

EÖTVÖS LORÁND TUDOMÁNYEGYETEM
TERMÉSZETTUDOMÁNYI KAR

NEMES-KOSTELECKZI ANNA RÓZA

Kombinatorikus számelméleti problémák

Szakdolgozat
Matematika BSc

Témavezető:
DR. FREUD RÓBERT PÁL



Budapest, 2025

Köszönetnyilvánítás

Nagyon hálás vagyok a témavezetőmnek, Freud Róbertnek a rengeteg segítségéért, idejéért, türelméért, amivel nagyban hozzájárult a szakdolgozatom elkészüléséhez. Sokat jelentett, hogy a folyamatos szakmai és technikai segítség mellett emberileg is biztatóan támogatott.

Köszönöm továbbá a családomnak, hogy tanulmányaim során mindenben támogattak és szeretettel álltak mellettem a nehéz időszakokban is.

Tartalomjegyzék

1. Bevezetés	2
2. Definíciók és tételek	3
2.1. Véges testek	3
2.2. Testbővítés	3
3. Sidon-sorozatok	5
3.1. Sidon-sorozatok	5
3.2. Egyszerű becslések az elemszámra	5
3.3. Alsó becslések	7
3.4. Alsó és felső becslés általános n -re	15
3.5. Többtagú összegek	19
3.6. Végtelen Sidon-sorozatok	21
3.7. Vegyes feladatok	26
4. Csupa különböző összegű sorozatok	28
4.1. Csupa különböző összeg	28
4.2. Felső becslés az elemszámra	28
4.3. Vegyes feladatok	31
4.4. Felső becslés a reciprokösszegre	35
4.5. Csupa különböző szorzatú sorozatok	39

1. fejezet

Bevezetés

Legfeljebb hány tagja lehet annak a sorozatnak, amelyben bármely két tag összege különböző? Legfeljebb hány egész számot tudunk kiválasztani úgy, hogy közülük bármennyit összeadva különböző értékeket kapjunk? Ezeket a kérdéseket nagyon egyszerű megérteni, de vajon a válaszok is ennyire egyszerűek? Erdős Pál 500 dollárt ígért a második kérdés megfejtőjének [6]. Ebből sejthetjük, hogy a problémák igencsak elgondolkodtatóak. A mai napig bizonyítatlan, hogy léteznek-e a már meglévő becsléseknél élesebb közelítések az elemszámokra nézve vagy sem.

A dolgozat három fő részre osztható. A 2. fejezetben összegyűjtjük azokat a véges testekkel kapcsolatos definíciókat és tételeket, amelyekre később a bizonyításokban hivatkozunk. Ezeket a tételeket itt bizonyítás nélkül említjük, csak eszközök lesznek a további fejezetekben. A 3. fejezetben a Sidon-sorozatok témakörét tárgyaljuk. Alsó és felső becsléseket adunk a sorozat elemszámára, és kapcsolódó problémákat is említünk egy-egy feladat erejéig. A 4. fejezetben át térünk a csupa különböző összegű sorozatok kérdésére. Az elemszámra vonatkozó becslések után itt is előkerülnek hasonló problémákat körüljáró feladatok, majd kitekintésként foglalkozunk a 4. fejezet alapkérdésével összegek helyett szorzatokra is.

A dolgozatban előkerülő feladatok megoldása mind önálló munka, esetenként kis segítséggel. A tételek bizonyításai alapos megértés után saját megfogalmazásban és szerkesztésben kerültek leírásra.

2. fejezet

Definíciók és tételek

A 3.3.3. és a 3.3.11. tétel, valamint a 3.5.2. állítás bizonyításában előkerül néhány fogalom és tétel a véges testek és a testbővítések témaköréből. Ebben a fejezetben ezeket bizonyítás nélkül felsoroljuk Freud Róbert *Lineáris algebra* tankönyve alapján [10].

2.1. Véges testek

2.1.1. Definíció (*Véges test*). A véges elemszámú testeket véges testeknek nevezzük.

2.1.2. Tétel. Bármely p^k prímszámhoz létezik p^k elemű véges test.

2.1.3. Tétel. Egy véges test nemnulla elemei a szorzásra nézve ciklikus csoportot alkotnak.

2.1.4. Definíció (*Multiplikatív csoport*). A 2.1.3. tételben említett ciklikus csoportot a véges test multiplikatív csoportjának nevezzük.

2.1.5. Tétel. Legyen T_k a p^k elemű véges test. Ekkor T_k -nak van egy p elemű részteste és efelett a p elemű részteste felett T_k egy k dimenziós vektorteret alkot.

2.2. Testbővítés

Jelölés. A továbbiakban T_k jelöli a p^k elemű, T_1 pedig a p elemű véges testet.

2.2.1. Definíció (*Testbővítés*). Az M testet az L test bővítésének nevezzük, ha L részteste M -nek, és az L testben a műveletek az M -beli műveletek megszorításai. Jelölés: $M : L$.

2.2.2. Megjegyzés. Ha M bővítése L -nek, akkor M vektortér is L felett a szokásos vektortér-műveletekkel: két vektor összeadásának megfelel két M -beli elem összeadása, illetve a skalárral való szorzásnak megfelel egy M -beli és egy L -beli elem összeszorozása az M -beli szorzás szerint. M mint L feletti vektortér dimenziója lesz a testbővítés foka, azaz $\deg(M : L)$.

2.2.3. Következmény. A 2.1.5. tételből és a 2.2.2. megjegyzésből következik, hogy $\deg(T_k : T_1) = k$.

2.2.4. Definíció (*Egyszerű bővítés*). Legyen L részteste M -nek, és $\Theta \in M$ tetszőleges. Ekkor

$$\left\{ \frac{\sum_{i=0}^n \alpha_i \Theta^i}{\sum_{j=0}^k \beta_j \Theta^j} \mid \alpha_i, \beta_j \in L; \sum_{j=0}^k \beta_j \Theta^j \neq 0; n, k = 0, 1, \dots \right\}$$

M -beli részhalmaz az L -nek Θ -val vett egyszerű bővítése, $L(\Theta)$.

2.2.5. Tétel. $L(\Theta)$ az a legszűkebb részteste M -nek, amely L -et és Θ -t is tartalmazza.

2.2.6. Következmény. $T_k : T_1$ egyszerű bővítés, hiszen $T_1(\Delta) = T_k$, ahol Δ a T_k multiplikatív csoportjának generátoreleme.

2.2.7. Definíció (*Algebrai elem*). Tegyük fel, hogy L részteste M -nek. Legyen $\Theta \in M$. Θ algebrai L felett, ha létezik olyan nemnulla $f \in L[x]$ polinom, amelynek Θ a gyöke.

2.2.8. Definíció (*Minimálpolinom*). Legyen $\Theta \in M$ algebrai L felett. Θ minimálpolinomjának azt a legalacsonyabb fokú L feletti polinomot nevezzük, amelynek Θ a gyöke. Jelölés: m_Θ . Ekkor Θ foka megegyezik a minimálpolinomjának a fokával, azaz $\deg \Theta = \deg(m_\Theta)$.

