, 2, 2, 47, 61, 19, ... (sequence A058013 in OEIS)

Least b such that $(b + 1)^{\text{prime}(n)} - b^{\text{prime}(n)}$ is prime are

> 1, 1, 1, 1, 5, 1, 1, 1, 5, 2, 1, 39, 6, 4, 12, 2, 2, 1, 6, 17, 46, 7, 5, 1, 25, 2, 41, 1, 12, 7, 1, 7, 327, 7, 8, 44, 26, 12, 75, 14, 51, 110, 4, 14, 49, 286, 15, 4, 39, 22, 109, 367, 22, 67, 27, 95, 80, 149, 2, 142, ... (sequence

A222119 in OEIS)

See also

- Repunit
- Fermat prime
- Power of 2
- Erdős–Borwein constant
- Mersenne conjectures
- Mersenne twister
- Double Mersenne number
- Prime95 / MPrime
- Great Internet Mersenne Prime Search (GIMPS)
- Largest known prime number
- Titanic prime
- Gigantic prime
- Megaprime
- Wieferich prime
- Wagstaff prime
- Cullen prime
- Woodall prime
- Proth prime
- Solinas prime
- Gillies' conjecture

References

1. Regius, Hudalricus. *Utrisque Arithmetices Epitome*.
2. "Largest Known Prime, 49th Known Mersenne Prime Found!!". *Great Internet Mersenne Prime Search*. Retrieved 2016-01-19.
3. Brook, Robert (January 19, 2016). "Prime number with 22 million digits is the biggest ever found". *New Scientist*. Retrieved 19 January 2016.
4. "Number of primes <= 32582657". Wolfram Alpha. Retrieved 2015-08-08.
5. Chris K. Caldwell, Mersenne Primes: History, Theorems and Lists (http://primes.utm.edu/mersenne/index.html)
6. The Prime Pages, Mersenne's conjecture (http://primes.utm.edu/glossary/page.php?sort=MersennesConjecture).
7. Cole, F. N. (1903), "On the factoring of large numbers", *Bull. Amer. Math. Soc.* **10**: 134–137, doi:10.1090/S0002-9904-1903-01079-9, JFM 34.0216.04
8. Bell, E.T. and Mathematical Association of America (1951). *Mathematics, queen and servant of science*. McGraw-Hill New York. p. 228.
9. "h2g2: Mersenne Numbers". *BBC News*. Archived from the original on December 5, 2014.
10. Brian Napper, The Mathematics Department and the Mark 1 (http://www.computer50.org/mark1/maths.html).
11. The Prime Pages, The Prime Glossary: megaprime (http://primes.utm.edu/glossary/page.php?sort=Megaprime).
12. Maugh II, Thomas H. (2008-09-27). "UCLA mathematicians discover a 13-million-digit prime number". Los Angeles Times. Retrieved 2011-05-21.
13. Tia Ghose. "Largest Prime Number Discovered". Scientific American. Retrieved 2013-02-07.
14. Will Edgington's Mersenne Page (http://www.garlic.com/~wedgingt/mersenne.html)
15. Proof of a result of Euler and Lagrange on Mersenne Divisors (http://primes.utm.edu/notes/proofs/MerDiv2.html)
16. There is no mentioning among the ancient Egyptians of prime numbers, and they did not have any concept for prime numbers known today. In the Rhind papyrus (1650 BC) the Egyptian fraction expansions have fairly different forms for primes and composites, so it may be argued that they knew about prime numbers. See Prime Numbers Divide (http://www.ukessays.com/essays/general-studies/prime-numbers-divide.php) [Retrieved 2012-11-11]. "The Egyptians used ($) in the table above for the first primes r=3, 5, 7, or 11 (also for r=23). Here is another intriguing observation: That the Egyptians stopped the use of ($) at 11 suggests they understood (at least some parts of) Eratosthenes's Sieve 2000 years before Eratosthenes 'discovered' it." The Rhind 2/n Table (http://www.math.buffalo.edu/mad/Ancient-Africa/mad_ancient_egyptroll2-n.html) [Retrieved 2012-11-11]. In the school of Pythagoras (b. about 570 – d. about 495 BC) and the Pythagoreans, we find the first sure observations of prime numbers. Hence the first two Mersenne primes, 3 and 7, were known to and may even be said to have been discovered by them. There is no reference, though, to their special form $2^2 - 1$ and $2^3 - 1$ as such. The sources to the

