Eötvös Loránd Tudományegyetem
Természettudományi Kar

Pach Péter Pál
matematikus szak

Öten egy szobában

Diplomamunka

témavezető :
Szabó Csaba, egyetemi docens
Eötvös Loránd Tudományegyetem, Algebra és Számelmélet Tanszék

Budapest, 2009.

Tartalomjegyzék

1. Bevezetés

Öten vannak egy szobában: 1, 2, 3, 4 és 5. Megszorozzuk őket 2-vel, és bejön 2, 4, 6, 8 és 10. Így már két 2-es és két 4-es lesz bent, ők megfogják egymás kezét és kimennek a szobából. A bent maradók: 1, 3, 5, 6, 8 és 10. Ezután megszorozzuk az 1, 2, 3, 4, 5 számokat 3-mal, és bejön 3, 6, 9, 12 és 15. Az így kialakuló párok: a két 3-as és a két 6-os kézen fogva elhagyják a szobát. Ezután a szobában 1, 5, 8, 9, 10, 12 és 15 marad. És így tovább: az n-edik lépésben $n+1$, $2(n+1)$, $3(n+1)$, $4(n+1)$ és $5(n+1)$ jön be a szobába, és az ezáltal kialakuló párok hagyják el azt. Igaz-e, hogy mindig legalább öten maradnak a szobában?

Az előbbi feladat Günter Pilztől származik és kódelméleti eredetű: egy majdnemgyűrű-kód minimális távolságával kapcsolatos. Mi csak azon majdnemgyűrűkre és majdnemgyűrű-kódokra vonatkozó fogalmakat és összefüggéseket ismertetjük, amelyek a probléma szempontjából legfontosabbak.

A majdnemgyűrű olyan, a gyűrűhöz hasonló algebrai struktúra, melyben a gyűrűaxiómák közül nem követeljük meg az összeadás kommutativitását, és a két disztributivitás közül is csak az egyiket követeljük meg. (Attól függően, hogy melyiket, beszélhetünk bal és jobb majdnemgyűrűkről.)

Úgynevezett sík majdnemgyűrűk segítségével blokkrendszereket és kódokat konstruálhatunk. Fő referenciáinkat: [1]-et, [2]-t és [3]-at felhasználva ismertetjük a sík majdnemgyűrű definícióját és egy olyan eljárást, amellyel blokkrendszer és kód adható meg.

Bevezetünk egy relációt N-en:

1. Definíció. Legyen N egy majdnemgyűrű és $a, b \in N$. Ha minden $n \in N$ esetén $na = nb$, akkor azt mondjuk, hogy a és b ekvivalens szorzók, és ezt $a \sim b$-vel jelöljük.

Természetesen ez egy ekvivalenciareláció, az ekvivalenciaosztályok halmazát jelölje $N/\sim$. Az N majdnemgyűrű $\sim$ reláció szerinti faktorizálása a gyűrűknél az annullátorral való faktorizálásnak az analógiája.

A sík majdnemgyűrű definíciója a következő:

2. Definíció. Egy majdnemgyűrűt sík majdnemgyűrűnek nevezünk, ha $|N/\sim| \geq 3$ és minden $xa = xb + c$ (ahol $a \not\sim b$) alakú egyenletnek pontosan egy megoldása van (N-ben).

A majdnemgyűrűket széles körben alkalmazzák, dolgozatunkban ismertetjük, hogy sík majdnemgyűrűk segítségével hogyan adhatók meg nagyon hatékony blokkrendszerek. Induljunk ki az N véges majdnemgyűrűből. Legyen $N^* = \{x \in N : x \nsim 0\}$ és $B^* = \{aN^* + b : a, b \in$

$N, a \neq 0\}$. A blokkrendszer pontjainak halmaza N, blokkjainak halmaza pedig B^*. Ekkor $D^* = (N, B^*, I)$ (ahol I a tartalmazás reláció) egy (v, k, λ)-blokkrendszer, melynek paraméterei:

$$\begin{aligned} v &= |N|, \\ k &= |N^*/\sim|, \\ \lambda &= k - 1. \end{aligned}$$

Itt v a pontok száma, k a blokkok mérete, és bármely 2 ponton pontosan λ blokk megy át. Ezenkívül $b = v(v-1)/k$ és $r = v - 1$ is teljesül, ahol b a blokkok, r pedig az egy ponton átmenő blokkok száma.

A blokkrendszer incidenciamátrixa

$$A = (1 - \delta_{B_j, B_j \setminus \{p_i\}})_{ij},$$

ahol δ a Kronecker-delta, p_i-k ($1 \leq i \leq v$) a blokkrendszer pontjai, B_j-k ($1 \leq j \leq b$) pedig a blokkok. Az incidenciamátrix elemei tehát 0-k és 1-esek, és az i-edik sor j-edik eleme pontosan akkor 1-es, ha a p_i pont eleme a B_j blokknak, különben 0. Ha kódszavaknak tekintjük az A mátrix sorait (oszlopait), akkor az A mátrix C^A sor kódját (C_A oszlop kódját) kapjuk. Ez két nemlineáris egyenlő súlyú kód. A kód paramétereit az A-hoz tartozó blokkrendszer paraméterei határozzák meg. C^A esetén

$$\begin{aligned} n &= b, \\ M &= v, \\ d &= 2(r - \lambda), \end{aligned}$$

C_A esetén pedig

$$\begin{aligned} n &= v, \\ M &= b, \\ d &= 2(k - \mu), \end{aligned}$$

ahol $\mu = \max(|B_i \cap B_j| : B_i, B_j \in B^*, B_i \neq B_j)$. Itt n jelöli a kód hosszát, M a kódszavak száma, d pedig a minimális távolság.

Megadott súlyú kódszavak lehetséges maximális száma vizsgált kérdés a kódelméletben. A kérdés akkor érdekes, ha a rögzített súlyon kívül a minimális távolság nagyságáról is megköveteljük, hogy legyen nagyobb egy rögzített korlátnál. Jelölje $A(n, d, w)$ a kódszavak maximális számát, ha a kódról feltesszük, hogy minimális távolsága legalább d legyen.

Megmutatjuk, hogy C^A, vagyis a sor kód maximális kód: $M = A(n, d, w)$ a fenti n, M, d értékek mellett és $w = r$ a C^A kódszavainak súlya.

Tegyük fel indirekten, hogy A kiegészíthető még egy $w = r$ súlyú sorral úgy, hogy az új mátrix sor kódjának minimális távolsága továbbra is legalább $d = 2(r-\lambda)$ marad. Az új sor tekinthető egy új pontnak, melyet hozzáveszünk azokhoz a blokkokhoz, melyeknek megfelelő oszlopban az új sor 1-est tartalmaz. Könnyen meggondolható, hogy akkor lesz továbbra is legalább $d = 2(r-\lambda)$ a kód minimális távolsága, ha kiválasztva az új pontot és bármelyiket a régi pontok közül, ezen két pontra illeszkedő blokkok száma legfeljebb λ. Legyen H egy rendezett párokból álló halmaz, melyet a következő módon definiálunk:

$$H = \{(P_i, B_j) : 1 \le i \le v, 1 \le j \le b, P_i \in B_j, \\ \text{és az új sor } j\text{-edik eleme 1-es}\}.$$

Kétféleképpen számoljuk meg, hány eleme van H-nak. Ha kiválasztunk egy P_i pontot ($1 \le i \le v$), akkor feltevésünk szerint legfeljebb λ olyan blokk lehet, mely P_i-re és az új pontra is illeszkedik. Így H elemszámára a $|H| \le v \cdot \lambda = v \cdot (k-1)$ becslést kapjuk. Másrészt, H-nak olyan rendezett párok elemei, melyeknek második tagja, vagyis B_j blokk illeszkedik az új pontra. Az ilyen tulajdonságú blokkok száma $w = r$, hiszen a kód egyenlő súlyú. Minden blokk a P_i pontok közül k-t tartalmaz, ezért $|H| = r \cdot k = (v-1) \cdot k$. Azt kaptuk tehát, hogy

$$(v-1) \cdot k = |H| \le v \cdot (k-1),$$

és ezért

$$\frac{v-1}{v} \le \frac{k-1}{k},$$

ebből pedig $v \le k$ következik. Mivel $v = |N|$ a pontok száma, $k = |N^*/\sim|$ pedig a blokkok mérete, ezért ez nem lehetséges. Ez az ellentmondás igazolja, hogy C_A sor kód maximális. Megjegyezzük, hogy általában nem igaz, hogy C_A, vagyis az oszlop kód is maximális.

Most [4] alapján bemutatjuk, hogyan kapcsolódik egymáshoz bizonyos lineáris kódok minimális távolsága és a fejezet elején ismertetett feladat. A polinomok az összeadás és a kompozíció műveletekkel majdnemgyűrűt alkotnak. Legyen $f \in \mathbb{Z}_2[x]$ egy polinom, és legyen $C(f,k)$ az a lineáris kód, amelyet $f \circ x$, $f \circ x^2$, …, $f \circ x^k$ polinomok generálnak. Az f polinom fokát jelölje n. Könnyen meggondolható, hogy $C(f,k)$ lineáris kód hossza (legfeljebb) nk, dimenziója pedig k. (Ugyanis a kódot generáló polinomok foka páronként különböző, így azok lineárisan függetlenek, valamint mindegyikük foka legfeljebb nk.)

A kódok egyik legfontosabb paramétere a kódszavak között fellépő minimális távolság. A C kód minimális távolságát jelöljük $d_{min}(C)$-vel. Ha C lineáris kód, akkor $d_{min}(C) = w(C)$, ahol $w(C)$ a C kód nemnulla kódszavai közül a minimális súlyúnak a súlya. Ha $f \in C(f,k)$, akkor f

súlya az f polinom nemnulla együtthatóinak száma. Ez magyarázza, hogy érdemes $f = x + x^2 + \cdots + x^n$ polinommal próbálkozni, hogy minél nagyobb minimális távolságú kódot kapjunk. (Természetesen ez a minimális távolság legfeljebb n lehet, hiszen az $f \circ x$ polinom súlya n.)

Tekintsük a következő példát:

$$(1 + x + x^2) \circ x + (1 + x + x^2) \circ x^2 = x + x^4$$

polinom súlya csak kettő, így a minimális távolság 3-nál kisebb. Hasonló példák mutatják, hogy olyan f polinomot érdemes választani, amelyre $f(0) = 0$.

Egy $\mathbb{Z}_2$ feletti polinomot egyértelműen megadhatunk a nemnulla együtthatójú tagok kitevőinek halmazával. Ha például az f polinom

$$f = x^{a_1} + \cdots + x^{a_l}$$

alakú, ahol $1 \leq a_1 < \ldots < a_l = n$, akkor f-et $\{a_1, \ldots, a_l\}$ számhalmazzal adjuk meg, és ezt f kitevőhalmazának nevezzük. Az f polinom és x^j kompozíciója

$$f \circ x^j = x^{ja_1} + \cdots + x^{ja_l},$$

tehát $f \circ x^j$ polinom kitevőhalmaza $\{ja_1, \ldots, ja_l\}$, ezt úgy kaphatjuk meg, hogy f kitevőhalmazának minden elemét megszorozzuk j-vel. Vizsgáljuk meg, mekkora $C(f, k)$ kód minimális távolsága. A nemnulla kódszavak úgy kaphatók, hogy vesszük $f \circ x$, $f \circ x^2$, $\ldots$, $f \circ x^k$ polinomok egy nemnulla lineáris kombinációját. Mivel $\mathbb{Z}_2$ felett vagyunk, ez közülük néhánynak az összege, mondjuk

$$f \circ x^{b_1} + \cdots + f \circ x^{b_m}.$$

Ha $f = x + x^2 + \cdots + x^n$, akkor $f \circ x^{b_1}$, $\ldots$, $f \circ x^{b_m}$ polinomok kitevőhalmaza rendre

$$(b_1, 2b_1, \ldots, nb_1), \ldots, (b_m, 2b_m, \ldots, nb_m).$$

Így $w(f \circ x^{b_1} + \cdots + f \circ x^{b_m})$ értékét az adja meg, hogy az ib_j alakú számokat véve $1 \leq i \leq n$, $1 \leq j \leq m$ mellett, hány olyan szám van, amely közöttük páratlan sokszor szerepel. A kérdés az, hogy melyik olyan b_1, $\ldots$, b_m kitevőhalmazra lesz a páratlan sokszor megkapott számok száma minimális, ahol $1 \leq b_1 < \ldots < b_m \leq k$. Erre felső becslést kapunk akkor, ha nem szorítkozunk k-nál kisebb kitevőkre.