2.2.9. Tétel. Ha $\Theta \in M$ algebrai L felett, akkor $\deg(L(\Theta), L) = \deg(m_\Theta) = \deg \Theta$.

2.2.10. Következmény. Minden $\Theta \in T_k$ algebrai T_1 felett és $(\deg \Theta) \mid k$.

2.2.11. Következmény. Ha Δ a T_k multiplikatív csoportjának generátoreleme, akkor Δ foka k .

3. fejezet

Sidon-sorozatok

3.1. Sidon-sorozatok

A definíciót, az alapvető kérdést és az egyszerű felső becslést Freud Róbert és Gyarmati Edit *Számelmélet* tankönyve alapján foglaljuk össze [11]. A mohó algoritmus végiggondolása önálló munka.

3.1.1. Definíció (*Sidon-sorozat*). Az $a_1 < a_2 < \dots$ sorozatot Sidon-sorozatnak nevezzük, ha minden i esetén $a_i \in \mathbb{N}$ és az $a_i + a_j$ összegek mind különbözőek minden $i \leq j$ -re. (Azaz máshogyan fogalmazva: az $a_i - a_j$ különbségek mind különbözőek, ha $i \neq j$.) A sorozat lehet véges vagy végtelen.

3.1.2. Kérdés (*Alapvető kérdés*). Legfeljebb hány eleme lehet annak a Sidon-sorozatnak, amelynek minden elemét az $[1, n]$ intervallumból választjuk?

A következőkben alsó, illetve felső becsléseket fogunk adni az elemszámra különböző feltételek mellett.

3.2. Egyszerű becslések az elemszámra

Jelölés. A továbbiakban legyen az $[1, n]$ intervallumon megadható leghosszabb Sidon-sorozat elemszáma s .

3.2.1. Egyszerű felső becslés. Először adjunk egy egyszerű felső becslést s -re. Ha minden i -re $a_i \in [1, n]$, akkor $a_i + a_j \in [2, 2n]$. Az $a_i + a_j$ összeg $\binom{s}{2} + s = \binom{s+1}{2} = \frac{s^2+s}{2}$ féle lehet. Ezekből:

$$\frac{s^2+s}{2} < 2n$$

$$s^2 < s^2 + s < 4n$$

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

Ha a sorozat Sidon-tulajdonságának különbségekkel vett felírását nézzük, akkor még jobb felső becslést kapunk, mert akkor az $(a_i - a_j)$ -ben nem lehetnek a tagok egyenlőek, így a különbség csak $\binom{s}{2}$ féle lehet, illetve tudjuk, hogy $a_i - a_j \in [1, n]$. Ebből:

$$\binom{s}{2} = \frac{s^2-2}{2} < n$$

$$(s-1)^2 < s^2 - s < 2n \text{ (mert } (s-1)^2 = s^2 - 2s + 1)$$

$$s-1 < \sqrt{2n}$$

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

Az egyszerű felső becslések után az elemszámra szeretnénk egyszerű alsó becslést is adni. Ehhez használjuk a mohó algoritmust.

3.2.2. Egyszerű alsó becslés (*Mohó algoritmus*). Kezdjünk el legyártani egy Sidon-sorozatot a mohó algoritmussal. Legyen $a_1 = 1$, $a_2 = 2$. A 3-at nem vehetjük be, mert $2 + 2 = 1 + 3$. Legyen $a_3 = 4$. Az 5-öt nem választhatjuk, mert $2 + 4 = 1 + 5$ és így tovább. A sorozat első néhány tagja: 1, 2, 4, 8, 13...

A mohó algoritmus során megyünk sorba a természetes számokon és bele vesszük a sorozatba az első olyan számot, amely nem rontja el az eddigi sorozat Sidon-tulajdonságát. Legyenek $a_1 < a_2 < \dots < a_s < n$ az eddig kiválasztott számok. Azt szeretnénk megvizsgálni, hogy vajon létezik-e egy olyan $a_s < r \leq n$ szám, amelyet hozzávehetünk a sorozathoz úgy, hogy az továbbra is Sidon-sorozat marad.

Az r szám két esetben lehet rossz nekünk. Az első eset az, ha létezik $i, j, k \leq s$, amelyekre igaz, hogy $r + a_i = a_j + a_k$, azaz ha előáll $r = a_j + a_k - a_i$ alakban. A második eset az, ha létezik $l, m \leq s$, amelyekre igaz, hogy $r + r = a_l + a_m$. Az utóbbival nem kell foglalkoznunk, mert $r + r = a_l + a_m$ esetén $r < \max(a_l, a_m)$, amiből következik, hogy $r < a_s$, vagyis r -et vagy már korábban bevettük volna, vagy akkor az első eset is probléma volt nála. Tehát csak az első esetet kell megvizsgálnunk. Az $r = a_j + a_k - a_i$ előállítás formálisan s^3 különböző összeget jelent. Emellett az eddig már kiválasztott a_i -ket is ki kell zárunk, de ez automatikusan teljesül, hiszen $a_i = a_i + a_j - a_j$. Vagyis legfeljebb s^3 számot nem vehetünk be a sorozatba. (Sőt, mivel a_j és a_k szerepe felcserélhető a képletben, ezért legfeljebb $s^3/2$ elemet zárhatunk ki.) Jegyezzük meg, hogy valójában $s^3/2$ -nél kevesebb elemet zárunk ki, mert az $a_j + a_k - a_i$

kifejezések között $a_j \neq a_k$ esetén is lesznek egyenlőek, illetve lesz olyan is, ami a_s -nél kisebb, vagy n -nél nagyobb, vagy akár negatív r -et ad. Nézzünk erre egy példát a fentebb elkezdett sorozat első öt tagján: $8 + 4 - 1 = 13 + 2 - 4 = 11 < a_s = 13$. Vagyis a kifejezés értéke szóba sem jön mint a legnagyobb tagnál nagyobb kizárandó elem. De az igaz, hogy legfeljebb s^3 elemet zártunk ki. Ebből következik, hogyha $s^3 < n$, akkor biztosan van jó r , amit még be tudunk venni a sorozatba. Így legfeljebb akkor állunk le, amikor már $s^3 \geq n$. Ekkor $s \geq \sqrt[3]{n}$. Ezzel beláttuk, hogy mohó algoritmussal tudunk legalább $\sqrt[3]{n}$ elemű Sidon-sorozatot készíteni.

3.3. Alsó becslések

A következőkben szeretnénk a mohó algoritmus alsó becslését megjavítani.

Jelölés. Jelölje $\langle i^2 \bmod p \rangle$ az i^2 legkisebb nemnegatív maradékát p -vel osztva.

3.3.1. Feladat (*Konstrukció: $n = 2p^2$ és $s = p$*). Legyen p prímszám és $a_i = 1 + 2ip + \langle i^2 \bmod p \rangle$ $i = 0, 1, \dots, p-1$. Lássuk be, hogy így $n = 2p^2$ -re egy $\sqrt{n/2}$ elemszámú Sidon-sorozatot kapunk az $[1, n]$ intervallumban.

Megoldás. Ha $n = 2p^2$, akkor $\sqrt{n/2} = \sqrt{2p^2/2} = \sqrt{p^2} = p$. Azaz, azt szeretnénk belátni, hogy az $[1, 2p^2]$ intervallumon egy p elemszámú Sidon-sorozatot kapunk, ha a megadott módon vesszük a tagokat.

