Általánosított Ikerprím tétel

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

Abstract

A [Dénes 2017]-ben bizonyított *Szimmetrikus prímszám tétel* kimondja, hogy bármely $N \geq 4$ természetes számhoz létezik szimmetrikus prím pár (p, q), amelyekre $p = N - m_N$ és $q = N + m_N$ úgy, hogy $m_N = \frac{q-p}{2}$ és $N = \frac{q+p}{2}$. Jelen dolgozatban bebizonyítjuk, hogy minden m_N természetes számhoz (távolsághoz) létezik végtelen sok szimmetrikus prím pár (*általánosított Ikerprím tétel*). A bizonyítást $m_N = 1$-re alkalmazva éppen az Ikerprím sejtés bizonyítását kapjuk, amelyet ezért a továbbiakban *Ikerprím tételnek* nevezhetünk.

Jelen dolgozat fő tételének bizonyítása a szerző 2001-ben bizonyított *komplementer prímszita tételére* épül (lásd [Dénes 2001]), amely szerint bármely $N=6k-1$ alakú természetes szám, akkor és csak akkor összetett, ha $k=6uv+u-v$, vagy $k=6uv-u+v$ alakú és bármely $N=6k+1$ alakú természetes szám, akkor és csak akkor összetett, ha $k=6uv+u+v$, vagy $k=6uv-u-v$ alakú természetes szám. E tételre alapozva adunk indirekt bizonyítást az *általánosított Ikerprím tételre.*

----- . -----

1. LEMMA

Bármely két prímszám különbsége és összege páros, tehát ha $q>p>2$ prímszámok, akkor mindig léteznek az $m_N = \frac{q-p}{2}$ és $N = \frac{q+p}{2}$ természetes számok.

Bizonyítás

Bármely 2-nél nagyobb prímszám páratlan. Tehát ha

(1) $p = 2k + 1 \rangle 2$ prímszám (k természetes szám)

(2) $q = 2l + 1 \rangle p$ prímszám (l természetes szám)

akkor

(3) $$\frac{q-p}{2} = \frac{2l+1-2k-1}{2} = l + k$$

(4) $$\frac{q+p}{2} = \frac{2l+1+2k+1}{2} = l + k + 1$$

Q.E.D.

----- . -----

Az 1. lemmából egyenesen következik a *Dénes-féle Szimmetrikus prímszám tétel* (lásd [Dénes 2017]) *megfordítása*, azaz igaz az alábbi 1. tétel:

1. TÉTEL

Bármely két $q>p>2$ prímszám esetén létezik $m_N = \frac{q-p}{2}$ és $N = \frac{q+p}{2}$, amelyekre teljesül, hogy $p = N - m_N$ és $q = N + m_N$

----- . -----

A [Dénes 2017]-ben bizonyított *Szimmetrikus prímszám tétel* kimondja, hogy bármely $N \geq 4$ természetes számhoz létezik szimmetrikus prím pár. Kérdés, hogy minden m_N természetes számhoz (távolsághoz) létezik-e szimmetrikus prím pár? Ezt bizonyítjuk az alábbi 2. tételben.

2. TÉTEL

Bármely m_N természetes számhoz létezik legalább egy $q>p$ szimmetrikus prím pár, amelyre teljesül, hogy $q = p + 2m_N$.

Bizonyítás (indirekt)

Tegyük fel, hogy létezik olyan $m_N = c$ természetes szám, amelyhez nincs a tétel feltételének megfelelő p, q szimmetrikus prím pár. Ekkor a [Dénes 2001]-ben bizonyított 2. tétel (*Komplementer prímszita*) alapján bármely p prímszámhoz az alábbi q számok valamelyike társítható, ha q nem prím:

(5) $q = 6r - 1 = p + 2c$ és $r=6uv+u-v$ $(u=1,2,3,\ldots)$, $(v=1,2,3,\ldots)$

(6) $q = 6r - 1 = p + 2c$ és $r=6uv-u+v$ $(u=1,2,3,\ldots)$, $(v=1,2,3,\ldots)$

(7) $q = 6r + 1 = p + 2c$ és $r=6uv+u+v$ $(u=1,2,3,\ldots)$, $(v=1,2,3,\ldots)$

(8) $q = 6r + 1 = p + 2c$ és $r=6uv-u-v$ $(u=1,2,3,\ldots)$, $(v=1,2,3,\ldots)$

Az (5)-(8) esetekből a p prímre a következőket kapjuk, amelyek valamelyikének minden u, v természetes számra teljesülni kell:

(9) $(5) \Rightarrow \quad p = 6r - 1 - 2c = 6(6uv + u - v) - 1 - 2c$

(10) $(6) \Rightarrow \quad p = 6r - 1 - 2c = 6(6uv - u + v) - 1 - 2c$

(11) $(7) \Rightarrow \quad p = 6r + 1 - 2c = 6(6uv + u + v) + 1 - 2c$

(12) $(8) \Rightarrow \quad p = 6r + 1 - 2c = 6(6uv - u - v) + 1 - 2c$

Megmutatjuk, hogy ha $u=v$, akkor létezik olyan u szám, amely esetén (9)-(12)-ben p összetett szám. Ez pedig ellentmond a tétel feltételének, amely szerint p prímszám.

(13)
$$Ha\ u = v = \frac{c+1}{6},\ akkor\ (9),(10) \Rightarrow$$
$$\Rightarrow p = 6(6u^2) - 1 - 2c = 6\left(6\frac{(c+1)^2}{6^2}\right) - 1 - 2c = (c+1)^2 - 1 - 2c = c^2$$

(14)
$$Ha\ u = v = \frac{c-1}{6},\ akkor\ (11) \Rightarrow$$
$$\Rightarrow p = 6(6u^2 + 2u) + 1 - 2c = 6\left(\frac{6(c-1)^2}{6^2} + \frac{2(c-1)}{6}\right) + 1 - 2c =$$
$$= (c-1)^2 + 2(c-1) + 1 - 2c = (c-1)^2 - 1 = (c-1-1)(c-1+1) = (c-2)c$$

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

$$Ha\ u = v = \frac{c+1}{6},\ akkor\ (12) \Rightarrow$$

(15) $$\Rightarrow p = 6(6u^2 - 2u) + 1 - 2c = 6\left(\frac{6(c+1)^2}{6^2} - \frac{2(c+1)}{6}\right) + 1 - 2c =$$

$$= (c+1)^2 - 2(c+1) + 1 - 2c = c^2 + 2c + 1 - 2c - 2 + 1 - 2c = c^2 - 2c = (c-2)c$$

A (13)-ban és (15)-ben szereplő $u = v = \frac{c+1}{6}$ feltétel mindig teljesül, ha $c=6s-1$, a (14)-ben szereplő $u = v = \frac{c-1}{6}$ feltétel pedig akkor teljesül, ha $c=6s+1$ ($s=1,2,3, \ldots$)

Q.E.D.

A 2. tételre mutatunk néhány példát az 1.-5. táblázatokban.

1. táblázat

p		***q=p+4***
3		7
7		11
13		17
19		23
…		…
349		353
…		…
1.579		1.583
…		…
1.019.173		1.019.177
…		…
10.082.623		10.082.627
…		…
15.484.243		15.484.247
…		…

2. táblázat

p		***q=p+6***
5		11
7		13
11		17
13		19
17		23
…		…
563		569
…		…
1.601		1.607
…		…
1.099.621		1.099.627
…		…
10.781.861		10.781.867
…		…
15.485.843		15.485.849
…		…

3. táblázat

p		***q=p+8***
3		11
5		13
11		19
23		31
29		37
…		…
449		457
…		…
1.571		1.579
…		…
1.000.151		1.000.159
…		…
10.000.349		10.000.357
…		…
15.416.699		15.416.707
…		…

4. táblázat

p		***q=p+10***
3		13
7		17
13		23
19		29
…		…
73		83
…		…
433		443
…		…
751		761
…		…
1.153		1.163
…		…
10.000.759		10.000.769
…		…
13.985.341		13.985.351
…		…
15.484.549		15.484.559
…		…
444.333.973		444.333.983
…		…
888.889.501		888.889.511
…		…

5. táblázat

p		***q=p+100***
3		103
7		107
13		113
31		131
…		…
487		587
…		…
1.723		1.823
…		…
1.000.033		1.000.133
…		…
10.000.591		10.000.691
…		…
15.485.341		15.485.441
…		…
444.333.313		444.333.413
…		…
888.889.501		888.889.601
…		…

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

Mivel a p, $q=p+2m_N$ szimmetrikus prím párok esetén $m_N=1$ éppen az ikerprímeket állítja elő, az alábbi 3. tételt *Általánosított Ikerprím tételnek* nevezzük.