Az "Öten vannak egy szobában..." feladat az

$$(x + x^2 + x^3 + x^4 + x^5) \circ x + (x + x^2 + x^3 + x^4 + x^5) \circ x^2 + \\ + \cdots + (x + x^2 + x^3 + x^4 + x^5) \circ x^k$$

polinom súlyára vonatkozó alsó becslésre kérdez rá. Például

$$(x+x^2+x^3+x^4+x^5)\circ x+(x+x^2+x^3+x^4+x^5)\circ x^2= \\ =x^1+x^3+x^5+x^6+x^8+x^{10},$$

ez azt jelenti, hogy az első lépés után a szobában 1, 3, 5, 6, 8 és 10 lesznek, amint azt korábban is láttuk. Hányan lesznek a szobában azután a lépés után, amikor 5, 10, 15, 20, 25 jönnek be, és az így kialakuló párok hagyják el azt?

$$(x+x^2+x^3+x^4+x^5)\circ x+(x+x^2+x^3+x^4+x^5)\circ x^2+ \\ +\cdots+(x+x^2+x^3+x^4+x^5)\circ x^5=x^1+x^4+x^9+x^{16}+x^{25},$$

vagyis a szobában öten: 1, 4, 9, 16 és 25 maradnak bent ekkor.

Mint láttuk, a kérdést a következő módon is megfogalmazhatjuk: $N=\{1,2,\dots,n\}=\underline{n}$ és $K\subseteq\mathbb{N}$ véges halmazok. (A továbbiakban az első n természetes számból álló halmazt $\underline{n}$ jelöli.) Az összes lehetséges módon összeszorzunk egy-egy N-beli és K-beli elemet, így kapunk $n\cdot|K|$ darab számot. Ezek közül bizonyosakat páros, bizonyosakat páratlan sokszor kapunk meg. A kérdés az, hogy (legalább) hány olyan szám lesz, amelyet páratlan sokszor kapunk meg. Illetve igaz-e, hogy mindig legalább n olyan lesz, amely páratlan sokszor szerepel.

Vezessük be a következő jelölést:

3. Definíció. Legyenek $A,B\subset\mathbb{N}$ a természetes számok véges részhalmazai, $A=\{a_1,a_2,\dots,a_n\}$ és $B=\{b_1,b_2,\dots,b_k\}$. Ekkor az A és B halmazok *-szorzatán az

$$A*B=\{a_1b_1\}\Delta\{a_1b_2\}\Delta\cdots\Delta\{a_1b_k\}\Delta\{a_2b_1\}\Delta\cdots\Delta\{a_nb_k\}$$

halmazt értjük, ahol Δ a szimmetrikus differenciát jelöli.

Megfogalmazunk néhány egyszerű állítást, amelyet a dolgozatban később többször is alkalmazunk.

4. Állítás. *Legyenek $A,B,C\subseteq\mathbb{N}$. Ekkor*

$$A*B=B*A,$$
$$A*(B\cup C)=(A*B)\Delta(A*C),$$
$$|A\Delta B|=|A|+|B|-2|A\cap B|,$$
$$A*A=\{a^2:a\in A\}.$$

Bizonyítás. A szimmetrikus differencia tulajdonságaiból egyszerűen adódnak az egyenlőségek, csak $A*A=\{a^2:a\in A\}$ egyenlőséget igazoljuk. Ha $a\neq b$ különböző A-beli elemek, akkor $a\cdot b$ szorzatot

párosíthatjuk $b \cdot a$ szorzattal. Ily módon az $A \cdot A$-beli szorzatokat párokba soroltuk, eltekintve az $a \cdot a$ alakú szorzatoktól. Mivel A elemei természetes számok, ezért ezek már páronként különbözők. □

Látható, hogy $A * B$ éppen az $A \cdot B$ halmazban páratlan sokszor előforduló elemeket tartalmazza. A kérdés tehát úgy is megfogalmazható, hogy $N = \underline{n}$ esetén igaz-e $|N * K| = |\underline{n} * K| \geq n$, illetőleg milyen n-től, vagy n-től és K-tól függő alsó korlátot tudunk adni $|\underline{n} * K|$ értékére. Ennek speciális esete, amikor $K = \underline{k}$ valamely k természetes számra, tehát ebben az esetben a kérdés az, hogy $|\underline{n} * \underline{k}| \geq n$ igaz-e.

Megjegyezzük, hogy ha N-ről nem követelnénk meg, hogy $N = \underline{n}$ teljesüljön valamely n természetes számra, hanem a természetes számok tetszőleges véges részhalmaza lehetne, akkor már nem igaz, hogy legalább $|N|$ számot kapunk meg páratlan sokszor:

Nem igaz, hogy tetszőleges $K, N \subseteq \mathbb{N}$ véges halmazokra

$$|K * N| \geq \max(|K|, |N|).$$

Tekintsük ugyanis a következő példát:

$$K = \{1, a\} \text{ (ahol } 1 < a \text{ egész)}, \; N = \{1, a, a^2, \ldots, a^{n-1}\}.$$

Ebben az esetben a $K \cdot N$-beli szorzatok:

$$1, a, a^2, \ldots, a^{n-1}, a, a^2, \ldots, a^n,$$

vagyis $K * N = \{1, a^n\}$, tehát $|K * N| = 2$.

Sőt, $|K * N| \geq \min(|K|, |N|)$ sem igaz, erre is mutatunk egy ellenpéldát:

$$K = \{2^1, 2^2, 2^4, \ldots, 2^{2^n}\}, N = \{1\} \cup K.$$

Ekkor

$$K * N = K * (\{1\} \cup K) = K \Delta (K * K) =$$
$$= \{2^1, 2^2, 2^4, \ldots, 2^{2^n}\} * \{2^2, 2^4, 2^8, \ldots, 2^{2^{n+1}}\} = \{2^1, 2^{2^{n+1}}\},$$

és így $|K * N| = 2$. Tehát $2 \leq |K * N|$-nél több nem igaz, ez viszont mindig teljesül a triviális $|K| = |N| = 1$ eset kivételével, hiszen

$$a = \min_{i \in K} i, b = \min_{j \in N} j, c = \max_{i \in K} i, d = \max_{j \in N} j$$

esetén könnyen láthatóan ab-t és cd-t csak egyszer-egyszer kapjuk meg K-beli és N-beli elem szorzataként, valamint $ab \neq cd$.

Több esetben a páratlan sokszor szereplő szorzatok számát a pontosan egyszer szereplők számával becsüljük alulról. Ez indokolja a következő jelölés bevezetését.

5. Definíció. Legyenek $K, N \subseteq \mathbb{N}$ véges halmazok. A $K \cdot N$ halmaz azon elemeinek halmazát, amelyek egyféleképpen állnak elő K-beli és N-beli elem szorzataként, $1(K, N)$-nel jelöljük.

Először az általános esettel fogunk foglalkozni. Bevezetjük a következő jelölést: $g(n)$ legyen $|\underline{n} * K|$ lehetséges legkisebb értéke, ha K a természetes számok véges részhalmaza lehet. Megmutatjuk, hogy $g(n)$ alulról becsülhető $c \cdot \frac{n}{(\log n)^{0,46}}$-nal, ahol c pozitív konstans. Korábban a legjobb ismert alsó becslés $\frac{n}{\log n}$ nagyságrendű volt. Bebizonyítjuk azt is, hogy minden K esetén létezik és pozitív a

$$\lim_{n\to\infty} \frac{|\underline{n} * K|}{n} = c(K)$$

határérték, sőt $|\underline{n} * K| - c(K) \cdot n$ abszolút értéke egy csak K elemszámától függő korlát alatt marad minden n-re.

Ezután rátérünk a $K = \underline{k}$, $N = \underline{n}$ speciális esetre (feltehető, hogy $k \leq n$), és megmutatjuk, hogy $|\underline{k} * \underline{n}| \geq n$ mindig teljesül. A bizonyításból az is kiderül, hogy egyenlőség csak

$$k = 1,$$
$$k = n,$$
$$k = 2 \text{ és } n \text{ páros},$$
$$k = 3 \text{ és } n = 4$$

esetekben áll fenn. A bizonyítás három részből áll, k és n viszonyától függően. A bizonyításhoz szükségünk lesz (főként prímszámokkal kapcsolatos) segédtételekre, ezeket a 3. fejezetben ismertetjük.

2. Általános eset

A bevezetésben ismertettünk bizonyos lineáris kódokat, melyek minimális távolságát a következő függvénnyel tudjuk alulról becsülni:

$$g(n) = \min_{K\subseteq\mathbb{N},|K|<\infty} |\underline{n} * K|,$$

ahol n pozitív egész szám. A minimális távolságra, vagyis g-re keresünk minél jobb alsó becslést. Igazolni fogjuk, hogy létezik olyan pozitív c konstans, hogy minden 1-nél nagyobb n természetes számra teljesül

$$g(n) \geq c\frac{n}{(\log n)^{0,46}}$$

egyenlőtlenség.

A $|K| = 1$ esetben például $|\underline{n} * K| = n$, hiszen K egyetlen elemét a-val jelölve $\underline{n} * K = \{a, 2a, \ldots, na\}$. Ebből következik, hogy minden n természetes számra érvényes a $g(n) \leq n$ egyenlőtlenség.

Először igazolunk egy a g függvényre vonatkozó egyszerűbb alsó becslést, amely megtalálható [4]-ben is.

6. Állítás. *Tetszőleges n természetes szám esetén $g(n) \geq 1 + \pi(n)$.*

Bizonyítás. Legyen $p \leq n$ tetszőleges prímszám. Legyen a az 1, 2, …, n számok közül az, amelynek prímtényezős felbontásában p kitevője maximális, amennyiben több ilyen is van, ezek közül válasszuk a legnagyobbat. Ehhez hasonlóan, legyen b a K halmaz elemei közül az, amelynek prímtényezős felbontásában p kitevője maximális, amennyiben több ilyen is van, ezek közül válasszuk a legnagyobbat. Azt állítjuk, hogy ab egyféleképpen áll elő $\underline{n} \cdot K$-beli szorzatként, amiből következik, hogy $ab \in \underline{n} * K$. Tegyük fel ugyanis, hogy $ab = cd$ valamely $c \in \underline{n}$, $d \in K$ elemekre. Az a és b elemeket úgy választottuk, hogy prímtényezős felbontásukban p kitevője maximális legyen, ezért $ab = cd$ csak úgy lehetséges, ha a és c prímtényezős felbontásában p kitevője egyenlő, továbbá ugyanez igaz b és d esetében. Ekkor viszont $c \leq a$ és $d \leq b$, vagyis $ab = cd$ csak akkor teljesülhet, ha $c = a$ és $d = b$. Tehát ab pontosan egyszer áll elő $\underline{n}$-beli és K-beli elem szorzataként, és így $ab \in \underline{n} * K$. Így minden $p \leq n$ prímszámhoz találunk egy $\underline{n} * K$-beli elemet.

