Mersenne prime

In mathematics, a Mersenne number, named after Marin Mersenne (a French monk who began the study of these numbers in the early 17th century), is a positive integer that is one less than a power of two:

\[ M_p = 2^p - 1. \]

Some definitions of Mersenne numbers require that the exponent \( p \) be prime, since the associated number must be composite if \( p \) is composite.

A Mersenne prime is a Mersenne number that is prime. It is known\(^2\) that if \( 2^p - 1 \) is prime then \( p \) is prime, so it makes no difference which Mersenne number definition is used. As of October 2009, 47 Mersenne primes are known. The largest known prime number \((2^{43,112,609} - 1)\) is a Mersenne prime.\(^3\) 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.

### Content

- 1 About Mersenne primes
- 2 Searching for Mersenne primes
- 3 Theorems about Mersenne numbers
- 4 History
- 5 List of known Mersenne primes
- 6 Factorization of Mersenne numbers
- 7 Perfect numbers
- 8 Generalization
- 9 Mersenne numbers in nature and elsewhere
- 10 See also
- 11 References
- 12 External links
  - 12.1 MathWorld links

### About Mersenne primes

Many fundamental questions about Mersenne primes remain unresolved. It is not even known whether the set of Mersenne primes is finite. The Lenstra–Pomerance–Wagstaff conjecture asserts that, on the contrary, 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 \( 3 \pmod{4} \).

A basic theorem about Mersenne numbers states that in order for \( M_p \) to be a Mersenne prime, the exponent \( p \) itself must be a prime number. This rules out primality for numbers such as \( M_4 = 2^4 - 1 = 15 \): since the exponent \( 4 = 2 \times 2 \) is composite, the theorem predicts that 15 is also composite; indeed, \( 15 = 3 \times 5 \). The three smallest Mersenne primes are

\[ M_2 = 3, M_3 = 7, M_5 = 31. \]

While it is true that only Mersenne numbers \( M_p \), where \( p = 2, 3, 5, \ldots \) could be prime, often \( M_p \) is not prime even for a prime exponent \( p \). The smallest counterexample is the Mersenne number

\[ 2^{11} - 1 = 2047 = 23 \times 89. \]
which is not prime, even though 11 is a prime number. The lack of an obvious rule to determine whether a given Mersenne number is prime makes the search for Mersenne primes an interesting task, which becomes difficult very quickly, 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.

**Searching for Mersenne primes**

The identity

\[ 2^{2^b - 1} = (2^a - 1) \cdot \left(1 + 2^a + 2^{2a} + \cdots + 2^{(b-1)a}\right) = (2^b - 1) \cdot \left(1 + 2^b + 2^{2b} + \cdots + 2^{(a-1)b}\right) \]

shows that \( M_p \) can be prime only if \( p \) itself is prime, which simplifies the search for Mersenne primes considerably. The converse statement, namely that \( M_p \) is necessarily prime if \( p \) is prime, is false. The smallest counterexample is \( 2^{11} - 1 = 2,047 = 23 \times 89 \), a composite number.

Fast algorithms for finding Mersenne primes are available, and the largest known prime numbers as of 2009 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 \( M_{61} \), found by Lucas in 1876, then \( M_{67} \) 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 \( k > 0 \),

\[ S_k = \frac{S_{k-1}^2 - 2}{S_k - 2} \]

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. But the first successful identification of a Mersenne prime, \( M_{521} \), by this means was achieved at 10:00 P.M. 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. All three were the first known prime of any kind of that size.

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.[6]

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 less than the largest known which was the 45th to be discovered.

### 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:** Suppose \(a \equiv 1 \pmod{p}\) and \(a^p \equiv 1 \pmod{p}\). Then \(a^p - 1 \equiv 0 \pmod{p}\), hence \(a - 1|a^p - 1\). 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 0 nor 1 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 \(p = ab\) with \(a > 1\) and \(b > 1\). Then \((2^a)^b - 1\) is prime, but \(b > 1\) and \(2^a > 2\), contradicting statement 1.

