Dénes-féle Szimmetrikus prímszám tétel
és alkalmazása a páros Goldbach-sejtés bizonyítására

Dénes Tamás matematikus-kriptográfus
Email: tdenest@freemail.hu

Abstract
A dolgozatban bizonyított tétel szerint, minden *N*≥*4* természetes számhoz létezik $m_N \geq 0$ természetes szám, hogy $p_{N-} = N - m_N$ és $p_{N+} = N + m_N$ prímszámok (Dénes-féle Szimmetrikus prímszám tétel). E tétel közvetlen következményeként adódik a páros Goldbach-sejtés bizonyítása, amelyet így 275 év után Goldbach-tételnek nevezhetünk.

----- . -----

1. Tétel *(Dénes-féle Szimmetrikus prímszám tétel)*

Minden *N*≥*4* **természetes számhoz létezik** $m_N \geq 0$ **természetes szám, hogy** $p_{N-} = N - m_N$ **és** $p_{N+} = N + m_N$ **prímszámok.**

Az 1. tétel ekvivalens megfogalmazása:
Minden *N*≥*4* **természetes számhoz létezik** $m_N \geq 0$ **természetes szám, hogy** ***N*** **előáll a** p_{N-} **és** p_{N+} **prímszámok számtani közepeként, azaz**

(s0) $$N = \frac{p_{N-} + p_{N+}}{2}$$

BIZONYÍTÁS

$N = 4 \Rightarrow m_N = 1 \Rightarrow \quad p_{N-} = 4 - 1 = 3, \quad p_{N+} = 4 + 1 = 5$

$N = 5 \Rightarrow m_N = 2 \Rightarrow \quad p_{N-} = 5 - 2 = 3, \quad p_{N+} = 5 + 2 = 7$

Tehát a tétel *N*=*4* és *N*=*5* esetén igaz.

Mivel a jelen tétel állítása szerint p_{N-} és p_{N+} prímszámok, így a [Dénes 2001]-ben bizonyított 1. tétel miatt, ha p_{N-} és p_{N+} 5-nél nagyobb prímek, akkor az alábbiak valamelyike teljesül:

(s1) $p_{N-} = 6k - 1$ *és* $p_{N+} = 6r - 1$ (*k*=*1,2,3,…*), (*r*=*1,2,3,…*)

(s2) $p_{N-} = 6k - 1$ *és* $p_{N+} = 6r + 1$ (*k*=*1,2,3,…*), (*r*=*1,2,3,…*)

(s3) $p_{N-} = 6k + 1$ *és* $p_{N+} = 6r - 1$ (*k*=*1,2,3,…*), (*r*=*1,2,3,…*)

(s4) $p_{N-} = 6k + 1$ *és* $p_{N+} = 6r + 1$ (*k*=*1,2,3,…*), (*r*=*1,2,3,…*)

Az (s1)-(s4) összefüggésekből *N*-re és m_n-re a következőket kapjuk:

(s5)
$$\begin{aligned} &(s1) \Rightarrow \quad p_{N-} = 6k - 1 = N - m_N \Rightarrow \quad m_N = N - 6k + 1 \Rightarrow \\ &\quad \Rightarrow \quad p_{N+} = 6r - 1 = N + N - 6k + 1 \Rightarrow \quad 0 = 2N - 6k - 6r + 2 \Rightarrow \\ &\quad \Rightarrow \quad N = 3(k + r) - 1 \quad \Rightarrow m_N = 3(r - k) \end{aligned}$$

(s6)
$$(s2) \Rightarrow \quad p_{N-} = 6k-1 = N - m_N \;\Rightarrow\; m_N = N - 6k + 1 \Rightarrow$$
$$\Rightarrow \quad p_{N+} = 6r+1 = N + N - 6k + 1 \;\Rightarrow\; 0 = 2N - 6k - 6r \Rightarrow$$
$$\Rightarrow \quad N = 3(k+r) \quad \Rightarrow m_N = 3(r-k)+1$$