Megmutatjuk, hogy különböző prímszámokhoz különböző elemet találunk, vagyis $p, q \leq n$ különböző prímszámok esetén, ha p-hez ab, q-hoz pedig $a'b'$ tartozik ($a, a' \in \underline{n}$ és $b, b' \in K$), akkor $ab \neq a'b'$. Tegyük fel, hogy $ab = a'b'$. Megmutattuk, hogy ab (és $a'b'$) előállítása $\underline{n}$-beli és K-beli elem szorzataként egyértelmű, így ez csak $a = a'$, $b = b'$ esetén lehetséges. Logikai szimmetria miatt feltehető, hogy $p < q$. Mivel $q \leq n$, ezért az 1, 2, …, n számok között van q-val osztható, vagyis

$q|a' = a$. Írjuk fel a-t $a = p^\alpha a_1$ alakban, ahol a_1 már nem osztható p-vel. Mivel $q \neq p$ prímszám, ezért $q|a_1$, következésképpen $p < q \leq a_1$. Ekkor viszont $\bar{a} = p^{\alpha+1} \leq a$, és így $\bar{a} \in \underline{n}$. Az $\bar{a}$ szám p-nek magasabb kitevős hatványával osztható, mint a, ez azonban ellentmond a megválasztásának. Ezzel igazoltuk az állítást.

Az ily módon kapott $\pi(n)$ darab páronként különböző $\underline{n} * K$-beli elemtől különböző, és szintén $\underline{n} * K$-beli K legkisebb eleme. Ezt ugyanis csak úgy kapjuk meg $\underline{n}$-beli és K-beli elem szorzataként, ha önmagát szorozzuk $1 \in \underline{n}$-nel, és mivel 1 semmilyen $p \leq n$ prímre nem lehet az az $\underline{n}$-beli elem, amely p-nek a legmagasabb kitevős hatványával osztható, ezért különbözik az eddig kapottaktól. Ezzel bizonyítottuk a 6. Állítást. □

Most bizonyítunk egy másik, g-re vonatkozó alsó becslést. A bizonyításunk a következő észrevételen alapul:

7. Állítás. *Minden n természetes számra $g(n) \geq \sum_{\sqrt{n}<p\leq n} g([n/p])$, ahol az összegzés a $(\sqrt{n}, n]$ intervallumba eső prímekre történik.*

Bizonyítás. Legyen $p \in (\sqrt{n}, n]$ prímszám és $K_p \subseteq K$ azon K-beli elemek halmaza, amelyek prímtényezős felbontásában p kitevője maximális. Ehhez hasonlóan legyen $\underline{n}_p \subseteq \underline{n}$ azon $\underline{n}$-beli elemek halmaza, amelyek prímtényezős felbontásában p kitevője maximális. A p prímszám kitevőjét vizsgálva látható, hogy ha $ab = cd$, ahol $a \in \underline{n}_p$, $b \in K_p$, $c \in \underline{n}$, $d \in K$, akkor $c \in K_p$ és $d \in \underline{n}_p$ is teljesül. Belátjuk, hogy $p, q \leq n$ különböző prímszámok esetén $\underline{n}_p \cdot K_p$ és $\underline{n}_q \cdot K_q$ halmazok diszjunktak. Logikai szimmetria miatt feltehető, hogy $p < q$. A p prímszám kitevőjét vizsgálva megállapíthatjuk, hogy $(\underline{n}_p \cdot K_p) \cap (\underline{n}_q \cdot K_q) \neq \emptyset$ csak úgy lehetséges, ha $\underline{n}_p \cap \underline{n}_q \neq \emptyset$. Azonban $d \in \underline{n}_p \cap \underline{n}_q$ esetén a d szám $d = pqd'$ alakban írható, így $\bar{d} = p^2 d' < d$ olyan eleme $\underline{n}$-nek, amelyben p kitevője nagyobb, mint d-ben, ami ellentmondás.

Az eddigiekből következik az alábbi egyenlőtlenség:

$$|N * K| \geq \sum_{\sqrt{n}<p\leq n} |N_p * K_p|. \tag{1}$$

Mivel $\sqrt{n} < p \leq n$, ezért N-nek van p-vel osztható eleme, de nincs olyan, ami p^2-tel is osztható lenne, ezért $\underline{n}_p = \{p, 2p, \ldots, [n/p]p\}$.

Könnyen látható, hogy $|\underline{n}_p * K_p| = |\underline{[n/p]} * K_p|$, így g definícióját felhasználva azt kapjuk, hogy:

$$|\underline{n}_p * K_p| = |\underline{[n/p]} * K_p| \geq g([n/p]).$$

Ezt (1)-gyel egybevetve a kívánt

$$g(n) \geq \sum_{\sqrt{n}<p\leq n} g\left([n/p]\right)$$

egyenlőtlenséget kapjuk. □

A bizonyításhoz felhasználjuk Mertens prímszámok reciprokösszegére vonatkozó alábbi nevezetes tételét:

8. Tétel. *Létezik olyan M konstans, hogy* $\sum_{p\leq x} \frac{1}{p} = \log\log x + M + o(1)$.

A tétel, amit bizonyítunk, a következő:

9. Tétel. *Létezik olyan $0 < c$ úgy, hogy minden 1-nél nagyobb n természetes számra*

$$g(n) \geq c\frac{n}{(\log n)^{0,46}} \tag{2}$$

teljesül.

Bizonyítás. Az 9. Tételt n-re vonatkozó indukcióval igazoljuk. Először megjegyezzük, hogy világos, hogy tetszőleges $0 < A$ számhoz választható olyan $0 < c = c(A)$ úgy, hogy minden $1 < n \leq A$ pozitív egész számra teljesül, hogy

$$g(n) \geq c\frac{n}{(\log n)^{0,46}}, \tag{3}$$

hiszen $g(n) \geq 1$ minden n-re. A bizonyítás során később fogjuk megválasztani A értékét.

Tegyük fel most, hogy az m-nél kisebb n-ekre (2) egyenlőtlenséget már igazoltuk, megmutatjuk, hogy $n = m$-re is teljesül. Feltehető, hogy $A < m$. A 7. Állítást és az indukciós feltevést használva

$$g(m) \geq \sum_{\sqrt{m}<p\leq m} g\left([m/p]\right) \geq \sum_{\sqrt{m}<p<m/2} c\frac{[m/p]}{\log([m/p])^{0,46}}, \tag{4}$$

hiszen $p < m/2$ esetén $1 < [m/p]$ és így az indukciós feltevésben szereplő egyenlőtlenség alkalmazható. Az $(m/2, m]$ intervallumba eső prímekre $g(1) = 1$-et kellett összegezni, ez az összeg $O(m/\log m)$, ezért az elhagyásával okozott hiba elhanyagolható.

Folytassuk (4) egyenlőtlenséget:

$$\sum_{\sqrt{m}<p<m/2} c\frac{[m/p]}{\log([m/p])^{0,46}} \geq \sum_{\sqrt{m}<p<m/2} c\frac{m/p-1}{\log([m/p])^{0,46}} =$$

$$= \sum_{\sqrt{m}<p<m/2} c\frac{m/p}{\log([m/p])^{0,46}} - \sum_{\sqrt{m}<p<m/2} c\frac{1}{\log([m/p])^{0,46}}.$$

Először megmutatjuk, hogy az egészrész elhagyásával keletkező hiba elhanyagolható.

$$\sum_{\sqrt{m}<p<m/2} c\frac{1}{\log([m/p])^{0,46}} \leq \sum_{\sqrt{m}<p<m/2} c\frac{1}{(\log 2)^{0,46}} \leq 2c\frac{m}{\log m},$$

hiszen $\pi(m/2) - \pi(\sqrt{m}) < 1,5 \cdot \dfrac{m}{\log m}$.

Folytassuk a fő tag becslésével:

$$\sum_{\sqrt{m}<p<m/2} c\frac{m/p}{(\log([m/p]))^{0,46}} \geq cm \sum_{\sqrt{m}<p<m/2} \frac{1/p}{(\log(m/p))^{0,46}}.$$

Csoportosítsuk aszerint a p prímeket, hogy mely j egész számra teljesül $m^{1-\frac{1}{j}} < p \leq m^{1-\frac{1}{j+1}}$. A tétel bizonyításához elég lesz, ha csak $j \leq 15$-ig megyünk el, vagyis csak az $m^{1-\frac{1}{16}}$-nál kisebb prímekre összegzünk. Ha $m > 2^{16}$, akkor $m^{1-\frac{1}{16}} < m/2$, ezért érvényes a következő becslés:

$$cm \sum_{\sqrt{m}<p<m/2} \frac{1/p}{(\log(m/p))^{0,46}} \geq cm \sum_{j=2}^{15} \sum_{m^{1-\frac{1}{j}}<p\leq m^{1-\frac{1}{j+1}}} \frac{1/p}{(\log(m/p))^{0,46}}.$$

Ha $m^{1-\frac{1}{j}} < p \leq m^{1-\frac{1}{j+1}}$, akkor $\log(m/p) < \dfrac{\log m}{j}$. Ezt felhasználva folytatjuk a becslést.

$$cm \sum_{j=2}^{15} \sum_{m^{1-\frac{1}{j}}<p\leq m^{1-\frac{1}{j+1}}} \frac{1/p}{(\log(m/p))^{0,46}} \geq$$

$$\geq cm \sum_{j=2}^{15} \sum_{m^{1-\frac{1}{j}}<p\leq m^{1-\frac{1}{j+1}}} \frac{1/p}{(\log(m)/j)^{0,46}} =$$

$$= \frac{cm}{(\log m)^{0,46}} \sum_{j=2}^{15} j^{0,46} \sum_{m^{1-\frac{1}{j}}<p\leq m^{1-\frac{1}{j+1}}} \frac{1}{p}$$

Az eddigieket összefoglalva, azt kaptuk, hogy teljesül az alábbi egyenlőtlenség:

$$g(m) \geq \frac{cm}{(\log(m))^{0,46}} \left(\sum_{j=2}^{15} j^{0,46} \sum_{m^{1-\frac{1}{j}} < p \leq m^{1-\frac{1}{j+1}}} \frac{1}{p} \right) - 2c\frac{m}{\log m} \tag{5}$$

A $\displaystyle\sum_{m^{1-\frac{1}{j}} < p \leq m^{1-\frac{1}{j+1}}} \frac{1}{p}$ összeg becsléséhez felhasználjuk a prímszámok reciprokösszegére vonatkozó 8. Tételt.