knowledge of prime numbers among the Pythagoreans are late. The Neoplatonic philosopher Iamblichus, AD c. 245–c. 325, states that the Greek Platonic philosopher Speusippus, c. 408 – 339/8 BC, wrote a book named *On Pythagorean Numbers*. According to Iamblichus this book was based on the works of the Pythagorean Philolaus, c. 470–c. 385 BC, who lived a century after Pythagoras, 570 – c. 495 BC. In his *Theology of Arithmetic* in the chapter *On the Decad*, Iamblichus writes: "Speusippus, the son of Plato's sister Potone, and head of the Academy before Xenocrates, compiled a polished little book from the Pythagorean writings which were particularly valued at any time, and especially from the writings of Philolaus; he entitled the book *On Pythagorean Numbers*. In the first half of the book, he elegantly expounds linear numbers [i.e. prime numbers], polygonal numbers and all sorts of plane numbers, solid numbers and the five figures which are assigned to the elements of the universe, discussing both their individual attributes and their shared features, and their proportionality and reciprocity." *Iamblichus* The Theology of Arithmetic translated by Robin Waterfiled, 1988, p. 112f. (http://www.scribd.com/doc/38568451/Theologoumena-Arithmeticae#page=112) [Retrieved 2012-11-11]. Iamblichus also gives us a direct quote from Speusippus' book where Speusippus among other things writes: "Secondly, it is necessary for a perfect number [the concept "perfect number" is not used here in a modern sense] to contain an equal amount of prime and incomposite numbers, and secondary and composite numbers." *Iamblichus* The Theology of Arithmetic translated by Robin Waterfiled, 1988, p. 113. (http://www.scribd.com/doc/38568451/Theologoumena-Arithmeticae#page=113) [Retrieved 2012-11-11]. For the Greek original text, see Speusippus of Athens: A Critical Study with a Collection of the Related Texts and Commentary by Leonardo Tarán, 1981, p. 140 line 21–22 (http://books.google.se/books?id=cUPXqSb7V1wC&lpg=PA276&ots=Q3QhUOGtvH&dq=Speusippus%20prime&hl=sv&pg=PA140#v=onepage&q&f=false) [Retrieved 2012-11-11] In his comments to Nicomachus of Gerasas's Introduction to Arithmetic, Iamblichus also mentions that Thymaridas, ca. 400 BC – ca. 350 BC, uses the term *rectilinear* for prime numbers, and that Theon of Smyrna, fl. AD 100, uses *euthymetric* and *linear* as alternative terms. Nicomachus of Gerasa, Introduction to Arithmetic, 1926, p. 127 (http://ia700709.us.archive.org//load_djvu_applet.php?file=27/items/NicomachusIntroToArithmetic/nicomachus_introduction_arithmetic.djvu) [Retrieved 2012-11-11] It is unclear though when this said Thymaridas lived. "In a highly suspect passage in Iamblichus, Thymaridas is listed as a pupil of Pythagoras himself." Pythagoreanism (http://plato.stanford.edu/entries/pythagoreanism/#hippasus) [Retrieved 2012-11-11] Before Philolaus, c. 470–c. 385 BC, we have no proof of any knowledge of prime numbers.

