Dénes Tamás

matematikus-kriptográfus

email: tdenest@freemail.hu

Komplementer prímszita és alkalmazása a prímszámok számának becslésére

ABSTRACT

A címbeli komplementer kifejezés azt jelzi, hogy a szokásossal ellentétes megközelítést követünk, azaz direkt képletet, szükséges és elegendő feltételt adunk meg az összes $6k+1$ és $6k$-1 alakú összetett számokra, az így előállított táblázat pontosan a prímszámokat nem tartalmazza, azaz a komplementer táblázatban találhatók meg az összes prímszámok, ezt nevezzük komplementer prímszitának.
A komplementer prímszita módszer lehetőséget nyújt a prímszámok előállítására faktorizáció nélkül, ugyanakkor a konstruktív bizonyításból adódik az összetett számok kéttényezős felbontása. Eljárásunk alkalmas a természetes számok bármely (m,n) intervallumába eső összes prímszámok előállítására, valamint az x-nél kisebb prímszámok számának $\pi(x)$-nek becslésére.

----- . -----

1. Tétel
Minden 3-nál nagyobb p prímszám $6k+1$ vagy $6k$-1 alakú, ahol $k=1,2,3,...$ természetes szám.

Bizonyítás:
Tegyük fel, hogy p prím, de nem $6k+1$ vagy $6k$-1 alakú. Ekkor csak a következő esetek állhatnak elő:

(1.1) $p= 6k+2$ vagy $p= 6k$-2 ez páros, így *nem lehet prím*.

(1.2) $p= 6k+3$ vagy $p= 6k$-3 ez osztható 3-al, így *nem lehet prím*.

(1.3) $p= 6k+4$ vagy $p= 6k$-4 ez páros, így *nem lehet prím*.

(1.4) $p= 6k+5$ vagy $p= 6k$-5 $\Rightarrow$ $p= 6k+5 = 6(k+1)$-1 vagy
$p= 6k$-$5 = 6(k$-$1)+1$ ezek viszont a feltételezett alakúak.

Q.E.D.

Az 1. tétel alapján tehát, ha a természetes számokat az alábbi módon rendezzük hat oszlopba (lásd 1. táblázat), akkor az összes prímszám az 1. és az 5. oszlopban helyezkedik el. Méghozzá az 1. oszlopban a $6k+1$, míg az 5. oszlopban a $6k$-1 alakúak.

1. Táblázat

6k+1 ↓				6k-1 ↓	
1	2	3	4	**5**	6
7	8	9	10	**11**	12
13	14	15	16	**17**	18
19	20	21	22	**23**	24
25	26	27	28	**29**	30
31	32	33	34	35	36
37	38	39	40	**41**	42
43	44	45	46	**47**	48
49	50	51	52	**53**	54
55	56	57	58	**59**	60
61	62	63	64	65	66
67	68	69	70	**71**	72
73	74	75	76	77	78
79	80	81	82	**83**	84
85	86	87	88	**89**	90
91	92	93	94	95	96
97	98	99	100	**101**	102
…	…	…	…	…	…

Az 1. tételből rögtön adódik egy gyors felsőkorlát az *N*-nél kisebb prímszámok számára:

(1.5) $$\pi(N) < \frac{N}{3} \Rightarrow \frac{\pi(N)}{N} < \frac{1}{3}$$

Az 1. tétel alapján a 3-nál nagyobb prímszámok szempontjából elegendő csupán a *6k±1* alakú természetes számokat vizsgálni. A következő 2. tétel szükséges és elegendő feltételt ad a *6k±1* alakú összetett számokra, azaz a *komplementer prímszitára*.

2. Tétel *(Komplementer prímszita)*

Legyenek *N, k, u, v* természetes számok, valamint $u,v \geq 1$.

