# Basic properties of Mersenne-numbers
## (Parallel algorithm for prime factorization of Mersenne-numbers)

**Dénes, Tamás mathematician**

**Budapest, 2001.**

**Abstract**
In the present paper we give a necessary and sufficient condition for if the *p* prime then when $M_p=2^p-1$ Mersenne-number is composite. We also give a test algorithm based on this theorem, which also gives the two-factorization of the Mersenne numbers.
The algorithm can be in parallel computed, so its speed can be significantly increased, which is important for the production of large prime numbers and prime testing.

**THEOREM 1.**
The $M_p=2^p-1$ Mersenne-numbers ($p\geq 3$ *prime*) are $6K+1$ form ($K$=1,2,3,…) for every *p* prime.

**PROOF**
By the Dénes-type prime number theorem [Dénes 2001] (according to which *„every prime number greater than 3 has the form* $6k\pm 1$ *where k is a natural number”*) two cases are possible:

$$p^- = 6k-1 \Rightarrow M_{p^-} = 2^{p^-}-1 = 2^{6k-1}-1 = \frac{2^{6^k}-2}{2} = \frac{64\cdot 64^{k-1}-2}{2} = 32\cdot 64^{k-1}-1 \Rightarrow$$

(1) $$\Rightarrow \quad 32 \bmod 6 = 2,\ 64 \bmod 6^{k-1} = 4 \Rightarrow \quad 2\cdot 4 \bmod 6 = 2 \quad \Rightarrow \quad M_{p^-} \bmod 6 = 1 \quad \Rightarrow$$

$$\Rightarrow \quad M_{p^-} = 6K+1$$

(2) $$p^+ = 6k+1 \Rightarrow M_{p^+} = 2^{p^+}-1 = 2^{6k+1}-1 \Rightarrow \quad 2^{6k+1} \bmod 6 = 2 \Rightarrow \quad M_{p^+} \bmod 6 = 1 \quad \Rightarrow$$

$$\Rightarrow \quad M_{p^+} = 6K+1$$

Q.E.D.

We employ the known mathematical relationship (3).

(3) $$a^n-1=(a-1)(a^{n-1}+a^{n-2}+a^{n-3}+\ldots+a^1+a^0)=(a-1)\sum_{i=0}^{n-1} a^i \quad \Rightarrow \sum_{i=0}^{n-1} a^i = \frac{a^n-1}{a-1}$$

# Basic properties of Mersenne-numbers

**Dénes, Tamás mathematician**

**Consequences of Theorem 1:**

**C0.** According to the Dénes-type prime number theorem and Theorem 1 above, then the $M_p$ Mersenne-primes can only be $6K+1$ form.

**C1.** If $p^- = 6k-1$ ($k=1,2,3,\ldots$) is a prime number, then for the Mersenne-number $M_{p^-}$ is true:

(4a)
$$M_{p^-} = 2^{6k-1} - 1 = 6K^- + 1 \Rightarrow 2^{6k-1} - 2 = 6K^- \Rightarrow 2^{2(3k-1)} = 3K^- + 1 \Rightarrow$$
$$\Rightarrow 4^{3k-1} - 1 = 3K^- \Rightarrow 3\sum_{i=0}^{3k-2} 4^i = 3K^- \quad \Rightarrow \quad K^- = \sum_{i=0}^{3k-2} 4^i = \sum_{i=0}^{\frac{p-3}{2}} 4^i$$

**C2.** If $p^+ = 6k+1$ ($k=1,2,3,\ldots$) is a prime number, then for the Mersenne-number $M_{p^+}$ is true:

(4b)
$$M_{p^+} = 2^{6k+1} - 1 = 6K^+ + 1 \Rightarrow 2^{6k} = 3K^+ + 1 \Rightarrow 4^{3k} - 1 = 3K^+ \Rightarrow$$
$$\Rightarrow \quad 3\sum_{i=0}^{3k-1} 4^i = 3K^+ \quad \Rightarrow \quad K^+ = \sum_{i=0}^{3k-1} 4^i = \sum_{i=0}^{\frac{p-3}{2}} 4^i$$