Ezen tétel szerint minden $0 < \varepsilon$ számhoz létezik olyan $B = B(\varepsilon)$ korlát, hogy $B \leq x$ esetén

$$\left| \sum_{p \leq x} \frac{1}{p} - \log\log x - M \right| < \varepsilon. \tag{6}$$

Az A szám megválasztásánál majd figyelünk arra, hogy $A \geq B^2$ teljesüljön, így korábbi megjegyzésünk szerint m-ről feltehető, hogy $m > A \geq B^2$, ezért $\sqrt{m} > B$ is teljesülni fog. Ekkor viszont alkalmazható a (6) egyenlőtlenség $x = m^{1-\frac{1}{j}}$ és $x = m^{1-\frac{1}{j+1}}$ választással minden $1 \leq j \leq 15$ esetén:

$$\sum_{m^{1-\frac{1}{j}} < p \leq m^{1-\frac{1}{j+1}}} \frac{1}{p} = \sum_{p \leq m^{1-\frac{1}{j+1}}} \frac{1}{p} - \sum_{p \leq m^{1-\frac{1}{j}}} \frac{1}{p} \geq$$

$$\geq \log\log\left(m^{1-\frac{1}{j+1}}\right) - \log\log\left(m^{1-\frac{1}{j}}\right) - 2\varepsilon = \log\left(\frac{j^2}{j^2-1}\right) - 2\varepsilon.$$

A kapott eredményt felhasználva folytatva (5) egyenlőtlenséget:

$$g(m) \geq \frac{cm}{(\log(m))^{0,46}} \left(\sum_{j=2}^{15} j^{0,46} \left(\log\frac{j^2}{j^2-1} - 2\varepsilon \right) \right) - 2c\frac{m}{\log m} =$$

$$= \frac{cm}{(\log(m))^{0,46}} \left(\sum_{j=2}^{15} j^{0,46} \cdot \log\frac{j^2}{j^2-1} \right) -$$

$$- 2\varepsilon \frac{cm}{(\log(m))^{0,46}} \left(\sum_{j=2}^{15} j^{0,46} \right) - 2c\frac{m}{\log m}.$$

Numerikus számítással ellenőrizhetjük, hogy

$$\sum_{j=2}^{15} j^{0,46} \cdot \log\frac{j^2}{j^2-1} > 1,1.$$

Ezért

$$g(m) \geq \frac{cm}{(\log m)^{0,46}} \left(1,1 - 2\varepsilon \sum_{j=2}^{15} j^{0,46} - \frac{2}{(\log m)^{0,54}} \right).$$

Létezik olyan $\varepsilon > 0$ és olyan C, hogy $C < m$ és ε mellett

$$1,1 - 2\varepsilon \sum_{j=2}^{15} j^{0,46} - \frac{2}{(\log m)^{0,54}} > 1,$$

és ilyenkor

$$g(m) \geq \frac{cm}{(\log m)^{0,46}}.$$

Ha tehát $A = \max(2^{16}, B^2, C)$-hez választjuk meg c pozitív konstanst úgy, hogy (3) teljesüljön $m \leq A$ esetén, akkor az indukciós bizonyítással a többi m-re is igazoljuk (3) egyenlőtlenséget. □

A 9. Tétel a $K * N$ halmaz elemszámára K-tól nem függő alsó becslést adott.

Most bizonyítunk egy olyan eredményt, amely rögzített K halmaz esetén ad becslést $|\underline{n} * K|$-ra. Legyen $K = \{a_1, a_2, \ldots, a_k\}$ és vezessük be $1 \leq i \leq k$ esetén az $A_i = a_i\underline{n} = \{a_i, 2a_i, \ldots, na_i\}$ jelölést. Könnyen meggondolható, hogy

$$\underline{n} * K = A_1 \Delta A_2 \Delta \cdots \Delta A_k.$$

Tetszőleges A_1, A_2, …, A_k véges halmazok esetén a következő lemma megad egy összefüggést az $A_1 \Delta A_2 \Delta \cdots \Delta A_k$ szimmetrikus differencia elemszámára.

10. Lemma. *Tetszőleges A_1, A_2, …, A_k véges halmazok esetén igaz a*

$$(7) \quad |A_1 \Delta A_2 \Delta \cdots \Delta A_k| = \sum_{1 \leq i_1 \leq k} |A_i| - 2 \sum_{1 \leq i_1 < i_2 \leq k} |A_{i_1} \cap A_{i_2}| +$$

$$+ 4 \sum_{1 \leq i_1 < i_2 < i_3 \leq k} |A_{i_1} \cap A_{i_2} \cap A_{i_3}| + \cdots + (-2)^{k-1} |A_1 \cap A_2 \cap \ldots \cap A_k|.$$

egyenlőség.

Bizonyítás. Legyen az a elem olyan, amely az A_i halmazok közül pontosan j-nek eleme ($0 \leq j \leq k$). Meghatározzuk, hogy a-t hányszor számoljuk a (7) egyenlet két oldalán.

A baloldalon 1-szer számoljuk, ha j páratlan, és 0-szor, ha j páros.

Azt pedig, hogy a jobboldalon hányszor számoljuk, a következő összeg adja meg:

$$T = j - 2\binom{j}{2} + 4\binom{j}{3} + \cdots + (-2)^{j-1}\binom{j}{j}.$$

A binomiális tételt használva $1 - 2T = (1-2)^j = (-1)^j$, vagyis $T = \frac{1-(-1)^j}{2}$. Tehát $T = 1$, ha j páratlan, és $T = 0$, ha j páros. Ez azt jelenti, hogy mindent ugyanannyiszor számolunk (7) két oldalán, ami igazolja a lemma állítását. □

Ahhoz, hogy 10. Lemmát alkalmazhassuk $|\underline{n} * K|$ kiszámolására, meg kell határoznunk az $A_{i_1 i_2 \ldots i_j} = A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_j}$ alakú halmazok elemszámát $A_m = m\underline{n}$ mellett. Mivel A_m elemei m-mel osztható pozitív egész számok, ezért $A_{i_1 i_2 \ldots i_j}$ halmaz elemei csak olyan pozitív egész számok lehetnek, amelyek oszthatók az a_{i_1}, a_{i_2}, …, a_{i_j} számok mindegyikével, így legkisebb közös többszörösükkel is. Vizsgáljuk meg, hogy $t \cdot lkkt(a_{i_1}, a_{i_2}, \ldots, a_{i_j})$ milyen $t \in \mathbb{N}$ értékek mellett lesz eleme $A_{i_1 i_2 \ldots i_j}$-nek. Legyen most $1 \le r \le j$ tetszőleges. Mivel $t \cdot lkkt(a_{i_1}, a_{i_2}, \ldots, a_{i_j})$ pozitív egész szám osztható a_{i_r}-rel, ezért $t \cdot lkkt(a_{i_1}, a_{i_2}, \ldots, a_{i_j}) \in A_{i_r}$ pontosan akkor teljesül, ha $t \cdot lkkt(a_{i_1}, a_{i_2}, \ldots, a_{i_j}) \le a_{i_r} n$, azaz, ha

$$t \le \left\lfloor \frac{a_{i_r}}{lkkt(a_{i_1}, a_{i_2}, \ldots, a_{i_j})} \right\rfloor.$$

Vagyis az r mind a j féle lehetséges megválasztása esetén egy felső korlát t-re a kapott feltétel, ezek közül a legszigorúbbat akkor kapjuk, amikor az a_{i_r} számok közül a legkisebbet választjuk.

Tehát $|A_{i_1 i_2 \ldots i_j}| = \left\lfloor \frac{\min_{1 \le i \le j} a_{i_r}}{lkkt(a_{i_1}, a_{i_2}, \ldots, a_{i_j})} n \right\rfloor$. Ezt és 10. Lemmát felhasználva:

$$(8)\quad |K * \underline{n}| = \sum_{1 \le i_1 \le k} |A_i| - 2 \sum_{1 \le i_1 < i_2 \le k} \left\lfloor \frac{\min(a_{i_1}, a_{i_2})}{lkkt(a_{i_1}, a_{i_2})} n \right\rfloor + 4 \sum_{1 \le i_1 < i_2 < i_3 \le k} \left\lfloor \frac{\min(a_{i_1}, a_{i_2}, a_{i_3})}{lkkt(a_{i_1}, a_{i_2}, a_{i_3})} n \right\rfloor + \cdots + (-2)^{k-1} \left\lfloor \frac{\min(a_1, \ldots, a_k)}{lkkt(a_1, \ldots, a_k)} n \right\rfloor.$$

A (8) egyenlőség jobboldalán szereplő egészrészek száma

$$R = 2\binom{k}{2} + 4\binom{k}{3} + \cdots + 2^{k-1}\binom{k}{k}.$$

A binomiális tétel szerint $1 + 2k + 2R = (1 + 2)^k = 3^k$, ezért $R = (3^k - 2k - 1)/2$. Ez azt jelenti, hogy ha $|\underline{n} * K|$ értékét úgy becsüljük meg, hogy (8) egyenlőség jobboldalán elhagyjuk az egészrészeket, akkor az így keletkező hiba legfeljebb $(3^k - 2k - 1)/2$, vagyis csak k értékétől függ. Felhasználva, hogy $|A_1| = \ldots = |A_k| = n$:

$$|\underline{n}*K| = \Big(k-2\sum_{1\le i_1<i_2\le k}\frac{\min(a_{i_1},a_{i_2})}{lkkt(a_{i_1},a_{i_2})}+4\sum_{1\le i_1<i_2<i_3\le k}\frac{\min(a_{i_1},a_{i_2},a_{i_3})}{lkkt(a_{i_1},a_{i_2},a_{i_3})}+$$
$$+\cdots+(-2)^{k-1}\frac{\min(a_1,\ldots,a_k)}{lkkt(a_1,\ldots,a_k)}\Big)n+h=cn+h,$$

ahol $c = c(a_1, \ldots, a_k)$ és $|h| \le \dfrac{3^k - 2k - 1}{2}$.

Ebből az következik, hogy létezik és c-vel egyenlő a $\lim\limits_{n\to\infty}\dfrac{|\underline{n} * K|}{n}$ határérték. Ezen sorozat tagjai pozitív számok, ezért $c \ge 0$. Megmutatjuk, hogy $c > 0$. Ha ugyanis $c = 0$ lenne, az azt jelentené, hogy $\underline{n} * K$ elemszáma tetszőleges n esetén egy csupán k-tól függő korlát alatt maradna, ez pedig ellentmondana a 6. Állításban, illetve a 9. Tételben bizonyítottaknak.

Igazoltuk tehát a következő tételt:

11. Tétel. *Tetszőleges n természetes szám és K természetes számokból álló k elemű véges halmaz esetén $|\underline{n} * K| = cn + O_k(1)$, ahol $0 < c = c(K)$ értéke*

$$c = k - 2\sum_{1\le i_1<i_2\le k}\frac{\min(a_{i_1},a_{i_2})}{lkkt(a_{i_1},a_{i_2})}+$$
$$+4\sum_{1\le i_1<i_2<i_3\le k}\frac{\min(a_{i_1},a_{i_2},a_{i_3})}{lkkt(a_{i_1},a_{i_2},a_{i_3})}+\ldots+(-2)^{k-1}\frac{\min(a_1,\ldots,a_k)}{lkkt(a_1,\ldots,a_k)}.$$

12. Következmény. *Létezik $0 < c' = c'(K)$ úgy, hogy minden n pozitív egész számra teljesül az $|\underline{n} * K| \ge c'n$ egyenlőtlenség.*

Bizonyítás. Ha c'-t c-nél kisebbnek választjuk, akkor elég nagy n-re, mondjuk $E \le n$ esetén már teljesül az egyenlőtlenség a 11. Tétel szerint. Mivel $|\underline{n} * K| \ge 1$ mindig teljesül, ezért ha c-t $1/E$-nél is kisebbre választjuk, akkor már az összes természetes számra igaz lesz a $|\underline{n} * K| \ge c'n$ egyenlőtlenség. □

3. Előkészületek

A következő fejezetben $K = \underline{k}$ és $N = \underline{n}$ esetén igazolni fogjuk, hogy $|K * N| \geq n$. Ehhez szükségünk lesz néhány segédtételre, ezeket tekintjük át ebben a fejezetben.

Az első tétel, amit használni fogunk a jól ismert logikai szita formula.

13. Tétel. *(Logikai szita formula). Tegyük fel, hogy adott egy véges, mondjuk L elemű halmaz, amelynek elemei közül egyesek rendelkeznek bizonyos $T_1, \ldots, T_r$ "rossz tulajdonságok" közül egyesekkel, és legyen $T_{i_1}, \ldots, T_{i_j}$ rossz tulajdonsággal rendelkezők száma $L_{i_1,\ldots,i_j}$. Ekkor a "jó" (rossz tulajdonsággal nem rendelkező) elemek száma*

$$L + \sum_{h=1}^{r} (-1)^h \sum_{1 \leq i_1 < \ldots < i_h \leq r} L_{i_1,\ldots,i_h}.$$

Szükségünk lesz néhány prímszámokkal kapcsolat becslésre.