$N=6k+1$ akkor és csak akkor összetett szám, ha $k= 6uv+u+v$ vagy $k= 6uv-u-v$

$N=6k-1$ akkor és csak akkor összetett szám, ha $k = 6uv-u+v$ vagy $k= 6uv+u-v$

Bizonyítás *(szükségesség)*

Ha $N=6k+1$ összetett szám, akkor $\mathbf{6k+1 = dr} \Rightarrow k = \frac{dr-1}{6} \Rightarrow dr \equiv 1 \bmod 6$

Ez két esetben lehetséges:

(2.1) $d \equiv 1 \bmod 6 \Rightarrow d=6u+1$ és $r \equiv 1 \bmod 6 \Rightarrow r= 6v+1$

$$\Rightarrow \quad k = \frac{(6u+1)(6v+1)-1}{6} = \frac{36uv+6u+6v+1-1}{6} = 6uv+u+v$$

(2.2) $d \equiv -1 \bmod 6 \Rightarrow d= 6u-1$ és $r \equiv -1 \bmod 6 \Rightarrow r= 6v-1$

$$\Rightarrow \quad k = \frac{(6u-1)(6v-1)-1}{6} = \frac{36uv-6u-6v+1-1}{6} = 6uv-u-v$$

Ha $N= 6k-1$ összetett szám, akkor $6k-1= dr \Rightarrow k = \dfrac{dr+1}{6} \Rightarrow dr \equiv -1 \bmod 6$

Ez két esetben lehetséges:

(2.3) $d \equiv 1 \bmod 6 \Rightarrow d= 6u+1$ és $r \equiv -1 \bmod 6 \Rightarrow r= 6v-1$

$$\Rightarrow \quad k = \frac{(6u+1)(6v-1)+1}{6} = \frac{36uv-6u+6v-1+1}{6} = 6uv-u+v$$

Mivel ez az összefüggés u, v-re szimmetrikus, így a másik megoldás

(2.4) $k = 6uv + u - v$

Ezzel a tétel szükséges ágát bebizonyítottuk.

Bizonyítás *(elégségesség)*

Legyen $k= 6uv+u+v$ és $N= 6k+1$, valamint $v=u+r$, ahol $u,v \geq 1$, $r \geq 0$, ekkor

(2.5) $N=6(6u(u+r)+u+u+r)+1 = 6(6u^2+6ur+2u+r)+1 = (6u)^2 + 6^2 ur + 12u + 6r + 1 =$
$= (6u+1)^2 + 6r(6u+1) = (6u+1)(6u+1+6r) = (6u+1)(6v+1)$
ez nyilvánvalóan nem prím.

Legyen $k= 6uv-u-v$ és $N= 6k+1$, valamint $v=u+r$, ahol $u,v \geq 1$, $r \geq 0$, ekkor

(2.6) $N=6(6u(u+r)-u-(u+r))+1 = 6(6u^2+6ur-2u-r)+1 = (6u)^2 + 6^2 ur - 12u - 6r + 1 =$
$= (6u-1)^2 + 6r(6u-1) = (6u-1)(6u-1+6r) = (6u-1)(6v-1)$
ez nyilvánvalóan nem prím.

Legyen $k=6uv-u+v$ és $N= 6k-1$, valamint $v=u+r$, ahol $u,v \geq 1$, $r \geq 0$, ekkor

(2.7) $N=6(6u(u+r)-u+u+r)-1 = 6(6u^2+6ur+r)-1 = (6u)^2 + 6^2 ur + 6r - 1 =$
$=(6u+1)(6u-1)+6r(6u+1) = (6u+1)(6u-1+6r) = (6u+1)(6v-1)$
ez nyilvánvalóan nem prím.

Legyen $k=6uv+u-v$ és $N=6k-1$, valamint $v=u+r$, ahol $u,v \geq 1$, $r \geq 0$, ekkor

(2.8) $N=6(6u(u+r)+u-(u+r))-1 = 6(6u^2+6ur-r)-1 = (6u)^2 + 6^2 ur - 6r - 1 =$
$=(6u+1)(6u-1)+6r(6u-1) = (6u-1)(6u+1+6r) = (6u-1)(6v+1)$
ez nyilvánvalóan nem prím.