17. Euclid's Elements, Book IX, Proposition 36 (http://aleph0.clarku.edu/~djoyce/java/elements/bookIX/propIX36.html)
18. The Prime Pages, Mersenne Primes: History, Theorems and Lists (http://primes.utm.edu/mersenne/).
19. We find the oldest (undisputed) note of the result in Codex nr. 14908, which origins from Bibliotheca monasterii ord. S. Benedicti ad S. Emmeramum Ratisbonensis now in the archive of the Bayerische Staatsbibliothek, see "Halm, Karl / Laubmann, Georg von / Meyer, Wilhelm: Catalogus codicum latinorum Bibliothecae Regiae Monacensis, Bd.: 2,2, Monachii, 1876, p. 250". (http://daten.digitale-sammlungen.de/~db/bsb00008253/images/index.html?fip=193.174.98.30&seite=254) [retrieved on 2012-09-17] The Codex nr. 14908 consists of 10 different medieval works on mathematics and related subjects. The authors of most of these writings are known. Some authors consider the monk Fridericus Gerhart (Amman), 1400–1465 (Frater Fridericus Gerhart monachus ordinis sancti Benedicti astrologus professus in monasterio sancti Emmerani diocesis Ratisponensis et in ciuitate eiusdem) to be the author of the part where the prime number 8191 is mentioned. Geschichte Der Mathematik (http://audio02.archive.org/stream/vorlesungenber02cantuoft#page/238/mode/2up) [retrieved on 2012-09-17] The second manuscript of Codex nr. 14908 has the name "Regulae et exempla arithmetica, algebraica, geometrica" and the 5th perfect number and all is factors, including 8191, are mentioned on folio no. 34 a tergo (backside of p. 34). Parts of the manuscript have been published in Archiv der Mathematik und Physik, 13 (1895), pp. 388–406 (http://archive.org/stream/archivdermathem91unkngoog#page/n389/mode/2up) [retrieved on 2012-09-23]
20. "A i lettori. Nel trattato de' numeri perfetti, che giàfino dell anno 1588 composi, oltrache se era passato auáti à trouarne molti auertite molte cose, se era anco amplamente dilatatala Tauola de' numeri composti , di ciascuno de' quali si vedeano per ordine li componenti, onde preposto unnum." p. 1 in *Trattato de' nvumeri perfetti Di Pietro Antonio Cataldo* 1603. http://fermi.imss.fi.it/rd/bdv?/bdviewer@selid=1373775#
21. pp. 13–18 in *Trattato de' nvumeri perfetti Di Pietro Antonio Cataldo* 1603. http://fermi.imss.fi.it/rd/bdv?/bdviewer@selid=1373775#
22. pp. 18–22 in *Trattato de' nvumeri perfetti Di Pietro Antonio Cataldo* 1603. http://fermi.imss.fi.it/rd/bdv?/bdviewer@selid=1373775#
23. http://bibliothek.bbaw.de/bbaw/bibliothek-digital/digitalequellen/schriften/anzeige/index_html?band=03-nouv/1772&seite:int=36 Nouveaux Mémoires de l'Académie Royale des Sciences et Belles-Lettres 1772, pp. 35–36 *EULER, Leonhard: Extrait d'une lettre à M. Bernoulli, concernant le Mémoire imprimé parmi ceux de 1771. p. 318 [intitulé: Recherches sur les diviseurs de quelques nombres très grands compris dans la somme de la progression géométrique 1 + 101 + 102 + 103 + ... + 10T = S]*. Retrieved 2011-10-02.
24. http://primes.utm.edu/notes/by_year.html#31 The date and year of discovery is unsure. Dates between 1752 and 1772 are possible.
25. Chris K. Caldwell. "Modular restrictions on Mersenne divisors". Primes.utm.edu. Retrieved 2011-05-21.
26. "En novembre de l'année 1883, dans la correspondance de notre Académie se trouve une communication qui contient l'assertion que le nombre $2^{61} - 1$ = 2305843009213693951 est un nombre premier. /…/ Le tome XLVIII des

Mémoires Russes de l'Académie /…/ contient le compte-rendu de la séance du 20 décembre 1883, dans lequel l'objet de la communication du père Pervouchine est indiqué avec précision." Bulletin de l'Académie Impériale des Sciences de St.-Pétersbourg, s. 3, v. 31, 1887, cols. 532–533. http://www.biodiversitylibrary.org/item/107789#page/277/mode/1up [retrieved 2012-09-17] See also Mélanges mathématiques et astronomiques tirés du Bulletin de l'Académie impériale des sciences de St.-Pétersbourg v. 6 (1881–1888), pp. 553–554. See also Mémoires de l'Académie impériale des sciences de St.-Pétersbourg: Sciences mathématiques, physiques et naturelles, vol. 48