3. If \(p\) is an odd prime, then any 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 is 1 plus a multiple of 2x5. Example II: \(2^{11} - 1 = 23\times89\), where 23 = 1 + 2x11, and 89 = 1 + 8x11.
   - **Proof:** If \(q\) divides \(2^p - 1\) then \(q^k \equiv 1 \pmod{2^p - 1}\) for some \(k\). By Fermat's Little Theorem, \(2^{q-1} \equiv 1 \pmod{q}\). Assume \(p\) and \(q - 1\) are relatively prime, a similar application of Fermat's Little Theorem says that \(q - 1|p - 1\). Thus there is a number \(x \equiv (q-1)/2\) for which \((q - 1)x \equiv 1 \pmod{p}\), and therefore a number \(k\) for which \((q - 1)x - 1 = kp\). Since \(2^{q-1} \equiv 1 \pmod{q}\), raising both sides of the congruence to the power \(x\) gives \(2^{(q - 1)x} \equiv 1 \pmod{q}\), and since \(2^p \equiv 1 \pmod{q}\), raising both sides of the congruence to the power \(k\) gives \(2^{kp} \equiv 1 \pmod{q}\). Thus \(2^{(q - 1)x} \equiv 1 \pmod{q}\), raising both sides of the congruence to the power \(k\) gives \(2^{kp} \equiv 1 \pmod{q}\). But by definition, \((q - 1)x - 1 = kp\), implying that \(2^k \equiv 1 \pmod{q}\); in other words, that \(q\) divides \(1\). Thus the initial assumption that \(p\) and \(q - 1\) are relatively prime is untenable. Since \(p\) is prime \(q - 1\) must be a multiple of \(p\). Of course, if the number \(m\) is odd, then \(q\) will be even, since it is equal to \(mp + 1\). But \(q\) is prime and cannot be equal to \(2\); therefore, \(m\) is even.
   - **Note:** This fact provides a proof of the infinitude of primes distinct from Euclid's Theorem: if there were finitely many primes, with \(p\) being the largest, we reach an immediate contradiction since all primes dividing \(2^p - 1\) must be larger than \(p\).

4. If \(p\) is an odd prime, then any prime \(q\) that divides \(2^p - 1\) must be 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 modulo \(q\). By quadratic reciprocity, any prime modulo which 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 \(2^{p-1} \equiv 1 \pmod{2^m}\) does not satisfy. By Fermat's Little theorem, \(m|p - 1\). Now write, \(p - 1 = ml\). If the given congruence satisfies, then \(p^2 | 2^{ml} - 1\), therefore \(0 \equiv (2^{ml} - 1)/(2^m - 1) = 1 + 2^m + 2^{2m} + \ldots + 2^{(\lambda-1)m} \equiv -\lambda \pmod{2^m - 1}\). Hence \(2^m - 1 | \lambda\), 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. A prime number divides at most one Mersenne number.[7]

### History

Mersenne primes were considered already by Euclid, who found a connection with the perfect numbers. They are named after 17th-century French scholar Marin Mersenne, who compiled what was supposed to be a list of Mersenne primes with exponents up to 257. His list was largely incorrect, as Mersenne mistakenly included \(M_{67}\) and \(M_{257}\) (which are composite), and omitted \(M_{61}\).
Mₙ₉ and M₁₀₇ (which are prime). Mersenne gave little indication how he came up with his list. A correct list of all Mersenne primes in this number range was completed and rigorously verified only about three centuries later.