**Based the C1. and C2. we can state the next Theorem 2:**

**THEOREM 2.**
If $p>3$ is a prime number and $M_p=2^p-1$ is a Mersenne-number, then the (5a) and (5b) connections are true:

(5a)
$$p^- = 6k-1 \ (k=1,2,3,\ldots) \overset{(4a)}{\Rightarrow} M_{p^-} = \left(6\sum_{i=0}^{3k-2} 4^i\right) + 1 = \left(6\sum_{i=0}^{\frac{p-3}{2}} 4^i\right) + 1$$

(5b)
$$p^+ = 6k+1 \ (k=1,2,3,\ldots) \overset{(4b)}{\Rightarrow} M_{p^+} = \left(6\sum_{i=0}^{3k-1} 4^i\right) + 1 = \left(6\sum_{i=0}^{\frac{p-3}{2}} 4^i\right) + 1$$

(6) $p>3$ prime number
$$\overset{(5a),(5b)}{\Rightarrow} K = \sum_{i=0}^{\frac{p-3}{2}} 4^i \overset{Theorem 1.}{\Rightarrow} M_p = 6K + 1 = \left(6\sum_{i=0}^{\frac{p-3}{2}} 4^i\right) + 1$$

Using the complementary prime-sive theorem [Dénes 2001, Theorem 2], we can say the following Theorem 3, which gives a necessary and sufficient condition for composit Mersenne-numbers.

# Basic properties of Mersenne-numbers

**Dénes, Tamás mathematician**

**THEOREM 3.**

For any $p>3$ prime number, the $M_p = 2^p - 1$ Mersenne number is composite if and only if one of the relations (8a) or (8b) holds. Let $u,v \geq 1$ are natural numbers.

(7) $$(6) \Rightarrow \quad K = \sum_{i=0}^{\frac{p-3}{2}} 4^i \overset{(3)}{=} \frac{4^{\frac{p-3}{2}+1} - 1}{3} = \frac{2^{p-1} - 1}{3}$$

(8a) $$(7) \Rightarrow \quad K^- = \frac{2^{p-1} - 1}{3} = 6uv - u - v \quad \Rightarrow \quad 2^{p-1} = 3(6uv - u - v) + 1$$

(8b) $$(7) \Rightarrow \quad K^+ = \frac{2^{p-1} - 1}{3} = 6uv + u + v \quad \Rightarrow \quad 2^{p-1} = 3(6uv + u + v) + 1$$

Every $p-1$ is an even number and by all means $2^{p-1} \bmod 3 = 1$, it follows that the (8a), (8b) equations can always be solved and the solutions are given by the solutions of these diophantine equations. That is, if $3(6uv-u-v)+1$, or $3(6uv+u+v)+1$ are $2^{p-1}$. So we can say the following Theorem 4, that

**THEOREM 4.**
There are infinitely many composite Mersenne numbers.

----- . -----

**For example:** $u=4$, $v=15 \Rightarrow 3(6uv-u-v)+1=1.024=2^{10} \Rightarrow p=11$ (see Table 1. 3. row)
$u=37$, $v=102.719.696 \Rightarrow 3(6uv-u-v)+1=68.103.158.338=2^{36} \Rightarrow p=37$ (see Table 1. 12. row)

**OPEN PROBLEM:** Are there infinite number of Mersenne primes?

## Algorithm for prime factorization of Mersenne numbers (prime test)

Theorem 3 provides an algorithm for deciding that a given $M_p$ Mersenne number is Mersenne prime or not. The algorithm is based on the relationships (8a-b).