(s7)
$$(s3) \Rightarrow \quad p_{N-} = 6k+1 = N - m_N \;\Rightarrow\; m_N = N - 6k - 1 \Rightarrow$$
$$\Rightarrow \quad p_{N+} = 6r-1 = N + N - 6k - 1 \Rightarrow \; 0 = 2N - 6k - 6r \Rightarrow$$
$$\Rightarrow \quad N = 3(k+r) \quad \Rightarrow m_N = 3(r-k)-1$$

(s8)
$$(s4) \Rightarrow \quad p_{N-} = 6k+1 = N - m_N \;\Rightarrow\; m_N = N - 6k - 1 \Rightarrow$$
$$\Rightarrow \quad p_{N+} = 6r+1 = N + N - 6k - 1 \Rightarrow \; 0 = 2N - 6k - 6r - 2 \Rightarrow$$
$$\Rightarrow \quad N = 3(k+r)+1 \quad \Rightarrow m_N = 3(r-k)$$

Könnyen belátható, hogy (s5)-(s8) előállítja az *N=3u-1*, *N=3u*, *N=3u+1* alakú természetes számokat. A kimaradt *N=3u-2* és *N=3u+2* alakok ezekre visszavezethetők az alábbi módon:

(s9) *N=3u-2=3u-2-1+1=3(u-1)+1*, ami megfelel (s8)-nak, ha *k+r=u-1*

(s10) *N=3u+2=3u+2+1-1=3(u+1)-1*, ami megfelel (s5)-nek, ha *k+r=u+1*

Tehát az (s5)-(s8) összefüggések előállítják az összes *N* természetes számot!

Továbbiakban bizonyítandó, hogy bármely *N≥6*, illetve m_N természetes szám esetén az (s5)-(s8) esetek valamelyikében van olyan p_{N-}, p_{N+} pár, hogy mindkettő prímszám. A fentiekre néhány példát mutat be az 1. Táblázat.

1. Táblázat

N			**k+r**	**k**	**r**	m_N	p_{N-}	p_{N+}
10	(s8)	*N=3(k+r)+1*	3	1	2	*3(r-k)=***3**	*6k+1=7(prím)*	*6r+1=13(prím)*
15	(s6)	*N=3(k+r)*	5	1	4	*3(r-k)+1=10*	*6k-1=5(prím)*	*6r+1=25=5x5 (nem prím)*
			5	2	3	*3(r-k)+1=***4**	*6k-1=11(prím)*	*6r+1=19(prím)*
15	(s7)	*N=3(k+r)*	5	1	4	*3(r-k)-1=***8**	*6k+1=7(prím)*	*6r-1=23(prím)*
			5	2	3	*3(r-k)-1=***2**	*6k+1=13(prím)*	*6r-1=17(prím)*
82	(s8)	*N=3(k+r)+1*	27	1	26	*3(r-k)=***75**	*6k+1=7(prím)*	*6r+1=157(prím)*
99	(s6)	*N=3(k+r)*	33	1	32	*3(r-k)+1=***94**	*6k-1=5(prím)*	*6r+1=193(prím)*
			33	2	31	*3(r-k)+1=88*	*6k-1=11(prím)*	*6r+1=187=11x17 (nem prím)*
			33	3	30	*3(r-k)+1=***82**	*6k-1=17(prím)*	*6r+1=181(prím)*
100	(s8)	*N=3(k+r)+1*	33	3	30	*3(r-k)=***81**	*6k+1=19(prím)*	*6r+1=181(prím)*
5.689	(s8)	*N=3(k+r)+1*	1.896	926	970	*3(r-k)=***132**	*6k+1=5.557 (prím)*	*6r+1=5.821(prím)*
				10	1.886	*3(r-k)=***5.628**	*6k+1=61(prím)*	*6r+1=11.317(prím)*
8. 956. 732	(s8)	N=3(k+r)+1	2.985.577	1.492.761	1.492.816	*3(r-k)=***165**	*6k+1=8.956.567 (prím)*	*6r+1=8.956.897 (prím)*