Először lássuk be, hogy ha $i = 0, 1, \dots, p-1$, akkor a sorozatban p különböző tag lesz. Hogy néznek ki a sorozat tagjai?

$$a_0 = 1$$

$$a_1 = 1 + 2p + 1 = 2p + 2$$

$$a_2 = 1 + 4p + 4 = 4p + 5$$

$$a_3 = 1 + 6p + 9 = 6p + 10$$

$$a_4 = 1 + 8p + 16 = 8p + 17$$

...

$$a_{(p-3)} = 1 + 2p^2 - 6p + 9 = 2p^2 - 6p + 10$$

$$a_{(p-2)} = 1 + 2p^2 - 4p + 4 = 2p^2 - 4p + 5$$

$$a_{(p-1)} = 1 + 2p^2 - 2p + 1 = 2p^2 - 2p + 2$$

Legyen a_i és a_{i+1} a sorozat két szomszédos tagja, k_i és k_{i+1} pedig a két tag konstans része (például a_1 esetén $k_1 = 2$). Vegyük észre, hogy a $+2ip$ miatt $a_{i+1} - a_i = 2p + (k_{i+1} - k_i) > 2p + (1 - p) = p + 1$. (Felhasználtuk, hogy $1 \leq k_i \leq p$, mert $0 \leq \langle i^2 \bmod p \rangle \leq (p-1)$.) Ezzel beláttuk, hogy minden tag különböző, tehát az a_i -k kiadnak egy p tagú sorozatot.

Ezenkívül a Sidon-tulajdonságot szeretnénk igazolni, vagyis azt, hogy az $a_i + a_j$ összegek mind különbözőek minden $i \leq j$ -re. Ehhez tegyük fel, hogy létezik i, j, k, l , hogy $a_i + a_j = a_k + a_l$. Bontsuk ki a tagokat és rendezzük át az egyenletet:

$$1 + 2ip + \langle i^2 \bmod p \rangle + 1 + 2jp + \langle j^2 \bmod p \rangle = 1 + 2kp + \langle k^2 \bmod p \rangle + 1 + 2lp + \langle l^2 \bmod p \rangle$$

$$2 + 2ip + \langle i^2 \bmod p \rangle + 2jp + \langle j^2 \bmod p \rangle - (2 + 2kp + \langle k^2 \bmod p \rangle + 2lp + \langle l^2 \bmod p \rangle) = 0$$

$$(3.3.1) \quad 2p(i + j - k - l) + (\langle i^2 \bmod p \rangle + \langle j^2 \bmod p \rangle - \langle k^2 \bmod p \rangle - \langle l^2 \bmod p \rangle) = 0$$

(3.3.1) mindkét oldala osztható $2p$ -vel, ebből következik, hogy a

$$(3.3.2) \quad (\langle i^2 \bmod p \rangle + \langle j^2 \bmod p \rangle - \langle k^2 \bmod p \rangle - \langle l^2 \bmod p \rangle)$$

kifejezés osztható $2p$ -vel. Azt is tudjuk, hogy (3.3.2) abszolút értéke maximum $2p - 2$ lehet, mindenképpen kisebb $2p$ -nél. Mivel egyszerre osztható $2p$ -vel és kisebb nála, ezért igaz, hogy

$$(3.3.3) \quad \langle i^2 \bmod p \rangle + \langle j^2 \bmod p \rangle - \langle k^2 \bmod p \rangle - \langle l^2 \bmod p \rangle = 0.$$

$$(3.3.4) \quad \text{Innen tudjuk, hogy } i^2 - k^2 \equiv l^2 - j^2 \pmod{p}.$$

(3.3.3)-ból következik, hogy (3.3.1) első tagja, azaz $2p(i + j - k - l) = 0$, tehát $(i + j - k - l) = 0$. Ebből következik, hogy

$$(3.3.5) \quad i - k = l - j.$$

(3.3.4)-et át tudjuk alakítani nevezetes algebrai azonosság alapján:

$$(i - k)(i + k) \equiv (l - j)(l + j) \pmod{p}$$

(3.3.5) alapján helyettesítsünk:

$$(i - k)(i + k) \equiv (i - k)(l + j) \pmod{p}$$

Ha $i - k = 0$, akkor $i = k$, és így $l = j$, azaz $a_i + a_j = a_k + a_l$ azért igaz, mert ugyanazt a két tagot adtuk össze mindkét oldalon. Ha $i - k \neq 0$, akkor $(i - k, p) = 1$, ezért a kongruenciát leoszthatjuk:

$$(3.3.6) \quad (i + k) \equiv (l + j) \pmod{p}$$

(3.3.5)-ből és (3.3.6)-ból szeretnénk levonni következtetéseket az i, j, k, l -re. Vegyük észre, hogy $p = 2$ -re automatikusan működik a konstrukció, mivel bármely két szám egy Sidon-sorozatot alkot. Emiatt feltehető, hogy $p > 2$ prím. Először adjuk össze (3.3.5)-öt és (3.3.6)-ot:

$$i - k + i + k \equiv l - j + l + j \pmod{p}$$

$2i \equiv 2l \pmod{p}$ Mivel $p > 2$, tudjuk, hogy $(2, p) = 1$, ezért leoszthatunk 2-vel:

$$(3.3.7) \quad i \equiv l \pmod{p}$$

Tudjuk, hogy $0 \leq i, l \leq p - 1$, ezért (3.3.7)-ből következik, hogy $i = l$. Ezt összevetve (3.3.5)-tel adódik, hogy ekkor $j = k$.

Ezzel beláttuk, hogy $a_i + a_j = a_k + a_l$ esetén vagy $i = k$ és $j = l$, vagy $i = l$ és $j = k$, azaz a sorozat teljesíti a Sidon-tulajdonságot.

3.3.2. Megjegyzés. Vegyük észre, hogy ezzel bármely n -re beláttuk, hogy az $[1, n]$ intervallumon létezik egy közelítőleg $\sqrt{n/2}$ elemszámú Sidon-sorozat, hiszen mindig vehetjük az n -hez legközelebbi $2p^2 < n$ számot, és elkészíthetjük a konstrukció alapján a p elemű sorozatot. Elég nagy n -re ez a $2p^2$ alakú szám elég közel lesz n -hez, így ha n elég nagy, akkor bármely ε -ra igaz lesz az $s \geq (1 - \varepsilon)\sqrt{n/2}$ alsó becslés. Ez azért fog teljesülni, mert a prímszámtételből következik, hogy a szomszédos prímek hányadosa 1-hez tart.

A következő három tételben azt fogjuk látni, hogy ennél élesebb alsó becslést is tudunk adni s -re. 1941-ben Erdős Pál és Turán Pál megmutatta, hogy a Sidon-sorozat maximális elemszáma $\sqrt{n}$ nagyságrendű [7]. Ezt többek eredménye alapján, többféle módon bizonyíthatjuk. Most bizonyos n -ek mellett meg fogunk adni három különböző konstrukciót a Sidon-sorozat elemeinek meghatározására úgy, hogy egy legalább $\sqrt{n}$ elemszámú Sidon-sorozatot kapjunk. A 3.3.3. tétel James Singer eredménye 1938-ból [14]. A tétel nem közvetlenül a Sidon-sorozatokra vonatkozik, de ad egy konstrukciót, amely pont a $\sqrt{n}$ -es alsó becslést biztosítja.

3.3.3. Tétel. Legyen p tetszőleges prímszám. Ekkor létezik $p+1$ darab a_i , amelyekre az $a_i + a_j$ összegek nemcsak különbözőek, hanem páronként inkongruensek modulo $p^2 + p + 1$.