(9) $$(8a) \Rightarrow \quad K^- = 6uv - u - v = v(6u-1) - u \quad \Rightarrow \quad v = \frac{K^- + u}{6u - 1} \quad (u = 1,2,3,\ldots)$$

(10) $$(8b) \Rightarrow \quad K^+ = 6uv + u + v = v(6u+1) + u \quad \Rightarrow \quad v = \frac{K^+ - u}{6u + 1} \quad (u = 1,2,3,\ldots)$$

Since the relations (9), (10) are symmetric for $u$, $v$, if we run $u$ all the way to $u=v$, then all possible values of $v$ are obtained.

# Basic properties of Mersenne-numbers

**Dénes, Tamás mathematician**

(11)
$$u = v \Rightarrow \quad K^- \overset{(9)}{=} 6u_{\max}^2 - 2u_{\max} \overset{(8a)}{=} \frac{2^{p-1}-1}{6} = \frac{M_{p^-}-1}{6} \Rightarrow$$
$$\Rightarrow \quad 36u_{\max}^2 - 12u_{\max} + 1 - M_{p^-} = 0 \quad \Rightarrow \quad u_{\max} = \frac{1 \pm \sqrt{M_{p^-}}}{6} \approx \frac{\sqrt{M_{p^-}}}{6}$$

(12)
$$u = v \Rightarrow \quad K^+ \overset{(10)}{=} 6u_{\max}^2 + 2u_{\max} \overset{(8b)}{=} \frac{2^{p-1}-1}{6} = \frac{M_{p^+}-1}{6} \Rightarrow$$
$$\Rightarrow \quad 36u_{\max}^2 + 12u_{\max} + 1 - M_{p^+} = 0 \quad \Rightarrow \quad u_{\max} = \frac{1 \pm \sqrt{M_{p^+}}}{6} \approx \frac{\sqrt{M_{p^+}}}{6}$$

If $p^-=6k-1$ is a prime number, then according to the Theorem 3. $M_{p^-} = 2^{p^-} - 1$ is a Mersenne prime if and only if there is no $1 \le u \le u_{max}$ value for which the value of $v$ in (9) is an integer.

Also follows from Theorem 3 that if $M_{p^-}$ is not a prime number, then there is a value $u$, $v$ pair for which $v$ takes an integer value in (9), so this algorithm directly produces the two-factorization of the Mersenne number:

(13)
$$M_{p^-} = 6K^- + 1 \overset{(9)}{=} 6(6uv - u - v) + 1 = (6u-1)(6v-1)$$

(14)
$$M_{p^+} = 6K^+ + 1 \overset{(10)}{=} 6(6uv + u + v) + 1 = (6u+1)(6v+1)$$

The maximum step number of the algorithm is $u_{max}$ if the Mersenne number is prime. If the Mersenne number is not prime, then the step number of the primefactorization of (13), (14) is $\left[\frac{p_1}{6}\right]$, where the smallest prime factor of $M_{p^-}$ (or $M_{p^+}$) is $p_1$.

It is worth noting that the present algorithm can be easily performed with parallelization with $u$, so its speed can be increased according to the number of processors. Table 1 provides some illustrative examples of factorizations (13), (14).

## Two basic properties of compozite Mersenne numbers

If $M_p$ is a compozite Mersenne number, then by the Theorem 1 of the [Dénes 2001] there exist a prime factorization of form (15).

(15) $M_p = p_1 \cdot p_2 \cdot \ldots \cdot p_s = (6r_1 \pm 1)(6r_2 \pm 1) \cdot \ldots \cdot (6r_s \pm 1)$, where $s \geq 1$, $r_1, r_2, \ldots, r_s$ *natural numbers*

(16)
$$\overset{(15)}{\Rightarrow} M_p = (6r_1 \pm 1)(6r_2 \pm 1)$$
($r_1$ and $r_2$ natural numbers)

# Basic properties of Mersenne-numbers

**Dénes, Tamás mathematician**

**THEOREM 5.**
If $M_p$ is a compozite Mersenne number, then of the factorizations (16), only those can occur when the two factors have the same sign of $\pm 1$.