Dénes Tamás *matematikus-kriptográfus* Email: tdenest@freemail.hu

BIZONYÍTÁS folytatása (indirekt)
Az 1. tétel tagadása:
Bármely m_N<N természetes szám esetén teljesül, hogy a $p_{N-} = N - m_N$ *és* $p_{N+} = N + m_N$ párnak legfeljebb az egyik tagja prím. Ez háromféleképpen állhat elő:
I. p_{N-} prím és p_{N+} összetett szám,
II. p_{N-} összetett szám és p_{N+} prím,
III. p_{N-} és p_{N+} egyaránt összetett szám.

I. ESET
(s11) $\forall 1 \le m_N \le N-2 \Rightarrow p_{N-} = N - m_N \ (prím) \Rightarrow p_{N+} = N + m_N = p_{N-} + 2m_N \ (nem\ prím)$

Ekkor a [Dénes 2001]-ben bizonyított 2. tétel miatt, p_{N+}-ra az alábbiak valamelyike teljesül:
(s12) $p_{N+} = 6r - 1$ és $r=6uv+u-v$ ($u=1,2,3, \ldots$), ($v=1,2,3,\ldots$)
(s13) $p_{N+} = 6r - 1$ és $r=6uv-u+v$ ($u=1,2,3, \ldots$), ($v=1,2,3,\ldots$)
(s14) $p_{N+} = 6r + 1$ és $r=6uv+u+v$ ($u=1,2,3, \ldots$), ($v=1,2,3,\ldots$)
(s15) $p_{N+} = 6r + 1$ és $r=6uv-u-v$ ($u=1,2,3, \ldots$), ($v=1,2,3,\ldots$)

(s11) és (s12) alapján adódik:

(s16)
$$p_{N+} = p_{N-} + 2m_N = 6(6uv + u - v) - 1 \Rightarrow \quad m_N = 3(6uv + u - v) - \frac{p_{N-} + 1}{2} \quad \Rightarrow$$
$$\Rightarrow \quad N = p_{N-} + m_N = p_{N-} + 3(6uv + u - v) - \frac{p_{N-} + 1}{2} = \frac{p_{N-} + 6(6uv + u - v) - 1}{2}$$

(s11) és (s13) alapján adódik:

(s17)
$$p_{N+} = p_{N-} + 2m_N = 6(6uv - u + v) - 1 \Rightarrow \quad m_N = 3(6uv - u + v) - \frac{p_{N-} + 1}{2} \quad \Rightarrow$$
$$\Rightarrow \quad N = p_{N-} + m_N = p_{N-} + 3(6uv - u + v) - \frac{p_{N-} + 1}{2} = \frac{p_{N-} + 6(6uv - u + v) - 1}{2}$$

(s11) és (s14) alapján adódik:

(s18)
$$p_{N+} = p_{N-} + 2m_N = 6(6uv + u + v) + 1 \Rightarrow \quad m_N = 3(6uv + u + v) - \frac{p_{N-} - 1}{2} \quad \Rightarrow$$
$$\Rightarrow \quad N = p_{N-} + m_N = p_{N-} + 3(6uv + u + v) - \frac{p_{N-} - 1}{2} = \frac{p_{N-} + 6(6uv + u + v) + 1}{2}$$

(s11) és (s15) alapján adódik:

(s19)
$$p_{N+} = p_{N-} + 2m_N = 6(6uv - u - v) + 1 \Rightarrow \quad m_N = 3(6uv - u - v) - \frac{p_{N-} - 1}{2} \quad \Rightarrow$$
$$\Rightarrow \quad N = p_{N-} + m_N = p_{N-} + 3(6uv - u - v) - \frac{p_{N-} - 1}{2} = \frac{p_{N-} + 6(6uv - u - v) + 1}{2}$$