3. TÉTEL (Általánosított Ikerprím tétel)

Legyenek $q>p>2$ N-re szimmetrikus $2m_N$ távolságú prímszámok, amelyekre $m_N = \frac{q-p}{2}$ és $N = \frac{q+p}{2}$, valamint $p=N-m_N$ és $q=N+m_N$. Ekkor bármely m_N természetes számhoz végtelen sok p, q szimmetrikus prím pár létezik.

Bizonyítás (indirekt)
Az előzőkben bizonyított 2. tétel szerint m_N felveheti az összes természetes szám értéket. [Dénes 2001] 1. tétele szerint az alábbi 6. táblázat tartalmazza az összes természetes számot úgy, hogy az 1. és 3. oszlopokban található az összes prímszám.
Tegyük fel, hogy a K-ik sor az utolsó, amelyben szereplő p_K és a tőle $2m_N$ távolságra lévő $q_K = p_K + 2m_N$ is prímszám. A tétel bizonyításának további részében a rövidebb írásmód kedvéért az $m_N=c$ jelölést fogjuk használni.

6. táblázat

k	1.	2.	3.	4.	5.	6.
	6k-1 ↓	***6k***	***6k+1*** ↓	***6k+2***	***6k+3***	***6k+4***
0			1	2	3	4
1	***5***	6	***7***	8	9	10
2	***11***	12	***13***	14	15	16
3	***17***	18	***19***	20	21	22
4	***23***	24	25	26	27	28
5	***29***	30	***31***	32	33	34
6	35	36	***37***	38	39	40
7	***41***	42	***43***	44	45	46
…	…	…	…	…	…	…
K	6K-1	6K	6K+1	6K+2	6K+3	6K+4
K+1	6(K+1)-1= 6K+5	6(K+1)= 6K+6	6(K+1)+1= 6K+7	6(K+1)+2= 6K+8	6(K+1)+3= 6K+9	6(K+1)+4= 6K+10
…	…	…	…	…	…	…
k=K+x	6k-1= 6(K+x)-1	6(K+x)	6k+1= 6(K+x)+1			
…	…	…	…	…	…	…

A 6. táblázat K-ik sorában két prímszám lehet, ezért a továbbiakban a (16) és (17) indirekt feltételeket kell vizsgálnunk.

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

Ha $p_K = 6K - 1$ és $q_K = p_K + 2c$ prímszámok, akkor minden x természetes szám esetén

(16)
$$\forall k = K + x \Rightarrow ha\ p_k = 6(K+x) - 1\ prím,\ akkor\quad q_k = p_k + 2c =$$
$$= 6(K+x) - 1 + 2c = \underbrace{6K - 1 + 2c}_{q_K} + 6x = q_K + 6x\ NEM\ \ prím$$

Ha $p_K = 6K + 1$ és $q_K = p_K + 2c$ prímszámok, akkor minden x természetes szám esetén

(17)
$$\forall k = K + x \Rightarrow ha\ p_k = 6(K+x) + 1\ prím,\ akkor\quad q_k = p_k + 2c =$$
$$= 6(K+x) + 1 + 2c = \underbrace{6K + 1 + 2c}_{q_K} + 6x = q_K + 6x\ NEM\ \ prím$$

Mivel q_k az indirekt feltétel szerint NEM prím, így (16) és (17) esetén egyaránt, bármely u, v természetes számra az (5)-(8) összefüggések valamelyike fennáll. Ebből következik, hogy a megfelelő jelöléseket alkalmazva, az alábbi összefüggéseket kapjuk q_k-ra, illetve q_K-ra.