3.3.4. Megjegyzés. Abból, hogy az $a_i + a_j$ összegek páronként inkongruensek modulo $p^2 + p + 1$, következik, hogy ezek az összegek nem egyenlők, de fordítva ez nem következik. Vagyis a tétel az a_i -kre a Sidon-tulajdonságnál erősebbet követel.

3.3.5. Megjegyzés. A 3.3.3. tétel feltételeinek megfelelő $p+2$ darab a_i -t már nem lehet megadni.

Bizonyítás. (A 3.3.5. megjegyzés bizonyítása) Vegyünk összegek helyett különbségeket. Mivel $p^2 + p$ nemnulla maradékosztály van modulo $p^2 + p + 1$, ezért legfeljebb ennyi különböző különbség állhat elő $a_i - a_j$ alakban. Ha lenne $p+2$ darab a_i , akkor $(p+2)(p+1) = p^2 + 3p + 2$ különbség állna elő. De minden $p > 0$ -ra teljesül, hogy $p^2 + 3p + 2 > p^2 + p$. Így ha $p+2$ különböző a_i lenne, akkor több különbség lenne, mint maradékosztály, ami ellentmondás.

Bizonyítás. (A 3.3.3. tétel bizonyítása) A bizonyításban használjunk véges testeket. Legyen T_3 a p^3 elemű véges test. T_1 pedig legyen T_3 -nak a p elemű részteste. Mivel T_3 véges test, ezért létezik egy $\Delta \in T_3$ generátorelem, vagyis T_3 bármely nemnulla eleme előáll Δ^k alakban, ahol $k = 1, 2, \dots, (p^3 - 1)$. Ekkor $T_3 = T_1(\Delta)$, és ennek a testbővítésnek a foka 3.

$$T_3 = \{0, \Delta, \Delta^2, \dots, \Delta^{p^3-1}\}, \text{ ahol } \Delta^{p^3-1} = 1.$$

Ekkor T_1 nemnulla elemeit tekinthetjük mint a T_3 multiplikatív részcsoporthat, melynek generáló eleme Δ^n , azaz

$$T_1 = \{0, \Delta^n, \Delta^{2n}, \dots, \Delta^{(p-1)n}\}, \text{ ahol } n = \frac{p^3-1}{p-1} = p^2 + p + 1.$$

Nézhetjük a T_3 -at vektortérként T_1 felett. Ebben a vektortérben a skalárral való szorzás a T_1 -beli elemmel való szorzásnak felel meg, így $\Delta^i \in T_3$ és $\Delta^j \in T_3$ vektorok pontosan akkor lineárisan összefüggőek T_1 felett, ha van egy olyan $\Delta^{kn} \in T_1$, hogy

$$\Delta^i = \Delta^j \Delta^{kn}$$

$$\Delta^i = \Delta^{j+kn}$$

Ez pontosan akkor igaz, ha

$$(3.3.8) \quad i \equiv j \text{ modulo } n.$$

A következőkben szeretnénk megadni $p + 1$ darab a_i -t, amelyekről belátjuk, hogy az $a_i + a_j$ összegek páronként inkongruensek modulo n . Ehhez vegyünk egy tetszőleges Θ elemet, amely benne van T_3 -ban, de nincs benne T_1 -ben, azaz $\Theta \in T_3 \setminus T_1$. Vegyük észre, hogy mivel T_3 egy harmadfokú testbővítés T_1 felett, ezért Θ mindenképpen egy harmadfokú elem. Ezt a tulajdonságát később ki fogjuk használni. Jelöljük továbbá T_1 elemeit γ_i -vel.

A $\Theta + \gamma_i$ összeget mindig fel lehet írni Δ^{a_i} alakban, mert $\Theta \in T_3$ és $\gamma_i \in T_3$, valamint $\Theta + \gamma_i \neq 0$, hiszen $\Theta \notin T_1$. Tekintsük a következő összegeket $i = 1, \dots, p$ -re:

$$(3.3.9) \quad \Theta + \gamma_i = \Delta^{a_i}$$

Legyen továbbá $a_{p+1} = 0$. Ezzel kijelöltünk $p + 1$ darab a_i egész számot. Lássuk be, hogy ezek jók lesznek. Tegyük fel, hogy létezik i, j, k, l úgy, hogy $a_i + a_j \equiv a_k + a_l$ modulo n , ahol továbbra is $n = p^2 + p + 1$. Ekkor (3.3.8) miatt egy $\gamma \in T_1$ -re:

$$\Delta^{a_i+a_j} = \gamma \Delta^{a_k+a_l}$$

Ebből a hatványozás azonosságai miatt következik, hogy:

$$\Delta^{a_i} \Delta^{a_j} = \gamma \Delta^{a_k} \Delta^{a_l}$$

Használva (3.3.9)-et:

$$(\Theta + \gamma_i)(\Theta + \gamma_j) = \gamma(\Theta + \gamma_k)(\Theta + \gamma_l)$$

$$(3.3.10) \quad (\Theta + \gamma_i)(\Theta + \gamma_j) - \gamma(\Theta + \gamma_k)(\Theta + \gamma_l) = 0$$

(3.3.10) bal oldala Θ -nak egy legfeljebb másodfokú polinomja. Mivel Θ harmadfokú T_1 felett, így csak az lehetséges, hogy (3.3.10) bal oldala az azonosan 0 polinom. Innen $\gamma = 1$ és a gyöktényezős alak egyértelműsége miatt $\{\gamma_i, \gamma_j\} = \{\gamma_k, \gamma_l\}$. (3.3.9) miatt ekkor $\{a_i, a_j\} = \{a_k, a_l\}$ is teljesül. A bizonyítás ugyanígy működik akkor is, ha az $a_{p+1} = 0$ is szerepel a kijelölt a_i -k között. Ezzel beláttuk, hogy a kijelölt a_i -kre valóban igaz a tétel állítása.

3.3.6. Következmény (*Konstrukció: $n = p^2 + p + 1$ és $s = p + 1$*). A 3.3.3. tételben az a_i -k páronként inkongruensek, ezért p tetszőleges prímszám esetén $n = p^2 + p + 1$ -re létezik olyan Sidon-sorozat az $[1, n]$ intervallumon, amelynek $\lceil \sqrt{n} \rceil = p + 1$ eleme van.

3.3.7. Megjegyzés. Ekkor a 3.3.2. megjegyzésben kifejtett gondolatmenet alapján igaz lesz, hogy ha n elég nagy, akkor bármely ε -ra teljesül az $s \geq (1 - \varepsilon)\sqrt{n}$ alsó becslés az $[1, n]$ inter-

vallumon.

Ugyanezt az alsó becslést be lehet látni véges testek használata nélkül is. Erre mutatunk egy konstrukciót a 3.3.8. tétel bizonyításában, amely Ruzsa Imrétől származik [13].

3.3.8. Tétel (Konstrukció: $n = p^2 - p$ és $s = p - 1$). Legyen p tetszőleges prímszám. Ekkor létezik $p - 1$ darab olyan a_i , amelyekre az $a_i + a_j$ összegek páronként inkongruensek modulo $p^2 - p$. (Ekkor az $[1, p^2 - p]$ intervallumon készíthetünk egy $p - 1$ tagú Sidon-sorozatot.)