***Dénes Tamás** matematikus-kriptográfus* Email: tdenest@freemail.hu

Mivel az indirekt feltevés miatt az (s11) állításnak, az adott N esetén minden $m_N<N$-re teljesülnie kell, ezért elegendő megmutatni, hogy *nincs olyan N*, amelyre az (s16)-(s19) egyenlőségek mindegyike teljesül. Ekkor ugyanis teljesülnie kell a következő (s20), (s22), (s23), (s25), (s26), (s27) egyenleteknek:

(s20) $$N \overset{(s16)}{=} \frac{p_{N-}+6(6uv+u-v)-1}{2} \overset{(s17)}{=} \frac{p_{N-}+6(6uv-u+v)-1}{2} \quad\Rightarrow\quad u=v$$

Az $u=v$ eredményt behelyettesítve az (s16)-(s19) egyenletekbe, p_{N+}-ra a következőket kapjuk:

(s21)
$$u=v \quad \overset{(s16),(s17)}{\Rightarrow} \quad p_{N+}=p_{N-}+2\left(3\cdot 6u^2-\frac{p_{N-}+1}{2}\right)=p_{N-}+36u^2-p_{N-}-1=$$
$$=36u^2-1=(6u-1)(6u+1)$$
$$u=v \quad \overset{(s18)}{\Rightarrow} p_{N+}=p_{N-}+2\left(3(6u^2+2u)-\frac{p_{N-}-1}{2}\right)=p_{N-}+36u^2+12u-p_{N-}+1=$$
$$=36u^2+12u+1=(6u+1)^2$$
$$u=v \quad \overset{(s19)}{\Rightarrow} p_{N+}=p_{N-}+2\left(3(6u^2-2u)-\frac{p_{N-}-1}{2}\right)=p_{N-}+36u^2-12u-p_{N-}+1=$$
$$=36u^2-12u+1=(6u-1)^2$$

(s21)-ből látható, hogy $u=v$ esetén p_{N+} soha sem prímszám, azaz teljesül az (s11) indirekt feltétel.

(s22)
$$N \overset{(s16)}{=} \frac{p_{N-}+6(6uv+u-v)-1}{2} \overset{(s18)}{=} \frac{p_{N-}+6(6uv+u+v)+1}{2} \quad\Rightarrow$$
$$\Rightarrow 6(6uv+u-v-6uv-u-v)=2 \quad\Rightarrow\quad v=-\frac{1}{6}$$

Az (s12)-(s15) feltételek szerint v természetes szám, így az (s22) eset nem állhat elő.

(s23)
$$N \overset{(s16)}{=} \frac{p_{N-}+6(6uv+u-v)-1}{2} \overset{(s19)}{=} \frac{p_{N-}+6(6uv-u-v)+1}{2} \quad\Rightarrow$$
$$\Rightarrow 6(6uv+u-v-6uv+u+v)=2 \quad\Rightarrow\quad u=\frac{1}{6}$$

Az $u=\frac{1}{6}$ eredményt behelyettesítve az (s16)-(s19) egyenletekbe, p_{N+}-ra a következőket kapjuk:

***Dénes Tamás** matematikus-kriptográfus* Email: tdenest@freemail.hu

(s24)
$$u=\frac{1}{6}\ \overset{(s16),(s17)}{\Rightarrow}\ p_{N+}=p_{N-}+2\left(3(v+\frac{1}{6}-v)-\frac{p_{N-}+1}{2}\right)=p_{N-}+1-p_{N-}-1=0$$
$$u=\frac{1}{6}\ \overset{(s18)}{\Rightarrow}\ p_{N+}=p_{N-}+2\left(3(v+\frac{1}{6}+v)-\frac{p_{N-}-1}{2}\right)=p_{N-}+12v+1-p_{N-}+1=$$
$$=2(6v+1)$$
$$u=\frac{1}{6}\ \overset{(s19)}{\Rightarrow}\ p_{N+}=p_{N-}+2\left(3(v-\frac{1}{6}-v)-\frac{p_{N-}-1}{2}\right)=p_{N-}-1-p_{N-}+1=0$$

(s25)
$$N\overset{(s17)}{=}\frac{p_{N-}+6(6uv-u+v)-1}{2}\overset{(s18)}{=}\frac{p_{N-}+6(6uv+u+v)+1}{2}\Rightarrow$$
$$\Rightarrow 6(6uv-u+v-6uv-u-v)=2\ \Rightarrow\ u=-\frac{1}{6}$$

Az (s12)-(s15) feltételek szerint *u* természetes szám, így az (s25) eset nem állhat elő.

