Eötvös Loránd Tudományegyetem

Természettudományi Kar

Sebők Richárd

Matematika BSc.

Matematikus szakirány

# Sidon-sorozatok

Szakdolgozat

Témavezető: Sárközy András és Gyarmati Katalin

Algebra és Számelmélet Tanszék

Budapest, 2012. május 25.

# Tartalomjegyzék

**1. Bevezetés** **2**

**2. Véges Sidon-sorozatok** **3**

**3. Végtelen Sidon-sorozatok** **10**

**4. Konstrukció egy sűrű, végtelen Sidon-sorozatra** **23**

**5. Általánosabb problémák** **28**

**6. Összefoglalás** **31**

**Hivatkozások** **32**

# 1. Bevezetés

Sidon Simon harmonikus analízissel foglalkozó matematikus 1932-es [12] munkájában felmerült az a kérdés, hogy a pozitív egész számok egy $\mathcal{A}$ részhalmazára definiált

$$\mathcal{A}^*(k) = |\{(a_i, a_j) \in \mathcal{A} \times \mathcal{A} :\ a_i + a_j = k\}|$$

$$\mathcal{A}^\circ(k) = |\{(a_i, a_j) \in \mathcal{A} \times \mathcal{A} : a_i - a_j = k\}|$$

kifejezések korlátosak-e. Itt jegyezzük meg, hogy később kiterjesztették a kérdést Abel-csoportokra is [13]. Ez a kérdés a [10]

$$\left(\sum_{a \in \mathcal{A}} z^a\right)^h$$

együtthatóinak vizsgálata során merült fel, és a cél az lett volna, hogy $\mathcal{A}$ megfelelő választása esetén az együtthatók felső korlátja $g$ legyen. $z^k$ együtthatójának a számelméleti jelentése, hogy hányféleképpen lehet $k$-t kapni $\mathcal{A}$-beli (és nem feltétlenül diszjunkt) $h$ tagú összegekből, azaz a megoldásszám korlátos legyen. $h = 2$-re, és a vizsgálódást a pozitív egészek közé szorítva, Sidon megkérdezte Erdős Pált, hogy milyen nagy lehet egy olyan részhalmaza az $\{1, 2, \ldots, n\}$ halmaznak, amire

$$\mathcal{A}^{**}(k) \leq 1, \quad \forall k \geq 0.$$

a következő jelöléssel élve:

$$\mathcal{A}^{**}(k) = |\{(a_i, a_j) \in \mathcal{A} \times \mathcal{A} :\ \text{ha } i < j,\ \text{akkor } a_i \leq a_j,\ a_i + a_j = k\}|.$$

A következő fejezetben megmutatjuk többek között, hogy ez a tulajdonság ekvivalens azzal, amikor

$$\mathcal{A}^\circ(k) \leq 1, \quad \forall k \leq 0.$$

tulajdonságú $\mathcal{A}$ részhalmazait vizsgáljuk az $\{1, 2, \ldots, n\}$ halmaznak.

Az egyszerűbb jelölés kedvéért a továbbiakban $\mathscr{A}$-val nemnegatív egészekből álló sorozatokat fogunk jelölni.

Legyenek $g, h$ természetes számok, ahol $g \geq 2$. $B_h[g]$-vel fogjuk azon (véges és végtelen) $\mathscr{A}$ sorozatok osztályát jelölni, melyek minden egész $n$-re legfeljebb $g$ olyan reprezentációval rendelkeznek, hogy teljesítik az alábbiakat:

$$n = a_1 + \cdots + a_h \qquad (a_1 \in \mathscr{A}, \ldots, a_h \in \mathscr{A}) \tag{1.1}$$

ahol

$$a_1 \leq a_2 \leq \cdots \leq a_h. \tag{1.2}$$

Ha $\mathscr{A}$ $B_h[g]$ osztálybeli elem, akkor azt mondjuk, hogy $\mathscr{A}$ $B_h[g]$-sorozat. A $B_h[1]$ osztályra egyszerűbben csak $B_h$ osztályként fogunk utalni, és ennek megfelelően, a $B_h$ osztály egy elemére $B_h$-sorozatként fogunk hivatkozni.

Megjegyezzük, hogy egy $\mathscr{A}$ sorozat akkor és csak akkor $B_h$-sorozat, ha teljesíti az alábbi tulajdonságot: minden $a_1 + a_2 \cdots + a_h$ összeg, ahol $a_1 \leq a_2 \leq \cdots \leq a_h$ $(a_1 \in \mathscr{A}, \ldots, a_h \in \mathscr{A})$ különböző.

$F_h(n)$-nel fogjuk jelölni az $n$-nél nem nagyobb elemekből álló $B_h$ sorozatok elemszámának a maximumát. Egy adott $\mathscr{A}$ $B_h$-sorozat elemszámát $A(n)$-nel fogjuk jelölni, és így az $A(n) \leq F_h(n)$ minden $n$ természetes számra telejsül.

A $B_2$-sorozatokat szokás Sidon-sorozatoknak nevezni, és világos, hogy ezek azok az $\mathcal{A}$ részhalmazai az $\{1, 2, \ldots, n\}$ halmaznak, amire

$$\mathcal{A}^{**}(k) \leq 1 \quad \forall k \geq 0.$$

# 2. Véges Sidon-sorozatok

A most következő fejezetben véges Sidon-sorozatok elemszámára fogunk alsó és felső becslést adni, sűrűségükre különböző észrevételeket tenni. Ehhez először teszünk pár apró megjegyzést.

A Sidon-sorozatok definíciójából könnyű látni, hogy:

$$((i=k) \wedge (j=l)) \vee ((i=l) \wedge (j=k)) \Leftrightarrow a_i + a_j = a_k + a_l \Leftrightarrow$$

$$\Leftrightarrow a_i - a_l = a_k - a_j$$

azaz, egy Sidon-sorozat elemeiből képzett különbségek is mind különbözőek.

A bevezetőben elhangzottakból és az előző megjegyzésből is már látszik, hogy a Sidon-sorozatainknak valamilyen értelemben ritkáknak kell lenniük, különben sérül a Sidon-tulajdonságuk, például, egy $\mathscr{A}$ Sidon-sorozatban nem lehet három konszekutív, egymást követő egész szám, mert különben az 1 előállna kétféleképpen is különbségként. [10]

Vegyük az $\mathcal{A} = \{2^k, 2^k+1 : k \geq 1\}$ sorozatot. Megkérdezhetnénk erről, hogy ez Sidon-sorozat-e. Mivel a $2, 3, 4$ számok is szerepelnek benne, ezért nem $B_2$-sorozat, ellenben $B_2[2]$-sorozat, mivel $\mathcal{A}^*(k) \leq 4$ minden $k$-ra. Ugyanakkor $\mathcal{A}^\circ(1) = \infty$ amiből látszik, hogy már a $B_2[2]$-sorozatokra sem áll fenn az $\mathcal{A}^{**}(k) \leq 1 \Leftrightarrow \mathcal{A}^\circ(k) \leq 1$ tulajdonság általánosítása. A Sidon-sorozatokra sok olyan tulajdonság igaz, ami a $B_h[g]$-sorozatokra nem, ezért is nagyságrendekkel könnyebb a velük való foglakozás, és sokkal több eredményt is értek el a vizsgálatukkal, mint az általánosabb problémával. Hasonló következtetést nyújt a következő sorozat: $\mathcal{A} = \{\pm 2^k : k \geq 1\}$ esetén $\mathcal{A}^\circ(k) \leq 3$ minden $k \neq 0$-ra, mivel

$$a_k = a_{k+1} - a_k = a_k - a_{-k} = a_{-k} - a_{-(k+1)}$$

és $\mathcal{A}^*(0) = \infty$. [10]

A fejezet hátralévő részében a becsléseinket [4] alapján fogjuk közölni. Legyen $\mathscr{A}$ egy $s = F_2(n)$ elemű $B_2$-sorozat,

$$1 \leq a_1 \leq a_2 \leq \cdots \leq a_s \leq n.$$

Az $a_i + a_j$ összegek mind különbözőek, $2n$-nél nem nagyobbak, és számuk $\binom{s+1}{2}$, ha megengedjük az $i = j$ esetet is. Így

$$\binom{s+1}{2} \leq 2n$$

$$s < 2\sqrt{n}$$

Pár egyszerű észrevétellel tovább javítható a becslésünk. Mivel egy Sidon-sorozat elemeiből képzett különbségek is mind különbözőek, ezért $\binom{s}{2} < n$ féleképpen választhatjuk meg őket, és ebből

$$s < \sqrt{2n+1}.$$

Ennél azonban tovább is mehetünk, a $\sqrt{2}$ tényezőtől is megszabadulhatunk. A következő tételre két bizonyítást is adunk, az elsőt Erdős és Turán adta [5], a második Lindstörm munkája [8].