3.3.9. Megjegyzés. A tétel az a_i -kre a Sidon-tulajdonságnál erősebbet követel (lásd a 3.3.4. megjegyzést).

3.3.10. Megjegyzés. A 3.3.8. tétel feltételeinek megfelelő p darab a_i -t már nem lehet megadni.

Bizonyítás. (A 3.3.10. megjegyzés bizonyítása) Vegyünk összegek helyett különbségeket. Mivel $p^2 - p - 1$ nemnulla maradékosztály van modulo $p^2 - p$, ezért legfeljebb ennyi különböző különbség állhat elő $a_i - a_j$ alakban. Ha lenne p darab a_i , akkor $p(p - 1) = p^2 - p$ különbség állna elő. De minden $p > 0$ -ra teljesül, hogy $p^2 - p > p^2 - p - 1$. Így ha p különböző a_i lenne, akkor több különbség lenne, mint maradékosztály, ami ellentmondás.

Bizonyítás. (A 3.3.8. tétel bizonyítása) Legyen g primitív gyök modulo p . Ekkor igaz, hogy a $g, g^2, \dots, g^{p-1}$ hatványok különböző maradékot adnak modulo p . Defináljuk a $p - 1$ darab a_i -t a következőképpen: a_1 legyen az

$$x \equiv 1 \text{ modulo } p - 1$$

$$x \equiv g \text{ modulo } p$$

szimultán kongruenciarendszer megoldása modulo $p(p - 1)$, a_2 legyen az

$$x \equiv 2 \text{ modulo } p - 1$$

$$x \equiv g^2 \text{ modulo } p$$

szimultán kongruenciarendszer megoldása modulo $p(p - 1)$, és így tovább. Azaz általánosan felírva: a_i legyen az

$$(3.3.11) \quad x \equiv i \text{ modulo } p - 1$$

$$(3.3.12) \quad x \equiv g^i \text{ modulo } p$$

szimultán kongruenciarendszer megoldása modulo $p(p-1)$, ha $i = 1, 2, \dots, p-1$. (3.3.11) miatt $a_i \not\equiv a_j$ modulo $p(p-1)$, ha $i \neq j$, azaz mind különbözőek lesznek.

Elég azt belátni, hogy $1 \leq i, j, k, l \leq p-1$ esetén nem lehet az, hogy $a_i + a_j \equiv a_k + a_l$ modulo $p(p-1)$. Ha $c \equiv a_i + a_j$ modulo $p(p-1)$, akkor (3.3.11) és (3.3.12) miatt tudjuk, hogy a következő két kongruencia teljesül:

$$(3.3.13) \quad c \equiv i + j \text{ modulo } (p-1)$$

$$(3.3.14) \quad c \equiv g^i + g^j \text{ modulo } p$$

(3.3.13)-ból adódik:

$$(3.3.15) \quad g^c \equiv g^i g^j \text{ modulo } p$$

(3.3.14) megadja a g^i, g^j számok összegét, (3.3.15) pedig a szorzatát modulo p . Vegyük azt a $z^2 + Bz + C \equiv 0$ modulo p másodfokú kongruenciát, amelynek a g^i és a g^j maradékosztályok a gyökei. Mivel modulo p tulajdonképpen egy test felett számolunk, és így minden elemnek létezik inverze, $p > 2$ -re működik a szokásos másodfokú megoldóképlet, és igazak az ismert összefüggések is. A gyökök és együtthatók közötti összefüggésekből, illetve (3.3.14) és (3.3.15) kongruenciákból következik, hogy ekkor $B = -c$ és $C = g^c$, azaz az egyenletet átírva:

$$(3.3.16) \quad z^2 - cz + g^c \equiv 0 \text{ modulo } p$$

(3.3.16) másodfokú kongruenciának legfeljebb egy $\{g^i, g^j\}$ pár lehet a megoldása, amiből következik, hogy $c \equiv a_i + a_j$ modulo $p(p-1)$ is legfeljebb egy $\{i, j\}$ párra teljesülhet. Ezzel a tétel állítását beláttuk.

A következő tételben ugyanerre az alsó becslésre adunk egy harmadik bizonyítást, amely a 3.3.3 tételhez hasonlóan szintén a véges testeket használja fel. Ezt a bizonyítást később ki fogjuk terjeszteni kéttagú összegekről többtagú összegekre (lásd a 3.5. szakaszt). A tétel Sarvadaman Chowla eredménye 1962-ből [2].

3.3.11. Tétel (*Konstrukció: $n = p^2 - 1$ és $s = p$*). Legyen p tetszőleges prímszám. Mutassuk meg, hogy ekkor létezik p darab olyan a_i , amelyekre az $a_i + a_j$ összegek páronként inkongruensek modulo $p^2 - 1$.

3.3.12. Megjegyzés. A tétel az a_i -kre a Sidon-tulajdonságnál erősebbet követel (lásd a 3.3.4. megjegyzést).

3.3.13. Megjegyzés. A 3.3.11. tétel feltételeinek megfelelő $p + 1$ darab a_i -t már nem lehet megadni.

Bizonyítás. (A 3.3.13. megjegyzés bizonyítása) Vegyünk összegek helyett különbségeket. Mivel $p^2 - 2$ nemnulla maradékosztály van modulo $p^2 - 1$, ezért legfeljebb ennyi különböző különbség állhat elő $a_i - a_j$ alakban. Ha lenne $p + 1$ darab a_i , akkor $p(p + 1) = p^2 + p$ különbség állna elő. De minden $p > 0$ -ra teljesül, hogy $p^2 + p > p^2 - 2$. Így ha $p + 1$ különböző a_i lenne, akkor több különbség lenne, mint maradékosztály, ami ellentmondás.

Bizonyítás. (A 3.3.11. tétel bizonyítása) A 3.3.3. tétel bizonyításához hasonlóan fogunk eljárni. Legyen T_2 a p^2 elemű véges test. T_2 -nek a p elemű résztestét jelölje T_1 . Legyen $\Delta \in T_2$ generátorelem. Ekkor $T_2 = T_1(\Delta)$, és ez egy másodfokú testbővítés. Legyen $T_1 = \{\gamma_1, \gamma_2, \dots, \gamma_p\}$, és legyen $\Theta \in T_2 \setminus T_1$ egy másodfokú elem. Vegyük a következő összegeket $i = 1, 2, \dots, p$ -re:

$$(3.3.17) \quad \Theta + \gamma_i = \Delta^{a_i}$$

Ezek az összegek mind különbözőek lesznek, így (3.3.17) megad p darab a_i -t, melyekre $1 \leq a_i \leq p^2 - 1$ teljesül. Azt szeretnénk megmutatni, hogyha ezek közül bárhogyan választva képezünk $a_i + a_j$ összegeket, akkor ezek az összegek mindig páronként inkongruensek lesznek modulo $p^2 - 1$.