14. Tétel. [5] *Minden $1 < k$ esetén*

$$\frac{e^{-\gamma}}{\log k}\left(1 - \frac{1}{\log^2 k}\right) \leq \prod_{p \leq k}\left(1 - \frac{1}{p}\right),$$

ahol γ az Euler-konstans.

A 14. Tételből levezetjük a következő becslést, a bizonyítás során ezt fogjuk felhaszálni.

15. Lemma. *Ha $k \geq 9$, akkor* $\displaystyle\prod_{p \leq k}\left(1 - \frac{1}{p}\right) \geq \frac{0,49}{\log k}.$

Bizonyítás. Először leellenőrizzük, hogy $9 \leq k \leq 16$ esetén fennáll az egyenlőtlenség. A logaritmus-függvény monotonitása miatt elég $k = 9$, 11, és 13 esetekre ellenőrizni. A $(\log k) \cdot \displaystyle\prod_{p \leq k}\left(1 - \frac{1}{p}\right)$ szorzat értéke $k = 9$ esetén $0,502\ldots$, $k = 11$ esetén $0,498\ldots$, $k = 13$ esetén pedig $0,491\ldots$. Ezek szerint ebben a három esetben, és így $9 \leq k \leq 16$ esetén fennáll a bizonyítandó egyenlőtlenség.

A $17 \leq k$ eset igazolásához felhasználjuk a 14. Tételt. A logaritmus függvény monoton növő és $k \geq 17$, ezért

$$\frac{e^{-\gamma}}{\log k}\left(1 - \frac{1}{\log^2 k}\right) \geq \frac{0,56}{\log k}\left(1 - \frac{1}{\log^2 17}\right) > \frac{0,49}{\log k},$$

hiszen $e^{-\gamma} > 0,56$. Ez bizonyítja az egyenlőtlenséget. □

Többször is alkalmazni fogjuk $\pi(x)$ becslésére a következő tételt.

16. Tétel. [6] *Ha $x \geq 17$, akkor fennáll a következő egyenlőtlenség:*

$$\frac{x}{\log x} \leq \pi(x) \leq \frac{x}{\log x}\left(1 + \frac{1,2762}{\log x}\right).$$

Az n-edik prímszám nagyságrendjére vonatkozó alábbi tételből levezetünk a szomszédos prímek közötti különbség nagyságrendjére vonatkozó becsléseket.

17. Tétel. [6] [7] *Jelölje $p(n)$ az n-edik prímszámot. Ha $n > 1$, akkor*

$$n(\log n + \log\log n - 1) < p(n)$$

és ha $n > 8601$, akkor

$$p(n) < n(\log n + \log\log n - 0,9385).$$

18. Tétel. *Tetszőleges $n > 89400$ esetén az $\left(n - \frac{0,0736}{\log n}, n\right)$ intervallum tartalmaz prímszámot.*

Bizonyítás. Tegyük fel, hogy valamely $n > 89400$ számra és $0 < c$-re az $\left(n - \frac{c}{\log n}, n\right)$ intervallumba nem esik egyetlen prímszám sem. Ez azt jelenti, hogy a $\pi(n-1) = t$ jelölést bevezetve egyrészt

$$p(t) \leq n - \frac{c}{\log n},$$

másrészt

$$n \leq p(t+1).$$

Mivel $90000 < n \leq p(t+1)$, ezért $t > 8601$, így alkalmazható a 17. Tétel, amely szerint

$$t(\log t + \log\log t - 1) < p(t)$$

és

$$p(t+1) < (t+1)(\log(t+1) + \log\log(t+1) - 0,9385).$$

A két egyenlet egybevetéséből pedig

$$\frac{c}{\log n} \leq p(t+1) - p(t) \leq$$
$$\leq (t+1)(\log(t+1) + \log\log(t+1) - 0,9385) - t(\log t + \log\log t - 1).$$

Felső becslést adunk az egyenlőtlenség jobboldalán szereplő kifejezésre. A könnyen igazolható $\log(1+1/t) < 1/t$ és $\log(\log(t+1)/\log(t)) <$

$1/t$ egyenlőtlenségeket felhasználva:

$$(t+1)(\log(t+1)+\log\log(t+1)-0,9385)-t(\log t+\log\log t-1)=$$
$$=t(\log(1+1/t)+\log(\log(t+1)/\log(t))+0,0625)+\log(t+1)+$$
$$+\log\log(t+1)-0,9385<t(1/t+1/t+0,0625)+\log(t+1)+$$
$$+\log\log(t+1)-0,9385=0,0625\cdot t+1,0615+\log(t+1)+\log\log(t+1)<$$
$$<0,064\cdot t,$$

hiszen $t>8601$ esetén

$$\frac{1,0615+\log(t+1)+\log\log(t+1)}{t}<0,0015.$$

Mivel a 16. Tétel szerint

$$t=\pi(n-1)\le\frac{n-1}{\log(n-1)}\left(1+\frac{1,28}{\log(n-1)}\right)<1,15\cdot\frac{n}{\log n},$$

ezért $c<0,064\cdot 1,15=0,0736$ következik. Ez pedig bizonyítja a tétel állítását. □

19. Következmény. *Tetszőleges $n>1361$ esetén az $\left(n-\frac{0,11}{\log n},n\right)$ intervallum tartalmaz prímszámot.*

Bizonyítás. Tudjuk, hogy az állítás $n>89600$ esetén igaz. Számítógéppel ellenőrizhető, hogy $n\in(1361,89600)$ esetén is az. Ehhez

$$\frac{p(i)-p(i-1)}{p(i)}\log p(i)\le 0,11 \tag{9}$$

egyenlőtlenséget kell ellenőrizni (ahol $p(i)$ az i-edik prímszám), az összes olyan i-re, ahol $p(i)\in(1361,90000)$. Ugyanis, ha ez igaz, de létezne olyan n, amelyre az állítás hamis, akkor $p(i)$-nek az n-nél nem kisebb számok közül a legkisebb prímet választva $p(i)\in(1361,90000)$ és $p(i)$-re (9) mégsem lenne igaz, ami ellentmondás.

Megjegyezzük, hogy az 1327 és 1361 egymást követő prímszámok, $\frac{1361-1327}{1361}\log 1361>0,18$. □

A számolás során szükségünk lesz az alábbi, monoton csökkenő függvényekre vonatkozó egyenlőtlenségre.

20. Tétel. *Ha $r<s$ egészek és $f:[r,s]\to\mathbb{R}$ monoton csökkenő, akkor*

$$\sum_{l=r}^{s}f(l)\le\int_r^s f(x)dx+f(r).$$

4. Speciális eset

Ebben a fejezetben bizonyítjuk, hogy a $K = \underline{k}$, $N = \underline{n}$ speciális esetben $|K * N| \geq n$ mindig teljesül. Természetesen feltehető, hogy $k \leq n$. A tétel, amit bizonyítunk, így szól:

21. Tétel. *Tetszőleges $k \leq n$ pozitív egész számok esetén $|\underline{k} * \underline{n}| \geq n$ és egyenlőség csak a következő esetekben áll fenn: $k = 1$ vagy $k = n$ vagy $k = 2$ és n páros vagy $k = 3$ és $n = 4$.*

Bizonyítás. Az állítás bizonyítását k és n viszonyától függően három részre bontjuk aszerint, hogy k kicsi, közepes, vagy nagy n-hez képest. Ennek pontos megfogalmazását később, a különböző eseteknél írjuk le.

A bizonyítást azzal az esettel kezdjük, amikor k kicsi: $k \leq 1,34 \cdot \log n$.
I. (a) eset, k kicsi: Legyen először $9 \leq k \leq 1,34 \cdot \log n$, a $k \leq 8$ esettel később, külön foglalkozunk. A bizonyításban döntő szerepet játszó észrevétel a következő:

Legyen $1 \leq i \leq k$ és legyen $n/2 < t \leq n$ olyan egész szám, amelyre $(t, k!) = 1$. Azt állítjuk, hogy ekkor $it \in 1(\underline{k}, \underline{n})$, és így $it \in \underline{k} * \underline{n}$.

Tegyük fel ugyanis, hogy $it = ab$, ahol $a \in \underline{k}$ és $b \in \underline{n}$. Mivel $1 \leq a \leq k$ és $(t, k!) = 1$, ezért $(t, a) = 1$. Ebből viszont $t|ab$ miatt $t|b$ következik, vagyis b egy t-vel osztható pozitív egész szám. Mivel $n/2 < t$, ezért $2t$ már nagyobb, mint n, azaz $\underline{n}$ elemei között t-nek egyetlen többszöröse van: t. Tehát csak $b = t$ lehetséges, ekkor szükségképpen $a = i$. Az $i \cdot t$ előállítás viszont megfelelő, ezzel az állítást igazoltuk.

Azt fogjuk megmutatni, hogy ily módon legalább n darab $\underline{k} * \underline{n}$-beli elemet kapunk. Ehhez a következőkben alsó becslést adunk arra, hogy az $(n/2, n]$ intervallum hány $k!$-hoz relatív prím számot tartalmaz. Ehhez a logikai szita formulát (13. Tétel) fogjuk alkalmazni. Legyenek a k-nál nem nagyobb (pozitív) prímszámok $p_1, \ldots, p_r$. $(r = \pi(k))$ Könnyen meggondolható, hogy t és $k!$ pontosan akkor relatív prímek, ha t a $p_1, \ldots, p_r$ prímszámok egyikével sem osztható.

Esetünkben a vizsgált halmaz $(n/2, n]$, vagyis a szitált halmaz elemszáma $L = n - [n/2]$, a T_i rossz tulajdonság pedig legyen a p_i-vel való oszthatóság. A jó elemek számára vagyunk kíváncsiak. Könnyen látható, hogy a $T_{i_1}, T_{i_2}, \ldots, T_{i_h}$ rossz tulajdonságok mindegyikével rendelkező elemek száma

$$L_{i_1,\ldots,i_h} = |\{a : n/2 < a \leq n, p_{i_1} \ldots p_{i_h} | a\}| = \left[\frac{n}{p_{i_1} \ldots p_{i_h}}\right] - \left[\frac{n/2}{p_{i_1} \ldots p_{i_h}}\right].$$

A logikai szita formula szerint a jó tulajdonságú, vagyis $k!$-hoz relatív prímek száma

$$(10)\quad D = n - [n/2] + \\ + \sum_{h=1}^{r} (-1)^h \sum_{1 \le i_1 < \ldots < i_h \le r} \left(\left[\frac{n}{p_{i_1} \ldots p_{i_h}} \right] - \left[\frac{n/2}{p_{i_1} \ldots p_{i_h}} \right] \right).$$

A becsléshez az $x - 1 < [x] \le x$ egyenlőtlenséget használjuk. A (10) egyenlet jobboldalán szereplő kifejezésben pozitív előjellel szereplő, azaz $[x]$ alakú tagokat becsüljük alulról $x - 1$-gyel, a negatív előjellel szereplő, vagyis $-[x]$ alakú tagokat pedig becsüljük alulról $-x$-szel. Számoljuk meg, hogy $[x]$ alakú tagból összesen hány van: számuk 1-gyel kisebb, mint a $\{p_1, \ldots, p_r\}$ halmaz részhalmazainak száma, vagyis kisebb, mint 2^r. Így D-re a következő becslést nyertük:

$$(11)\quad D \ge n - n/2 + \\ + \sum_{h=1}^{r} (-1)^h \sum_{1 \le i_1 < \ldots < i_h \le r} \left(\frac{n}{p_{i_1} \ldots p_{i_h}} - \frac{n/2}{p_{i_1} \ldots p_{i_h}} \right) - 2^r = \\ = \frac{n}{2} \prod_{p \le k} \left(1 - \frac{1}{p} \right) - 2^r.$$

