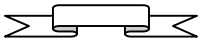
Mersenne-számok alapvető tulajdonságai

(Párhuzamos algoritmus a Mersenne-számok prímfelbontására)

Dénes Tamás matematikus

Budapest, 2001.

Abstract
Jelen dolgozatban szükséges és elegendő feltételt adunk arra, hogy ha *p* prím, akkor egy $M_p=2^p-1$ Mersenne-szám mikor összetett. Valamint megadjuk az erre a tételre épülő teszt algoritmust, amely megadja a Mersenne-számok kéttényezős felbontását is. Az algoritmus párhuzamos számítással végezhető, így a sebessége jelentősen növelhető, aminek a nagy prímszámok előállításánál és prím tesztelésnél van jelentősége.



1. TÉTEL
Az $M_p=2^p-1$ Mersenne-szám ($p\geq 3$ *prím*) minden *p* esetén $6K+1$ alakú (K=1,2,3,…).

BIZONYÍTÁS
A Dénes-féle prímszám tétel [Dénes 2001a-b] alapján (mely szerint *„minden 3-nál nagyobb prímszám* $6k\pm 1$ *alakú, ahol k term.szám”*) két eset lehetséges:

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

(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.

A továbbiakban felhasználjuk az ismert (3) összefüggést.

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

Mersenne-számok alapvető tulajdonságai

Dénes Tamás matematikus

Az 1. tétel következményei:

K0. A hivatkozott Dénes-féle prímszám tétel és a fenti 1. tétel szerint tehát, ha M_p Mersenne-prím, akkor csak *6K+1* alakú lehet.

K1. Ha $p^- = 6k-1$ (*k=1,2,3,…*) prímszám, akkor az ehhez tartozó Mersenne-számra fennáll a következő:

$$M_{p^-} = 2^{6k-1} - 1 = 6K^- + 1 \Rightarrow 2^{6k-1} - 2 = 6K^- \Rightarrow 2^{2(3k-1)} = 3K^- + 1 \Rightarrow$$

(4a)

$$\Rightarrow 4^{3k-1} - 1 = 3K^- \Rightarrow 3\sum_{i=0}^{3k-2} 4^i = 3K^- \quad \Rightarrow \quad K^- = \sum_{i=0}^{3k-2} 4^i = \sum_{i=0}^{\frac{p-3}{2}} 4^i$$

K2. Ha $p^+ = 6k+1$ (*k=1,2,3,…*) prímszám, akkor az ehhez tartozó Mersenne-számra fennáll a következő:

$$M_{p^+} = 2^{6k+1} - 1 = 6K^+ + 1 \Rightarrow 2^{6k} = 3K^+ + 1 \Rightarrow 4^{3k} - 1 = 3K^+ \Rightarrow$$

(4b)

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

K1. és K2. alapján kimondhatjuk az alábbi 2. tételt:

2. TÉTEL

Ha *p>3* prímszám és $M_p=2^p-1$ Mersenne-szám, akkor igaz az alábbi (5a) és (5b) összefüggés.

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

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

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

Ekkor a [Dénes 2001b 2.tétel] komplementer prímszita tételt felhasználva, kimondhatjuk az alábbi 3. tételt, amely szükséges és elegendő feltételt ad az összetett Mersenne-számokra.

3. TÉTEL

Bármely *p*>3 prímszám esetén az $M_p = 2^p - 1$ Mersenne-szám akkor és csak akkor összetett, ha (8a) vagy (8b) összefüggések valamelyike teljesül. Legyenek $u,v \geq 1$ természetes számok.

Dénes Tamás matematikus

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

Mivel *2*-nek minden páros hatványa (*p-1* páros) *mod 3=1*, így a (8a), (8b) egyenletek mindig megoldhatók, és a megoldást az adott diophantosi egyenletek megoldásai adják, vagyis ha *3*(*6uv-u-v*)*+1*, vagy *3*(*6uv+u+v*)*+1 2*-hatvány. Tehát kimondhatjuk a következő 4. tételt.
, hogy végtelen sok összetett Mersenne-szám létezik.

4. TÉTEL
Végtelen sok összetett Mersenne-szám létezik.

----- . -----

Például: *u=4*, *v=15* $\Rightarrow$ *3*(*6uv-u-v*)*+1=1.024=2*^{10} $\Rightarrow$ *p=11* (lásd 1. 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)

NYITOTT PROBLÉMA: Van-e végtelen sok Mersenne-prím?