Tegyük fel, hogy létezik i, j, k, l , hogy $a_i + a_j \equiv a_k + a_l$ modulo $p^2 - 1$. Ez a generátorelem tulajdonságai és (3.3.17) miatt pontosan azt jelenti, hogy:

$$\Delta^{a_i + a_j} = \Delta^{a_k + a_l}$$

A hatványazonosság alapján ebből:

$$\Delta^{a_i} \Delta^{a_j} = \Delta^{a_k} \Delta^{a_l}$$

(3.3.17) alapján ezt át tudjuk írni, és rendezni tudjuk Θ szerint:

$$(3.3.18) \quad (\Theta + \gamma_i)(\Theta + \gamma_j) = (\Theta + \gamma_k)(\Theta + \gamma_l)$$

$$(3.3.19) \quad \Theta^2 + (\gamma_i + \gamma_j)\Theta + \gamma_i\gamma_j - \Theta^2 - (\gamma_k + \gamma_l)\Theta - \gamma_k\gamma_l = 0$$

(3.3.19)-ből Θ^2 kiesik, így:

$$(3.3.20) \quad \Theta(\gamma_i + \gamma_j - \gamma_k - \gamma_l) + \gamma_i \gamma_j - \gamma_k \gamma_l = 0$$

(3.3.20) a Θ -nak egy legfeljebb elsőfokú polinomja. Mivel Θ másodfokú T_1 felett, így (3.3.20) bal oldala csak az azonosan 0 polinom lehet. (3.3.18)-ból a gyöktényezős alak egyértelműsége miatt $\{\gamma_i, \gamma_j\} = \{\gamma_k, \gamma_l\}$, ahol $i = j$ is megengedett. Ebből következik, hogy $\{i, j\} = \{k, l\}$, ami pont azt jelenti, hogy $\{a_i, a_j\} = \{a_k, a_l\}$. Ezzel beláttuk a tétel állítását.

3.4. Alsó és felső becslés általános n -re

Eddig láttuk, hogy a 3.3.3., 3.3.8. és a 3.3.11. tételből is következik, hogy az $[1, n]$ intervallumon $s \geq (1 - \varepsilon)\sqrt{n}$ (lásd a 3.3.7. megjegyzést). Ez úgy értendő, hogy bármely ε -hoz tudunk venni egy n_0 -t úgy, hogy minden $n > n_0$ -ra az $[1, n]$ intervallumon teljesüljön az alsó becslés s -re. A következő tétel ennél erősebbet állít, mégpedig azt, hogy bármely elég nagy n -re $s \geq \sqrt{n} - n^{0,27}$. Ennek egy 0,27-nél kicsivel nagyobb kitevős változatát Erdős mellett Chowla is megmutatta már 1944-ben [1].

3.4.1. Tétel. Ha n elég nagy, akkor létezik olyan Sidon-sorozat az $[1, n]$ intervallumon, amelynek legalább $n^{1/2} - n^{0,27}$ eleme van.

Bizonyítás. A 3.3.3. tétel bizonyításában szereplő konstrukciót szeretnénk alkalmazni egy megfelelő p -re. Ez a konstrukció $p + 1$ darab elemet ad meg nekünk. Válasszuk ki a p -t úgy, hogy a lehető legnagyobb legyen, amire teljesül, hogy $p^2 + p + 1 \leq n$. Ha látnánk, hogy erre a p -re mindig teljesül, hogy $p > n^{1/2} - n^{0,27}$, akkor készen lennénk, mert ekkor a konstrukciónk által megadott $p + 1$ elem legalább $n^{1/2} - n^{0,27}$ elem lenne. A következő tételt bizonyítás nélkül fogjuk felhasználni ennek megmutatásához [11].

Tétel. Minden elég nagy n -re létezik prímszám n és $n + n^{0,525}$ között.

A tétel segítségével belátjuk, hogy elég nagy n -re mindig létezik prímszám $n^{1/2} - n^{0,27}$ és $n^{1/2}$ között, vagyis valóban mindig teljesül, hogy $p > n^{1/2} - n^{0,27}$. Legyen $k = n^{1/2} - n^{0,27}$. Ekkor elég belátnunk, hogy $k + k^{0,525} < n^{1/2}$ teljesül, hiszen ez pont azt jelenti, hogy biztosan fog létezni prímszám k és $n^{1/2}$ között.

$$(3.4.1) \quad k + k^{0,525} = n^{1/2} - n^{0,27} + (n^{1/2} - n^{0,27})^{0,525} < n^{1/2}$$

Átrendezve:

$$(n^{1/2} - n^{0,27})^{0,525} < n^{0,27}$$

Az exponenciális függvény monoton növekedése miatt ekkor:

$$(n^{1/2} - n^{0,27})^{0,525} < (n^{1/2})^{0,525} = n^{0,2625} < n^{0,27}$$

Tehát a (3.4.1) egyenlőtlenség valóban teljesül minden elég nagy n -re. Ezzel a tétel állítását beláttuk.

Erdős és Turán 1941-ben, majd más bizonyítással Bernt Lindström 1969-ben azt is megmutatta, hogy legfeljebb mennyi lehet az s értéke [7] [12]. (Ugyanezt a felső becslést 1993-ban Ruzsa Imre is belátta más megközelítésből [13].) Az alábbiakban részletesen feldolgozzuk Erdős és Turán bizonyítását.

3.4.2. Tétel. Az $[1, n]$ intervallumba eső Sidon-sorozat elemszáma maximum $n^{1/2} + n^{1/4} + 1$.

Bizonyítás. Legyen az S Sidon-sorozat elemszáma s , és legyen t egy bizonyos alkalmas egész szám, amelyet később fogunk meghatározni. Vegyünk egy $t - 1$ hosszúságú intervallumot és toljuk végig a $[0, n]$ intervallumon úgy, hogy egy-egy lépésben a következő intervallumokat fedje le:

$$I_1 = [-t + 1, 0], I_2 = [-t + 2, 1], \dots, I_{n+t} = [n, n + t - 1]$$

Legyen A_i az I_i intervallumba eső sorozatelemeknek a száma. Amikor végigtoljuk az intervallumunkat és minden lépésben összeadjuk az intervallum által lefedett részen levő sorozatelemeknek a számát, akkor minden elemet t -szer számolunk meg, vagyis:

$$(3.4.2) \quad \sum_{i=1}^{n+t} A_i = ts$$

Mivel a sorozatunk rendelkezik a Sidon-tulajdonsággal, ezért bármely két elemének a különbsége különböző. Legyen D azon $\{a_i, a_j\}, i \neq j$ elempároknak a száma multiplicitással számolva, amelyek egy intervallumba esnek. Az, hogy multiplicitással számoljuk össze őket, azt jelenti, hogy mindegyik $\{a_i, a_j\}$ párt annyiszor számolunk, ahány intervallumba a_i és a_j együtt beleesik. Ekkor

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

$$\text{Mivel } \binom{A_i}{2} = \frac{A_i!}{2!(A_i - 2)!} = \frac{A_i(A_i - 1)}{2} = \frac{A_i^2 - A_i}{2} = \frac{A_i^2}{2} - \frac{A_i}{2}, \text{ így}$$

$$(3.4.3) \quad D = \sum_{i=1}^{n+t} \frac{A_i^2}{2} - \sum_{i=1}^{n+t} \frac{A_i}{2}$$