27. http://www.jstor.org/stable/2972574 The American Mathematical Monthly, Vol. 18, No. 11 (Nov., 1911), pp. 195–197. The article is signed "DENVER, COLORADO, June, 1911". Retrieved 2011-10-02.
28. "M. E. Fauquenbergue a trouvé ses résultats depuis Février, et j'en ai reçu communication le 7 Juin; M. Powers a envoyé le 1er Juin un cablógramme à M. Bromwich [secretary of London Mathematical Society] pour M_{107}. Sur ma demande, ces deux auteurs m'ont adressé leurs remarquables résultats, et je m'empresse de les publier dans nos colonnes, avec nos felicitations." p. 103, André Gérardin, *Nombres de Mersenne* pp. 85, 103–108 in Sphinx-Œdipe. [Journal mensuel de la curiosité, de concours & de mathématiques.] v. 9, No. 1, 1914.
29. "Power's cable announcing this same result was sent to the London Math. So. on 1 June 1914." Mersenne's Numbers, *Scripta Mathematica*, v. 3, 1935, pp. 112–119 http://primes.utm.edu/mersenne/LukeMirror/lit/lit_008s.htm [retrieved 2012-10-13]
30. http://plms.oxfordjournals.org/content/s2-13/1/1.1.full.pdf Proceedings / London Mathematical Society (1914) s2–13 (1): 1. Result presented at a meeting with London Mathematical Society on June 11, 1914. Retrieved 2011-10-02.
31. The Prime Pages, M_{107}: Fauquembergue or Powers? (http://primes.utm.edu/notes/fauquem.html).
32. http://visualiseur.bnf.fr/CadresFenetre?O=NUMM-3039&I=166&M=chemindefer Presented at a meeting with Académie des sciences (France) on January 10, 1876. Retrieved 2011-10-02.
33. "Using the standard Lucas test for Mersenne primes as programmed by R. M. Robinson, the SWAC has discovered the primes $2^{521} - 1$ and $2^{607} - 1$ on January 30, 1952." D. H. Lehmer, *Recent Discoveries of Large Primes*, Mathematics of Computation, vol. 6, No. 37 (1952), p. 61, http://www.ams.org/journals/mcom/1952-06-037/S0025-5718-52-99404-0/S0025-5718-52-99404-0.pdf [Retrieved 2012-09-18]
34. "The program described in Note 131 (c) has produced the 15th Mersenne prime $2^{1279} - 1$ on June 25. The SWAC tests this number in 13 minutes and 25 seconds." D. H. Lehmer, *A New Mersenne Prime*, Mathematics of Computation, vol. 6, No. 39 (1952), p. 205, http://www.ams.org/journals/mcom/1952-06-039/S0025-5718-52-99387-3/S0025-5718-52-99387-3.pdf [Retrieved 2012-09-18]
35. "Two more Mersenne primes, $2^{2203} - 1$ and $2^{2281} - 1$, were discovered by the SWAC on October 7 and 9, 1952." D. H. Lehmer, *Two New Mersenne Primes*, Mathematics of Computation, vol. 7, No. 41 (1952), p. 72, http://www.ams.org/journals/mcom/1953-07-041/S0025-5718-53-99371-5/S0025-5718-53-99371-5.pdf [Retrieved 2012-09-18]
36. "On September 8, 1957, the Swedish electronic computer BESK established that the Mersenne number $M_{3217} = 2^{3217} - 1$ is a prime." Hans Riesel, *A New Mersenne Prime*, Mathematics of Computation, vol. 12 (1958), p. 60, http://www.ams.org/journals/mcom/1958-12-061/S0025-5718-1958-0099752-6/S0025-5718-1958-0099752-6.pdf [Retrieved 2012-09-18]
37. A. Hurwitz and J. L. Selfridge, *Fermat numbers and perfect numbers*, Notices of the American Mathematical Society, v. 8, 1961, p. 601, abstract 587-104.
38. "If p is prime, $M_p = 2^p - 1$ is called a Mersenne number. The primes M_{4253} and M_{4423} were discovered by coding the Lucas-Lehmer test for the IBM 7090." Alexander Hurwitz, *New Mersenne Primes*, Mathematics of Computation, vol. 16, No. 78 (1962), pp. 249–251, http://www.ams.org/journals/mcom/1962-16-078/S0025-5718-1962-0146162-X/S0025-5718-1962-0146162-X.pdf [Retrieved 2012-09-18]
39. "The primes M_{9689}, M_{9941}, and M_{11213} which are now the largest known primes, were discovered by Illiac II at the Digital Computer Laboratory of the University of Illinois." Donald B. Gillies, *Three New Mersenne Primes and a Statistical Theory*, Mathematics of Computation, vol. 18, No. 85 (1964), pp. 93–97, http://www.ams.org/journals/mcom/1964-18-085/S0025-5718-1964-0159774-6/S0025-5718-1964-0159774-6.pdf [Retrieved 2012-09-18]
40. "On the evening of March 4, 1971, a zero Lucas-Lehmer residue for $p = p_{24} = 19937$ was found. Hence, M_{19937} is the 24th Mersenne prime." Bryant Tuckerman, *The 24th Mersenne Prime*, Proceedings of the National Academy of Sciences of the United States of America, vol. 68:10 (1971), pp. 2319–2320, http://www.pnas.org/content/68/10/2319.full.pdf [Retrieved 2012-09-18]
41. "On October 30, 1978 at 9:40 pm, we found M_{21701} to be prime. The CPU time required for this test was 7:40:20. Tuckerman and Lehmer later provided confirmation of this result." Curt Noll and Laura Nickel, *The 25th and 26th Mersenne Primes*, Mathematics of Computation, vol. 35, No. 152 (1980), pp. 1387–1390, http://www.ams.org/journals/mcom/1980-35-152/S0025-5718-1980-0583517-4/S0025-5718-1980-0583517-4.pdf [Retrieved 2012-09-18]
42. "Of the 125 remaining M_p only M_{23209} was found to be prime. The test was completed on February 9, 1979 at 4:06 after 8:39:37 of CPU time. Lehmer and McGrogan later confirmed the result." Curt Noll and Laura Nickel, *The 25th*