Q.E.D.

Következmények

K2.1.
A (2.5) - (2.8) levezetések megadják bármely $6k\pm1$ alakú N természetes szám egy szorzattá bontását is. Ha $6u\text{-}1$, $6u+1$, $6v\text{-}1$, $6v+1$ prímszámok (ami az 1. tétel szerint lehetséges), akkor pontosan az N szám prímfelbontását kapjuk.

Ha bevezetjük az $a=6u+1$ és $b=6u\text{-}1$ jelöléseket, akkor tehát minden $6k\pm1$ alakú természetes szám felírható az alábbi négy alak valamelyikeként:

(2.9) $N_1=a(a+6r)$ $N_2=b(b+6r)$ $N_3=a(b+6r)$ $N_4=b(a+6r)$

Példa: $u=23,\ r=29 \Rightarrow a=139,\ b=137 \Rightarrow$ $N_1 = 139 \cdot 313 = 43.507$ $N_2 = 137 \cdot 311 = 42.607$
$N_3 = 139 \cdot 311 = 43.229$ $N_4 = 137 \cdot 313 = 42.881$

K2.2.
Mivel a **K2.1.**-ben bevezetett jelölések szerint $a>b$ mindig teljesül, így a (2.9)-beli N_i $(i=1,2,3,4)$ kifejezések soha nem egyenlők, kivéve azt az egy esetet, mikor $r=0 \Rightarrow N_3=N_4$

Ha megvizsgáljuk az N_i számok nagyságviszonyait, a 2. táblázat relációs mátrixát kapjuk.

$N_1\text{-}N_2 = a^2+6ar\text{-}b^2\text{-}6br > 0$ tehát $N_1 > N_2$

$N_1\text{-}N_3 = a^2+6ar\text{-}ab\text{-}6ar > 0$ tehát $N_1 > N_3$

$N_1\text{-}N_4 = a^2+6ar\text{-}ab\text{-}6br > 0$ tehát $N_1 > N_4$

$N_2\text{-}N_3 = b^2+6br\text{-}ab\text{-}6ar < 0$ tehát $N_2 < N_3$

$N_2\text{-}N_4 = b^2+6br\text{-}ab\text{-}6br < 0$ tehát $N_2 < N_4$

$N_3\text{-}N_4 = ab+6ar\text{-}ab\text{-}6br \geq 0$ tehát $N_3 \geq N_4$

2. Táblázat

	N_1	N_2	N_3	N_4
N_1	-	>	>	>
N_2	<	-	<	<
N_3	<	>	-	≥
N_4	<	>	≤	-

Tehát mindig fennáll az $N_1 > N_3 \geq N_4 > N_2$ reláció.

Az 1. és 2. tételből könnyen bizonyítható, hogy végtelen sok prímszám van.

3. Tétel
Végtelen sok prímszám van.

Bizonyítás *(indirekt)*
Az 1. tétel alapján elegendő csak a $6k\pm1$ alakú természetes számokat vizsgálni.

Tegyük fel, hogy véges sok prímszám van, és ezek közül $P=6K+1$ az utolsó $6k+1$ alakú prímszám. Ekkor minden $p>P$ természetes szám összetett.

Így a 2. tétel szerint p prímtényezős felbontása: $p = \prod_{i=1}^{n} (6u_i \pm 1)(6v_i \pm 1)$, ahol minden $1 \le i \le n$ esetén $6u_i \pm 1$ és $6v_i \pm 1$ prím. A feltételezés szerint a prímtényezős felbontásban mindegyik u_i, $v_i < K$ amiből következik, hogy $p \langle \left[(6K \pm 1)(6K \pm 1) \right]^n$

Ez azt jelenti, hogy a $6k+1$ alakú számok száma véges, ami nem igaz, tehát nincs ilyen K. A levezetés hasonlóan végezhető a $6k-1$ alakú prímszámokra is.