Legyen a_i és a_j két elem a sorozatunkból, $a_i - a_j = d$. Mivel a_i és a_j között $d - 1$ egész szám van, a_i és a_j együtt pontosan $(t - 1) - (d - 1) = t - d$ darab intervallumban lesz benne. Minden d maximum egyszer állhat elő, hiszen Sidon-sorozatáról van szó. Továbbá azt is vegyük észre, hogy a $(t - 1)$ -nél nagyobb különbségű elempárok nem tudnak beleesni egyetlen intervallumba sem. Így az előző D -t tudjuk felülről becsülni az 1-től $t - 1$ -ig vett egész számok összegével:

$$(3.4.4) \quad D \leq \sum_{d=1}^{t-1} (t - d) = \frac{t(t - 1)}{2}$$

(3.4.3)-ból és (3.4.4)-ből következik, hogy:

$$(3.4.5) \quad \sum_{i=1}^{n+t} A_i^2 - \sum_{i=1}^{n+t} A_i \leq t(t - 1)$$

A számtani és négyzetes közepek közötti egyenlőtlenség alapján tudjuk, hogy:

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

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

$$(3.4.6) \quad \sum_{i=1}^{n+t} A_i^2 \geq \frac{(\sum_{i=1}^{n+t} A_i)^2}{n + t}$$

Így (3.4.2), (3.4.5) és (3.4.6) alapján tovább tudunk becsülni:

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

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

Rendezzük 0-ra, majd szorozzunk $(n + t)$ -vel és osszunk t^2 -tel:

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

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

$$(3.4.7) \quad s^2 - s\left(\frac{n}{t} + 1\right) - \left(\frac{n}{t} + 1\right)(t - 1) \leq 0$$

(3.4.7) másodfokú egyenlőtlenséget megoldva s -re a következő becslést kapjuk:

$$(3.4.8) \quad s \leq \frac{n}{2t} + \frac{1}{2} + \sqrt{n + t + \frac{n^2}{4t^2} - \frac{n}{2t} - \frac{3}{4}}$$

Válasszuk meg t -t úgy, hogy (3.4.8) jobb oldala a lehető legkisebb legyen. Minél nagyobb számnak választjuk t -t, az $n/2t$ értéke annál kisebb, ugyanakkor a négyzetgyök értéke annál nagyobb lesz. Ha t kisebb nagyságrendű, mint $n^{3/4}$, akkor $n/2t$ biztosan nagyobb nagyságrendű lesz, mint $n^{1/4}$. Vagyis t -t nem választhatjuk $n^{3/4}$ -nél kisebb nagyságrendűnek. Viszont ha $n^{3/4}$ -nél nagyobb nagyságrendűnek választjuk, akkor a négyzetgyök értékének nagyságrendje már nagyobb lehet $n^{1/2}$ -nél. Mivel t -nek egész számnak kell lennie, legyen $t = \lfloor n^{3/4} \rfloor + 1$.

Becsüljük felülről (3.4.8) jobb oldalát $t = \lfloor n^{3/4} \rfloor + 1$ esetén. Mivel ekkor $t \geq n^{3/4}$, így a következő teljesül:

$$(3.4.9) \quad \frac{n}{2t} \leq \frac{n}{2n^{3/4}} = \frac{1}{2}n^{1/4}$$

A gyökjel alatt az első t helyére írjunk $n^{3/4} + 1$ -et, a nevezőkben pedig $n^{3/4}$ -et. Így a gyökös kifejezés értékét növeltük.

$$(3.4.10) \quad \sqrt{n + n^{3/4} + 1 + \frac{n^2}{4n^{3/2}} - \frac{n}{2n^{3/4}} - \frac{3}{4}} = \sqrt{n + n^{3/4} + 1 + \frac{1}{4}n^{1/2} - \frac{1}{2}n^{1/4} - \frac{3}{4}}$$

Mivel igaz, hogy

$$1 - \frac{3}{4} - \frac{1}{2}n^{1/4} < 0, \text{ ha } n \geq \left(\frac{1}{2}\right)^4 = \frac{1}{16},$$

(3.4.10)-et tovább növelhetjük $1 - \frac{3}{4} - \frac{1}{2}n^{1/4}$ elhagyásával.

$$(3.4.11) \quad \sqrt{n + n^{3/4} + 1 + \frac{1}{4}n^{1/2} - \frac{1}{2}n^{1/4} - \frac{3}{4}} \leq \sqrt{n + n^{3/4} + \frac{1}{4}n^{1/2}} = \sqrt{n} + \frac{1}{2}n^{1/4}$$

(3.4.9) és (3.4.11) alapján $t = \lfloor n^{3/4} \rfloor + 1$ esetén teljesül, hogy

$$\begin{aligned} s &\leq \frac{n}{2t} + \frac{1}{2} + \sqrt{n + t + \frac{n^2}{4t^2} - \frac{n}{2t} - \frac{3}{4}} \leq \frac{n^{1/4}}{2} + \frac{1}{2} + \sqrt{n} + \frac{n^{1/4}}{2} = \\ &= n^{1/2} + n^{1/4} + \frac{1}{2} \leq n^{1/2} + n^{1/4} + 1 \end{aligned}$$

Ezzel a tétel állítását beláttuk.

3.5. Többtagú összegek

A Sidon-problémát szeretnénk többtagú összegekre általánosítani.

3.5.1. Definíció. Az $a_1 < a_2 < \dots$ sorozatra igaz a Sidon-tulajdonság általánosítása h tagra, ha minden i esetén $a_i \in \mathbb{N}$ és az $a_{i_1} + \dots + a_{i_h}$ összegek mind különbözőek, azaz bárhogyan veszünk ki h elemet a sorozatból, azok összege mindig különböző lesz.

A következő állításban egy alsó becslést adunk az ilyen sorozatok elemszámára. Az állítás bizonyítása a 3.3.11. tétel bizonyításának általánosítása lesz Chowla eredményei alapján [2].

3.5.2. Állítás. Legyen $h \geq 2$ rögzített természetes szám, és vegyünk az olyan sorozatokat az $[1, n]$ intervallumon, amelyekre igaz, hogy az elemeikből képzett h -tagú összegek mind különbözőek. Ekkor ezek között létezik olyan A sorozat, amelynek körülbelül $n^{1/h}$ eleme van.

Bizonyítás. A 3.3.3. és a 3.3.11. tétel bizonyításához hasonlóan fogunk eljárni. Legyen T_h a p^h elemű véges test. T_h -nak a p elemű résztestét jelölje T_1 . Legyen $\Delta \in T_h$ a multiplikatív csoport generátoreleme. Ekkor $T_h = T_1(\Delta)$ és ez egy h -adfokú testbővítés, tehát Δ foka h . Legyen $T_1 = \{\gamma_1, \gamma_2, \dots, \gamma_p\}$. A két korábbi hasonló bizonyítással ellentétben most nem tetszőleges $\Theta \in T_h \setminus T_1$ elemet választunk, hanem a $\Delta \in T_h \setminus T_1$ elemet választjuk. A tetszőleges Θ elem foka lehet kisebb is, mint h , hiszen $T_1(\Theta)$ lehet egy T_h -nál szűkebb egyszerű bővítése T_1 -nek. Viszont Δ biztosan h -adfokú T_1 felett. Ezt a tulajdonságát később használni fogjuk. Vegyük a következő összegeket $i = 1, 2, \dots, p$ -re:

$$(3.5.1) \quad \Delta + \gamma_i = \Delta^{a_i}$$

Mivel a γ_i -k különbözőek, ezek az összegek mind különbözőek lesznek. Ez megad p darab a_i -t, amelyekre teljesül, hogy $1 \leq a_i \leq p^h - 1$. Azt szeretnénk megmutatni, hogy ezek közül bárhogyan választva képezünk h tagú $a_{i_1} + a_{i_2} + \dots + a_{i_h}$ összegeket, ezek az összegek minden esetben páronként inkongruensek lesznek modulo $p^h - 1$.