**2.1. Tétel** *Egy $n$-nél nem nagyobb elemekből álló $B_2$-sorozat elemszámának a maximuma*

$$F_2(n) < \sqrt{n} + \sqrt[4]{n} + 1. \tag{2.1}$$

*Bizonyítás.* Egy később megválasztandó $t$ egésszel toljunk végig egy $t-1$ hosszúságú intervallumot az a $[0, n]$ intervallumon, azaz tekintsük a

$$[-t+1, 0], \qquad [-t+2, 1], \qquad \ldots, \qquad [n, n+t-1]$$

zárt intervallumokat. Az $\mathscr{A}$ $B_2$-sorozat egyes intervallumokba eső elemeinek a száma legyen $A_1, A_2, \ldots, A_{n+t}$. Az összes $a_i$ $t$ darab egymás utáni intervallumban van benne, ezért

$$\sum_{i=1}^{n+t} A_i = ts.$$

Az $(a_i, a_j), i > j$ párokat összeszámolva annyiszor, ahány intervallum tartalmazza őket, az összeget $D$-vel jelölve, azt kaphatjuk, hogy

$$D = \sum_{i=1}^{n+t} \binom{A_i}{2} = \frac{1}{2}\sum_{i=1}^{n+t} A_i^2 - \frac{1}{2}\sum_{i=1}^{n+t} A_i. \tag{2.2}$$

Másrészt, ha egy elempár különbsége $d$, akkor ez $t-d$ intervallumba esik bele. Mivel a különbségek mind különbözőek, minden $d$ csak egyszer fordulhat elő. Ezért

$$D \leq \sum_{d=1}^{t-1} (t-d) = \frac{t(t-1)}{2}. \tag{2.3}$$

A (2.2) és (2.3) összefüggések összehasonlításából

$$\sum_{i=1}^{n+t} A_i^2 - \sum_{i=1}^{n+t} A_i \leq t(t-1). \tag{2.4}$$

A bal oldal második összegéről láttuk, hogy $ts$ az értéke. Az elsőre a Cauchy-Bunyakovszkij-Schwartz egyenlőtlenségből

$$\sqrt{\sum_{i=1}^{n+t} A_i^2} \cdot \sqrt{\sum_{i=1}^{n+t} 1} \geq \sum_{i=1}^{n+t} A_i.$$

$$\sum_{i=1}^{n+t} A_i^2 \geq \frac{\left(\sum_{i=1}^{n+t} A_i\right)^2}{n+t} = \frac{t^2 s^2}{n+t}$$

Ezeket beírva a (2.4) egyenlőtlenségbe, nullára redukálva, majd szorozva $(n+t)/t^2$-tel, azt kapjuk, hogy

$$s^2 - s(\frac{n}{t}+1) - ((\frac{n}{t}+1)(t-1) \leq 0$$

Az ezt a másodfokú egyenlőtlenséget kielégítő $s$ értékekre

$$s \leq \frac{n}{2t} + \frac{1}{2} + \sqrt{n + t + \frac{n^2}{4t^2} - \frac{n}{2t} - \frac{3}{4}}$$

A $t = \left\lfloor \sqrt[4]{n^3} \right\rfloor + 1$ választás mellett $\frac{n}{2t} < \frac{1}{2}\sqrt[4]{n}$, a négyzetgyök alatti kifejezés pedig kisebb $\sqrt{n} + \frac{1}{2}\sqrt[4]{n} + \frac{1}{2}$ négyzeténél. Ezzel bebizonyítottuk az állítást. $\square$

*Bizonyítás.* Ebben a második bizonyításban ismét $t$-vel jelölünk egy később alkalmasan megválasztandó paramétert. Legyen

$$K = \sum_{1 \leq i-j \leq t} (a_i - a_j).$$

$K$ kétféle becslésén alapszik a bizonyításunk. Ha $1 \leq \mu \leq t$, egy $\mu$ érték az $i - j$ értékek közt $s - \mu$-féleképpen fordulhat elő. Így az összegnek

$$(s-1) + (s-2) + \cdots + (s-t) = ts - \frac{t(t+1)}{2} = tw$$

tagja van, ahol

$$w = s - \frac{t+1}{2}.$$

A különbségek mind különbözőek, így összegük nem kisebb az első $tw$ egész szám összegénél:

$$K \geq \frac{tw(tw+1)}{2} > \frac{t^2w^2}{2}. \tag{2.5}$$

Ugyanakkor azok a különbségek, melyekben az indexek különbsége $\mu$,

$$(a_{s-\sigma} - a_{s-\sigma-\mu}) + (a_{s-\sigma-\mu} - a_{s-\sigma-2\mu}) + \cdots < a_{s-\sigma} \leq n$$

alakú teleszkopikus összegekbe rendezhető. Itt

$$0 \leq \sigma < \mu$$

azaz $\mu$ darab ilyen teleszkopikus összegünk van, és mindegyiket addig folytatjuk csak, amíg $s - \sigma - r\mu$ nemnegatív marad. Így $K$ minden tagja benne van valamelyik összegben. Mivel $1 \leq \mu \leq t$, ez összesen

$$1 + 2 + \cdots + t = \frac{t(t+1)}{2}$$

teleszkopikus összeget jelent, tehát

$$K < nt\frac{t+1}{2}. \tag{2.6}$$

A (2.5) és (2.6) kétoldali egyenlőtlenség összevetéséből, és $2/t^2$-tel való szorzás után

$$w^2 = \left(s - \frac{t+1}{2}\right)^2 < n + \frac{n}{t},$$

amiből $s$-re

$$s < \frac{t+1}{2} + \sqrt{n + \frac{n}{t}}$$

egyenlőtlenség adódik. Innen $t = \lfloor \sqrt[4]{n} \rfloor + 1$ választással a bizonyítandó becsléshez jutunk. $\square$

Az $F_2(n)/\sqrt{n}$ hányados elég nagy $n$-re tetszőlegesen közel van 1-hez, azaz $F_2(n)$ aszimptotikus értéke $\sqrt{n}$, ebben az értelemben éles a 2.1 tétel. Ezen állítás bizonyítására megmutatjuk a következő alsó becslést $F_2(n)$-re.

**2.2. Tétel** *Megadható olyan $B_2$-sorozat, amelyiknek $s$ elemszámára*

$$s > \sqrt{n} - n^{\frac{11}{40}}.$$

Ezen tételre is több bizonyítás ismert. Itt egy kevés előismeretre építőt mutatunk be. Az összes bizonyítás hasonló jellegű számelméleti állításra alapszik.

**2.3. Tétel** *Legyen $p$ páratlan prímszám. Létezik $p-1$ darab olyan $a_i$, amelyekre az $a_i - a_j, i \neq j$ különbségek inkongruensek modulo $p^2 - p$.*

*Bizonyítás.* Véve egy $g$ primitív gyököt modulo $p$, legyen $a_i$ az

$$\begin{aligned} x &\equiv i \pmod{p-1}, \\ x &\equiv g^i \pmod{p} \end{aligned}$$

szimultán kongruencia-rendszer legkisebb nemnegatív megoldása modulo ($p^2 - p$). Célunk megmutatni, hogy az $a_i - a_j \equiv a_r - a_s \pmod{p^2 - p}$ kongruencia, vagy átalakítva az

$$a_i + a_s \equiv a_r + a_j \pmod{p^2 - p}$$

kongruencia csak a triviális módon teljesül, azaz, tetszés szerinti $c$-re, sorrendtől eltekintve legfeljebb egy $i, j$ párral áll fenn a

$$c \equiv a_i + a_j \pmod{p^2 - p}$$

kongruencia. Az $a_i$-k értelmezése alapján ez egyenértékű az

$$\begin{aligned} c &\equiv i + j \pmod{p-1}, \\ c &\equiv g^i + g^j \pmod{p} \end{aligned}$$

kongruenciapár egyidejű teljesülésével. Innen az Euler-Fermat tétel segítségével az első kongruencia átírható

$$g^c \equiv g^i g^j \pmod{p}$$

formára. A másodfokú egyenlet gyökei és együtthatói közti kapcsolatot kifejező Viète-formulák alapján $(g^i)_p$ és $(g^j)_p$ maradékosztályok az

$$x^2 - cx + g^c \equiv 0 \pmod{p}$$

másodfokú kongruenciának a $p$ prím volta miatt egyértelműen meghatározott gyökpárja és így az $i, j$ pár is egyértelmű □

Most már rátérhetünk a 2.2 tétel bizonyítására

*Bizonyítás.* Az előző bizonyításban konstruált $a_i$-k $B_2$-sorozatot alkotnak, azaz azt kaptuk, hogy ha $n$ az $p^2 - p$ alakú, akkor

$$F_2(n) \geq p - 1 = \frac{1}{2}(\sqrt{4n+1}+1) - 1 > \sqrt{n} - 1.$$

Tetszés szerinti $n$-re úgy térhetünk át, ha olyan $p$-t választunk, amelyre $p^2 - p$ közel van $n$-hez, azaz lényegében $p$ közel van $\sqrt{n}$-hez. [2] szerint minden elég nagy $m$-re $m - m^{\frac{11}{20}}$ és $m$ között van prímszám. Ennek megfelelően válasszunk egy prímet $\sqrt{n} - n^{\frac{11}{40}}$ és $\sqrt{n}$ között, így

$$F_2(n) \geq F_2(p^2 - p) \geq p - 1 \geq \sqrt{n} - n^{\frac{11}{40}}.$$

$\square$

# 3. Végtelen Sidon-sorozatok

Ezen fejezetben végtelen $\mathscr{A}$ $B_2$-sorozatokra vonatkozó eredményeket tárgyalunk [6].