Q.E.D.

K2.3.

A (2.5) - (2.8) levezetések alapján vizsgáljuk egy tetszőleges N természetes számig az összes $6k+1$ és $6k-1$ alakú összetett számok számát. Azaz vizsgáljuk az $N_i < N$ $(i= 1,2,3,4)$ egyenlőtlenségeket.

(2.10) $N_1 \le N \Rightarrow (6u+1)(6u+1+6r) \le N \Rightarrow r \le \dfrac{N}{6(6u+1)} - \dfrac{6u+1}{6} = \dfrac{N-(6u+1)^2}{6(6u+1)} \xrightarrow{v=u+r\ (def)}$

(2.11) $v \le \dfrac{N-(6u+1)^2}{6(6u+1)} + u \Rightarrow v \le \dfrac{N-6u-1}{6(6u+1)}$

(2.12) $N_2 \le N \Rightarrow (6u-1)(6u-1+6r) \le N \Rightarrow r \le \dfrac{N}{6(6u-1)} - \dfrac{6u-1}{6} = \dfrac{N-(6u-1)^2}{6(6u-1)} \xrightarrow{v=u+r\ (def)}$

(2.13) $v \le \dfrac{N-(6u-1)^2}{6(6u-1)} + u \Rightarrow v \le \dfrac{N+6u-1}{6(6u-1)}$

(2.14) $N_3 \le N \Rightarrow (6u+1)(6u-1+6r) \le N \Rightarrow r \le \dfrac{N}{6(6u+1)} - \dfrac{6u-1}{6} = \dfrac{N-(6u)^2+1}{6(6u+1)} \xrightarrow{v=u+r\ (def)}$

(2.15) $v \le \dfrac{N-(6u)^2+1}{6(6u+1)} + u \Rightarrow v \le \dfrac{N+6u+1}{6(6u+1)}$

(2.16) $N_3 \le N \Rightarrow (6u-1)(6u+1+6r) \le N \Rightarrow r \le \dfrac{N}{6(6u-1)} - \dfrac{6u+1}{6} = \dfrac{N-(6u)^2+1}{6(6u-1)} \xrightarrow{v=u+r\ (def)}$

(2.17) $v \le \dfrac{N-(6u)^2+1}{6(6u-1)} + u \Rightarrow v \le \dfrac{N-6u+1}{6(6u-1)}$

Mivel az u,v paraméter párok az N_i $(i=1,2,3,4)$ kifejezésekben szimmetrikusak, így nyilvánvaló, hogy csak az $u \ne v$, azaz az $r>0$ esetekre kell az N_i értékeket előállítani ahhoz, hogy N-ig az összes $6k+1$ és $6k-1$ alakú összetett számok legalább egyszer előálljanak. Ebből következnek az alábbi összefüggések:

(2.18) $r=0 \Rightarrow N_1=(6u+1)^2$ tehát $N_1 \le N \Rightarrow (6u+1)^2 \le N \Rightarrow u \le \frac{\sqrt{N}-1}{6}$

(2.19) $r=0 \Rightarrow N_2=(6u-1)^2$ tehát $N_2 \le N \Rightarrow (6u-1)^2 \le N \Rightarrow u \le \frac{\sqrt{N}+1}{6}$

(2.20) $r=0 \Rightarrow N_3=N_4=(6u)^2$ -1 tehát $N_3, N_4 \le N \Rightarrow (6u)^2-1 \le N \Rightarrow u \le \frac{\sqrt{N}+1}{6}$

Vezessük be a $K_i(N)$ jelölést, amely az összes $N_i \le N$ típusú összetett számok előállításához elegendő *u,v* párok számát jelöli.