**PROOF**
Assume that $M_p = (6r_1+1)(6r_2-1)$, then

(17) $$M_p = (6r_1+1)(6r_2-1) = 36r_1r_2 - 6r_1 + 6r_2 - 1 = 3(12r_1r_2 - 2r_1 + 2r_2) - 1$$

for $p$, one of cases (1) and (2) may exist.

(18) $$(1),(4),(18) \Rightarrow \quad M_p = 6\frac{4^{3k-1}-1}{3} + 1 = 2\cdot 4^{3k-1} - 1 \overset{(17)}{=} 3(12r_1r_2 - 2r_1 + 2r_2) - 1$$

However, equality (18) is not possible because $2\cdot 4^{3k-1} \bmod 3 \neq 0$

(19) $$(2),(5),(18) \Rightarrow \quad M_p = 6\frac{4^{3k}-1}{3} + 1 = 2\cdot 4^{3k} - 1 \overset{(17)}{=} 3(12r_1r_2 - 2r_1 + 2r_2) - 1$$

However, *equality (19) is not possible* because $2\cdot 4^{3k} \bmod 3 \neq 0$

Mivel a (17) egyenlőség $r_1$ és $r_2$-re szimmetrikus, így a (18), (19) levezetések mindkét esetben érvényesek.
Since equation (17) is symmetric for $r_1$ and $r_2$, the derivations (18), (19) are valid in both cases.
Assume that $M_p = (6r_1+1)(6r_2+1)$, then

(20) $$M_p = (6r_1+1)(6r_2+1) = 36r_1r_2 + 6r_1 + 6r_2 + 1 = 3(12r_1r_2 + 2r_1 + 2r_2) + 1$$

for $p$, one of the cases (5a) and (5b) may exist.

(21) $$(5a),(20) \Rightarrow \quad M_p = 6\frac{4^{3k-1}-1}{3} + 1 = 2\cdot 4^{3k-1} - 1 \overset{(20)}{=} 3(12r_1r_2 + 2r_1 + 2r_2) + 1 \Rightarrow$$
$$\Rightarrow \quad 2\left(4^{3k-1}-1\right) = 3(12r_1r_2 + 2r_1 + 2r_2)$$

*Equation (21) is possible* because both sides are divisible by 3.

(22) $$(5a),(20) \Rightarrow \quad M_p = 6\frac{4^{3k}-1}{3} + 1 = 2\cdot 4^{3k} - 1 \overset{(20)}{=} 3(12r_1r_2 + 2r_1 + 2r_2) + 1 \Rightarrow$$
$$\Rightarrow \quad 2\left(4^{3k}-1\right) = 3(12r_1r_2 + 2r_1 + 2r_2)$$

Equation *(22) is possible* because both sides are divisible by 3.

Q.E.D.

**THEOREM 6.**
If $M_p$ is a compozit Mersenne number, then $M_p \bmod 3 = 1$

**PROOF**
For $p$, one of cases (5a) and (5b) may exist.

(23) $$(5a) \Rightarrow \quad M_p = 6\frac{4^{3k-1}-1}{3}+1 = 2\underbrace{\left(4^{3k-1}-1\right)}_{\mathrm{mod}\,3=0}+1 \Rightarrow M_p \bmod 3 = 1$$

(24) $$(5b) \Rightarrow \quad M_p = 6\frac{4^{3k}-1}{3}+1 = 2\underbrace{\left(4^{3k}-1\right)}_{\mathrm{mod}\,3=0}+1 \Rightarrow M_p \bmod 3 = 1$$

Q.E.D.

See illustration the 3., 7., 9., 12.-15. and 17. rows of Table 1.