Erdős Pál következő eredményei először Stöhr [14] összefoglaló cikkében láttak napvilágot.

$$\liminf_{n\to\infty} n^{-\frac{1}{2}} A(n) = 0 \qquad \textit{minden (végtelen) } \mathscr{A}\ B_2\textit{-sorozatra}; \tag{3.1}$$

és konstruktívan bizonyította, hogy

$$\textit{létezik olyan (végtelen) } \mathscr{A}\ B_2\textit{-sorozat, amire} \tag{3.2}$$

$$\limsup_{n\to\infty} n^{-\frac{1}{2}} A(n) \geq \frac{1}{2} \qquad \textit{teljesül.}$$

(3.1) és (3.2) esetében pontosabb becslések is ismertek. Erdős maga is kijelentette [14], hogy (3.1)-es bizonyítására használt érvelése tovább finomítható, hogy pontosabb eredményt adjon (az alábbi 3.1 tétel), míg Krückeberg [7] konstruált egy $\mathscr{A}$ $B_2$-sorozatot, amire teljesül, hogy

$$\limsup_{n\to\infty} n^{-\frac{1}{2}} A(n) \geq \frac{1}{\sqrt{2}}. \tag{3.3}$$

Habár Krückeberg fenti eredménye élesebb becslést ad Erdős (3.2) eredményénél, mind a két bizonyítást ismertetjük a bennük használt technika miatt.

**3.1. Tétel**

$$\liminf_{n\to\infty} n^{-\frac{1}{2}}(\log n)^{\frac{1}{2}}A(n) \ll 1 \tag{3.4}$$

*teljesül minden végtelen $\mathscr{A}$ $B_2$-sorozatra.*

*Megjegyzés.* $f \ll g$ jelentése egy $f$ függvény és egy $g$ nemnegatív függvénnyel kapcsolatban, hogy létezik egy olyan $c$ konstans, amire

$$|f| \ll c \cdot g.$$

*Bizonyítás.* Legyen $N$ nagy egész. Definiáljuk a következő kifejezést

$$\tau_{\mathscr{A}}(N) = \inf_{n\geq N} A(n)(\log n/n)^{\frac{1}{2}}$$

elég bebizonyítani, hogy $\tau_{\mathscr{A}}(N) \ll 1$, és az alkalmazott konstans abszolút.

Jelölje $D_l$ egy adott $\mathscr{A}$ $B_2$-sorozat $(l-1)N < a \leq lN$ intervallumba eső elemeinek a számát. A

$$0 < a_i - a_j < N$$

$a_i, a_j \in \mathscr{A}$ megoldásainak a száma $N$-nél kevesebb, tehát

$$\sum_{l=1}^{\infty} \frac{1}{2} D_l(D_l - 1) < N.$$

Ha $D_l > 1$, akkor $D_l(D_l-1) \geq \frac{1}{2}D_l^2$, és az előző egyenlőtlenségből kifolyólag

$$\sum_{l=1}^{N} D_l^2 = \sum_{\substack{l=1 \\ D_l=1}}^{N} 1 + \sum_{\substack{l=1 \\ D_l>1}}^{N} D_l^2 \leq N + 2\sum_{l=1}^{\infty} \frac{1}{2} D_l(D_l-1) < 5N. \tag{3.5}$$

A Cauchy-Bunyakovszkij-Schwartz-egyenlőtlenség felhasználásával adódik, hogy

$$\left(\sum_{l=1}^{N} \frac{1}{l}\right)\left(\sum_{l=1}^{N} D_l^2\right) \geq \left(\sum_{l=1}^{N} \frac{D_l}{l^{\frac{1}{2}}}\right)^2 \tag{3.6}$$

Továbbá

$$\begin{aligned}
\sum_{l=1}^{N} \frac{D_l}{l^{\frac{1}{2}}} &= \sum_{l=1}^{N} \{A(lN) - A((l-1)N\} \frac{1}{l^{\frac{1}{2}}} \\
&= \sum_{l=1}^{N} A(lN) \left\{ \frac{1}{l^{\frac{1}{2}}} - \frac{1}{(l+1)^{\frac{1}{2}}} \right\} + \frac{A(N^2)}{(N+1)^{\frac{1}{2}}} \\
&\geq \tau_{\mathscr{A}}(N) \sum_{l=1}^{N} \left(\frac{lN}{\log lN}\right)^{\frac{1}{2}} \left\{ \frac{1}{l^{\frac{1}{2}}} - \frac{1}{(l+1)^{\frac{1}{2}}} \right\} \\
&\gg \tau_{\mathscr{A}}(N) \sum_{l=1}^{N} \left(\frac{lN}{\log lN}\right)^{\frac{1}{2}} \frac{1}{l^{\frac{3}{2}}} \\
&\gg \tau_{\mathscr{A}}(N) \left(\frac{N}{\log N}\right)^{\frac{1}{2}} \sum_{l=1}^{N} \frac{1}{l}
\end{aligned}$$

ahol az utolsó előtti becslésben azt használtuk, hogy

$$\tau_{\mathscr{A}}(N) \leq \frac{A(n)(\log n)^{\frac{1}{2}}}{\sqrt{n}} \qquad (\forall n \geq N)$$

$$\frac{\tau_{\mathscr{A}}(N)\sqrt{n}}{(\log n)^{\frac{1}{2}}} \leq A(n) \qquad \text{speciálisan,} \qquad \frac{\tau_{\mathscr{A}}(N)\sqrt{n}}{(\log n)^{\frac{1}{2}}} \leq A(N).$$

(3.6)-ba behelyettesítve

$$\sum_{l=1}^{N} D_l^2 \gg N\tau_{\mathscr{A}}^2(N)$$

adódik, ami (3.5)-tel összevetve eredményezi a kívánt $\tau_{\mathscr{A}}(N) \ll 1$ egyenlőtlenséget. $\square$

Erdős [14] (3.2)-beli eredményének bizonyítását a következő tételben ismertetjük.

**3.2. Tétel** *Létezik olyan (végtelen) $\mathscr{A}$ $B_2$-sorozat, amire*

$$\limsup_{n\to\infty} n^{-\frac{1}{2}} A(n) \geq \frac{1}{2}. \tag{3.7}$$

*Bizonyítás.* Minden páratlan $p$ prímre konstruáljunk $\mathscr{A}_p$ $p-1$ elemű halmazokat a következő módon

$$a_k = 2p(k+p) + (k^2)_p \qquad (k = 1, 2, \ldots, p-1) \tag{3.8}$$

ahol $(k^2)_p$ azt az $u$ egész számot jelöli, amire $u \equiv k^2 \pmod p, 1 \leq u \leq p-1$. Megjegyezzük, hogy $\mathscr{A}_p$ Sidon-sorozat, hiszen

$$a_{k_1} + a_{k_2} = a_{k_3} + a_{k_4}$$

esetén $2p(k_1 + k_2 - k_3 - k_4) = (k_3^2)_p + (k_4^2)_p - (k_1^2)_p - (k_2^2)_p$,
és mivel $|(k_3^2)_p + (k_4^2)_p - (k_1^2)_p - (k_2^2)_p| < 2p$, ezért $k_1 + k_2 = k_3 + k_4$ és $k_3^2 + k_4^2 \equiv k_1^2 + k_2^2 \pmod p$. Innen már következik, hogy vagy $k_1 = k_3$ és $k_2 = k_4$, vagy $k_1 = k_4$ és $k_2 = k_3$.