A $\displaystyle\prod_{p \le k} \left(1 - \frac{1}{p} \right)$ szorzat alsó becsléséhez a 15. Lemmát használjuk. A 15. Lemmából és (11)-ből $k \ge 9$ mellett a következő adódik:

$$(12)\qquad D \ge \frac{0,245 \cdot n}{\log k} - 2^r.$$

D alsó becsléséhez 2^r értékére felső becslést adunk. Ha $k \ge 8$, akkor $r = \pi(k) \le k/2$. (Ez a $k = 8$ esetben egyenlőséggel teljesülő, azonban nagy k értékekre durva becslés elegendő lesz számunkra.) Felhasználva, hogy $k < 1,34 \cdot \log n$, belátjuk a következő egyenlőtlenséget, amely számunkra elegendően pontos felső becslést ad 2^r értékére:

$$2^r \le \frac{n}{2000 \log k}.$$

Ekvivalens átalakítást végrehajtva:

$$e^{r \log 2} \le \frac{e^{\log n}}{2000 \log k},$$

ez pedig $k < 1,34 \cdot \log n$ miatt igaz, ha teljesül a következő egyenlőtlenség:

$$2000 \log k < e^{1,34 \cdot k - (\log 2) r},$$

de ez $r \leq k/2$ miatt következik az alábbi egyenlőtlenségből:

$$2000 \log k < e^{(1,34-\frac{\log 2}{2})k}.$$

Mivel $1,34 - \dfrac{\log 2}{2} > 0,99$, ezért elég $2000 \log k < e^{0,99k}$-t igazolni. Könnyen ellenőrizhető, hogy $\dfrac{e^{0,99k}}{\log k}$ monoton növő, így az egyenlőtlenséget elég $k = 9$ esetén ellenőrizni. Mivel $k = 9$-re a hányados értéke nagyobb, mint 2000, ezért bebizonyítottuk, hogy

$$2^r < \frac{n}{2000 \log k}.$$

(A hányados értéke $k = 9$ esetén valójában 3370 és 3371 közé esik, de számunkra elég lesz, hogy nagyobb, mint 2000.)

Ebből, és (12) egyenlőtlenségből $D \geq \dfrac{0,2445 \cdot n}{\log k}$ következik. Korábban bizonyítottuk azt az észrevételt, hogy páronként különböző $1(\underline{k}, \underline{n})$-beli elemeket kapunk, ha $\underline{k}$ tetszőleges elemét szorozzuk egy olyan $(n/2, n]$ intervallumba eső számmal, amely relatív prím $k!$-hoz. Így

$$|1(\underline{k}, \underline{n})| \geq Dk \geq \frac{0,2445 \cdot k}{\log k} n,$$

hiszen a bizonyítás elején igazolt észrevételben szereplő t értéke D féle lehet, i pedig $\underline{k}$ tetszőleges eleme, így megválasztására a lehetőségek száma k. Mivel az $[1, \infty)$ intervallumon $x/\log x$ monoton növő, ezért $k \geq 9$ esetén ebből

$$\frac{0,2445 \cdot k}{\log k} > \frac{0,2445 \cdot 9}{\log 9} > 1,001 > 1$$

következik, tehát igazoltuk, hogy $|1(\underline{k} * \underline{n})| > n$, amiből természetesen következik a bizonyítandó

$$|\underline{k} * \underline{n}| > n$$

egyenlőtlenség.

A bizonyítást a $k \leq 8$ esettel folytatjuk.

I. (b) eset, k nagyon kicsi: Legyen $1 \leq k \leq 8$.

Ha $k = 1$, akkor $\underline{k} * \underline{n} = \underline{n}$, vagyis $|\underline{k} * \underline{n}| = n$ minden n-re.

Ha $k = 2$, akkor $\underline{k} * \underline{n} = \underline{n} \Delta 2\underline{n} = \{1, 2, \ldots, n\} \Delta \{2, 4, \ldots, 2n\}$, amely nem más mint az n-nél nem nagyobb pozitív páratlan és az $(n, 2n]$ intervallumba eső páros számok uniója. Tehát $|\underline{k} * \underline{n}| = \lceil n/2 \rceil + n - [n/2]$, ami páros n esetén n, páratlan n esetén pedig $n + 1$.

Azt kaptuk, hogy ha $n = 2n_1$ páros szám, akkor

$$\underline{2} * \underline{n} = \{1, 3, 5, \ldots, 2n_1 - 1\} \cup \{2n_1 + 2, 2n_1 + 4, \ldots, 4n_1\}.$$

Ha pedig $n = 2n_1 - 1$ páratlan, akkor

$$\underline{2} * \underline{n} = \{1, 3, 5, \ldots, 2n_1 - 1\} \cup \{2n_1, 2n_1 + 2, \ldots, 4n_1 - 2\}.$$

Most $\underline{3} * \underline{n} = \{3, 6, \ldots, 3n\} \Delta (\underline{2} * \underline{n})$ elemszámát fogjuk alulról becsülni. Ehhez felső becslést adunk $|\{3, 6, \ldots, 3n\} \cap (\underline{2} * \underline{n})|$-re. Az n-nél nem nagyobb páratlan számok, és az $(n, 2n]$ intervallumba eső páros számok közül is minden harmadik osztható 3-mal, így

$$|\{3, 6, \ldots, 3n\} \cap (\underline{2} * \underline{n})| \leq 2 \cdot \lceil n/6 \rceil.$$

Ezért $|\underline{3} * \underline{n}| \geq n + n - 2\lceil n/6 \rceil > 2n - n/3 - 2 = 4n/3 - 2 > n$, ha $n > 6$. Az $n = 3, 4, 5, 6$ esetekben $|\underline{3} * \underline{n}|$ rendre 3, 4, 7, 8. Tehát $|\underline{3} * \underline{n}| \geq n$ és egyenlőség $n = 3$, $n = 4$ esetén áll fenn.

Végül, a $4 \leq k \leq 8$ esetben bizonyítjuk az állítást. Az 1, 2, …, n számok közül pontosan azok szerepelnek $\underline{n} \Delta 2\underline{n} \Delta \cdots \Delta k\underline{n}$-ben, amelyek az 1, 2, …, k számok közül páratlan sokkal oszthatók. Az $n + 1$, $n+2$, …, $2n$ számok közül pedig pontosan azok elemei $\underline{n} \Delta 2\underline{n} \Delta \cdots \Delta k\underline{n}$ halmaznak, amelyek $2\underline{n} \Delta 3\underline{n} \Delta \cdots \Delta k\underline{n}$ halmaznak elemei, ezek pedig azok közülük, amelyek a 2, 3, …, k számok közül páratlan sokkal, vagyis az 1, 2, …, k számok közül páros sokkal oszthatók. Jelöljük s-sel az 1, 2, …, k számok legkisebb közös többszörösét. Azt, hogy egy egész szám az 1, 2, …, k számok közül hánnyal osztható, meghatározza a szám s-sel osztva adott maradéka. Tehát létezik egy olyan $0 \leq v \leq s$ szám, hogy s egymást követő egész szám közül mindig v darab osztható az 1, 2, …, k számok közül páratlan sokkal és $s - v$ darab osztható páros sokkal. Az $[1, n]$ és az $[n+1, 2n]$ intervallum is tartalmaz $\left[\frac{n}{s}\right]$ páronként diszjunkt, s egymást követő egész számból álló intervallumot. Ezért az 1, 2, …, $2n$ számok közül legalább

$$t\left[\frac{n}{s}\right] + (s - t)\left[\frac{n}{s}\right] = s\left[\frac{n}{s}\right] \geq s\left(\frac{n}{s} - 1\right) = n - s$$

eleme $\underline{n} \Delta 2\underline{n} \Delta \cdots \Delta k\underline{n}$-nek.

A $(k-1)n + 1$, $(k-2)n + 2$, …, kn számok közül egyik sem eleme $\underline{n} \cup 2\underline{n} \cup \cdots \cup (k-1)\underline{n}$-nek, $k\underline{n}$-nek pedig a k-val oszthatók elemei, így $\underline{n} \Delta 2\underline{n} \Delta \cdots \Delta k\underline{n}$ halmazba $\left[\frac{n}{k}\right] \geq \frac{n}{k} - 1$ esik közülük. A $(k-2)n + 1$, $(k-2)n+2$, …, $(k-1)n$ számok egyike sem eleme $\underline{n} \cup 2\underline{n} \cup \cdots \cup (k-2)\underline{n}$-nek, közülük azok elemei $\underline{n} \Delta 2\underline{n} \Delta \cdots \Delta k\underline{n}$-nek, amelyek $k-1$ és k közül pontosan az egyikkel oszthatók. Mivel $k - 1$ és k relatív prímek, ezért egyrészt egy $k - 1$ differenciájú számtani sorozat minden k-adik tagja osztható k-val, másrészt egy k differenciájú számtani sorozat minden $k - 1$-edik tagja osztható $k - 1$-gyel. Ebből az következik, hogy

$\underline{n}\Delta 2\underline{n}\Delta\cdots\Delta k\underline{n}$-ba legalább

$$\left[\left[\frac{n}{k-1}\right]\cdot\frac{k-1}{k}\right]+\left[\left[\frac{n}{k}\right]\cdot\frac{k-2}{k-1}\right]\mid\geq\frac{1}{k}n+\frac{(k-2)}{k(k-1)}n-4$$

esik a $(k-2)n+1$, $(k-2)n+2$, ...,$(k-1)n$ számok közül, ugyanis

$$[\alpha[\beta n]]\geq\alpha(\beta n-1)-1=\alpha\beta n-\alpha-1.$$

Mivel $k\geq 4$, ezért $2n<(k-2)n+1$, tehát ezeket a számokat eddig nem számoltuk. Azt kaptuk, hogy

$$|\underline{k}*\underline{n}|\geq n-s+\frac{1}{k}n+\frac{1}{k}n+\frac{(k-2)}{k(k-1)}n-5,$$

amiből $|\underline{k}*\underline{n}|>n$ következik, ha $n>\dfrac{k}{3-\frac{1}{k-1}}(s+5)$.

$k=4,5,6,7,8$ esetén $k(s+5)$ értéke rendre

$$\begin{aligned}\frac{3}{2}\cdot(12+5)&<26,\\ \frac{20}{11}\cdot(60+5)&<119,\\ \frac{30}{14}\cdot(60+5)&<140,\\ \frac{42}{17}\cdot(420+5)&<1051,\\ \frac{56}{20}\cdot(840+5)&<2367.\end{aligned}$$

Számítógéppel ellenőrizhetjük, hogy

$$\begin{aligned}&k=4\text{ és }4<n<26,\\ &k=5\text{ és }5<n<119,\\ &k=6\text{ és }6<n<140,\\ &k=7\text{ és }7<n<1051,\\ &k=8\text{ és }8<n<2367\end{aligned}$$

esetén $|\underline{k}*\underline{n}|>n$ teljesül. A II. eset bizonyítása során a $k\leq 6$ esetben kapott eredményt fogjuk felhasználni, ezekben az esetekben az ellenőrzés számítógép segítsége nélkül is könnyen elvégezhető.

Bizonyítottuk, hogy $k\leq 1,34\cdot\log n$ esetén $|\underline{k}*\underline{n}|\geq n$ mindig teljesül, és egyenlőség csak $k=n$, $k=1$, $k=2$ és n páros, $k=3$ és $n=4$ esetekben teljesül.