and 26th Mersenne Primes, Mathematics of Computation, vol. 35, No. 152 (1980), pp. 1387–1390, http://www.ams.org/journals/mcom/1980-35-152/S0025-5718-1980-0583517-4/S0025-5718-1980-0583517-4.pdf [Retrieved 2012-09-18]

43. David Slowinski, "Searching for the 27th Mersenne Prime", *Journal of Recreational Mathematics*, v. 11(4), 1978–79, pp. 258–261, MR 80g #10013
44. "The 27th Mersenne prime. It has 13395 digits and equals $2^{44497} - 1$. [...] Its primeness was determined on April 8, 1979 using the Lucas–Lehmer test. The test was programmed on a CRAY-1 computer by David Slowinski & Harry Nelson." (p. 15) "The result was that after applying the Lucas–Lehmer test to about a thousand numbers, the code determined, on Sunday, April 8th, that $2^{44497} - 1$ is, in fact, the 27th Mersenne prime." (p. 17), David Slowinski, "Searching for the 27th Mersenne Prime", *Cray Channels*, vol. 4, no. 1, (1982), pp. 15–17.
45. "An FFT containing 8192 complex elements, which was the minimum size required to test M_{110503}, ran approximately 11 minutes on the SX-2. The discovery of M_{110503} (January 29, 1988) has been confirmed." W. N. Colquitt and L. Welsh, Jr., *A New Mersenne Prime*, Mathematics of Computation, vol. 56, No. 194 (April 1991), pp. 867–870, http://www.ams.org/journals/mcom/1991-56-194/S0025-5718-1991-1068823-9/S0025-5718-1991-1068823-9.pdf [Retrieved 2012-09-18]
46. "This week, two computer experts found the 31st Mersenne prime. But to their surprise, the newly discovered prime number falls between two previously known Mersenne primes. It occurs when p = 110,503, making it the third-largest Mersenne prime known." I. Peterson, *Priming for a lucky strike* Science News; 2/6/88, Vol. 133 Issue 6, pp. 85–85. http://ehis.ebscohost.com/ehost/detail?vid=3&hid=23&sid=9a9d7493-ffed-410b-9b59-b86c63a93bc4%40sessionmgr10&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=afh&AN=8824187 [Retrieved 2012-09-18]
47. "Mersenne Prime Numbers". Omes.uni-bielefeld.de. 2011-01-05. Retrieved 2011-05-21.
48. "Slowinski, a software engineer for Cray Research Inc. in Chippewa Falls, discovered the number at 11:36 a.m. Monday. [i.e. 1983 September 19]" Jim Higgins, "Elusive numeral's number is up" and "Scientist finds big number" in *The Milwaukee Sentinel* – Sep 24, 1983, p. 1, (http://news.google.com/newspapers?id=roFQAAAAIBAJ&sjid=VRIEAAAAIBAJ&pg=1717%2C4841183) p. 11 (http://news.google.com/newspapers?id=roFQAAAAIBAJ&sjid=VRIEAAAAIBAJ&pg=4379%2C4887110) [retrieved 2012-10-23]