Megjegyezzük továbbá, hogy

$$\mathscr{A}_p \text{ része a } 2p^2 < a < 4p^2 - p \text{ intervallumnak.} \tag{3.9}$$

és ha $a_i, a_j$ két különböző eleme $\mathscr{A}_p$-nek, akkor (3.9)-ből könnyen kapható

$$p < |a_i - a_j| < 2p^2 - p. \tag{3.10}$$

Célunk megmutatni, hogy ha egy kellően gyorsan növő, $p$ prímekből álló $\mathscr{P}$ sorozatot veszünk, akkor az $\mathscr{A}_p$ halmazokat ezekre a $p$-kre összegezve egy

$$\mathscr{A} = \mathscr{A}(\mathscr{P}) = \bigcup_{p\in\mathscr{P}} \mathscr{A}_p$$

$B_2$-sorozatot kapunk. Ebből már következik a tétel bizonyítása is, mivel $A_p$ $p-1$ elemet tartalmaz, ezért (3.9) szerint

$$A(4p^2 - p - 1) \geq p - 1 \qquad (\forall p \in \mathscr{P}).$$

Tegyük fel, hogy $p_1 < p_2 < \dots$ $\mathscr{P}$-beli prímek, továbbá

$$p_{r+1} \geq 4p_r^2 \qquad (r = 1, 2, \dots). \tag{3.11}$$

Elegendő megmutatni, hogy ha $a_1, a_2, a_3, a_4$ elemei $\mathscr{A}(\mathscr{P})$-nek, $a_1 \neq a_2$ és $a_3 \neq a_4$, akkor

$$a_1 - a_2 = a_3 - a_4$$

nem teljesülhet. A könnyebb kezelhetőség érdekében feltételezhetjük, hogy

$$a_1 > a_2 \geq a_3 > a_4.$$

Tegyük fel, hogy $a_1 \in \mathscr{A}_{p_s}$. Mivel $a_1 - a_2 = a_3 - a_4$ nem teljesülhet, ha minden $a$ $\mathscr{A}_{p_s}$-beli, ezért feltehetjük, hogy $a_4 \notin \mathscr{A}_{p_s}$, és $s > 1$. Két esetet különböztetünk meg attól függően, hogy $a_3$ eleme, vagy nem eleme $\mathscr{A}_{p_s}$-nek.

Először vizsgáljuk meg azt az esetet, amikor $a_3 \in \mathscr{A}_{p_s}$. Ekkor $a_2 \geq a_3$ miatt $a_2$ szintén $\mathscr{A}_{p_s}$-ben van. Innen, (3.10) szerint

$$a_1 - a_2 < 2p_s^2 - p_s,$$

miközben (3.9) és (3.11) következménye, hogy

$$a_3 - a_4 > 2p_s^2 - 4p_{s-1}^2 \geq 2p_s^2 - p_s,$$

azaz $a_1 - a_2 = a_3 - a_4$ nem teljesülhet.

Most feltételezve, hogy $a_3$ nem eleme $\mathscr{A}_{p_s}$-nek, (3.9), (3.10), és (3.11) szerint

$$a_1 - a_2 > \min(p_s, 2p_s^2 - 4p_{s-1}) = p_s$$

és (3.9), valamint (3.11) alapján

$$a_3 - a_4 < 4p_{s-1}^2 \leq p_s,$$

azaz $a_1 - a_2 = a_3 - a_4$ nem teljesülhet. □

A 3.3 tétel Krückeberg [7] már korábban említett eredményét ismerteti.

**3.3. Tétel** *Létezik olyan (végtelen) $\mathscr{A}$ $B_2$-sorozat, amire*

$$\limsup_{n\to\infty} n^{-\frac{1}{2}} A(n) \geq \frac{1}{\sqrt{2}}.$$

*Bizonyítás.* A bizonyításban fontos szerepet kap az alábbi, 3.4 Lemma.

**3.4. Lemma.** *Legyen $\mathscr{V}$ egy (véges) $B_2$-sorozat, ami a $[V_1, V_2]$ intervallumban fekszik, és legyen $\mathscr{W}$ egy $B_2$-sorozat, ami a $[W_1, W_2]$ intervallumban helyezkedik el, ahol $V_1, V_2, W_1, W_2$ egész számok, és $V_1 \leq V_2$ és $W_1 \leq W_2$ teljesül rájuk.*

*Tegyük fel, hogy*

$$W_1 - V_2 > \max(V_2 - V_1, W_2 - W_1). \tag{3.12}$$

*Ekkor léteik $\mathscr{W}$-nek egy $\mathscr{W}^*$ részsorozata, amire az is igaz, hogy*

$$|\mathscr{W}^*| \geq |\mathscr{W}| - |\mathscr{V}|(|\mathscr{V}| - 1) \tag{3.13}$$

*és a $\mathscr{V} \cup \mathscr{W}^*$ $B_2$-sorozat.*

*Megjegyzés.* (3.12)-ből triviálisan következik, hogy a $[V_1, V_2]$, $[W_1, W_2]$ intervallumok diszjunktak.

*Bizonyítás.* Az

$$u_1 - u_2 = u_3 - u_4 \tag{3.14}$$

egyenletet fogjuk vizsgálni (hasonlóan az előző tétel bizonyításában szereplő gondolatmenethez), ahol az $u$-k elemei az $\mathscr{U} = \mathscr{V} \cup \mathscr{W}$ sorozatnak, és kielégítik az alábbi összefüggést

$$u_1 > u_2 \geq u_3 > u_4. \tag{3.15}$$

A lemma bizonyításához megmutatjuk, hogy lehetséges $\mathscr{W}^*$ sorozat létrehozása, amit $\mathscr{W}$-ből legfeljebb

$$|\mathscr{V}|(|\mathscr{V}|-1)$$

elem elhagyásával kapunk, amire (3.14)-nek (3.15) feltétel mellett nincs olyan megoldása, ahol minden $u$ $\mathscr{U} = \mathscr{V} \cup \mathscr{W}^*$-beli.

Először megmutatjuk, hogy (3.14)-nek (3.15) feltétel melletti összes $u \in \mathscr{U}$ megoldásra,

$$u_1 \in \mathscr{W}, \qquad u_2 \in \mathscr{W}, \qquad u_3 \in \mathscr{V}, \qquad u_4 \in \mathscr{V} \tag{3.16}$$

teljesül.

Először is, $u_1 \in \mathscr{V}$ lehetetlen, mivel ez (3.15) és $V_2 < W_1$ miatt azt implikálná, hogy $u_2, u_3, u_4$ is szintén $\mathscr{V}$-beli, ellentmondva annak a ténynek, hogy $\mathscr{V}$ $B_2$-sorozat. Továbbá, $u_4 \in \mathscr{W}$ hasonló módon azt implikálná, hogy minden $u$ $\mathscr{W}$-beli, azaz $\mathscr{W}$ $B_2$-sorozat. Így azt kaptuk, hogy

$$u_1 \in \mathscr{W}, \qquad u_4 \in \mathscr{V}.$$

Ugyanakkor $u_2, u_3$ egyszerre nem lehetnek elemei $\mathscr{W}$-nek, mert akkor igaz lenne a következő két egyenlőtlenség is,

$$u_1 - u_2 \leq W_2 - W_1, \qquad u_3 - u_4 \geq W_1 - V_2,$$

amelyek ellentmondanának (3.14)-nek (3.12) fényében. Ehhez hasonlóan, $u_2, u_3$ nem lehet egyszerre $\mathscr{V}$-ben, ben, mert ekkor

$$u_1 - u_2 \geq W_1 - V_2, \qquad u_3 - u_4 \leq V_2 - V_1,$$

és ezek is ellentmondanának (3.14)-nek (3.12) miatt. Ezzel és a bizonyítás előtti megjegyzéssel a (3.16) állítást beláttuk.

Pontosan $\frac{1}{2}|\mathscr{V}|(|\mathscr{V}|-1)$ diszjunkt párt lehet képezni $u_3$-akból és $u_4$-ekből, amikre $u_3 > u_4$, a (3.15)-öt és (3.16)-ot kielégítve. Minden ilyen $u_3, u_4$ párra legfeljebb egy olyan $u_1, u_2$ pár létezik a $\mathscr{W}$ $B_2$-sorozatban, amire (3.15) teljesül (3.16) mellett; és nem nulla különbségek egy $B_2$-sorozat különböző elemeiből különbözőek lesznek. Így a $\mathscr{W}'$ uniója az ilyen $u_1, u_2$ elemeknek legfeljebb

$$\mathscr{V}|(|\mathscr{V}|-1)$$

elem, és világos, hogy a kívánt $\mathscr{W}^*$ sorozatot nyerjük, ha $\mathscr{W}$-ből elhagyjuk $\mathscr{W}'$-t. □

Visszatérünk a 3.3 tétel bizonyítására.

$|\mathscr{S}|$ jelölje az $\mathscr{S}$ véges sorozat elemszámát a továbbiakban.