Algoritmus a Mersenne-számok prímfelbontására (prím-teszt)

A 3. tétel algoritmust biztosít ahhoz, hogy adott M_p Mersenne-számról eldöntsük, hogy Mersenne-prím-e. Az algoritmus a (8a-b) összefüggésekre épül, azaz

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

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

Mivel a (9), (10) összefüggések *u*,*v*-re szimmetrikusak, így ha *u*-t végig futtatjuk *u=v*-ig, akkor az összes lehetséges *v* érték előáll.

Dénes Tamás matematikus

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

Ha $p^-=6k-1$ prímszám, akkor a 3. tétel szerint $M_{p^-} = 2^{p^-} - 1$ akkor és csak akkor Mersenne-prím, ha nincs olyan $1 \le u \le u_{max}$ érték, amelyre a (9)-beli v érték egész szám. A 3. tételből az is következik, hogy ha M_{p^-} nem prímszám, akkor van olyan u,v értékpár, amelyre (9)-ben v egész értéket vesz fel, így ez az algoritmus közvetlenül előállítja a Mersenne-szám kéttényezős felbontását:

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

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

Az algoritmus maximum u_{max} lépést végez, ha a Mersenne-szám prím, ha azonban nem prím, akkor $\left[\frac{p_1}{6}\right]$ lépésben állítja elő a (13), (14) prímfelbontást, ahol p_1 az M_{p^-} (vagy M_{p^+}) legkisebb prímtényezője.

Érdemes megjegyezni, hogy jelen algoritmus könnyen végezhető u-szerinti párhuzamosítással, így sebessége a processzorok száma szerint növelhető. Az 1. táblázatban közlünk néhány illusztráló példát a (13), (14) felbontásra.

Összetett Mersenne-számok két alaptulajdonsága

Ha M_p összetett Mersenne-szám, akkor a [Dénes 2001a]-ban bizonyított 1. tétel szerint van (15) alakú prímfelbontása.

(15) $M_p = p_1 \cdot p_2 \cdot \ldots \cdot p_s = (6r_1 \pm 1)(6r_2 \pm 1) \cdot \ldots \cdot (6r_s \pm 1)$, ahol $s \ge 1$, $r_1, r_2, \ldots, r_s$ *term.számok*

(15)-ból könnyen adódik, hogy ha M_p összetett Mersenne-szám, akkor felírható (16) alakban.

(16) $M_p = (6r_1 \pm 1)(6r_2 \pm 1)$ (r_1 és r_2 természetes számok)

Dénes Tamás matematikus

5. TÉTEL
Ha M_p összetett Mersenne-szám, akkor a (16) felbontások közül csak azok fordulhatnak elő, amikor a két tényezőben ± 1 azonos előjelű.

BIZONYÍTÁS
Tegyük fel, hogy $M_p = (6r_1 + 1)(6r_2 - 1)$, ekkor

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

p-re az (1) és (2) esetek valamelyike állhat fenn.

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

A (18) egyenlőség azonban *nem lehetséges*, mivel $2 \cdot 4^{3k-1} \bmod 3 \neq 0$

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

A (19) egyenlőség szintén *nem lehetséges*, mivel $2 \cdot 4^{3k} \bmod 3 \neq 0$

Mivel a (17) egyenlőség r_1 és r_2-re szimmetrikus, így a (18), (19) levezetések mindkét esetben érvényesek.

Tegyük fel, hogy $M_p = (6r_1 + 1)(6r_2 + 1)$, ekkor

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

p-re az (5a) és (5b) esetek valamelyike állhat fenn.

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

A (21) egyenlőség *lehetséges*, mivel mindkét oldala osztható 3-al.

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

A (22) egyenlőség *lehetséges*, mivel mindkét oldala osztható 3-al.

Q.E.D.

6. TÉTEL
Ha M_p összetett Mersenne-szám, akkor $M_p \bmod 3 = 1$.

BIZONYÍTÁS
p-re az (5a) és (5b) esetek valamelyike állhat fenn.

Dénes Tamás matematikus

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

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

Q.E.D.

Illusztrációként lásd az 1. táblázat 3., 7., 9., 12.-15. és 17. sorait.

Mersenne-számok alapvető tulajdonságai

Dénes Tamás matematikus

1. 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***$=$ $(6\cdot32.284.620+1)(6\cdot126.973.042.881+1)$

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