(s26)
$$N\overset{(s17)}{=}\frac{p_{N-}+6(6uv-u+v)-1}{2}\overset{(s19)}{=}\frac{p_{N-}+6(6uv-u-v)+1}{2}\Rightarrow$$
$$\Rightarrow 6(6uv-u+v-6uv+u+v)=2\ \Rightarrow\ v=\frac{1}{6}$$

Mivel *u* és *v* az (s12)-(s15) feltételekben szimmetrikus, így ez az eset az (s24)-beli eredményeket adja.

(s27)
$$N\overset{(s18)}{=}\frac{p_{N-}+6(6uv+u+v)+1}{2}\overset{(s19)}{=}\frac{p_{N-}+6(6uv-u-v)+1}{2}\Rightarrow\ u=-v$$

Az (s12)-(s15) feltételek szerint *u* és *v* természetes számok, azonban (s27) szerint az egyikük mindenképpen negatív, így ez az eset nem állhat elő.

Az (s22)-(s27) levezetésekből világos, hogy adott *N*-re $u\neq v$ esetén nem minden m_N-re teljesül az (s11) indirekt feltétel, ami éppen a tétel állítását igazolja. Példaként lásd az 1. táblázat 7-9. sorát az *N=99* esetre.

II. ESET

Ha az (s12)-(s15) összefüggéseket p_{N-}-ra alkalmazzuk, akkor az (s16)-(s27) levezetésekben csupán a p_{N+} miatti előjel cserék lesznek, így a p_{N-}-ra vonatkozó következtetések, az I. eset szimmetrikus párjaként megmaradnak.

Dénes Tamás *matematikus-kriptográfus* Email: tdenest@freemail.hu

III. ESET

Ez az eset (s11)-hez hasonlóan, így írható fel:

(s28) $\forall 1 \le m_N \le N-2 \Rightarrow p_{N-} = N - m_N \ (nem\ prím) \Rightarrow p_{N+} = N + m_N \ (nem\ prím)$

Az (s28) állítást a következő 2.Táblázat foglalja össze, amelynek így a 2. és 4. oszlopában csak összetett számok lehetnek.

2. Táblázat

m_N	$p_{N-} = N - m_N$	$\boldsymbol{N}$	$p_{N+} = N + m_N$
1	*N-1*	*N*	*N+1*
2	*N-2*	*N*	*N+2*
3	*N-3*	*N*	*N+3*
4	*N-4*	*N*	*N+4*
…	…	…	…
i	*N-i*	*N*	*N+i*
…	…	…	…
N-5	***5***	*N*	*2N-5*
N-4	*4*	*N*	*2N-4*
N-3	***3***	*N*	*2N-3*
N-2	***2***	*N*	*2N-2*

Mivel az 1. tétel feltétele, hogy $N \ge 4$, valamint a III. eset (s28) feltétele szerint $1 \le m_N \le N-2$, ezért a feltételeknek megfelelő bármely *N* esetén a 2. táblázatban szerepel az *i*=*N-2* és *i*=*N-3* sor, így az ezekhez tartozó $p_{N-} = 2$ és $p_{N-} = 3$ értékek, vagyis az egyetlen páros és az első páratlan prímszám. Már ez elegendő az (s28) állítás cáfolatához. Ezt erősíti, hogy a 2. táblázat konstrukciójából adódik, hogy a 2. oszlopban p_{N-} befutja a teljes $2 \le p_{N-} \le N-1$ zárt intervallum egész értékeit, így felveszi az összes *N-1*-nél kisebb, vagy egyenlő prímszám értékeket. Ez viszont ellentmond az (s28) állításnak, vagyis a III. eset nem állhat elő.