## List of known Mersenne primes

The table below lists all known Mersenne primes (sequence A000668 in OEIS):

<table>
<thead>
<tr>
<th>#</th>
<th>p</th>
<th>Mₓ</th>
<th>Mₓ digits</th>
<th>Date of discovery</th>
<th>Discoverer</th>
<th>Method used</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>c. 500 BCE</td>
<td>Ancient Greek mathematicians</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>7</td>
<td>1</td>
<td>c. 500 BCE</td>
<td>Ancient Greek mathematicians</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>5</td>
<td>31</td>
<td>2</td>
<td>c. 275 BCE</td>
<td>Ancient Greek mathematicians</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>7</td>
<td>127</td>
<td>3</td>
<td>c. 275 BCE</td>
<td>Ancient Greek mathematicians</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>13</td>
<td>8191</td>
<td>4</td>
<td>1456</td>
<td>Anonymous</td>
<td>Trial division</td>
</tr>
<tr>
<td>6</td>
<td>17</td>
<td>13107</td>
<td>6</td>
<td>1588</td>
<td>Pietro Cataldi</td>
<td>Trial division</td>
</tr>
<tr>
<td>7</td>
<td>19</td>
<td>524287</td>
<td>6</td>
<td>1588</td>
<td>Pietro Cataldi</td>
<td>Trial division</td>
</tr>
<tr>
<td>8</td>
<td>31</td>
<td>2147483647</td>
<td>10</td>
<td>1772</td>
<td>Leonhard Euler</td>
<td>Enhanced trial division</td>
</tr>
<tr>
<td>9</td>
<td>61</td>
<td>2305843009213693951</td>
<td>19</td>
<td>1883</td>
<td>I. M. Pervushin</td>
<td>Lucas sequences</td>
</tr>
<tr>
<td>10</td>
<td>89</td>
<td>618970019...449562111</td>
<td>27</td>
<td>1911</td>
<td>R. E. Powers</td>
<td>Lucas sequences</td>
</tr>
<tr>
<td>11</td>
<td>107</td>
<td>162259276...010288127</td>
<td>33</td>
<td>1914</td>
<td>R. E. Powers</td>
<td>Lucas sequences</td>
</tr>
<tr>
<td>12</td>
<td>127</td>
<td>170141183...884105727</td>
<td>39</td>
<td>1876</td>
<td>Edouard Lucas</td>
<td>Lucas sequences</td>
</tr>
<tr>
<td>13</td>
<td>521</td>
<td>686479766...115057151</td>
<td>157</td>
<td>1952 January 30</td>
<td>Raphael M. Robinson</td>
<td>LLT / SWAC</td>
</tr>
<tr>
<td>14</td>
<td>607</td>
<td>531137992...031728127</td>
<td>183</td>
<td>1952 January 30</td>
<td>Raphael M. Robinson</td>
<td>LLT / SWAC</td>
</tr>
<tr>
<td>15</td>
<td>1,279</td>
<td>104079321...168729087</td>
<td>386</td>
<td>1952 June 25</td>
<td>Raphael M. Robinson</td>
<td>LLT / SWAC</td>
</tr>
<tr>
<td>16</td>
<td>2,203</td>
<td>147597991...697771007</td>
<td>664</td>
<td>1952 October 7</td>
<td>Raphael M. Robinson</td>
<td>LLT / SWAC</td>
</tr>
<tr>
<td>17</td>
<td>2,281</td>
<td>446087557...132836351</td>
<td>687</td>
<td>1952 October 9</td>
<td>Raphael M. Robinson</td>
<td>LLT / SWAC</td>
</tr>
<tr>
<td>18</td>
<td>3,217</td>
<td>259117086...909315071</td>
<td>969</td>
<td>1957 September 8</td>
<td>Hans Riesel</td>
<td>LLT / BESK</td>
</tr>
<tr>
<td>19</td>
<td>4,253</td>
<td>190797007...350484991</td>
<td>1,281</td>
<td>1961 November 3</td>
<td>Alexander Hurwitz</td>
<td>LLT / IBM 7090</td>
</tr>
<tr>
<td>20</td>
<td>4,423</td>
<td>285542542...608580607</td>
<td>1,332</td>
<td>1961 November 3</td>
<td>Alexander Hurwitz</td>
<td>LLT / IBM 7090</td>
</tr>
<tr>
<td>21</td>
<td>9,689</td>
<td>478220278...225754111</td>
<td>2,917</td>
<td>1963 May 11</td>
<td>Donald B. Gillies</td>
<td>LLT / ILLIAC II</td>
</tr>
<tr>
<td>22</td>
<td>9,941</td>
<td>346088282...789463551</td>
<td>2,993</td>
<td>1963 May 16</td>
<td>Donald B. Gillies</td>
<td>LLT / ILLIAC II</td>
</tr>
<tr>
<td>23</td>
<td>11,213</td>
<td>281411201...696392191</td>
<td>3,376</td>
<td>1963 June 2</td>
<td>Donald B. Gillies</td>
<td>LLT / ILLIAC II</td>
</tr>
<tr>
<td>24</td>
<td>19,937</td>
<td>431542479...968041471</td>
<td>6,002</td>
<td>1971 March 4</td>
<td>Bryant Tuckerman</td>
<td>LLT / IBM 360/91</td>
</tr>
<tr>
<td>Mersenne Prime</td>
<td>Exponent</td>
<td>Prime Number</td>
<td>Date</td>
<td>Found by</td>
<td>Comments</td>
<td></td>
</tr>
<tr>