49. "The number is the 30th known example of a Mersenne prime, a number divisible only by 1 and itself and written in the form $2^p - 1$, where the exponent p is also a prime number. For instance, 127 is a Mersenne number for which the exponent is 7. The record prime number's exponent is 216,091." I. Peterson, *Prime time for supercomputers* Science News; 9/28/85, Vol. 128 Issue 13, p. 199. http://ehis.ebscohost.com/ehost/detail?vid=4&hid=22&sid=c11090a2-4670-469f-8f75-947b593a56a0%40sessionmgr10&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=afh&AN=8840537 [Retrieved 2012-09-18]
50. "Slowinski's program also found the 28th in 1982, the 29th in 1983, and the 30th [known at that time] this past Labor Day weekend. [i.e. August 31-September 1, 1985]" Rad Sallee, "`Supercomputer'/Chevron calculating device finds a bigger prime number" *Houston Chronicle*, Friday 09/20/1985, Section 1, Page 26, 4 Star Edition (http://www.chron.com/CDA/archives/archive.mpl/1985_39205/supercomputer-chevron-calculating-device-finds-a-b.html) [retrieved 2012-10-23]
51. The Prime Pages, The finding of the 32*nd* Mersenne (http://primes.utm.edu/notes/756839.html).
52. Chris Caldwell, The Largest Known Primes (http://www.math.unicaen.fr/~reyssat/largest.html).
53. Crays press release (http://www.0x07bell.net/WWWMASTER/CrayWWWStuff/prfoldercomp/PRIME_NUMBER.940110.txt)
54. Slowinskis email (https://groups.google.com/forum/#!msg/sci.crypt/XXNkt07IE2s/eDeaWg5-mtIJ)
55. Silicon Graphics' press release http://web.archive.org/web/19970606011821/http://www.sgi.com/Headlines/1996/September/prime.html [Retrieved 2012-09-20]
56. The Prime Pages, A Prime of Record Size! $2^{1257787} - 1$ (http://primes.utm.edu/notes/1257787.html).
57. GIMPS Discovers 35th Mersenne Prime (http://www.mersenne.org/primes/1398269.htm).
58. GIMPS Discovers 36th Known Mersenne Prime (http://www.mersenne.org/primes/2976221.htm).
59. GIMPS Discovers 37th Known Mersenne Prime (http://www.mersenne.org/primes/3021377.htm).
60. GIMPS Finds First Million-Digit Prime, Stakes Claim to $50,000 EFF Award (http://www.mersenne.org/primes/6972593.htm).
61. GIMPS, Researchers Discover Largest Multi-Million-Digit Prime Using Entropia Distributed Computing Grid (http://www.mersenne.org/primes/13466917.htm).
62. GIMPS, Mersenne Project Discovers Largest Known Prime Number on World-Wide Volunteer Computer Grid (http://www.mersenne.org/primes/20996011.htm).
63. GIMPS, Mersenne.org Project Discovers New Largest Known Prime Number, $2^{24,036,583} - 1$ (http://www.mersenne.org/primes/24036583.htm).
64. GIMPS, Mersenne.org Project Discovers New Largest Known Prime Number, $2^{25,964,951} - 1$ (http://www.mersenne.org/primes/25964951.htm).