Itt most $\mathscr{P}$ szintén prímek egy kellőképpen gyorsan növő $p_1, p_2, \dots$ sorozatát fogja jelölni (lásd később). A konstruálni kívánt $\mathscr{A}$ sorozat

$$\mathscr{A} = \mathscr{A}(\mathscr{P}) = \bigcup_{p \in \mathscr{P}} \mathscr{A}_p,$$

ahol minden egyes $\mathscr{A}_p$ egy véges Sidon-sorozat. Minden $p \in \mathscr{P}$-re, $\mathscr{A}_p$ úgy lesz definiálva, hogy

$$\mathscr{I}_p = [t(p), t(p) + p^2] \tag{3.17}$$

intervallumban legyen, ahol $t(n)$ legyen

$$t(n) = n^2 + n \qquad (n = 1, 2, 3, \dots). \tag{3.18}$$

Megjegyezzük, hogy $t(n)$-nek csak a következő két tulajdonsága számít nekünk

$$\lim_{n\to\infty} (t(n) - n^2) = \infty, \qquad \lim_{n\to\infty} \frac{t(n)}{n^2} = 1. \tag{3.19}$$

A 2.3 tételből következik, hogy $[t(p), t(p)+p^2-p-1]$ hosszú intervallumból kiválasztható egy $p-1$ elemű $B_2$-sorozat, nekünk egy kicsit gyengébb eredmény is elég, azaz, hogy létezik $B_2$-sorozat $\mathscr{T}_p$, $|\mathscr{T}_p| = p-1$ elemmel, ami teljesen $\mathscr{I}_p = [t(p), t(p)+p^2]$-beli. A $\mathscr{T}_p$ halmazok sajnos nem lehetnek a fent említett $\mathscr{A}_p$ halmazok, mert az uniójuk nem feltétlenül lenne $B_2$-sorozat.

A 3.4 lemma feltételei mellett, megfelelő szereposztás után elérhetjük, hogy a $\mathscr{V}$, $\mathscr{W}$ $B_2$-sorozatokból új $B_2$-sorozatokat gyártsunk le. Ha már $\mathscr{A}_{p_1}, \mathscr{A}_{p_2}, \ldots, \mathscr{A}_{p_i}$ sorozatokat kiválasztottuk, hogy

$$\mathscr{V}_i = \bigcup_{j=1}^{i} \mathscr{A}_{p_j}, \tag{3.20}$$

szintén $B_2$-sorozat, $t(n)$ és $p_{i+1}$ helyes megválasztása mellett tudjuk alkalmazni a 3.4 lemmát $\mathscr{V} = \mathscr{V}_i$ és $\mathscr{W} = \mathscr{T}_p$ szereposztással, hogy találjunk $\mathscr{T}_{p+1}$-nek egy alkalmas $\mathscr{A}_{p_{i+1}}$ részsorozatát, amire

$$\mathscr{V}_{i+1} = \mathscr{V}_i \cup \mathscr{A}_{p_{i+1}}$$

Sidon-sorozat. A $\mathscr{T}_{p_j}$-ből kihagyandó elemek hányada, hogy azok $\mathscr{A}_{p_j}$-t alkossanak, majd tart a nullához, ahogy $j \to \infty$, és ha a $p_1, p_2, \ldots$ sorozatunk kellően gyorsan növekedő lesz, ez utóbbi feltétel nem fogja elrontani az élességét a következő egyenlőtlenségnek

$$\limsup_{n\to\infty} \frac{A(t(p_j)+p_j^2)}{p_j-1} \geq \lim_{n\to\infty} \frac{|\mathscr{A}_{p_j}|}{p_j} = 1, \tag{3.21}$$

ahol $A(n)$ az $\mathscr{A} = \mathscr{A}(\mathscr{P}) = \bigcup \mathscr{A}_p$ sorozat elemszámát jelöli.

$t(n)$ fenti választása mellett az is látszik, hogy

$$\frac{1}{p_j-1} \sim \frac{\sqrt{2}}{\sqrt{t(p_j)+p_j^2}}, \tag{3.22}$$

teljesül, ami (3.21)-gyel a a tétel bizonyítását adja.

$$\limsup_{n\to\infty} \frac{\sqrt{2}(A(t(p_j)+p_j^2))}{\sqrt{t(p_j)+p_j^2}} \geq 1,$$

és ebből rendezéssel

$$\limsup_{n\to\infty} n^{-\frac{1}{2}} A(n) \geq \frac{1}{\sqrt{2}}.$$

Veszünk egy $\{\varepsilon_j\}$ pozitív számokból álló, nullához konvergáló sorozatot, ami az egyszerűség kedvéért lehet akár az $\varepsilon_j = j^{-1}$, $(j = 1, 2, \dots)$ sorozat. Még tisztáznunk kell, hogy pontosan hogyan kell a $p$-ket és az $\mathscr{A}_p$-ket definiálnunk.

$$p_1, \mathscr{A}_{p_1}, p_2, \mathscr{A}_{p_2}, p_3, \mathscr{A}_{p_3}, dots$$

ilyen sorrendben lesz definiálva indukcióval olyan módon, hogy (3.20) sorozat szintén $B_2$-sorozat legyen minden $i$-re, és

$$|\mathscr{A}_{p_j}| > (1-\varepsilon_j)(p_j - 1) \qquad (j = 2, 3, \dots); \tag{3.23}$$

valamint, ahogy már fentebb írtuk, minden $p \in \mathscr{P}$-re, $\mathscr{A}_p$ részsorozata lesz a $\mathscr{T}_p$ sorozatnak, és $p-1$ elemét a (3.17) intervallum tartalmazza. Mivel (3.23) implikálja (3.21)-et, és (3.19) implikálja (3.22)-ot, ezek a feltételek biztosítani fogják a tétel teljesülését.

Legyen $p_1 = 2$ és $\mathscr{A}_{p_1} = \emptyset$. Legyen $i \geq 1$, és tegyük fel, hogy

$$p_1, \mathscr{A}_{p_1}, \dots, p_i, \mathscr{A}_{p_i}$$

már előállt az indukciós eljárásunkkal. Legyen $p_{i+1}$ a legkisebb $p$ prím, ami teljesíti (3.24) és (3.25) feltételeket, ahol $\mathscr{V}_i$ a (3.20) alatt definiált halmaz. Hogy ilyen $p$ prím létezik, azt a (3.19) első állítása biztosítja nekünk.

$$t(p) - (t(p_i) + p_i^2) > \max(t(p_i) + p_i^2, p^2), \tag{3.24}$$

$$|\mathscr{V}_i|(|\mathscr{V}_i|-1) < \varepsilon_{i+1}(p-1). \tag{3.25}$$

Az indukció miatt $\mathscr{V}_i$ $B_2$-sorozat, és a 2.3 tétel szerint létezik $\mathscr{T}$ $B_2$-sorozat, amire

$$\mathscr{T} \subset [t(p_{i+1}), t(p_{i+1}) + p_{i+1}^2], \qquad |\mathscr{T}| = p_{i+1} - 1.$$

Alkalmazzuk a 3.4 lemmát $\mathscr{V} = \mathscr{V}_i$, $\mathscr{V} = \mathscr{T}$ szereposztással, és

$$V_1 = 0, \qquad V_2 = t(p_i) + p_i^2, \qquad W_1 = t(p_{i+1}), \qquad W_2 = t(p_{i+1}) + p_{i+1}^2,$$

a lemma (3.12) feltétele ekkor

$$t(p_{i+1}) - (t(p_i) + p_i^2) > \max(t(p_i) + p_i^2, p_{i+1}^2)$$

teljesül, mivel (3.24) fennáll $p = p_{i+1}$-gyel. Legyen $\mathscr{A}_{p_{i+1}} = \mathscr{W}^*$, ahol $\mathscr{W}^*$ $\mathscr{T}$ azon részsorozata, amit a lemma alkalmazásával nyerünk. Ekkor

$$\mathscr{V}_{i+1} = \mathscr{V}_i \cup \mathscr{A}_{p_{i+1}}$$

$B_2$-sorozat, és

$$|\mathscr{A}_{p_{i+1}}| \geq |\mathscr{T}| - |\mathscr{V}_i|(|\mathscr{V}_i| - 1) > (p_{i+1} - 1) - \varepsilon_j(p_{i+1} - 1) = (p_{i+1} - 1)(1 - \varepsilon_j)$$

teljesül, felhasználva az előző sorban (3.25)-öt, és $p = p_{i+1}$-re, (3.23) teljesül $j = i + 1$-re. Ezzel igazoltuk az indukciós folyamatunk helyességét. □

*Megjegyzés.* A [6]-ben ismertetett bizonyítás a fenti tételre némileg eltérő, mert ott a 2.3 tétel helyett egy jóval általánosabb tétel speciálisabb alakját használták fel a szerzők.

**3.5. Tétel** *(Bose-Chowla) Legyen $m$ prímhatvány, és legyen $h \geq 2$ egész. Ekkor léteznek olyan $a_1, \dots, a_m$ egészek, amikre az összes*

$$a_{j_1}, a_{j_2}, \dots, a_{j_h}, \qquad \textit{összeg, ahol} \quad 1 \leq j_1 \leq \dots \leq j_h \leq m,$$

*különböző modulo* $m^h - 1$.

