Proof of the existence
of infinite number of Mersenne primes

Dénes, Tamás mathematicians

Budapest, 2020.

Abstract
In the present paper, using the results of the [Dénes 2001c] article, we prove by an indirect method that there are infinitely many Mersenne primes.

According to the Theorem 3. of [Dénes 2001c] article, for any *p*> *3* prime number, the $M_p = 2^p - 1$ Mersenne number is composite if and only if one of the relations (2) or (3) holds where *u*,*v*≥*1* are natural numbers.

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

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

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

1. Consider case (2) and assume that *v*=*u*+*c* (*c* is a natural number)!

(4) $$v = u + c \quad \Rightarrow 6uv - u - v = 6u(u + c) - u - (u + c) = 6u^2 + 6uc - 2u - c$$

(5) $$(2),(4) \quad \Rightarrow \frac{2^{p-1} - 1}{3} = 6u^2 + 6uc - 2u - c \quad \Rightarrow 2^{p-1} = 18u^2 + 18uc - 6u - 3c + 1$$

(6) $$\begin{aligned} (5) \quad & \Rightarrow 0 = 18u^2 + 6u(3c - 1) - 3c + 1 - 2^{p-1} \quad \Rightarrow \\ & \Rightarrow u_{1,2} = \frac{6(1 - 3c) \pm \sqrt{(6(3c - 1))^2 - 4 \cdot 18\left(-3c + 1 - 2^{p-1}\right)}}{2 \cdot 18} = \\ & = \frac{1 - 3c \pm \sqrt{(3c - 1)^2 - 2\left(-3c + 1 - 2^{p-1}\right)}}{6} = \\ & = \frac{1 - 3c \pm \sqrt{9c^2 - 6c + 1 + 6c - 2 + 2^p}}{6} \end{aligned}$$

Since *1-3c* must be negative, then the squareroot expression must be positive, thus the (7) is hold.

(7) $$u = \frac{1-3c+\sqrt{9c^2-1+2^p}}{6} = \frac{1-3c+\sqrt{(3c)^2-1+2^p}}{6}$$

To make u a natural number, there must be a complete square below the root, denote this by x^2 , where x is a natural number.

(8) $$(3c)^2-1+2^p = x^2 \Rightarrow \quad 2^p-1 = x^2-(3c)^2 \Rightarrow \quad M_p = (x-3c)(x+3c)$$

Thus, for any pair of natural numbers u, v that satisfies equation (2), M_p is indeed a compozite number, which one possible resolution is given by equation (8).

2. Consider case (3) and assume that $v=u+c$ (c is a natural number)!

(9) $$v = u+c \quad \Rightarrow 6uv+u+v = 6u(u+c)+u+(u+c) = 6u^2+6uc+2u+c$$

(10) $$(3),(9) \quad \Rightarrow \frac{2^{p-1}-1}{3} = 6u^2+6uc+2u+c \quad \Rightarrow 2^{p-1} = 18u^2+18uc+6u+3c+1$$

$$(10) \quad \Rightarrow 0 = 18u^2+6u(3c+1)+3c+1-2^{p-1} \quad \Rightarrow$$

(11) $$\Rightarrow u_{1,2} = \frac{-6(3c+1)\pm\sqrt{\left(6(3c+1)\right)^2-4\cdot 18\left(3c+1-2^{p-1}\right)}}{2\cdot 18} = \frac{-(3c+1)\pm\sqrt{(3c+1)^2-2\left(3c+1-2^{p-1}\right)}}{6} = \frac{-(3c+1)\pm\sqrt{9c^2+6c+1-6c-2+2^p}}{6}$$

Since *–(3c+1)* must be negative, then the squareroot expression must be positive, thus the (12) is hold.

(12) $$u = \frac{-(3c+1)+\sqrt{9c^2-1+2^p}}{6} = \frac{-(3c+1)+\sqrt{(3c)^2-1+2^p}}{6}$$

That is, in this case too, relation (8) holds.

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

Proof of the existence of infinite number of Mersenne primes

Dénes, Tamás mathematicians

Now suppose that there exists a finite number of Mersenne primes. Then there must be a last Mersenne prime for which the following Theorem 1. is satisfied:

THEOREM 1.
There exists a prime number q such that M_q is a Mersenne prime and for every prime $p> q$ that hold

(13) $$\forall p\rangle q \Rightarrow \quad M_p = 2^p - 1 \text{ compozite number.}$$

PROOF (*indirect*)
We proved in Theorem 1. in [Dénes 2001c] that every $M_p = 2^p - 1$ Mersenne number is *6K+1 form* (*K=1,2,3,…*). On the other hand, in the same article, we provided a necessary and sufficient condition for when the M_p Mersenne number is compozite, see relation (2), (3) above.
Comparing this with the statement of the present theorem, we get that

(14) $$M_q = 6K + 1 \quad \text{és} \quad K^{'} = K + C \quad \Rightarrow \quad M_p = 6K^{'} + 1 = M_q + 6C$$

Consider cases (2) and (3)!