A tétel bizonyítását azzal az esettel folytatjuk, amikor k közepes: $1,34 \cdot \log n \leq k < n - \dfrac{0,22 \cdot n}{\log n}$. A k-ra vonatkozó alsó korlát megegyezik az I. esetben szereplő felső korláttal.

II. eset, k közepes: Legyen $1,34 \cdot \log n \leq k < n - \dfrac{0,22 \cdot n}{\log n}$ és $n \geq 1410$.

Legyen $k_1 = \max(k, n/7)$ és legyen $k_1 < p \leq n$ prímszám. A következő állítás segítségével megadunk p-vel osztható $\underline{k} * \underline{n}$-beli elemeket.

Azt állítjuk, hogy a $\underline{k} \cdot \underline{n}$ halmaz p-vel osztható elemei közül legalább k eleme $\underline{k} * \underline{n}$ halmaznak is.

Mivel $k < p$, ezért $\underline{k}$-nak nincsen a p prímszámmal osztható eleme. Így csak úgy kaphatunk p-vel osztható szorzatot, ha $\underline{n}$-ből p-vel osztható számot választunk. Az $\underline{n}$ halmaz p-vel osztható elemei: p, $2p$, $\ldots$, $[n/p]p$. Ebből az következik, hogy a $\underline{k} * \underline{n}$ halmaz p-vel osztható elemeinek halmaza a következő:

$$K * \{p, 2p, \ldots, [n/p]\, p\}.$$

Ennek a halmaznak az elemszáma nyilván megegyezik a

$$\underline{k} * \{1, 2, \ldots, [n/p]\}$$

halmaz elemszámával. Mivel $n/7 < p$, ezért $[n/p] \leq 6$. Felhasználva, hogy a $|\underline{k} * \underline{n}| \geq n$ állítás igaz $k \leq 6$ esetén, és hogy $[n/p] \leq 6$, teljesül, hogy

$$|\underline{k} * \underline{[n/p]}| \geq k.$$

Ebből már következik, hogy az állítás igaz.

Megmutatjuk, hogy $k_1 < p, q$ különböző prímszámok esetén $\underline{k} \cdot \underline{n}$-nek, és így $\underline{k} * \underline{n}$-nek egyetlen eleme sem lehet egyszerre p-vel és q-val is osztható. Mivel $k < p, q$, ezért csak úgy kaphatnánk p-vel és q-val is osztható $\underline{k} \cdot \underline{n}$-beli elemet, ha $\underline{n}$-nek lenne p-vel és q-val is, következésképpen pq-val is osztható eleme. De $pq \geq (n/7)^2 > n$, hiszen $n > 49$.

Ebből és az előbbi állításból következik az alábbi egyenlőtlenség:

$$|\underline{k} * \underline{n}| \geq (\pi(n) - \pi(k_1))k. \tag{13}$$

Tegyük fel először, hogy $k \leq n/7$. A következőkben felhasználjuk Dusart $\pi(x)$ nagyságrendjére vonatkozó tételét (16. Tétel). Az $n \geq 1410$ feltétel miatt a 16. Tétel alkalmazható $\pi(n)$ és $\pi(n/7)$ becslésére,

így:

$$\pi(n)-\pi(n/7)\geq\frac{n}{\log n}-\frac{n/7}{\log(n/7)}\left(1+\frac{1,2762}{\log(n/7)}\right)=$$

$$=\frac{n}{\log n}\left\{1-\frac{1/7}{1+\frac{\log\frac{1}{7}}{\log n}}\cdot\left(1+\frac{1,2762}{\log\frac{1}{7}+\log n}\right)\right\}\geq 0,749\frac{n}{\log n}.$$

Az $1,34\cdot\log n\geq k$ feltételt és (13) egyenlőtlenséget felhasználva:

$$|\underline{k}*\underline{n}|\geq(1,34\log n)\cdot 0,749\frac{n}{\log n}>n.$$

Ezzel ebben az esetben is igazoltuk az állítást.

Tegyük fel most, hogy $n/7<k\leq n/2$. Ismét a 16. Tételt használva könnyen megmutatható, hogy $\pi(n)-\pi(k_1)=\pi(n)-\pi(n/2)\geq 7$, ha $n\geq 100$. Hiszen

$$\pi(n)-\pi(n/2)\geq\frac{n}{\log n}-\frac{n/2}{\log(n/2)}\cdot\left(1+\frac{1,2762}{\log(n/2)}\right)\geq$$

$$\geq\frac{n}{\log n}\cdot\left(\frac{1}{2}-\frac{0,6381}{\log n}\right)\geq 7.$$

Így (13) egyenlőtlenség szerint $|\underline{k}*\underline{n}|\geq(\pi(n)-\pi(k_1))k>7\cdot(n/7)=n$, amint azt igazolni akartuk.

Tegyük fel végül, hogy $n/2<k<n-\dfrac{0,22\cdot n}{\log n}$ teljesül. Ekkor

$$|\underline{k}*\underline{n}|\geq(\pi(n)-\pi(k_1))k=(\pi(n)-\pi(k))k>2\cdot(n/2)=n,$$

ha $\pi(n)-\pi(k)\geq 2$.

A $\pi(n)-\pi(k)\geq 2$ egyenlőtlenséget a 19. Következmény segítségével igazoljuk. Legyen

$$n_1=n-\frac{0,11\cdot n}{\log n}\text{ és }n_2=n_1-\frac{0,11\cdot n_1}{\log n_1}.$$

Megjegyezzük, hogy $n_2\geq n-\dfrac{0,22\cdot n}{\log n}$. Ha $n>1410$, akkor $n_1>1361$, ezért a 19. Következmény szerint (n_2,n_1) és (n_1,n) intervallum is tartalmaz prímszámot. Mivel $k<n-\dfrac{0,22\cdot n}{\log n}\leq n_2$, ezért ezzel beláttuk, hogy $\pi(n)-\pi(k)\geq 2$, és így $|\underline{k}*\underline{n}|>n$ állítást igazoltuk ebben az esetben is.

Végül rátérünk annak az esetnek a bizonyítására, amikor k nagy: $k>n-\dfrac{0,4\cdot n}{\log(n)+1,02}$. A bizonyítás előtt azonban vizsgáljuk meg,

hogy n mely értékeire teljesül

$$n - \frac{0,4 \cdot n}{\log(n) + 1,02} \leq n - \frac{0,22 \cdot n}{\log n},$$

hiszen ezen egyenlőtlenség fennállása garantálja, hogy k és n esetében az I., II., III. esetek valamelyike alkalmazható. Ekvivalens átalakításokat hajtunk végre.

$$n - \frac{0,4 \cdot n}{\log(n) + 1,02} \leq n - \frac{0,22 \cdot n}{\log n}$$
$$\frac{0,22 \cdot 1,02}{0,4 - 0,22} \leq \log n$$

Ez pedig teljesül, ha $1,26 \leq \log n$, ami igaz $n \geq 4$ esetén.

Annak az esetnek a bizonyításával folytatjuk tehát, amikor k nagy: $k > n - \frac{0,4 \cdot n}{\log(n) + 1,02}$. Ebben az esetben az $n \geq 350$ feltétel mellett igazoljuk, hogy $|\underline{k} * \underline{n}| \geq n$, és egyenlőség csak $k = n$ esetén áll fenn.

III. eset, k nagy: Legyen most $k > n - \frac{0,4 \cdot n}{\log(n) + 1,02}$ és $n \geq 350$.

Ha $k = n$, akkor $\underline{k} * \underline{n} = \{1, \ldots, n\} * \{1, \ldots, n\} = \{1^2, 2^2, \ldots, n^2\}$, hiszen $a \neq b$ esetén az ab szorzatot a ba szorzattal párosíthatjuk, csak az $a \cdot a$ típusú szorzatoknak nem lesz párja. Ekkor tehát

$$|\underline{k} * \underline{n}| = |\underline{n} * \underline{n}| = n$$

így az állítás teljesül és az egyenlőtlenség éles.

Tegyük fel most, hogy $k < n$, ekkor a 4. Állítás alapján:

$$|\underline{k} * \underline{n}| = |(\underline{k} * \underline{k}) \Delta (\underline{k} * (\underline{n} \setminus \underline{k}))| =$$
$$= |\underline{k} * \underline{k}| + |\underline{k} * (\underline{n} \setminus \underline{k})| - 2|(\underline{k} * \underline{k}) \cap (\underline{k} * (\underline{n} \setminus \underline{k}))|$$

Számoljuk ki, illetve becsüljük meg a jobboldalon szereplő halmazok elemszámát. Mint láttuk, az első tagra

$$|\underline{k} * \underline{k}| = |\{1^2, 2^2, \ldots, k^2\}| = k \tag{14}$$

teljesül.

Térjünk rá a második tag elemszámának becslésére. Azt állítjuk, hogy ha

$$i \leq \frac{k}{n-k} \text{ és } k+1 \leq j \leq n,$$

akkor $ij \in 1(\underline{k}, \underline{n})$, és így $ij \in \underline{k} * (\underline{n} \setminus \underline{k})$. Ehhez azt kell megmutatni, hogy ha $1 \leq i' \leq k$ és $k+1 \leq j' \leq n$, továbbá $ij = i'j'$ teljesül, akkor szükségképpen $i = i'$ és $j = j'$. Ha $i = i'$, akkor nyilván $j = j'$. Ha $i' < i$, akkor $1 \leq i' \leq \frac{k}{n-k}$ és természetesen $k+1 \leq j' \leq n$, azaz

(i,j) és (i',j') szerepe fölcserélhető. Föltehető tehát, hogy $i<i'$. Mivel $ij=i'j'$, ezért $\dfrac{i}{i'}=\dfrac{j'}{j}$. Ekkor,

$$\frac{i}{i'}\le\frac{i}{i+1}\le\frac{\frac{k}{n-k}}{\frac{k}{n-k}+1}=\frac{k}{n}<\frac{k+1}{n}\le\frac{j'}{j},$$

ami ellentmondás. Ebből $\underline{k}*(\underline{n}\setminus\underline{k})$ elemszámára a

$$(15)\quad |\underline{k}*(\underline{n}\setminus\underline{k})|\ge\left[\frac{k}{n-k}\right](n-k)\ge$$
$$\ge\left(\frac{k}{n-k}-1\right)(n-k)=k-(n-k)=2k-n$$

alsó becslés adódik. Végül felső becslést adunk $(\underline{k}*\underline{k})\cap(\underline{k}*(\underline{n}\setminus\underline{k}))$ elemszámára. Megmutatjuk, hogy

$$(16)\qquad |(\underline{k}*\underline{k})\cap(\underline{k}*(\underline{n}\setminus\underline{k}))|\le 0,436\cdot k.$$

Nyilván elég bizonyítani, hogy az $1^2, 2^2, \dots, k^2$ számok közül legfeljebb $0,436\cdot k$ áll elő ab alakban $1\le a\le k$, $k+1\le b\le n$ mellett. Az első k négyzetszám közül csak azok állhatnak elő ilyen alakban, amelyeknek van a $[k+1,n]$ intervallumban osztójuk. Legyen $k+1\le m\le n$, vizsgáljuk meg, hogy m-mel az első k négyzetszám közül hány osztható. Ehhez m-et írjuk fel $m=\alpha(m)\beta^2(m)$ alakban, ahol $\beta^2(m)$ az m szám legnagyobb négyzetszám osztója. Megjegyezzük, hogy ekkor $\alpha(m)$ négyzetmentes szám. Könnyen meggondolhatjuk, hogy $m|i^2$ pontosan akkor teljesül, ha $\alpha(m)\beta(m)|i$ (hiszen $\alpha(m)$ négyzetmentes).