A 3.5 tétel bizonyítása véges kommutatív testek segítségével történik, amit ajánlunk az olvasóknak, hogy nézzenek meg, ha nem ismerik a bizonyítást. Mi ebben a dolgozatban nem ismertetjük. Egyrészt, mert eltér a többi bizonyítás jellegétől és a felhasznált eszközöktől, így eléggé elkülönülne a dolgozat többi részétől, miközben ezeket az eredményeket nem használjuk fel. Másrészt terjedelmi okok miatt.

Ebből a tételből egyszerűen következik, hogy ha $m$ prímhatvány, és $h \geq 2$ egész, akkor

$$F_h(m^h - 1) \geq m.$$

Emiatt teljesül az is, hogy ha $t$ nemnegatív egész, $m$ és $h$, mint a tételben, akkor létezik $B_h$-sorozat, ami legalább $m$ elemet tartalmaz és teljesen a $[t, t+m^h-2]$ intervallumban fekszik. Ez utóbbi állítással $m = p, h = 2$-re elegánsan kijön a 3.3 tétel bizonyítása a 2.3 tétel felhasználása nélkül.

A 3.1 és 3.2 tétel következményeként kaphatjuk a következő állításokat.

$$\textit{Minden } \mathscr{A} = \{a_j\}\ B_2\textit{-sorozatra,} \quad \limsup_{j\to\infty} \frac{a_j}{j^2 \log j} > 0. \tag{3.26}$$

$$\textit{Létezik olyan } \mathscr{A} = \{a_j\}\ B_2\textit{-sorozat, amire} \quad \liminf_{j\to\infty} \frac{a_j}{j^2} < \infty. \tag{3.27}$$

Erdős Pál [3] azt sejtette, hogy minden $\varepsilon > 0$ számhoz létezik $\mathscr{A}$ $B_2$-sorozat, amire $a_n \ll n^{2+\varepsilon}$ minden $n$-re. Két részeredményt ismertetünk ebben a témában, de a sejtés maga megoldatlan.

Mian-Chowla cikkükben [9] megmutatták, hogy

**3.6. Tétel**

$$\textit{létezik olyan } \mathscr{A} = \{a_j\}\ B_2\textit{-sorozat, amire} \quad a_n \ll n^3. \tag{3.28}$$

*Bizonyítás.* A fenti eredmény bizonyítására rekurzív konstrukciót adtak az úgynevezett mohó algoritmus segítségével. Legyen $a_1 = 1$, és tegyük fel, hogy $a_1, a_2, \dots, a_m$ már ki lett választva, ahol $m \geq 1$. Vegyük $a_{m+1}$-et a lehető legkisebb természetes számnak, ami különbözik az összes $a_r + a_s - a_t$ értéktől, ahol $1 \leq r, s, t \leq m$. Mivel legfeljebb $m^3$ $r, s, t$ hármas létezik, a megfelelő $a_r + a_s - a_t$ számok legfeljebb $m^3$ különböző egész értéket vehetnek fel, így $a_{m+1} < (m+1)^3$. Így $a_n \leq n^3$ minden $n$-re, és az $\mathscr{A} = \{a_n\}$ sorozat Sidon-sorozat. Megjegyezzük, hogy ezzel az eljárással konstruált sorozat első tíz tagja $1, 2, 4, 8, 13, 21, 31, 45, 66, 81$, így látszik, hogy ez az állítás sajnos nem éles. $\square$

Itt említjük meg, hogy a mohó algoritmussal nem csak $B_2$-sorozatokat lehet előállítani, hanem $B_h[g]$-sorozatokat is. A mohó algoritmus flexibilis és könnyen, sokfelé általánosítható, így nem csoda, hogy a matematika számos területén érnek el vele olyan eredményeket, melyeken elemi lépésekkel nem lehet sokat javítani, csak komoly ötletekkel és jól felépített elméletekkel.

A Mian-Chowla eredmény évtizedekig a legpontosabb ismert eredmény volt. Azonban Erdős és Rényi bizonyított egy mélyebb eredményt, ami más természetű kicsit, mégis részleges választ ad Erdős kérdésére. Ezt a tételt [6] mi most nem bizonyítjuk, csak kimondjuk.

$$\textit{Minden } \varepsilon > 0\textit{-hoz létezik } g = g(\varepsilon) \textit{ szám és egy} \tag{3.29}$$

$$\mathscr{A} = \{a_n\}\ B_2[g]\textit{-sorozat, amire } a_n \ll n^{2+\varepsilon}.$$

# 4. Konstrukció egy sűrű, végtelen Sidon-sorozatra

Chowla és Mian (3.28) eredményét a következő alakban is felírhatjuk: létezik olyan Sidon-sorozat, amire

$$F_2(N) \gg N^{\frac{1}{3}}. \tag{4.1}$$

Erdős-Rényi (3.29) eredményének a hasonló átfogalmazásával azt kapjuk, hogy minden $\varepsilon > 0$-hoz létezik olyan $\mathscr{A}$ $B_2[g]$-sorozat, amire

$$A(N) \gg N^{\frac{1}{2}-\varepsilon}, \tag{4.2}$$

ahol $A(N)$ a $B_2[g]$-sorozat elemszámát jelöli. Más megfogalmazásban, az $n = a + b, a, b \in \mathscr{A}$ megoldások száma korlátos.

Ajtai, Komlós és Szemerédi [1] 1981-es munkája adta a legjobb ismert eredményt közel húsz évig, ami azt mutatta meg, hogy létezik olyan végtelen Sidon-sorozat, amire

$$F_2(N) \gg (N \log N)^{\frac{1}{3}} \tag{4.3}$$

teljesül.

Ruzsa Imre [11] 1998-ban konstruktívan javította a (4.3) eredméyt. A dolgozat ezen fejezetének célja ezen konstrukció és a mögötte rejlő alapötlet ismertetése. Terjedelmi okok miatt a tétel bizonyítása során felhasznált, egymásra épülő lemmák közül csak az utolsót mondjuk ki, azt is bizonyítás nélkül.

**4.1. Tétel** *Létezik olyan (végtelen) $\mathscr{A}$ $B_2$-sorozat, amire*

$$B(N) = N^{\gamma+o(1)}, \qquad \gamma = \sqrt{2} - 1 = 0.41421356\ldots, \tag{4.4}$$

*ahol $B(N)$ a konstruálandó Sidon-sorozat $N$-nél nem nagyobb elemeinek a számát jelöli.*

*Bizonyítás.* A kiindulási pontunk az a megfigyelés lesz, hogy a különböző $p$ prímekre a $\log p$ valós számok Sidon-tulajdonsággal rendelkeznek. Az az ötletünk, hogy ezen számok kettes számrendszerbeli alakjának számjegyeit átrendezzük, hogy az egészek közötti Sidon-sorozatot kapjunk. Ha a $\log p$ számok kettes számrendszerbeli felírása véges lenne, és nem túl hosszú, akkor ez könnyen megtehető lenne. Azonban végtelen hosszú a felírásuk, így valahogyan majd le kell vágnunk a végüket. Bebizonyítható, hogy az így keletkező sorozatnak kis részét elhagyva már egy Sidon-részsorozatot kaphatunk.

A konstrukciónkban kicsit szokatlan módon fog a véletlen megjelenni. Ahelyett, hogy egymástól független elemeket választanánk meg véletlenszerűen, egy véletlen $\alpha$ paramétert választunk a $[1, 2]$ intervallumból a bizonyítás kezdetén. Ez meghatároz majd egy halmazt, és megmutatható, hogy majdnem minden $\alpha$-ra az $[1, 2]$ intervallumból az így nyert halmaz rendelkezik a kívánt tulajdonsággal.

