

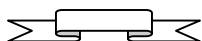
Ikerprím alapú Mersenne-ikerprímek tulajdonságai

Dénes Tamás matematikus

Budapest, 2001.

Abstract

Jelen dolgozatban megmutatjuk, hogy nincs két szomszédos Mersenne-prím amely ikerprím lenne. Majd definiáljuk az ikerprím párra épülő Mersenne-ikerprímeket és megvizsgáljuk ezek alapvető tulajdonságait.



A [Dénes 2001c]-ben bizonyított 2. tétel szerint, ha $p > 3$ prímszám és $M_p = 2^p - 1$ Mersenne-prím, akkor igaz az alábbi (1) és (2) összefüggés.

$$(1) \quad p = 6k - 1 \quad (k = 1, 2, 3, \dots) \Rightarrow M_p = \left(6 \sum_{i=0}^{3k-2} 4^i \right) + 1$$

$$(2) \quad p = 6k + 1 \quad (k = 1, 2, 3, \dots) \Rightarrow M_p = \left(6 \sum_{i=0}^{3k-1} 4^i \right) + 1$$

Használjuk fel a következő ismert azonosságot:

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

és vezessük be a (4), (5) jelöléseket.

$$(4) \quad m^-(k) = \sum_{i=0}^{3k-2} 4^i \stackrel{(3)}{=} \frac{4^{3k-1} - 1}{3} \quad (k = 1, 2, 3, \dots)$$

$$(5) \quad m^+(k) = \sum_{i=0}^{3k-1} 4^i \stackrel{(3)}{=} \frac{4^{3k} - 1}{3} \quad (k = 1, 2, 3, \dots)$$

A [Dénes 2001c]-ben bizonyított 1. tétel szerint ha M_p Mersenne-prím, akkor mindig $6K + 1$ alakú (K term.szám). Az ikerprímekről viszont tudjuk, hogy ha p és $p + 2$ ikerprím, akkor $p = 6k - 1$ és $p + 2 = 6k + 1$ alakú (k term.szám), tehát két Mersenne-prím soha nem lehet ikerprím.

Vizsgálhatjuk azonban a p , $p + 2$ ikerprímekhez tartozó M_p , M_{p+2} egymásutáni Mersenne-számokat.

1. DEFINÍCIÓ (Mersenne-ikerprím)

Legyenek M_p, M_{p+2} a $p > 3, p+2$ ikerprímekhez tartozó Mersenne-számok. Ha $M_p = 2^p - 1$ és $M_{p+2} = 2^{p+2} - 1$ prímszámok, akkor $p, p+2$ alapú Mersenne-ikerprímeknek nevezzük.

----- . -----

Az 1. definícióból adódik a $p, p+2$ alapú Mersenne-ikerprímekre a következő:

$$(6) \quad p = 6k - 1, p + 2 = 6k + 1 \quad (k = 1, 2, 3, \dots) \Rightarrow M_p = 2^{6k-1} - 1, M_{p+2} = 2^{6k+1} - 1$$

$$(7) \quad M_{p+2} - M_p = 2^{6k+1} - 2^{6k-1} = 3 \cdot 2^{6k-1} = 3(M_p + 1) \Rightarrow M_{p+2} = 4M_p + 3$$

A Mersenne-ikerprímekre vonatkozó (7) eredményt demonstrálják az 1. táblázat 1.-2., 5.-6. és 19.-20. sorai. Természetesen az egymás utáni Mersenne-számokra levezetett (7) összefüggés minden esetben érvényes, ha $k = k^+ = k^-$ (az 1. táblázat jelöléseit használva), így az M_p és M_{p+2} Mersenne-szám párja elméletileg a következő négy eset lehetséges:

(8)

	a. Mersenne- ikerprímek	b.	c.	d.
M_p	prím	prím	Nem prím	Nem prím
M_{p+2}	prím	Nem prím	prím	Nem prím
Példák az 1. tábla soraiban	1.-2. 5.-6. 19.-20.	NEM LEHETSÉGES! (lásd 1.tétel)	3.-4. 9.-10.	13.-14.

Érdekes problémát vet fel, hogy a (8)/b. esetre az első húsz Mersenne-szám között nem találunk példát (lásd 1. táblázat). Ennek oka a következő 1. tétel.

1. TÉTEL

Ha M_p Mersenne-prím, akkor M_{p+2} nem lehet összetett szám.