<td>---------------</td>
<td>----------</td>
<td>--------------</td>
<td>------</td>
<td>----------</td>
<td>----------</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>21,701</td>
<td>448679166...511882751</td>
<td>1978 October 30</td>
<td>Landon Curt Noll &amp; Laura Nickel</td>
<td>LLT / CDC Cyber 174</td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>23,209</td>
<td>402874115...792964511</td>
<td>1979 February 9</td>
<td>Landon Curt Noll</td>
<td>LLT / CDC Cyber 174</td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>44,497</td>
<td>854509824...011228671</td>
<td>1979 April 8</td>
<td>Harry Lewis Nelson &amp; David Slowinski</td>
<td>LLT / Cray 1</td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>86,243</td>
<td>536927995...433438207</td>
<td>1982 September 25</td>
<td>David Slowinski</td>
<td>LLT / Cray 1</td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>216,091</td>
<td>746093103...815528447</td>
<td>1985 September 1[9]</td>
<td>David Slowinski</td>
<td>LLT / Cray X-MP/24</td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>756,839</td>
<td>174135906...544677887</td>
<td>1992 February 19</td>
<td>David Slowinski &amp; Paul Gage</td>
<td>LLT / Maple on Harwell Lab Cray-2[13]</td>
<td></td>
</tr>
<tr>
<td>35</td>
<td>1,398,269</td>
<td>814171564...451315711</td>
<td>1996 November 13</td>
<td>GIMPS / Joel Armengaud[16]</td>
<td>LLT / Prime95 on 90 MHz Pentium PC</td>
<td></td>
</tr>
<tr>
<td>36</td>
<td>2,976,221</td>
<td>623340076...729201151</td>
<td>1997 August 24</td>
<td>GIMPS / Gordon Spence[17]</td>
<td>LLT / Prime95 on 100 MHz Pentium PC</td>
<td></td>
</tr>
<tr>
<td>37</td>
<td>3,021,377</td>
<td>127411683...024694271</td>
<td>1998 January 27</td>
<td>GIMPS / Roland Clarkson[18]</td>
<td>LLT / Prime95 on 200 MHz Pentium PC</td>
<td></td>
</tr>
<tr>
<td>38</td>
<td>6,972,593</td>
<td>437075744...924193791</td>
<td>1999 June 1</td>
<td>GIMPS / Nayan Hajratwala[19]</td>
<td>LLT / Prime95 on 350 MHz IBM Aptiva</td>
<td></td>
</tr>
<tr>
<td>39</td>
<td>13,466,917</td>
<td>924947738...256259071</td>
<td>2001 November 14</td>
<td>GIMPS / Michael Cameron[20]</td>
<td>LLT / Prime95 on 800 MHz Athlon T-Bird</td>
<td></td>
</tr>
<tr>
<td>40</td>
<td>20,996,011</td>
<td>125976895...855680247</td>
<td>2003 November 17</td>
<td>GIMPS / Michael Shafer[21]</td>
<td>LLT / Prime95 on 2 GHz Dell Dimension</td>
<td></td>
</tr>
<tr>
<td>41[+]</td>
<td>24,036,583</td>
<td>299410429...733969407</td>
<td>2004 May 15</td>
<td>GIMPS / Josh Findley[22]</td>
<td>LLT / Prime95 on 2.4 GHz Pentium 4 PC</td>
<td></td>
</tr>
<tr>
<td>42[+]</td>
<td>25,964,951</td>
<td>122164630...577077247</td>
<td>2005 February 18</td>
<td>GIMPS / Martin Nowak[23]</td>
<td>LLT / Prime95 on 2.4 GHz Pentium 4 PC</td>
<td></td>
</tr>
<tr>
<td>43[+]</td>
<td>30,402,457</td>
<td>315416475...652943871</td>
<td>2005 December 15</td>
<td>GIMPS / Curtis Cooper &amp; Steven Boone[24]</td>
<td>LLT / Prime95 on 2 GHz Pentium 4 PC</td>
<td></td>
</tr>
<tr>
<td>44[+]</td>
<td>32,582,657</td>
<td>124575026...053967871</td>
<td>2006 September 4</td>
<td>GIMPS / Curtis Cooper &amp; Steven Boone[25]</td>
<td>LLT / Prime95 on 3 GHz Pentium 4 PC</td>
<td></td>
</tr>
<tr>
<td>45[+]</td>
<td>37,156,667</td>
<td>202254406...308220927</td>
<td>2008 September 6</td>
<td>GIMPS / Hans-Michael Elvenich[26]</td>
<td>LLT / Prime95 on 2.83 GHz Core 2 Duo PC</td>
<td></td>
</tr>
</tbody>
</table>
It is not known whether any undiscovered Mersenne primes exist between the 40th \( (M_{20,996,011}) \) and the 47th \( (M_{43,112,609}) \) on this chart; the ranking is therefore provisional. Primes are not always discovered in increasing order. For example, the 29th Mersenne prime was discovered after the 30th and the 31st. Similarly, the current record holder was followed by two smaller Mersenne primes, first 2 weeks later and then 8 months later.