Most rögzítjük a $\beta$-t és $\gamma$-t, hogy a következő számokat jelöljék

$$\beta = \sqrt{2} + 1 \quad \gamma = 1/\beta = \sqrt{2} - 1.$$

$p \geq 3$ prímekre írjuk fel az $\alpha \log p$ számokat kettes számrendszerben

$$\alpha \log p = \sum_{i=0}^{k} \varepsilon_{ip} 2^i + \sum_{i=1}^{\infty} \delta_{ip} 2^{-i},$$

ahol

$$k = k_p = \lfloor log_2(\alpha \log p) \rfloor .$$

Ezt a felírást a négyzetszámoknak megfelelően blokkokra vágjuk, és a blokkokat átrendezzük, hogy $p^\beta$ körüli egész számot alkossanak. Ehhez még bevezetünk néhány jelölést.

$$K = K_p = \min\{i > 2 : 2^{(i-1)^2} > p^\beta\},$$

amiből átrendezve látszik, hogy

$$K_p = 2 + \left\lfloor \sqrt{\beta \log_2 p} \right\rfloor .$$

Ellenőrizhető, hogy $K_p > k_p$ minden $p$-re. Definiáljuk még a következőket:

$$P_K = \{p : K_p = K\},$$

$$\lambda_p = \sum_{i=0}^{k} \varepsilon_{ip} 2^i + \sum_{i=1}^{K^2} \delta_{ip} 2^{-i}.$$

$K$ definíciójából látszik, hogy

$$|\lambda_p - \alpha \log p| \le 2^{-K^2} < 2^{-(K-1)^2} < p^{-\beta}. \tag{4.5}$$

Összerakjuk a számjegyeket az $(i-1)^2+1, \ldots, i^2$ helyiértékeken egy külön, $\Delta_{ip}$ számmá, az alábbi módon:

$$\Delta_{ip} = \sum_{j=(i-1)^2+1}^{i^2} \delta_{jp} 2^{i^2-j} \qquad (i = 1, \ldots, K),$$

így

$$\Delta_{ip} < 2^{i^2-(i-1)^2} = 2^{2i-1}.$$

Ezzel a jelöléssel $\lambda_p$-t a következő féleképpen lehet kifejezni

$$\lambda_p = \sum_{i=0}^{k} \varepsilon_{ip} 2^i + \sum_{i=1}^{K} \delta_{ip} 2^{-i^2}. \tag{4.6}$$

Most alkotunk minden $p$ prímhez egy $b_p$ természetes számot. A Sidon-sorozatunk ezen számok halmazának egy megfelelő részhalmaza lesz.

Először csak elmondjuk az ötletet, hogy hogyan akarjuk megalkotni a $b_p$ számokat. Leírjuk a $\Delta_{1p}, \ldots, \Delta_{Kp}$ blokkokat egymás után, köztük 5 helyiértéket kihagyva. Az első, a harmadik és az ötödik mindig nulla lesz. A második helyiértékre az $\varepsilon_{ip}$ számjegyeket írjuk. A negyedik helyiértékre mindig nullát írunk a $K$-adikat leszámítva (azaz a $\Delta_{Kp}$ utáni). Ez fogja meghatározni a $b_p$ nagyságrendjét és ez fogja megmutatni, hogy melyik $P_K$-ból jött a $p$ prím.

Formálisan leírva a fent megfogalmazottakat, ($k = k_p, K = K_p$) mellett

$$b_p = \sum_{i=1}^{K} \Delta_{ip} 2^{(i-1)^2+5i} + \sum_{i=0}^{k} \varepsilon_{ip} 2^{i^2+5i+2} + 2^{K^2+5K+4}.$$

Mivel $k < K$

$$2^{K^2+5K+4} < b_p < 2^{K^2+5K+5},$$

ebből következik, hogy

$$b_p = p^{\beta+o(1)}.$$

Most a

$$b_p + b_s = b_q + b_r \tag{4.7}$$

egyenlet megoldásainak a számára szeretnénk felső korlátot találni. Az általánosság megszorítása nélkül feltételezhető, hogy

$$b_p > b_q \geq b_r > b_s \tag{4.8}$$

hasonló érvelésnek köszönhetően, mint amiről már volt szó a dolgozat korábbi fejezeteiben.

Eddig tart a konstrukció alapötletének felvázolása, ami után a bizonyításhoz szükséges lemmák hosszú sora következhetne, de ezeket terjedelmi okokból itt nem ismertetjük. Azonban az ötletes számelméleti bizonyításokkal, és a becsülendő mennyiségek jó megválasztásával eljuthatunk addig a segédállításig, hogy ha a

$$G_K(\alpha) = |\{p, q, r, s : p, q \in P_K, (4.7) \text{ és } (4.8) \text{ teljesül}\}|$$

kifejezést bevezetjük, akkor

**4.2. Lemma.**
$$\int_1^2 G_K(\alpha)\,d\alpha \ll 2^{\gamma(K-1)^2-2K} \tag{4.9}$$
lemma teljesül. Nekünk ez az utolsó segédállítás elegendő lesz a $B_2$-sorozatunk előállításához.

A tétel bizonyításához szeretnénk felhasználni az alábbi összefüggést:

$$G_K(\alpha) < 2^{\gamma(K-1)^2-K}$$

véges sok $K$ kivételével. Az ötletünk az, hogy alkalmazzuk a Borel-Cantelli lemmát egy megfelelően választott eseményrendszerre. Legyen

$$A_K = \{(x,y) : 1 \le x \le 2;\, y \le \frac{G_K(\alpha)}{2^{\gamma(K-1)^2-K}}\},$$

ekkor, ha $\mu$-vel jelöljük a Lebesgue-mértéket,

$$\mu(A_K) = \int_1^2 \frac{G_K(\alpha)}{2^{\gamma(K-1)^2-K}}\,d\alpha \ll 2^{-K}$$

a (4.9) miatt. Alkalmazható a Borel-Cantelli lemma,

$$(\forall\varepsilon > 0)(\exists K_0)(\forall K > K_0) : \mu(A_K \cap A_{K+1} \cap \dots) < \varepsilon\}, \qquad \text{azaz}$$
$$\int_1^2 \min_{K>K_0} \frac{G_K(\alpha)}{2^{\gamma(K-1)^2-K}}\,d\alpha < \varepsilon$$
ez véges sok $K$ kivétellel teljesül, mert minden kivétel kisebb, mint $K_0$. Létezik olyan $\alpha$ érték, ahol az integrandus értéke kisebb, mint $\varepsilon$.

$$\frac{G_K(\alpha)}{2^{\gamma(K-1)^2-K}} < \varepsilon < 1$$

ebből átszorzással kapjuk a kívánt

$$G_K(\alpha) < 2^{\gamma(K-1)^2-K}$$

egyenlőtlenséget. Mostantól rögzítjük $\alpha$-t egy ilyen értéknek.

$P_K$ számosságára az igaz, hogy

$$|P_K| = \pi(2^{\gamma(K-1)^2}) - \pi(2^{\gamma(K-2)^2}) \sim \frac{2^{\gamma(K-1)^2}}{(\gamma \log 2)K^2},$$

így $K > K_0$ esetén, $G_K(\alpha) < |P_K|/2$ . Ezért, ha $p, q, r, s$ kielégíti (4.7) és (4.8) feltételeket $p \in P_K$ mellett, akkor elhagyjuk $p$-t a $P_K$-ból, és a megmaradó $Q_K$ halmaz elemeinek számosságára teljesül az, hogy $|Q_K| > |P_K|/2$. A Sidon-sorozatunk

$$\bigcup_{K>K_0} Q_K$$

halmaz elemeiből fog állni.

Hogy megbecsülhessük a $B$ halmaz elemeinek a számát $x$-ig, vegyük észre, hogy

$$b_p < 2^{K^2+5K+5} < 2^{(K+3)^2}.$$

Így $K = \lfloor \sqrt{\log_2 x} - 3 \rfloor$ esetén a $Q_K$ halmaz $x$-nél kisebb elemeket tartalmaz. Így

$$B(x) \gg (1/2 - \varepsilon)\pi(2^{\gamma(K-1)^2}) = x^{\gamma+o(1)}.$$

Egy hasonló számolás vezethet el minket a felső becsléshez is. $\square$

# 5. Általánosabb problémák

Ezen fejezet Kevin O'Bryant összefoglaló cikkéből [10] említ meg bizonyos, $B_h[g]$-sorozatokkal kapcsolatos problémákat, illetve eddig elért eredményeket. Helyenként, ahol lehetőség van rá, szeretném megmutatni a dolgozatban bizonyított tételekkel való kapcsolatukat.

$F_h(n)$-nel jelöltük az $n$-nél nem nagyobb elemekből álló $B_h$ sorozatok elemszámának a maximumát. Ennek megfelelő általánosításaként vezessük be az $F_{h,g}(n)$ jelölést azon $B_h[g]$-sorozat maximális elemszámára, amely elemei $\{1, 2, \ldots, n\}$-beliek.

$F_{h,g}(n)$ aszimptotikus becslése egyike a téma megoldatlan kérdéseinek, amikor $h > 2, g > 1$. Egy másik kérdés, hogy tudunk-e olyan $B_h[g]$ sorozatot konstruálni, amire $g > h$, amire a sorozatunk sűrű, de nem csupán néhány $B_h$-sorozat uniója. Ezt Erdős Pál és Donald Newman egymástól függetlenül belátta $B_2[g]$-sorozatokra, hogy ilyenek léteznek, bizonyos $g$-kre. Érdekességként megemlítjük, hogy Erdős a Ramsey-tétel segítségével látta be ezt az állítást.