BIZONYÍTÁS

A (7) összefüggés szerint $M_{p+2} = 4M_p + 3$, ami akkor és csak akkor lehet összetett szám, ha M_p osztható 3-al. Ez viszont ellentmond annak, hogy a tétel feltétele szerint M_p Mersenne-prím.

Q.E.D.

Az 1. tételből következik a következő 2. tétel:

2. TÉTEL

Ha $p, p+2$ ikerprímek és M_p Mersenne-prím, akkor M_{p+2} is Mersenne-prím. Vagyis M_p és M_{p+2} mindig $p, p+2$ alapú Mersenne-ikerprímek.

----- . -----

NYITOTT PROBLÉMA: Van-e végtelen sok $p, p+2$ ikerprím, amelyhez van $p, p+2$ alapú M_p, M_{p+2} Mersenne-ikerprím?

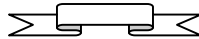
Dénes Tamás matematikus

Tételezzük fel, hogy *véges sok* $p, p+2$ alapú M_p, M_{p+2} Mersenne-ikerprím van. Ekkor létezik olyan q prímszám, hogy minden $p=6k-1$ alakú $p > q$ prímszám esetén, M_p, M_{p+2} nem Mersenne-ikerprím. Ez a (8) összefüggések szerint csak úgy lehet, ha M_p nem prímszám.

A fenti nyitott probléma megválaszolása tehát ekvivalens a következő 3. tétel bizonyításával, vagy annak cáfolatával.

3. TÉTEL

Véges sok $p=6k-1$ (k term.szám) prímszám létezik, amelyre $M_p=2^p-1$ Mersenne-prím.



1. Táblázat

	k^-	k^+	$p = 6k \pm 1$	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	$M_{11}=2^{11}-1=2.047=(6 \cdot 4-1)(6 \cdot 15-1)$
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	$M_{23}=2^{23}-1=8.388.607=(6 \cdot 8-1)(6 \cdot 29.747-1)$
8.		4	25	NEM Mersenne-szám $2^{25}-1=33.554.431=(6 \cdot 5+1)(6 \cdot 100+1)(6 \cdot 300+1)$
9.	5		29	$M_{29}=2^{29}-1=536.870.911=(6 \cdot 39-1)(6 \cdot 384.028-1)$
10.		5	31	$M_{31}=2^{31}-1=2.147.483.647$ (prím)
11.	6		35	NEM Mersenne-szám $2^{35}-1=34.359.738.367=(6 \cdot 5+1)(6 \cdot 12-1)(6 \cdot 21+1)(6 \cdot 20.487-1)$
12.		6	37	$M_{37}=2^{37}-1=137.438.953.471=(6 \cdot 37+1)(6 \cdot 102.719.696+1)$
13.	7		41	$M_{41}=2^{41}-1=2.199.023.255.551=(6 \cdot 2.228-1)(6 \cdot 27.418.559-1)$
14.		7	43	$M_{43}=2^{43}-1=8.796.093.022.207=(6 \cdot 698.148+1)(6 \cdot 349.977+1)$
15.	8		47	$M_{47}=2^{47}-1=140.737.488.355.327=(6 \cdot 392-1)(6 \cdot 9.977.136.563-1)$
16.		8	49	NEM Mersenne-szám $2^{49}-1=562.949.953.421.311=(6 \cdot 21+1)(6 \cdot 738.779.466.432+1)$
17.	9		53	$M_{53}=2^{53}-1=9.007.199.254.740.991=(6 \cdot 11.572-1)(6 \cdot 21.621.464.127-1)$
18.		9	55	NEM Mersenne-szám $2^{55}-1=36.028.797.018.963.967=(6 \cdot 4-1)(6 \cdot 5+1)(6 \cdot 15-1)(6 \cdot 147-1)(6 \cdot 532-1)(6 \cdot 33.660+1)$
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 $2^{65}-1=36.893.488.147.419.103.231=(6 \cdot 5+1)(6 \cdot 1.365+1)(6 \cdot 24.215.857.259.685+1)$
22.		11	67	$M_{67}=2^{67}-1=147.573.952.589.676.412.927=(6 \cdot 32.284.620+1)(6 \cdot 126.973.042.881+1)$

Hivatkozás jegyzék

[Dénes 2001a] Complementary prime-sieve P_Ure 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