Így az $1^2, 2^2, \dots, k^2$ számok közül azoknak a száma, amelyek rendelkeznek a $[k+1,n]$ intervallumba eső osztóval felülről becsülhető a következő összeggel:

$$S=\sum_{m=k+1}^{n}\left[\frac{k}{\alpha(m)\beta(m)}\right]\le\sum_{m=k+1}^{n}\frac{k}{\alpha(m)\beta(m)}.$$

Ennél a becslésnél azokat a számokat, amelyeknek több ilyen osztójuk is van, többször számoltuk. A tagokat $j=\beta(m)$ szerint csoportosítva (nyilván minden szóba jövő m-re $\beta(m)\le\sqrt{n}$):

$$S=k\sum_{j=1}^{[\sqrt{n}]}\sum_{\substack{j^2|m,\\ k+1\le m\le n,\\ |\mu(m/j^2)|=1}}\frac{j}{m}\le k\sum_{j=1}^{[\sqrt{n}]}j\sum_{\substack{j^2|m,\\ k+1\le m\le n}}\frac{1}{m},$$

hiszen $j=\beta(m)$ esetén $\dfrac{1}{\alpha(m)\beta(m)}=\dfrac{\beta(m)}{\alpha(m)\beta^2(m)}=\dfrac{j}{m}$ teljesül.

Ezt a j szerinti összegzést bontsuk két részre a következőképpen:

$$S_1 := \sum_{j=1}^{[\sqrt{n}/2]} j \sum_{\substack{j^2|m,\\ k+1\le m\le n}} \frac{1}{m}$$

$$S_2 := \sum_{j=[\sqrt{n}/2]+1}^{[\sqrt{n}]} j \sum_{\substack{j^2|m,\\ k+1\le m\le n}} \frac{1}{m}$$

Először az S_1 összegre adunk felső becslést. Bevezetve az $r_j = \left\lceil \frac{k+1}{j^2} \right\rceil$, $s_j = \left[\frac{n}{j^2} \right]$ jelöléseket:

$$S_1 = \sum_{j=1}^{[\sqrt{n}/2]} j \sum_{l=r_j}^{s_j} \frac{1}{lj^2} = \sum_{j=1}^{[\sqrt{n}/2]} \frac{1}{j} \sum_{l=r_j}^{s_j} \frac{1}{l}.$$

Felhasználjuk a nemnegatív, monoton csökkenő függvényekre vonatkozó 20. Tételt. Az $f(x) = \frac{1}{x}$, $r = r_j$, $s = s_j$ választással alkalmazva a tételt a következő adódik:

$$\sum_{l=r_j}^{s_j} \frac{1}{l} \le \log(s_j) - \log(r_j) + \frac{1}{r_j},$$

amiből

$$(17) \quad S_1 \le \sum_{j=1}^{[\sqrt{n}/2]} \frac{1}{j} \left(\log(s_j) - \log(r_j) + \frac{1}{r_j} \right) \le$$

$$\le \sum_{j=1}^{[\sqrt{n}/2]} \frac{1}{j} \left(\log(n) - \log(k) + \frac{j^2}{k} \right)$$

következik, hiszen r_j és s_j definíciójából világos, hogy $\frac{k}{j^2} \le r_j$ és $s_j \le \frac{n}{j^2}$ és így

$$\log(s_j) - \log(r_j) = \log \frac{s_j}{r_j} \le \log \frac{n/j^2}{k/j^2} = \log(n) - \log(k).$$

A 20. Tétel ismételt alkalmazásával

$$\sum_{j=1}^{[\sqrt{n}/2]} \frac{1}{j} \leq \log[\sqrt{n}/2] + 1 \leq \frac{\log n}{2} - \log 2 + 1 < \frac{\log n}{2} + 0,31. \tag{18}$$

Továbbá

$$\sum_{j=1}^{[\sqrt{n}/2]} j = \frac{[\sqrt{n}/2] \cdot ([\sqrt{n}/2] + 1)}{2} \leq \frac{n + 2\sqrt{n}}{8}. \tag{19}$$

Így (17), (18), (19) egyenlőtlenségeket egybevetve az

$$S_1 \leq \left(\frac{\log n}{2} + 0,31\right)(\log(n) - \log(k)) + \frac{n + 2\sqrt{n}}{8k} \tag{20}$$

becslést kapjuk.

Térjünk most rá S_2 felső becslésére.

$$S_2 = \sum_{j=[\sqrt{n}/2]+1}^{[\sqrt{n}]} \sum_{\substack{j^2|m, \\ k+1 \leq m \leq n}} \frac{j}{m} \tag{21}$$

Az összegzésben szereplő j-kre teljesül, hogy

$$j^2 \geq ([\sqrt{n}/2] + 1)^2 > \frac{n}{4}.$$

A (21) egyenlet jobboldalán a második összegzésnél a j^2-tel osztható $(k, n]$ intervallumba eső m-ekre kell összegezni, $4j^2 > n$ miatt m értéke csak j^2, $2j^2$, $3j^2$ valamelyike lehet. Legyen tehát $1 \leq i \leq 3$, és becsüljük meg felülről, hogy hány j-re esik $m = ij^2$ a $(k, n]$ intervallumba.

$$k < ij^2 \leq n$$

$$\sqrt{\frac{k}{i}} < j \leq \sqrt{\frac{n}{i}}$$

Így az ilyen tulajdonságú j-k száma felülről becsülhető a következővel:

$$\frac{\sqrt{n} - \sqrt{k}}{\sqrt{i}} = \frac{1}{\sqrt{i}} \cdot \frac{n - k}{\sqrt{n} + \sqrt{k}} \leq \frac{1}{\sqrt{i}} \cdot \frac{n - k}{2\sqrt{k}}.$$

Ez a becslés $i = 1$, 2, és 3 esetén egyaránt érvényes. Mivel (21) jobboldalán összegzendő $\frac{j}{m}$-ek értékére $\frac{j}{m} \leq \frac{\sqrt{n}}{k}$ teljesül, továbbá az összegben a tagok száma az előzőek szerint legfeljebb

$$\left(1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}}\right) \cdot \frac{n - k}{2\sqrt{k}},$$

ezért

$$S_2 \le \left(1+\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{3}}\right)\cdot\frac{n-k}{2\sqrt{k}}\cdot\frac{\sqrt{n}}{k} < 1,15\cdot\frac{(n-k)\sqrt{n}}{k^{3/2}}. \tag{22}$$

Az eddigieket összefoglalva, (20) és (22) egyenlőtlenségeket felhasználva:

$$\begin{aligned} S = k(S_1+S_2) \le \\ \le k\Big\{\left(\frac{\log n}{2}+0,31\right)(\log(n)-\log(k)) + \frac{n+2\sqrt{n}}{8k} + \\ + 1,15\cdot\frac{(n-k)\sqrt{n}}{k^{3/2}}\Big\}. \end{aligned} \tag{23}$$

Először megmutatjuk, hogy $ne^{-\frac{0,2}{\frac{\log n}{2}+0,31}} < k$ és $n \ge 350$ esetén teljesülnek a következő egyenlőtlenségek:

$$\left(\frac{\log n}{2}+0,31\right)(\log(n)-\log(k)) < 0,2 \tag{24}$$

$$\frac{n+2\sqrt{n}}{8k} < 0,16 \tag{25}$$

$$1,15\cdot\frac{(n-k)\sqrt{n}}{k^{3/2}} < 0,076 \tag{26}$$

Először (24) igazolásához tekintsük a következő ekvivalens átalakításokat:

$$\left(\frac{\log n}{2}+0,31\right)(\log(n)-\log(k)) < 0,2$$

$$\frac{n}{k} < e^{\frac{0,2}{\frac{\log n}{2}+0,31}}$$

$$ne^{-\frac{0,2}{\frac{\log n}{2}+0,31}} < k$$

Tehát (24) valóban teljesül.

Ha $n \ge 350$, akkor

$$\frac{k}{n} > e^{-\frac{0,2}{\frac{\log n}{2}+0,31}} \ge e^{-\frac{0,2}{\frac{\log 350}{2}+0,31}} > 0,94.$$

(25) becslésével folytatva:

$$\frac{n+2\sqrt{n}}{8k} \le \frac{1}{8}\cdot\frac{1}{k/n}+\frac{1}{4\sqrt{n}}\cdot\frac{1}{k/n} < \frac{1}{8\cdot 0,94}+\frac{1}{4\sqrt{100}}\cdot\frac{1}{0,94} < 0,16,$$

hiszen $n \ge 350$.

Végül, (26) is igaz, ugyanis:

$$1,15 \cdot \frac{(n-k)\sqrt{n}}{k^{3/2}} < 1,15 \cdot \frac{(0,06 \cdot n)\sqrt{n}}{(0,94 \cdot n)^{3/2}} < 0,076.$$

Így (24), (25), (26) és (23) egyenlőtlenségeket használva a következőt kapjuk:

$$S \leq k\,(0,2 + 0,16 + 0,076) = 0,436 \cdot k.$$

A (14), (15) és (16) egyenlőtlenségeket felhasználva azt kapjuk, hogy ekkor

$$|\underline{k} * \underline{n}| \geq k + 2k - n - 2S \geq 2,128 \cdot k - n > n,$$

ha $k/n > 0,94$, ez pedig igaz.

Tekintsük a feltételként kapott

$$ne^{-\frac{0,2}{\frac{\log n}{2}+0,31}} < k \tag{27}$$

egyenlőtlenséget. Az $1 + x \leq e^x$ egyenlőtlenségből következik, hogy $-1 < x$ esetén érvényes az $e^{-x} \leq \frac{1}{1+x}$ egyenlőtlenség. Ez azt jelenti, hogy

$$e^{-\frac{0,2}{\frac{\log n}{2}+0,31}} \leq \frac{1}{1+\frac{0,2}{\frac{\log n}{2}+0,31}} = 1 - \frac{0,4}{\log(n)+1,02}.$$

Vagyis (27) automatikusan teljesül, ha fennáll a következő egyenlőtlenség:

$$k > n\left(1 - \frac{0,4}{\log(n)+1,02}\right) = n - \frac{0,4 \cdot n}{\log(n)+1,02}.$$

Ezzel bizonyítottuk az állítást a III. esetben is.

Minden olyan k, n esetén igazoltuk az állítást, amikor $n \geq 1410$. A véges sok $k \leq n \leq 1410$ esetben számítógép segítségével ellenőrizhető, hogy igaz az állítás.

□

Hivatkozások

[1] G. Pilz: *Near-Rings*, North-Holland Publishing Company, 1983, ISBN: 0 7204 0566 1

[2] G. Pilz: *Near-rings: What they are and what they are good for*, http://www.algebra.uni-linz.ac.at/Nearrings/what-are.html

[3] R. Eggertsberger: *On Constructing Codes from Planar Nearrings*, http://www.algebra.uni-linz.ac.at/Nearrings/nrcodes.html

[4] G. Pilz, *On polynomial near-ring codes*, Contributions to general algebra 8, Verlag Hölder-Pichler-Tempsky, Wien, 1992 - Verlag B. G. Teubner, Stuttgart

[5] J. B. Rosser, L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Ill. Journ. Math. 6 (1962) 64-94.

[6] P. Dusart, *The k^{th} prime is greater than $k(lnk + lnlnk - 1)$ for $k > 2$*, Math. Comp., 68:225 (January 1999) 411-415.

[7] G. Robin, *Estimation de la fonction de tschebyshef theta sur le k-ieme nombre premier et grandes valeurs de la fonction $w(n)$, nombre de diviseurs premiers de n*, Acta. Arith., 42:4 (1983) 367-389.