(18)
$$q_k \overset{(5)}{=} 6r - 1 = q_K + 6x \quad \text{és}\ \ r=6uv+u-v \quad (u=1,2,3,\ldots),\ (v=1,2,3,\ldots) \Rightarrow$$
$$\Rightarrow\ q_K = 6r - 1 - 6x = 6(6uv + u - v) - 1 - 6x$$

(19)
$$q_k \overset{(6)}{=} 6r - 1 = q_K + 6x \quad \text{és}\ \ r=6uv-u+v \quad (u=1,2,3,\ldots),\ (v=1,2,3,\ldots) \Rightarrow$$
$$\Rightarrow\ q_K = 6r - 1 - 6x = 6(6uv - u + v) - 1 - 6x$$

(20)
$$q_k \overset{(7)}{=} 6r + 1 = q_K + 6x \quad \text{és}\ \ r=6uv+u+v \quad (u=1,2,3,\ldots),\ (v=1,2,3,\ldots) \Rightarrow$$
$$\Rightarrow\ q_K = 6r + 1 - 6x = 6(6uv + u + v) + 1 - 6x$$

(21)
$$q_k \overset{(8)}{=} 6r + 1 = q_K + 6x \quad \text{és}\ \ r=6uv-u-v \quad (u=1,2,3,\ldots),\ (v=1,2,3,\ldots) \Rightarrow$$
$$\Rightarrow\ q_K = 6r + 1 - 6x = 6(6uv - u - v) + 1 - 6x$$

A (16), (17) indirekt feltételek szerint q_K az u, v természetes számok bármely választása esetén prímszám. Most megmutatjuk, hogy az u=v megfelelő választása esetén a (18)-(21) esetek mindegyikében végtelen sok x érték van, amelyre q_K összetett szám, ami ellentmond az indirekt feltételeknek.

(22)
$$u = v \overset{(18),(19)}{\Rightarrow} \quad q_K = 6(6u^2) - 1 - 6x \quad és \quad u = \frac{x+1}{6} \Rightarrow q_K = 6\frac{6(x+1)^2}{6^2} - 1 - 6x =$$
$$= x^2 + 2x + 1 - 1 - 6x = x^2 - 4x = x(x-4)$$

Mivel u természetes szám, ezért az $u = \frac{x+1}{6}$ feltétel mindig teljesül, ha x=*6l-1* alakú, ahol l természetes szám (tehát x=*5,11,17,23, …*).

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

(23)
$$u = v \overset{(20)}{\Rightarrow} \quad q_K = 6(6u^2 + 2u) + 1 - 6x \quad \textit{és} \quad u = \frac{x-1}{6} \Rightarrow$$
$$\Rightarrow q_K = 6\left(\frac{6(x-1)^2}{6^2} + \frac{2(x-1)}{6}\right) + 1 - 6x = (x-1)^2 + 2(x-1) + 1 - 6x = x(x-6)$$

(24)
$$u = v \overset{(21)}{\Rightarrow} \quad q_K = 6(6u^2 - 2u) + 1 - 6x \quad \textit{és} \quad u = \frac{x+1}{6} \Rightarrow$$
$$\Rightarrow q_K = 6\left(\frac{6(x+1)^2}{6^2} - \frac{2(x+1)}{6}\right) + 1 - 6x = (x+1)^2 - 2(2+1) + 1 - 6x = x(x-6)$$

Mivel u természetes szám, ezért az $u = \frac{x-1}{6}$ feltétel mindig teljesül, ha $x=6l+1$ alakú, ahol l természetes szám (tehát $x=7,13,19,25, \ldots$).

Q.E.D.

Világos, hogy a 3. tételt az $m_N=1$ esetre alkalmazva, éppen a klasszikus Ikerprím sejtés bizonyítását kapjuk, amelyet ettől kezdve *Ikerprím tételnek* nevezhetünk.

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

[Dénes 2017] Dénes, Tamás: Dénes-féle Szimmetrikus Prímszám tétel és alkalmazása a páros Goldbach-sejtés bizonyítására
http://www.titoktan.hu/_raktar/_e_vilagi_gondolatok/DT-SzimmPrimTetel.pdf