If *q≥5* is a prime number, then *q=6k-1*, or *q=6k+1* form (*k=1,2,3,…*)
Thus, the subcases of (2), (3) that need to be examined for full proof are summarized in Table 1. below:

Table 1.

	(2)			(3)	
I.	*q=6k-1*	*p=6k'-1*	V.	*q=6k-1*	*p=6k'-1*
II.	*q=6k-1*	*p=6k'+1*	VI.	*q=6k-1*	*p=6k'+1*
III.	*q=6k+1*	*p=6k'-1*	VII.	*q=6k+1*	*p=6k'-1*
IV.	*q=6k+1*	*p=6k'+1*	VIII.	*q=6k+1*	*p=6k'+1*

I. Let *q=6k-1, k'=k+d* (*d=1,2,3,…*) and *p=6k'-1*

(15) $$\overset{(2),(14)}{\Rightarrow} K^{'} = K + C = 6uv - u - v \overset{(2)}{=} K^{-}$$

(16) $$q = 6k - 1,\ k' = k + d,\ p = 6k' - 1 \quad \Rightarrow \quad M_q = 6K + 1 = 2^q - 1 = 2^{6k-1} - 1$$

(17) $$M_p = 6K^{'} + 1 = 2^p - 1 = 2^{6k'-1} - 1 = 2^{6(k+d)-1} - 1 = 2^{6k+6d-1} - 1 = \\ = 2^{6d} \cdot 2^{6k-1} - 1 = 2^{6d}(M_q + 1) - 1 \quad \Rightarrow \quad \frac{M_p + 1}{M_q + 1} = 2^{6d}$$

(18) $$\overset{(14),(17)}{\Rightarrow} 2^{6d} = \frac{M_q + 6C + 1}{M_q + 1} = \frac{6C}{M_q + 1} + 1 \overset{(14),(15)}{\Rightarrow} 2^{6d} = \frac{6(K^- - K)}{6K + 2} + 1 =$$
$$= \frac{6K^- - 6K}{6K + 2} + 1 = \frac{6K^- - 6K + 6K + 2}{6K + 2} \Rightarrow 2^{6d-1} = \frac{3K^- + 1}{3K + 1}$$

(19) $$\overset{(15)}{\Rightarrow} K = K^- - C \overset{(18)}{\Rightarrow} 2^{6d-1} = \frac{3K^- + 1}{3K^- - 3C + 1}$$

The (19) fraction only an integer if *C=0*. However, it would follow that

(20) $$2^{6d-1} = 1 \Rightarrow 6d - 1 = 0 \Rightarrow d = \frac{1}{6}$$

This contradicts condition **I.**, from this we can conclude that case **I.** is not possible.

II. Let *q=6k-1*, *k'=k+d* (*d=1,2,3,…*) and *p=6k'+1*, then

(21) $$q = 6k - 1,\ k' = k + d,\ p = 6k' + 1 \Rightarrow M_q = 6K + 1 = 2^q - 1 = 2^{6k-1} - 1$$

(22) $$M_p = 6K' + 1 = 2^p - 1 = 2^{6k'+1} - 1 = 2^{6(k+d)+1} - 1 = 2^{6k+6d+1} - 1 =$$
$$= 2^{6d} \cdot 2^{6k+1} - 1 = 2^{6d+2}(M_q + 1) - 1 \Rightarrow \frac{M_p + 1}{M_q + 1} = 2^{6d+2}$$

(23) $$\overset{(14),(22)}{\Rightarrow} 2^{6d+2} = \frac{M_q + 6C + 1}{M_q + 1} = \frac{6C}{M_q + 1} + 1 \overset{(14),(15)}{\Rightarrow} 2^{6d+2} = \frac{6(K^- - K)}{6K + 2} + 1 =$$
$$= \frac{6K^- - 6K}{6K + 2} + 1 = \frac{6K^- - 6K + 6K + 2}{6K + 2} \Rightarrow 2^{6d+1} = \frac{3K^- + 1}{3K + 1}$$

(24) $$\overset{(15)}{\Rightarrow} K = K^- - C \overset{(23)}{\Rightarrow} 2^{6d+1} = \frac{3K^- + 1}{3K^- - 3C + 1}$$

The (24) fraction only an integer if *C=0*. However, it would follow that

(25) $$2^{6d+1} = 1 \Rightarrow 6d + 1 = 0 \Rightarrow d = -\frac{1}{6}$$

This contradicts condition **II.**, from this we can conclude that case **II.** is not possible.

