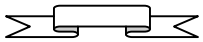
Végtelen sok Mersenne-prím létezésének bizonyítása

Dénes Tamás matematikus

Budapest, 2020.

Abstract
Jelen dolgozatban a [Dénes 2001c] dolgozat eredményeit felhasználva indirekt módszerrel bebizonyítjuk, hogy végtelen sok Mersenne-prím létezik.



A [Dénes 2001c] dolgozat 3. tétele szeint, bármely *p>3* prímszám esetén az $M_p=2^p-1$ Mersenne-szám akkor és csak akkor összetett, ha a (2) vagy (3) összefüggések valamelyike teljesül, ahol u,v≥1 természetes számok.

(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. Vizsgáljuk a (2) esetet és tételezzük fel, hogy *v=u+c* (*c* term. szám)!

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

Végtelen sok Mersenne-prím létezésének bizonyítása

Dénes Tamás matematikus

Mivel *1-3c* biztos negatív, így a gyökös kifejezésnek mindenképpen pozitívnak kell lennie, tehát

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

Ahhoz, hogy *u* egész szám legyen, a gyök alatt teljes négyzetnek kell lenni, jelöljük x^2-tel, ahol *x* term.szám.

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

Tehát, minden olyan *u,v* term.szám pár esetén, amely a (2) egyenletet kielégíti, M_p valóban összetett szám, amelynek egy lehetséges felbontását a (8) összefüggés adja.

2. Vizsgáljuk a (3) esetet és tételezzük fel, hogy *v=u+c* (*c* term. szám)!

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

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

$$\begin{aligned}
&(10) \quad \Rightarrow 0 = 18u^2 + 6u(3c+1) + 3c + 1 - 2^{p-1} \quad \Rightarrow \\
&\Rightarrow u_{1,2} = \frac{-6(3c+1) \pm \sqrt{(6(3c+1))^2 - 4\cdot 18\left(3c+1-2^{p-1}\right)}}{2\cdot 18} = \\
&= \frac{-(3c+1) \pm \sqrt{(3c+1)^2 - 2\left(3c+1-2^{p-1}\right)}}{6} = \\
&= \frac{-(3c+1) \pm \sqrt{9c^2+6c+1-6c-2+2^p}}{6}
\end{aligned} \tag{11}$$

Mivel *–(3c+1)* biztos negatív, így a gyökös kifejezésnek mindenképpen pozitívnak kell lennie, tehát

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

Vagyis ebben az esetben is teljesül a (8) összefüggés.

Példa: *u=4, v=15* (*c=11*) $\Rightarrow$ *3*(*6uv-u-v*)*+1=1.024=*2^{10} $\Rightarrow$ *p=11* (lásd 2. táblázat 3. sor)
u=37, v=102.719.696 $\Rightarrow$ *3*(*6uv-u-v*)*+1=68.103.158.338=*2^{36} $\Rightarrow$ *p=37* (lásd 1. táblázat 12. sor)

Végtelen sok Mersenne-prím létezésének bizonyítása

Dénes Tamás matematikus

Most tételezzük fel, hogy véges számú Mersenne-prím létezik. Ekkor kell lennie egy utolsó Mersenne-prímnek, amelyre teljesül a következő tétel:

1. TÉTEL
Létezik q prímszám, amelyre M_q Mersenne-prím és minden $p>q$ prímre fennáll, hogy

(13) $\forall p \rangle q \Rightarrow \quad M_p = 2^p - 1$ összetett szám.

Bizonyítás (indirekt)
A [Dénes 2001c]-beli 1.tételben bizonyítottuk, hogy minden $M_p = 2^p - 1$ Mersenne-szám *6K+1* alakú (*K=1,2,3,…*). Másrészt ugyanebben a dolgozatban szükséges és elegendő feltételt adtunk meg arra, hogy az M_p Mersenne-szám mikor összetett, lásd a fenti (2), (3) összefüggést.
Ezt a jelen tétel állításával összevetve kapjuk, hogy

(14) $$M_q = 6K+1 \quad \acute{e}s \quad K' = K + C \quad \Rightarrow \quad M_p = 6K' + 1 = M_q + 6C$$

Vizsgáljuk meg a (2) és a (3) eseteket!
Ha $q \geq 5$ prímszám, akkor *q=6k-1*, vagy *q=6k+1* (*k=1,2,3,…*) alakú. Így a (2), (3) esetek azon aleseteit, melyeket vizsgálni kell a teljes bizonyításhoz, az alábbi 1. Táblázat foglalja össze:

1. Táblázat

	(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. Legyen *q=6k-1*, *k'=k+d* (*d=1,2,3,…*) és *p=6k'-1*

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

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

Végtelen sok Mersenne-prím létezésének bizonyítása

Dénes Tamás matematikus

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

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

A (19) tört csak akkor egész szám, ha *C=0*. Ebből azonban az következne, hogy

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

ami ellentmond a **I.** feltételnek, tehát a **I.** eset nem lehetséges.