# Basic properties of Mersenne-numbers

**Dénes, Tamás mathematician**

**Table 1**

| | $k^-$ | $k^+$ | $p=6k\pm1$ | Mersenne-numbers ($M_p$) |
|---|---|---|---|---|
| 1. | 1 | | 5 | $M_5=2^5-1=$**31 (prime)** |
| 2. | | 1 | 7 | $M_7=2^7-1=$**127 (prime)** |
| 3. | 2 | | 11 | $M_{11}=2^{11}-1=$**2.047**$=(6\cdot4-1)(6\cdot15-1)$ |
| 4. | | 2 | 13 | $M_{13}=2^{13}-1=$**8.191 (prime)** |
| 5. | 3 | | 17 | $M_{17}=2^{17}-1=$**131.071 (prime)** |
| 6. | | 3 | 19 | $M_{19}=2^{19}-1=$**524.287 (prime)** |
| 7. | 4 | | 23 | $M_{23}=2^{23}-1=$**8.388.607**$=(6\cdot8-1)(6\cdot29.747-1)$ |
| 8. | | 4 | 25 | **NOT Mersenne-number**<br>$2^{25}-1=33.554.431=(6\cdot5+1)(6\cdot100+1)(6\cdot300+1)$ |
| 9. | 5 | | 29 | $M_{29}=2^{29}-1=$**536.870.911**$=(6\cdot39-1)(6\cdot384.028-1)$ |
| 10. | | 5 | 31 | $M_{31}=2^{31}-1=$**2.147.483.647 (prime)** |
| 11. | 6 | | 35 | **NOT Mersenne-number**<br>$2^{35}-1=34.359.738.367=(6\cdot5+1)(6\cdot12-1)(6\cdot21+1)(6\cdot20.487-1)$ |
| 12. | | 6 | 37 | $M_{37}=2^{37}-1=$**137.438.953.471**$=(6\cdot37+1)(6\cdot102.719.696+1)$ |
| 13. | 7 | | 41 | $M_{41}=2^{41}-1=$**2.199.023.255.551**$=(6\cdot2.228-1)(6\cdot27.418.559-1)$ |
| 14. | | 7 | 43 | $M_{43}=2^{43}-1=$**8.796.093.022.207**$=(6\cdot698.148+1)(6\cdot349.977+1)$ |
| 15. | 8 | | 47 | $M_{47}=2^{47}-1=$**140.737.488.355.327**$=(6\cdot392-1)(6\cdot9.977.136.563-1)$ |
| 16. | | 8 | 49 | **NOT Mersenne-number**<br>$2^{49}-1=562.949.953.421.311=(6\cdot21+1)(6\cdot738.779.466.432+1)$ |
| 17. | 9 | | 53 | $M_{53}=2^{53}-1=$**9.007.199.254.740.991**$=(6\cdot11.572-1)(6\cdot21.621.464.127-1)$ |
| 18. | | 9 | 55 | **NOT Mersenne-number**<br>$2^{55}-1=36.028.797.018.963.967=(6\cdot4-1)(6\cdot5+1)(6\cdot15-1)(6\cdot147-1)$<br>$(6\cdot532-1)(6\cdot33.660+1)$ |
| 19. | 10 | | 59 | $M_{59}=2^{59}-1=$**576.460.752.303.423.487 (prime)** |
| 20. | | 10 | 61 | $M_{61}=2^{61}-1=$**2.305.843.009.213.693.951 (prime)** |
| 21. | 11 | | 65 | **NOT Mersenne-number**<br>$2^{65}-1=36.893.488.147.419.103.231=(6\cdot5+1)(6\cdot1.365+1)$<br>$(6\cdot24.215.857.259.685+1)$ |
| 22. | | 11 | 67 | $M_{67}=2^{67}-1=$**147.573.952.589.676.412.927**$=$<br>$(6\cdot32.284.620+1)(6\cdot126.973.042.881+1)$ |

## References

[Dénes 2001] Complementary prime-sieve PUre Mathematics and Applications, Vol.12 (2001), No. 2, pp. 197-207
http://www.titoktan.hu/_raktar/_e_vilagi_gondolatok/PUMA-CPS.pdf