III. Let *q=6k+1*, *k'=k+d* (*d=1,2,3,…*) and *p=6k'-1*, then

(26) $$q = 6k + 1,\ k' = k + d,\ p = 6k' - 1 \Rightarrow M_q = 6K + 1 = 2^q - 1 = 2^{6k+1} - 1$$

(27) $$M_p = 6K' + 1 = 2^p - 1 = 2^{6k'-1} - 1 = 2^{6(k+d)-1} - 1 = 2^{6k+6d-1} - 1 =$$
$$= 2^{6d} \cdot 2^{6k-1} - 1 = 2^{6d-2}(M_q + 1) - 1 \Rightarrow \frac{M_p + 1}{M_q + 1} = 2^{6d-2}$$

$$\overset{(14),(27)}{\Rightarrow} 2^{6d-2} = \frac{M_q + 6C + 1}{M_q + 1} = \frac{6C}{M_q + 1} + 1 \overset{(14),(15)}{\Rightarrow} 2^{6d-2} = \frac{6(K^- - K)}{6K + 2} + 1 =$$

(28)
$$= \frac{6K^- - 6K}{6K + 2} + 1 = \frac{6K^- - 6K + 6K + 2}{6K + 2} \Rightarrow$$

$$\Rightarrow 2^{6d-3} = \frac{3K^- + 1}{3K + 1}$$

(29)
$$\overset{(15)}{\Rightarrow} K = K^- - C \overset{(28)}{\Rightarrow} 2^{6d-3} = \frac{3K^- + 1}{3K^- - 3C + 1}$$

The (29) fraction only an integer if *C=0*. However, it would follow that

(30)
$$2^{6d-3} = 1 \Rightarrow 6d - 3 = 0 \Rightarrow d = \frac{1}{2}$$

This contradicts condition **III.**, from this we can conclude that case **III.** is not possible.

IV. Let *q=6k+1*, *k'=k+d* (*d=1,2,3,…*) and *p=6k'+1*, then

(31)
$$q = 6k + 1,\ k' = k + d,\ p = 6k' + 1 \Rightarrow M_q = 6K + 1 = 2^q - 1 = 2^{6k+1} - 1$$

(32)
$$M_p = 6K' + 1 = 2^p - 1 = 2^{6k'+1} - 1 = 2^{6(k+d)+1} - 1 = 2^{6k+6d+1} - 1 =$$

$$= 2^{6d} \cdot 2^{6k+1} - 1 = 2^{6d}(M_q + 1) - 1 \Rightarrow \frac{M_p + 1}{M_q + 1} = 2^{6d}$$

$$\overset{(14),(32)}{\Rightarrow} 2^{6d} = \frac{M_q + 6C + 1}{M_q + 1} = \frac{6C}{M_q + 1} + 1 \overset{(14),(15)}{\Rightarrow} 2^{6d+2} = \frac{6(K^- - K)}{6K + 2} + 1 =$$

(33)
$$= \frac{6K^- - 6K}{6K + 2} + 1 = \frac{6K^- - 6K + 6K + 2}{6K + 2} \Rightarrow$$

$$\Rightarrow 2^{6d-1} = \frac{3K^- + 1}{3K + 1}$$

(34)
$$\overset{(15)}{\Rightarrow} K = K^- - C \overset{(33)}{\Rightarrow} 2^{6d-1} = \frac{3K^- + 1}{3K^- - 3C + 1}$$

The (34) fraction only an integer if *C=0*. However, it would follow that

(35)
$$2^{6d-1} = 1 \Rightarrow 6d - 1 = 0 \Rightarrow d = \frac{1}{6}$$

This contradicts condition **IV.**, from this we can conclude that case **IV.** is not possible.

Since the relations (19), (24), (29), (34) remain valid if we write K^- them in their place K^+, therefore **V.-VIII.** cases are not possible either. So the statement of the theorem is false.
In other words, that it is not true that there are a finite number of Mersenne primes, from which it follows that the number of Mersenne primes are infinite.

Q.E.D.

Table 2.

	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*** $2^{25}-1=33.554.431=(6\cdot5+1)(6\cdot100+1)(6\cdot300+1)$
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*** $2^{35}-1=34.359.738.367=(6\cdot5+1)(6\cdot12-1)(6\cdot21+1)(6\cdot20.487-1)$
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*** $2^{49}-1=562.949.953.421.311=(6\cdot21+1)(6\cdot738.779.466.432+1)$
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*** $2^{55}-1=36.028.797.018.963.967=(6\cdot4-1)(6\cdot5+1)(6\cdot15-1)(6\cdot147-1)$ $(6\cdot532-1)(6\cdot33.660+1)$
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*** $2^{65}-1=36.893.488.147.419.103.231=(6\cdot5+1)(6\cdot1.365+1)$ $(6\cdot24.215.857.259.685+1)$
22.		11	67	$M_{67}=2^{67}-1=$***147.573.952.589.676.412.927***$=$ $(6\cdot32.284.620+1)(6\cdot126.973.042.881+1)$

References

[Dénes 2001a] 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

[Dénes 2001b] Komplementer prímszita és alkalmazása a prímszámok számának becslésére
http://www.titoktan.hu/_raktar/_e_vilagi_gondolatok/KomplementerPrimszita.pdf

[Dénes 2001c] Basic properties of Mersenne-numbers
(Parallel algorithm for prime factorization of Mersenne-numbers)
http://www.titoktan.hu/_raktar/_e_vilagi_gondolatok/Mersenne-primes1.pdf