65. GIMPS, Mersenne.org Project Discovers New Largest Known Prime Number, $2^{30,402,457} - 1$ (http://www.mersenne.org/primes/30402457.htm).
66. GIMPS, Mersenne.org Project Discovers Largest Known Prime Number, $2^{32,582,657} - 1$ (http://www.mersenne.org/primes/32582657.htm).
67. Titanic Primes Raced to Win $100,000 Research Award (http://mersenne.org/primes/m45and46.htm). Retrieved on 2008-09-16.
68. "On April 12th [2009], the 47th known Mersenne prime, $2^{42,643,801} - 1$, a 12,837,064 digit number was found by Odd Magnar Strindmo from Melhus, Norway! This prime is the second largest known prime number, a "mere" 141,125 digits smaller than the Mersenne prime found last August.", *The List of Largest Known Primes Home Page*, http://primes.utm.edu/primes/page.php?id=88847 [retrieved 2012-09-18]
69. "GIMPS Discovers 48th Mersenne Prime, $2^{57,885,161} - 1$ is now the Largest Known Prime.". *Great Internet Mersenne Prime Search*. Retrieved 2016-01-19.
70. "List of known Mersenne prime numbers". Retrieved 29 November 2014.
71. GIMPS Milestones Report (http://www.mersenne.org/report_milestones/). Retrieved 2015-10-04
72. The largest known prime has been a Mersenne prime since 1952, except between 1989 and 1992; see Caldwell, "The Largest Known Prime by Year: A Brief History (http://primes.utm.edu/notes/by_year.html)" from the Prime Pages website, University of Tennessee at Martin.
73. Thorsten Kleinjung, Joppe Bos, Arjen Lenstra "Mersenne Factorization Factory" http://eprint.iacr.org/2014/653.pdf
74. Henri Lifchitz and Renaud Lifchitz. "PRP Top Records". Retrieved 2015-01-08.
75. Petković, Miodrag (2009). *Famous Puzzles of Great Mathematicians*. AMS Bookstore. p. 197. ISBN 0-8218-4814-3.
76. Alan Chamberlin. "JPL Small-Body Database Browser". Ssd.jpl.nasa.gov. Retrieved 2011-05-21.
77. A research of Mersenne and Fermat primes (http://staff.spd.dcu.ie/johnbcos/fermat6.htm)
78. Chris Caldwell: The Prime Glossary: Gaussian Mersenne (http://primes.utm.edu/glossary/xpage/GaussianMersenne.html) (part of the Prime Pages)
79. Ali Zalnezhad, Hossein Zalnezhad, Ghasem Shabani, Mehdi Zalnezhad "Relationships and Algorithm in order to Achieve the Largest Primes" http://arxiv.org/pdf/1503.07688.pdf
80. $(x, 1)$ and $(x, -1)$ for $x = 2$ to 50 (http://www.primenumbers.net/Henri/us/MersFermus.htm)
81. $(x, 1)$ for $x = 2$ to 152 (http://www.fermatquotient.com/PrimSerien/GenRepu.txt)
82. $(x, -1)$ for $x = 2$ to 151 (http://www.fermatquotient.com/PrimSerien/GenRepuP.txt)
83. $(x + 1, x)$ for $x = 1$ to 150 (http://www.fermatquotient.com/PrimSerien/PrimPot.txt)
84. $(x + 1, -x)$ for $x = 1$ to 40 (http://www.fermatquotient.com/PrimSerien/PrimPotP.txt)
85. $(x + 2, x)$ for $x = 1$ to 107 (http://www.fermatquotient.com/PrimSerien/PrimPot2.txt)
86. $(x, -1)$ for $x = 2$ to 200 (https://cs.uwaterloo.ca/journals/JIS/VOL3/DUBNER/dubner.pdf#search=%22107%20811%202819%204817%209601%22)
87. Deriving the Wagstaff Mersenne Conjecture (http://primes.utm.edu/mersenne/heuristic.html)
88. Generalized Repunit Conjecture (https://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind0906&L=NMBRTHRY&P=R295&1=NMBRTHRY&9=A&J=on&d=No+Match%3BMatch%3BMatches&z=4)

External links

Look up ***Mersenne prime*** in Wiktionary, the free dictionary.