(2.21) $$K_1(N) = \sum_{u=1}^{\frac{\sqrt{N}-1}{6}} \left(\frac{N-6u-1}{6(6u+1)} - u + 1 \right)$$

(2.22) $$K_2(N) = \sum_{u=1}^{\frac{\sqrt{N}-1}{6}} \left(\frac{N+6u-1}{6(6u-1)} - u + 1 \right)$$

(2.23) $$K_3(N) = \sum_{u=1}^{\frac{\sqrt{N}-1}{6}} \left(\frac{N+6u+1}{6(6u+1)} - u + 1 \right)$$

(2.24) $$K_4(N) = \sum_{u=1}^{\frac{\sqrt{N}-1}{6}} \left(\frac{N-6u+1}{6(6u-1)} - u + 1 \right)$$

(2.25) $$K(N)=K_1(N)+K_2(N)+K_3(N)+K_4(N)$$

A fenti levezetés csupán az elegendőséget biztosítja, azaz az összes különböző *u,v* párok előállítását. Ez viszont megengedi, hogy az előállítás során bizonyos összetett számok többször forduljanak elő, így *K(N)* annyival nagyobb az *N*-ig előforduló összes *6k+1* és *6k-1* alakú összetett számok számánál (jele: $K\pi(N)$), amennyi ezeknek a többszörös multiplicitással szereplő elemeknek a száma (jele: *m(N)*), azaz

(2.26) $$K\pi(N)=K(N)-m(N)$$

Ha *KP(N)*-nel jelöljük a jelen komplementer prímszita eljárással előállított prímszámok számát, akkor adódik, hogy

(2.27) $$KP(N)=\left[\frac{N}{3}\right]-K\pi(N)$$

A fenti levezetések alapján *K(N)* értékét pontosan meghatároztuk, *m(N)*-re viszont jelenleg csak becslést tudunk adni, illetve számítógépes algoritmussal a pontos érték előállítható. Amennyiben tehát *m(N)*-re pontos értékkel rendelkezünk, akkor fennáll, hogy

(2.28) $$\pi(N)=\left[\frac{N}{3}\right]-K\pi(N)=KP(N)$$

K2.4.
Most a (2.21)-(2.25) összefüggésekből közelítő formulát képezünk, amely *K(N)*-et direkt képlettel állítja elő *N*-ből. Könnyen látható, hogy

(2.29) $$\left|\left(\sqrt{N}\pm 1\right)-\sqrt{N}\right|=1 \quad \text{valamint} \quad \sqrt{N+1}-\sqrt{N}\ \langle\ 1$$

Így szinte semmit nem ront a pontosságon, ha a (2.21)-(2.24) összefüggésekben az összegzéseket egységesen $\frac{\sqrt{N}}{6}$-ig végezzük:

(2.30) $$K(N)=\sum_{u=1}^{\frac{\sqrt{N}}{6}}\left(\frac{N-6u-1}{6(6u+1)}+\frac{N+6u-1}{6(6u-1)}+\frac{N+6u+1}{6(6u+1)}+\frac{N-6u+1}{6(6u-1)}-4u+4\right)$$

Tehát ha *a= 6u+1* és *b= 6u-1* , akkor

$$K(N)=\sum_{u=1}^{\frac{\sqrt{N}}{6}}\left(\frac{N-a}{6a}+\frac{N+b}{6b}+\frac{N+a}{6a}+\frac{N-b}{6b}-4u+4\right)=$$

(2.31) $$=\sum_{u=1}^{\frac{\sqrt{N}}{6}}\left(\frac{2N}{6a}+\frac{2N}{6b}-4u+4\right)=\frac{2N}{6}\sum_{u=1}^{\frac{\sqrt{N}}{6}}\left(\frac{a+b}{ab}\right)-\frac{4\left(1+\frac{\sqrt{N}}{6}\right)\frac{\sqrt{N}}{6}}{2}+\frac{4\sqrt{N}}{6}=$$

$$=\frac{2N}{6}\sum_{u=1}^{\frac{\sqrt{N}}{6}}\left(\frac{12u}{36u^2-1}\right)-\frac{N}{18}+\frac{\sqrt{N}}{3}=4N\sum_{u=1}^{\frac{\sqrt{N}}{6}}\left(\frac{u}{36u^2-1}\right)-\frac{N}{18}+\frac{\sqrt{N}}{3}$$