\* \( M_{42,643,801} \) 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. The discoverer, Strindmo, apparently used the alias Stig M. Valstad.

To help visualize the size of the 47th known Mersenne prime, it would require 3,461 pages to display the number in base 10 with 75 digits per line and 50 lines per page.\[9\]

The largest known Mersenne prime \( (2^{43,112,609} - 1) \) is also the largest known prime number,\[3\] and was the first discovered prime number with more than 10 million base-10 digits.

In modern times, the largest known prime has almost always been a Mersenne prime.\[27\]

**Factorization of Mersenne numbers**

The factorization of a prime number is by definition 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 March 2007, \( 2^{1039} - 1 \) is the record-holder,\[28\] after a calculation taking about a year on a couple of hundred computers, mostly at NTT in Japan and at EPFL in Switzerland. 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 2011, the composite Mersenne number with largest proven prime factors is \( 2^{20887} - 1 \), which is known to have a factor \( p \) with 6229 digits that was proven prime with ECPP.\[29\] The largest with probable prime factors allowed is \( 2^{1168183} - 1 = 54763676838381762583 \times q \), where \( q \) is a probable prime.\[30\]

**Perfect numbers**

Mersenne primes are interesting to many for their connection to perfect numbers. In the 4th century BCE, Euclid demonstrated that if \( M_p \) is a Mersenne prime then

\[
2^{p-1} \cdot (2^p - 1) = M_p (M_p + 1) / 2
\]

is an even perfect number (Elements ix.36)—which is also 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. It is unknown whether there are any odd perfect numbers, but it appears unlikely.

**Generalization**

The binary representation of \( 2^p - 1 \) is the digit 1 repeated \( p \) times, for example, \( 2^5 - 1 = 11111 \_2 \) in the binary notation. A Mersenne number is therefore a repunit in base 2, and Mersenne primes are the base 2 repunit primes.