Q.E.D.

Dénes Tamás *matematikus-kriptográfus* Email: tdenest@freemail.hu

A fenti III. esetre példaként bemutatjuk az *N=6* és *N=10* esetekhez tartozó, 2. táblázat szerinti 3. és 4. táblázatot, ahol a prímeket ***bold*** számok jelölik.

3. táblázat

m_N	$p_{N-} = N - m_N$	**N**	$p_{N+} = N + m_N$
1	***5***	6	***7***
2	*4*	6	*8*
3	***3***	6	*9*
4	***2***	6	*10*

4. táblázat

m_N	$p_{N-} = N - m_N$	**N**	$p_{N+} = N + m_N$
1	*9*	10	***11***
2	*8*	10	*12*
3	***7***	10	***13***
4	*6*	10	*14*
5	***5***	10	*15*
6	*4*	10	*16*
7	***3***	10	***17***
8	***2***	10	*18*

A fenti 1. Tétel következménye a páros Goldbach-sejtés bizonyítása.

Ugyanis az 1.Tétel (s0) megfogalmazásából következik, hogy minden *N*≥*4* természetes számhoz léteznek a $p_{N-} = N - m_N$, $p_{N+} = N + m_N$ prímek, amelyekre igaz, hogy

(s29) $$2N = p_{N-} + p_{N+}$$

Azaz minden páros szám előáll két prímszám összegeként.

Ezzel bizonyítottá vált ***az erős (páros) Goldbach sejtés,*** amelyet ezután ***Goldbach-tételnek*** nevezhetünk**.**[1]

[1] **Erős (páros) Goldbach-sejtés (1742)**: *Minden 2-nél nagyobb páros szám előáll két prímszám összegeként.*

Dénes Tamás *matematikus-kriptográfus* Email: tdenest@freemail.hu

5. Táblázat *(Példák a Dénes-féle Szimmetrikus prímszám tétel és a Goldbach-tétel illusztrálására)*

2N	***N***	m_N	$p_{N-} = N - m_N$	$p_{N+} = N + m_N$
8	4	1	***3***=4-1	***5***=4+1
10	5	2	***3***=5-2	***7***=5+2
20	10	3	***7***=10-3	***13***=10+3
30	15	2	***13***=15-2	***17***=15+2
32	16	3	***13***=16-3	***19***=16+3
100	50	3	***47***=50-3	***53***=50+3
112	56	3	***53***=56-3	***59***=56+3
202	101	12	***89***=101-12	***113***=101+12
1.000	500	9	**491**=500-9	***509***=500+9
10.000	5.000	81	***4.919***=5.000-81	***5.081***=5.000+81
100.000	50.000	123	***49.877***=50.000-123	***50.123***=50.000+123
1.000.000	500.000	57	***499.943***=500.000-57	***500.057***=500.000+57
8.000.000	4.000.000	237	***3.999.763***=4.000.000-237	***4.000.237***=4.000.000+237
10.000.000	5.000.000	87	***4.999.913***=5.000.000-87	***5.000.087***=5.000.000+87
30.800.000	15.400.000	237	***15.399.763***=15.400.000-237	***15.400.237***=15.400.000+237
30.971.720	15.485.860	3	***15.485.857***=15.485.860-3	***15.485.863***=15.485.860+3

Köszönetemet fejezem ki Győry Kálmán professzornak támogató segítségéért, és Szikszai Márton matematikus kollégának konstruktív észrevételeiért, amelyek hozzájárultak a bizonyítás teljessé tételéhez.

Hivatkozások

[Dénes 2001] Dénes, Tamás: *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
http://www.titoktan.hu/_raktar/_e_vilagi_gondolatok/KomplementerPrimszita.pdf