Vegyük észre, hogy $36u^2-1\approx 36u^2 \Rightarrow \frac{u}{36u^2-1}\approx\frac{u}{36u^2}=\frac{1}{36u}$, így *K(N)*-re az alábbi eredmény adódik:

(2.32) $$K(N)\approx 4N\sum_{u=1}^{\frac{\sqrt{N}}{6}}\left(\frac{1}{36u}\right)-\frac{N}{18}+\frac{\sqrt{N}}{3}=\frac{\sqrt{N}}{3}-\frac{N}{18}+\frac{N}{9}\sum_{u=1}^{\frac{\sqrt{N}}{6}}\left(\frac{1}{u}\right)$$

$\sum \frac{1}{u}$ becslésére felhasználjuk az alábbi egyenlőtlenségpárt (Erdős-Surányi 2.old. 6.):

(2.33) $$1 + \log(n) \geq \sum_{u=1}^{n} \frac{1}{u} \rangle \log(n+1)$$

Alkalmazzuk a (2.33) egyenlőtlenségpárt (2.32)-re, így kapjuk hogy

(2.34) $$\frac{N}{18} + \frac{\sqrt{N}}{3} + \frac{N}{9}\log\left(\frac{\sqrt{N}}{6}\right) \geq K(N) \rangle \frac{\sqrt{N}}{3} - \frac{N}{18} + \frac{N}{9}\log\left(\frac{\sqrt{N}}{6} + 1\right)$$

A (2.34) alsó és felső korlátjának számtani közepét használjuk K(N) közelítő értékének (jele: *KK(N)*).

(2.35) $$KK(N) = \frac{\sqrt{N}}{3} + \frac{N}{18}\log\frac{N + 6\sqrt{N}}{36}$$

K2.5.

A (2.10)-(2.17) levezetésekhez hasonlóan vizsgáljuk most az $N_i \geq M$ $(i=1,2,3,4)$ egyenlőtlenségeket, ahol $M<N$ természetes szám.

(2.36) $$N_1 \geq M \Rightarrow \quad v \geq \frac{M - 6u - 1}{6(6u+1)}$$

(2.37) $$N_2 \geq M \Rightarrow \quad v \geq \frac{M + 6u - 1}{6(6u-1)}$$

(2.38) $$N_3 \geq M \Rightarrow \quad v \geq \frac{M + 6u + 1}{6(6u+1)}$$

(2.39) $$N_4 \geq M \Rightarrow \quad v \geq \frac{M - 6u + 1}{6(6u-1)}$$

Vezessük be a $K_i(M,N)$ $(i=1,2,3,4)$ jelölést, amely az összes u,v párok számát jelöli, amelyek az (M,N) intervallumba eső összes összetett számokat generálják. Ekkor a (2.21)-(2.25) összefüggések analógiájára a következőket kapjuk:

(2.40) $$K_1(M,N) = \sum_{u=1}^{\frac{\sqrt{N}-1}{6}} \left(\frac{N-6u-1}{6(6u+1)} - \frac{M-6u-1}{6(6u+1)} + 1\right) = \sum_{u=1}^{\frac{\sqrt{N}-1}{6}} \left(\frac{N-M}{6(6u+1)} + 1\right)$$

(2.41) $$K_2(M,N) = \sum_{u=1}^{\frac{\sqrt{N}+1}{6}} \left(\frac{N+6u-1}{6(6u-1)} - \frac{M+6u-1}{6(6u-1)} + 1\right) = \sum_{u=1}^{\frac{\sqrt{N}+1}{6}} \left(\frac{N-M}{6(6u-1)} + 1\right)$$