The base 2 representation of a Mersenne number shows the factorization pattern for composite exponent. For example:

\[
M_{35} = 2^{35} - 1 = (1111111111111111111111111111111111111)_2
\]

\[
= (1111111111111111111111111111111111111)_2 \cdot (1000010000100001000010000100001)_2
\]

\[
= (1111111111111111111111111111111111111)_2 \cdot (100000010000001000000100000010000001)_2
\]

\[
= (1111111111111111111111111111111111111)_2 \cdot (10000000100000001000000010000000100000001)_2
\]
\begin{align*}
= (11111)_2 \cdot (1111111)_2 \cdot (1000101001010100100001)_2 - (0100001010010100101000010)_2 \\
= M_5 \cdot M_7 \cdot (10001010010110111111)_2.
\end{align*}

## Mersenne numbers in nature and elsewhere

In computer science, unsigned \( p \)-bit integers can be used to express numbers up to \( M_p \).

In the mathematical problem Tower of Hanoi, solving a puzzle with a \( p \)-disc tower requires at least \( M_p \) steps.

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 nineteenth century). [31]

### See also

- Repunit
- Fermat prime
- Erdős–Borwein constant
- Mersenne conjectures
- Mersenne Twister
- Prime95 / MPrime
- Largest known prime number
- Double Mersenne number
- Wieferich prime
- Wagstaff prime
- Solinas prime

### References

2. ^ a b The Prime Pages, Mersenne Primes: History, Theorems and Lists (http://primes.utm.edu/mersenne/).
8. ^ The Prime Pages, Mersenne's conjecture (http://primes.utm.edu/notes/merc.html).
15. ^ The Prime Pages, A Prime of Record Size! 2^1257787-1 (http://primes.utm.edu/notes/1257787.html).
19. ^ GIMPS Finds First Million-Digit Prime, Stakes Claim to $50,000 EFF Award (http://www.mersenne.org/primes/6972593.htm).
GIMPS, the Great Internet Mersenne Prime Search, has discovered the largest known prime number, $2^{32,582,657} - 1$ (http://www.mersenne.org/primes/32582657.htm).

Titanic Primes Raced to Win $100,000 Research Award (http://mersenne.org/primes/m45and46.htm). Retrieved on 2008-09-16.

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.

Paul Zimmermann, "Integer Factoring Records" (http://www.loria.fr/~zimmerma/records/factor.html).


External links

- GIMPS home page (http://www.mersenne.org)
- Mersenne Primes: History, Theorems and Lists (http://primes.utm.edu/mersenne/) — explanation
- 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 40–47
- $M_q = (8x)^2 - (3qy)^2$ Mersenne proof (http://tony.reix.free.fr/Mersenne/Mersenne8x3qy.pdf) (pdf)
- $M_q = x^2 + dy^2$ math thesis (http://www.math.leidenuniv.nl/scripties/jansen.ps) (ps)
- Mersenne prime bibliography (http://www.utm.edu/research/primes/mersenne/LukeMirror/biblio.htm) with hyperlinks to original publications
- (German) report about Mersenne primes (http://www.taz.de/de/pt/2005/03/11/a0355.nf/text) — detection in detail
- GIMPS wiki (http://mersennewiki.org/index.php/Main_Page)
- a file (ftp://mersenne.org/gimps/factors.zip) containing the smallest known factors of all tested Mersenne numbers (requires program (ftp://mersenne.org/gimps/decomp.zip) to open)
- Decimal digits and English names of Mersenne primes (http://www.isthe.com/chongo/tech/math/prime/mersenne.html)

MathWorld links

- Weisstein, Eric W., "Mersenne number (http://mathworld.wolfram.com/MersenneNumber.html)" from MathWorld.

Retrieved from "http://en.wikipedia.org/wiki/Mersenne_prime"

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

- This page was last modified on 12 August 2011 at 10:19.
- Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. See Terms of use for details. Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.