II. Legyen *q=6k-1*, *k'=k+d* (*d=1,2,3,…*) és *p=6k'+1*, ekkor

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

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

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

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

A (24) tört csak akkor egész szám, ha *C=0*. Ebből azonban az következne, hogy

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

ami ellentmond a **II.** feltételnek, tehát a **II.** eset nem lehetséges.

III. Legyen *q=6k+1*, *k'=k+d* (*d=1,2,3,…*) és *p=6k'-1*, ekkor

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

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

Végtelen sok Mersenne-prím létezésének bizonyítása

Dénes Tamás matematikus

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

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

A (29) tört csak akkor egész szám, ha *C=0*. Ebből azonban az következne, hogy

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

ami ellentmond a **III.** feltételnek, tehát a **III.** eset nem lehetséges.

IV. Legyen *q=6k+1*, *k'=k+d* (*d=1,2,3,…*) és *p=6k'+1*, ekkor

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

(32)
$$M_p = 6K^{'} + 1 = 2^p - 1 = 2^{6k'+1} - 1 = 2^{6(k+d)+1} - 1 = 2^{6k+6d+1} - 1 =$$
$$= 2^{6d} \cdot 2^{6k+1} - 1 = 2^{6d}(M_q + 1) - 1 \quad \Rightarrow \quad \frac{M_p + 1}{M_q + 1} = 2^{6d}$$

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

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

A (34) tört csak akkor egész szám, ha *C=0*. Ebből azonban az következne, hogy

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

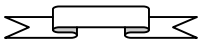
ami ellentmond a **IV.** feltételnek, tehát a **IV.** eset nem lehetséges.

Végtelen sok Mersenne-prím létezésének bizonyítása

Dénes Tamás matematikus

Mivel a (19), (24), (29), (34) összefüggések érvényesek maradnak, ha K^- helyére K^+-t írunk, ezért a V.-VIII. esetek sem lehetségesek. Tehát a tétel állítása hamis. Vagyis nem igaz, hogy véges számú Mersenne-prím van, amiből következik, hogy a Mersenne-prímek száma végtelen.

Q.E.D.



Végtelen sok Mersenne-prím létezésének bizonyítása

Dénes Tamás matematikus

2. Táblázat

	k^-	k^+	$p=$ $=6k\pm1$	**Mersenne-számok** (M_p)
1.	1		5	$M_5=2^5-1=$***31 (prím)***
2.		1	7	$M_7=2^7-1=$***127 (prím)***
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 (prím)***
5.	3		17	$M_{17}=2^{17}-1=$***131.071 (prím)***
6.		3	19	$M_{19}=2^{19}-1=$***524.287 (prím)***
7.	4		23	$M_{23}=2^{23}-1=$***8.388.607***$=(6\cdot8-1)(6\cdot29.747-1)$
8.		4	25	***NEM Mersenne-szám*** $2^{25}-1=33.554.431=(6\cdot5+1)(6\cdot100+1)(6\cdot300+1)$
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 (prím)***
11.	6		35	***NEM Mersenne-szám*** $2^{35}-1=34.359.738.367=(6\cdot5+1)(6\cdot12-1)(6\cdot21+1)(6\cdot20.487-1)$
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	***NEM Mersenne-szám*** $2^{49}-1=562.949.953.421.311=(6\cdot21+1)(6\cdot738.779.466.432+1)$
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	***NEM Mersenne-szám*** $2^{55}-1=36.028.797.018.963.967=(6\cdot4-1)(6\cdot5+1)(6\cdot15-1)(6\cdot147-1)$ $(6\cdot532-1)(6\cdot33.660+1)$
19.	10		59	$M_{59}=2^{59}-1=$***576.460.752.303.423.487 (prím)***
20.		10	61	$M_{61}=2^{61}-1=$***2.305.843.009.213.693.951 (prím)***
21.	11		65	***NEM Mersenne-szám*** $2^{65}-1=36.893.488.147.419.103.231=(6\cdot5+1)(6\cdot1.365+1)$ $(6\cdot24.215.857.259.685+1)$
22.		11	67	$M_{67}=2^{67}-1=$***147.573.952.589.676.412.927***$=$ $(6\cdot32.284.620+1)(6\cdot126.973.042.881+1)$

Dénes Tamás matematikus

Hivatkozás jegyzék

[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] Mersenne-számok alapvető tulajdonságai
(Párhuzamos algoritmus a Mersenne-számok prímfelbontására)
http://www.titoktan.hu/_raktar/_e_vilagi_gondolatok/Mersenne-primek1.pdf