Wikinews has related news:

Record size 17.4 million-digit prime found

Two largest known prime numbers discovered just two weeks apart, one qualifies for $100k prize

Distributed computing

- Hazewinkel, Michiel, ed. (2001), "Mersenne number", *Encyclopedia of Mathematics*, Springer, ISBN 978-1-55608-010-4
- GIMPS home page (http://www.mersenne.org)
- GIMPS status (http://v5www.mersenne.org/report_milestones/) — status page gives various statistics on search progress, typically updated every week, including progress towards proving the ordering of primes 42–47
- GIMPS, known factors of Mersenne numbers (http://www.mersenne.org/report_factors/)
- $M_q = (8x)^2 - (3qy)^2$ Property of Mersenne numbers with prime exponent that are composite (http://tony.reix.free.fr/Mersenne/Mersenne8x3qy.pdf) (PDF)
- $M_q = x^2 + d{\cdot}y^2$ math thesis (http://www.math.leidenuniv.nl/scripties/jansen.ps) (PS)
- Grime, James. "31 and Mersenne Primes". *Numberphile*. Brady

Haran.
- Mersenne prime bibliography (http://www.utm.edu/research/primes/mersenne/LukeMirror/biblio.htm) with hyperlinks to original publications

discovers largest known prime number
CMSU computing team discovers another record size prime

- report about Mersenne primes (http://www.taz.de/pt/2005/03/11/a0355.nf/text) — detection in detail **(German)**
- GIMPS wiki (http://mersennewiki.org/index.php/Main_Page)
- Will Edgington's Mersenne Page (https://web.archive.org/web/20141014102940/http://www.garlic.com/~wedgingt/mersenne.html) — contains factors for small Mersenne numbers
- Known factors of Mersenne numbers (http://www.mersenne.org/report_factors/)
- Decimal digits and English names of Mersenne primes (http://www.isthe.com/chongo/tech/math/prime/mersenne.html)
- Prime curios: 2305843009213693951 (http://primes.utm.edu/curios/page.php/2305843009213693951.html)
- Factorization of Mersenne numbers M_n, with n odd, n up to 1199 (http://www.leyland.vispa.com/numth/factorization/cunningham/2-.txt)
- Factorization of Mersenne numbers M_{2n}, $2n$ up to 2398 (n up to 1199) or $2n$ is on the form $8k$+4 up to 4796 (n is on the form $4k$+2 up to 2398) (http://www.leyland.vispa.com/numth/factorization/cunningham/2+.txt)
- Factorization of Mersenne numbers M_n (n up to 1280) (http://oeis.org/A250197/a250197_1.txt)
- Factorization of completely factored Mersenne numbers (https://web.archive.org/web/20141015022019/http://www.garlic.com/~wedgingt/factoredM.txt)
- The Cunningham project, factorization of $b^n \pm 1$, b = 2, 3, 5, 6, 7, 10, 11, 12 (http://homes.cerias.purdue.edu/~ssw/cun/pmain814)
- Factorization of $b^n \pm 1$, $2 \le b \le 12$ (http://www.leyland.vispa.com/numth/factorization/cunningham/main.htm)
- Factorization of $a^n \pm b^n$, with coprime a, b, $2 \le b < a \le 12$ (http://www.leyland.vispa.com/numth/factorization/anbn/main.htm)

MathWorld links

- Weisstein, Eric W., "Mersenne number" (http://mathworld.wolfram.com/MersenneNumber.html), *MathWorld*.
- Weisstein, Eric W., "Mersenne prime" (http://mathworld.wolfram.com/MersennePrime.html), *MathWorld*.
- 47th Mersenne Prime Found (http://mathworld.wolfram.com/news/2009-06-07/mersenne-47/)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Mersenne_prime&oldid=700814838"

Categories: Unsolved problems in mathematics | Classes of prime numbers | Integer sequences

---