Bevezetjük a következő függvényt a $B_h[g]$-sorozatok sűrűségének vizsgálatára, ha a következő határérték létezik:

$$\sigma_h(g) = \lim_{n\to\infty} \frac{F_{h,g}(n)}{\sqrt[h]{g \cdot n}}.$$

Sajnos ezen határérték létezéséről nem tudunk határozottan nyilatkozni $h > 2$ és $g > 1$ esetén. Ilyenkor $\sigma_h(g)$-re vonatkozó alsó becslés alatt a $\liminf$-re vonatkozó alsó becslés értendő, míg a felső becslés pedig a $\limsup$-ra felső becslés. Ha $g = 1$, akkor $\sigma_h$ jelöléssel élünk.

A következő egyszerű sejtéseket fogalmazhatjuk meg $\sigma_h(g)$-vel kapcsolatban.

1. A $\sigma_h(g)$ definíciójában szereplő határérték jóldefiniált.

2. Minden $h$-ra, $\sigma_h(g)$ monoton növő függvénye $g$-nek.

3. Minden $h$-ra, $\lim_{g\to\infty} \sigma_h(g)$ jóldefiniált és véges.

Bár ezek a kérdések nem tűnnek annyira nehéznek, még senkinek sem sikerült rájuk választ adni. A 3. kérdésről annyit tudunk, hogy a $\liminf$ és a $\limsup$ két pozitív konstans között van. $\sigma_h$ növekedésére, mint $h$ függvényére még megalapozottnak tűnő sejtés sincs, az is elképzelhető, hogy $h$ paritásától függ a kifejezés.

Megjegyezzük, hogy a $\sigma_2 = 1$-et ismerjük a második fejezetben bizonyított tételekből.

Erdős Pál egyik, 500 dolláros kérdése volt az, hogy $F_2(n) - \sqrt{n}$ korlátos-e. A válasz úgy tűnik, hogy nemleges, és az is csak sejtés, hogy pozitív a kifejezés. A legjobb ismert eredmény a kérdéskörben az általunk is ismertetett

$$-n^{\frac{\alpha}{2}} < F_2(n) - \sqrt{n} < +\sqrt[4]{n} + 1$$

becslések, ahol $\alpha = \frac{11}{20}$ volt a második fejezetben.

$h = 2$-re, a 3. kérdésre a válasz

$$1.122 < \lim_{g \to \infty} \sigma_2(g) \leq 1.839$$

Egy $a_1 < a_2 < \cdots < k$ Sidon-sorozatot rövidnek hívunk, ha az $a_k - a_1$ érték minimális. Most következzen $k = 13$-ig a rövid Sidon-sorozatokat tartalmazó táblázat. A mai napig ennyi ismert.

| k | $\min\{a_k - a_1\}$ | Tanú |
|---|---|---|
| 2 | 1 | $\{0, 1\}$ |
| 3 | 3 | $\{0, 1, 3\}$ |
| 4 | 6 | $\{0, 1, 4, 6\}$ |
| 5 | 11 | $\{0, 1, 4, 9, 11\}$ |
| | | $\{0, 2, 7, 8, 11\}$ |
| 6 | 17 | $\{0, 1, 4, 10, 12, 17\}$ |
| | | $\{0, 1, 4, 10, 15, 17\}$ |
| | | $\{0, 1, 8, 11, 13, 17\}$ |
| | | $\{0, 1, 8, 12, 14, 17\}$ |
| 7 | 25 | $\{0, 1, 4, 10, 18, 23, 25\}$ |
| | | $\{0, 1, 7, 11, 20, 23, 25\}$ |
| | | $\{0, 1, 11, 16, 19, 23, 25\}$ |
| | | $\{0, 2, 3, 10, 16, 21, 25\}$ |
| | | $\{0, 2, 7, 13, 21, 22, 25\}$ |
| 8 | 34 | $\{0, 1, 4, 9, 15, 22, 32, 34\}$ |
| 9 | 44 | $\{0, 1, 5, 12, 25, 27, 35, 41, 44\}$ |
| 10 | 55 | $\{0, 1, 6, 10, 23, 26, 34, 41, 53, 55\}$ |
| 11 | 72 | $\{0, 1, 4, 13, 28, 33, 47, 54, 64, 70, 72\}$ |
| | | $\{0, 1, 9, 19, 24, 31, 52, 56, 58, 69, 72\}$ |
| 12 | 85 | $\{0, 2, 6, 24, 29, 40, 43, 55, 68, 75, 76, 85\}$ |
| 13 | 106 | $\{0, 2, 5, 25, 37, 43, 59, 70, 85, 89, 98, 99, 106\}$ |

Összehasonlításként, Mian-Chowla mohó algoritmussal kapott sorozatában a tizedik tag 81 volt a táblázatban kapott 55-tel szemben.

$h > 2$-re sajnos nagyon kevesett tudunk a $B_h$-sorozatokról. A Bose-Chowla 3.5 tételünkből bebizonyítható, hogy $\sigma_h \geq 1$ és ez a legjobb ismert alsó becslés, míg felső becsléseken nagyon sokan dolgoztak, de még mindig nagyon messze van az alsótól.

# 6. Összefoglalás

A szakdolgozat elején definiáltuk a később használatos jelöléseket, amelyek alkalmasak a $B_h[g]$-sorozatok általános vizsgálatára, ami nem kifejezetten egységes a szakirodalomban. Érzékeltettük, hogy milyen jellegű kérdésekkel kapcsolatban merült fel a probléma Sidon Simon munkássága során. Főként kombinatorikus úton vizsgáltuk a véges Sidon-sorozatokat, ahol a legtöbb eredmény még Erdőshöz kötődik. Megmutattuk, hogy sűrű Sidon-sorozatra $F_2(n)$ aszimptotikusan tart az 1-hez.

Ezután áttértünk a végtelen Sidon-sorozatok vizsgálatára, ahol az alsó és felső becslések mind a ma napig nem a lehető legélesebbek, egy alsó becslés után a felső becslések közül Erdős és Krückeberg élesebb eredményét bizonyítottuk. Ezt követően rátértünk a Mian-Chowla és az Erdős-Rényi tételekkel a konstrukción alapuló alsó becslésekre, ahol Ruzsa Imre sűrű Sidon-sorozatának konstrukcióját ismertettük. Ezen sorozat sűrűsége $B(N) = N^{\sqrt{2}-1+o(1)}$ volt. Végezetül a számos, általánosabb probléma közül néhányat megemlítettünk, illetve az eddig elért eredményeket ismertettük.

Ezúton szeretném megköszönni Sárközy Andrásnak és Gyarmati Katalinnak a szakdolgozat megírásához nyújtott segítséget, és hogy bátran fordulhattam hozzájuk a felmerülő kérdéseimmel, ötleteimmel.

# Hivatkozások


[1] M. Ajtai, J. Komlós, E. Szemerédi: *A dense infinite Sidon sequence*, European J. Comb. **2**, (1981), 1-11.

[2] R. C. Baker, G. Harman, J. Pintz: *The difference between consecutive primes, II.,* Proc. London Math. Soc. (3) **83** (2001), 532-562.

[3] P. Erdős: *Colloque sur la Théorie des Nombres*, Bruxelles, 1956, section 3, 127-137.

[4] P. Erdős, J. Surányi: *Válogatott fejezetek a számelméletből*, Polygon, Szeged, 2004, 234-239.

[5] P. Erdős, P. Turán: *On a problem of Sidon in additive number theory, and on some related problems*, J. London Math. Soc. **16** (1941), 212-215.

[6] H. Halberstam, K. F. Roth: *Sequences*, Spinger-Verlag, New York/Berlin, 1983, 88-97.

[7] F. Krückeberg: *$B_2$-Folgen und verwandte Zahlenfolgen*, II. J. reine. angew, Math. **206**, (1961), 53-60.

[8] B. Lindström: *An inequality for $B_2$-seguencse*, J. Comb. Theory **6** (1969), 211-212.

[9] A. Mian, S. Chowla: *On the $B_2$-sequences of Sidon*, Proc. natn. Acad. Sci. India. Sect. A, **14**, (1944), 3-4.

[10] K. O'Bryant, *A complete annotated bibliography of work related to Sidon sequences*, Electronic J. Combinatorics, **11**, (2004), 39.

[11] I. Z. Ruzsa, *An infinite Sidon sequence*, J. Number Theory, **68**, (1998), 63-71.

[12] S. Sidon: *Ein Satz über trigonomietrische Polynome und seine Anwendungen in der Theorie der Fourier-Reihen*, Math. Annalen **106** (1932), 536-539.

[13] V. T. Sós: *An additive problem in different structures*, in: Graph Theory, Combinatorics, Algorithms and Applications, ed:, Y. Alavi et al., SIAM, Philadelphia, 1991, 486-510.

[14] A. Stöhr: *Stöhr Gelöste und ungelöste Fragen über Basen der naturlichen Zahlenreihe*, II. J. reine angew. Math. **194**, (1955), 111-140.