(2.42) $$K_3(M,N) = \sum_{u=1}^{\frac{\sqrt{N+1}}{6}} \left(\frac{N+6u+1}{6(6u+1)} - \frac{M+6u+1}{6(6u+1)} + 1 \right) = \sum_{u=1}^{\frac{\sqrt{N+1}}{6}} \left(\frac{N-M}{6(6u+1)} + 1 \right)$$

(2.43) $$K_4(M,N) = \sum_{u=1}^{\frac{\sqrt{N+1}}{6}} \left(\frac{N-6u+1}{6(6u.1)} - \frac{M-6u+1}{6(6u-1)} + 1 \right) = \sum_{u=1}^{\frac{\sqrt{N+1}}{6}} \left(\frac{N-M}{6(6u-1)} + 1 \right)$$

(2.44) $$K(M,N) = K_1(M,N)+K_2(M,N)+K_3(M,N)+K_4(M,N)$$

Világos, hogy az eddig levezetett összefüggések mindegyike értelmezhető tetszőleges *(M,N)* intervallumra. Az alábbiakban megadjuk a (2.26), (2.27), (2.32), (2.35) összefüggések megfelelőit tetszőleges *(M,N)* intervallumra.

(2.45) $$K\pi(M,N) = K(M,N)-m(M,N)$$

(2.46) $$KP(M,N) = \left[\frac{N-M}{3} \right] - K\pi(M,N)$$

(2.47) $$K(M,N) = \sum_{u=1}^{\frac{\sqrt{N}}{6}} \left(\frac{N-M}{6(6u+1)} + \frac{N-M}{6(6u-1)} + \frac{N-M}{6(6u+1)} + \frac{N-M}{6(6u-1)} + 4 \right) =$$
$$= 4(N-M) \sum_{u=1}^{\frac{\sqrt{N}}{6}} \left(\frac{u}{36u^2 - 1)} \right) + \frac{2\sqrt{N}}{3}$$

Mivel $36u^2 - 1 \approx 36u^2 \Rightarrow \frac{u}{36u^2-1} \approx \frac{1}{36u}$, így *K(M,N)*-re adódik:

(2.48) $$K(M,N) \approx 4(N-M) \sum_{u=1}^{\frac{\sqrt{N}}{6}} \left(\frac{1}{36u} \right) + \frac{2\sqrt{N}}{3} = \frac{2\sqrt{N}}{3} + \frac{N-M}{9} \sum_{u=1}^{\frac{\sqrt{N}}{6}} \left(\frac{1}{u} \right)$$

$\sum \frac{1}{u}$ közelítésére felhasználjuk a (2.33) egyenlőtlenségpár két oldalának középértékét:

(2.49) $$KK(M,N) \approx \frac{2\sqrt{N}}{3} + \frac{N-M}{18} \left(1 + \log \frac{N+6\sqrt{N}}{36} \right)$$

Tehát, ha *N=6k+1* vagy *N=6k-1* alakú összetett szám, akkor *N* kéttényezős felbontásához (2.49) szerint maximum az alábbi lépésszám szükséges:

(2.50) $$N = M \xrightarrow{(2.49)} KK(M,N) \approx \frac{2\sqrt{N}}{3}$$

A komplementer prímszita tehát direkt eljárást ad tetszőleges *(M,N)* intervallumban az összes összetett (és így az intervallumba eső összes prímszám) előállítására. Ezzel igen hatékony módszert kaptunk a prímekkel kapcsolatos három alapfeladat megoldására:

1. Keressük az *(M,N)* intervallumba eső összes prímszámokat.

2. Állítsuk elő az összes prímszámokat *N*-ig. (Ekkor *M=1*)

3. Állapítsuk meg egy adott *p* természetes számról, hogy prímszám-e.

Nyitott probléma: az *m(N)* függvény analitikus meghatározása, vagy jó aproximációja.

A 3. Táblázat néhány összehasonlító értéket mutat be a fenti eredmények illusztrálására.

3. Táblázat

N	*K(N)*	*KK(N)*	*m(N)*	*KP(N)*	*π(N)*	$\frac{N}{\log N}$	*KP(N) hiba %*	$\frac{N}{\log N}$ *hiba%*
1.000	205	195	34	162	168	144	3.5%	14.3%
2.000	484	461	112	294	303	263	3.0%	13.2%
3.000	794	755	214	420	430	375	2.3%	12.8%
4.000	1.118	1.067	325	540	552	482	2.2%	12.7%
5.000	1.452	1.394	442	656	669	587	2.0%	12.3%
6.000	1.807	1.731	577	770	783	690	1.7%	11.8%
7.000	2.160	2.077	713	886	900	791	1.5%	12.1%
8.000	2.532	2.431	857	991	1.007	890	1.5%	11.6%
9.000	2.905	2.792	1.006	1.101	1.117	988	1.4%	11.5%
10.000	3.281	3.159	1.160	1.212	1.229	1.086	1.4%	11.6%
11.000	3.666	3.531	1.316	1.316	1.335	1.182	1.4%	11.5%
12.000	4.055	3.909	1.474	1.419	1.438	1.278	1.3%	11.1%
13.000	4.454	4.291	1.648	1.527	1.547	1.372	1.3%	11.3%
14.000	4.850	4.677	1.815	1.631	1.652	1.466	1.2%	11.3%
30.000	11.641	11.266	4.891	3.250	3.245	2.910	0.2%	10.3%
50.000	20.796	20.175	9.263	5.133	5.133	4.621	0.0%	10.0%
70.000	30.409	29.537	14.013	6.937	6.935	6.275	0.0%	9.5%
90.000	40.335	39.220	19.053	8.718	8.713	7.890	0.0%	9.4%
190.000	92.971	90.619	46.813	17.175	17.170	15.632	0.0%	8.9%
350.000	183.080	178.739	96.357	29.943	29.977	27.417	0.1%	8.5%
900.000	517.786	506.647	289.266	71.480	71.274	65.645	0.1%	7.9%
1.000.000	581.158	568.777	326.493	78.668	78.498	72.382	0.2%	7.8%
1.500.000	905.437	886.863	520.366	114.929	114.155	105.478	0.6%	7.6%
2.000.000	1.239.132	1.214.375	721.684	149.218	148.933	137.849	0.2%	7.4%
3.000.000	1.926.146	1.889.011	1.143.113	216.967	216.818	201.152	0.6%	7.2%
4.000.000	2.632.033	2.582.508	1.581.846	283.146	283.148	263.127	0.0%	7.0%
5.000.000	3.351.917	3.290.031	2.033.930	348.679	348.515	324.150	0.4%	7.0%
6.000.000	4.083.022	4.008.733	2.495.735	412.713	412.851	384.436	0.3%	6.9%
7.000.000	4.823.413	4.736.732	2.966.794	476.714	476.650	444.122	0.1%	6.8%
8.000.000	5.571.739	5.472.690	3.445.726	540.653	539.779	503.304	0.1%	6.7%
10.000.000	7.088.528	6.964.708	4.416.529	661.334	664.579	620.421	0.4%	6.6%

Irodalomjegyzék

[1] Erdős Pál, Surányi János: Válogatott fejezetek a számelméletből, Polygon, Szeged, 1996.

[2] H.Halberstam, K.F.Roth: SEQUENCES, IV. Sieve methods, Oxford at the Clarendon Press, 1966

[3] K.Ramachandra: Many famous conjectures on primes, Meagre but precious progress of a deep nature, The Mathematics Student, Vol. 67, 1-4 (1998), 187-199

[4] A.V. Spivak: The Sieve of Eratosthenes and Wallis's Product: How Two Wrong Arguments Give One Correct Answer, The Mathematical Intelligencer, 23(2001) 64-65