Tegyük fel, hogy létezik $\{i_1, i_2, \dots, i_h\}$ és $\{j_1, j_2, \dots, j_h\}$ úgy, hogy

$$(3.5.2) \quad a_{i_1} + a_{i_2} + \dots + a_{i_h} \equiv a_{j_1} + a_{j_2} + \dots + a_{j_h} \text{ modulo } p^h - 1$$

Megmutatjuk, hogy ekkor a két multihalmaz egyenlő. (Multihalmazok, mert egy elem többször is előfordulhat bennük.)

A Δ generátorelem generálja T_h multiplikatív csoportját, amely egy $p^h - 1$ rendű ciklikus csoport. Emiatt tudjuk, hogy pontosan akkor igaz, hogy $\Delta^n = \Delta^m$, ha $n \equiv m$ modulo $p^h - 1$. Ebből következik, hogy (3.5.2) összevetve (3.5.1)-gyel azt jelenti, hogy

$$\Delta^{a_{i_1}+a_{i_2}+\dots+a_{i_h}} = \Delta^{a_{j_1}+a_{j_2}+\dots+a_{j_h}}$$

A hatványazonosság alapján ebből következik, hogy:

$$\Delta^{a_{i_1}} \Delta^{a_{i_2}} \dots \Delta^{a_{i_h}} = \Delta^{a_{j_1}} \Delta^{a_{j_2}} \dots \Delta^{a_{j_h}}$$

(3.5.1) alapján ezt át tudjuk írni, és rendezni tudjuk Δ szerint:

$$(3.5.3) \quad (\Delta + \gamma_{i_1})(\Delta + \gamma_{i_2}) \dots (\Delta + \gamma_{i_h}) = (\Delta + \gamma_{j_1})(\Delta + \gamma_{j_2}) \dots (\Delta + \gamma_{j_h})$$

$$(\Delta + \gamma_{i_1})(\Delta + \gamma_{i_2}) \dots (\Delta + \gamma_{i_h}) - (\Delta + \gamma_{j_1})(\Delta + \gamma_{j_2}) \dots (\Delta + \gamma_{j_h}) = 0$$

$$(3.5.4) \quad \Delta^h + (\gamma_{i_1} + \dots + \gamma_{i_h})\Delta^{h-1} + \dots - \Delta^h - \dots = 0$$

(3.5.4)-ből kiesik Δ^h , így (3.5.3) Δ -nak egy maximum $(h - 1)$ -edfokú polinomja. Mivel Δ h -adfokú T_1 felett, ezért (3.5.3) bal oldala csak az azonosan 0 polinom lehet. A (3.5.3) alakból a gyöktényezős alak egyértelműsége miatt következik, hogy $\{i_1, i_2, \dots, i_h\} = \{j_1, j_2, \dots, j_h\}$. Azaz a h -tagú összegek páronként inkongruensek modulo $p^h - 1$. A prímszámtétel segítségével (lásd a 3.3.2. és a 3.3.7. megjegyzést) ebből következik, hogy létezik A sorozat az $[1, n]$ intervallumban, amelynek körülbelül $n^{1/h}$ tagja van. Ezzel az állítást beláttuk.

3.5.3. Egyszerű felső becslés. A kéttagú összegek mintájára a többtagú összegek esetén is tudunk egyszerű felső becslést adni a sorozat elemszámára. Legyen a sorozatunknak s tagja. Mindegyikre igaz, hogy $a_i \in [1, n]$. Ebből következik, hogy $a_{i_1} + \dots + a_{i_h} \in [h, hn]$. Az s elemből hány h tagú összeget lehet készíteni, ha lehet ismétlődés is az elemek között? Ehhez használjuk az ismétléses kombinációt.

$$\binom{s+h-1}{h} = \frac{(s+h-1)!}{h!(s-1)!}$$

Mivel az összegek mind kisebbek, mint hn , ezért:

$$(3.5.5) \quad \frac{(s+h-1)!}{h!(s-1)!} < hn$$

(3.5.5) bal oldalát szeretnénk alulról becsülni, ehhez a számlálót csökkentjük:

$$\frac{(s+h-1)!}{h!(s-1)!} = \frac{(s+h-1)(s+h-2)\dots \cdot s}{h!} > \frac{s^h}{h!}$$

Ezt összevetve (3.3.5)-tel azt kapjuk, hogy:

$$\frac{s^h}{h!} < hn$$

$$s < \sqrt[h]{h!hn} = c\sqrt[h]{n}, \text{ ahol } c = \sqrt[h]{h!h}$$

Vegyük észre, hogy a 3.2.1. pontban ugyanezt a becslést megkaptuk a $h = 2$ esetre.

3.6. Végtelen Sidon-sorozatok

Jelölés. Jelölje $A(n)$ az A végtelen Sidon-sorozat elemszámát az $[1, n]$ intervallumon.

A következőkben $A(n)$ -ről szeretnénk megállapításokat tenni. A 3.6.1. feladat állítását Erdős és Turán már 1941-ben belátták [7].

3.6.1. Feladat. Konstruáljunk olyan A végtelen Sidon-sorozatot, amelyre bármely $\varepsilon > 0$ esetén végtelen sok n -re

$$(3.6.1) \quad A(n) > \left(\frac{1}{\sqrt{2}} - \varepsilon\right)\sqrt{n}$$

3.6.2. Megjegyzés. Fontos megjegyezni, hogy nem egy erős alsó becslést szeretnénk belátni, amely minden n -re teljesül, hanem az a célunk, hogy találjunk végtelen sok n -et, amelyre igaz a (3.6.1). Így elég nekünk, ha a végtelen Sidon-sorozatunk végtelen sok helyen elég sűrű, máshol pedig ritkább is lehet.

Megoldás. Válasszunk egy n_1 -et úgy, hogy legyen $n_1 = p^2 + p + 1$, így a 3.3.4. következmény szerint létezik az $[1, n_1]$ intervallumon hozzávetőlegesen $\sqrt{n_1}$ elemszámú Sidon-sorozat, ezt jelölje S_1 . Válasszuk n_2 -t úgy, hogy $n_2 \gg n_1$, azaz n_2 legyen jóval nagyobb, mint n_1 . Az $[n_1 + 1, n_1 + n_2]$ intervallumból ne válasszunk ki semmit, de az $[n_1 + n_2 + 1, n_1 + 2n_2]$ intervallumból megint válasszunk ki elemeket. Mivel az $[n_1 + n_2 + 1, n_1 + 2n_2]$ intervallumban n_2 elem van, innen ki tudunk választani egy körülbelül $\sqrt{n_2}$ elemszámú Sidon-tulajdonságú halmazt. (Ezt megtehetjük, mert ugyan eddig csak azt láttuk, hogy az $[1, n]$ intervallumból ki tudunk választani egy körülbelül $\sqrt{n}$ elemű Sidon-sorozatot, de az is igaz, hogyha ennek a sorozatnak az a_i tagjait bármely konstanssal eltoljuk, akkor az n elemű $[1 + t, n + t]$ intervallumon vett $a_i + t$ tagokból álló sorozat egy körülbelül $\sqrt{n}$ elemszámú Sidon-halmazt

alkot.) Ezt a Sidon-tulajdonságú halmazt jelöljük S_2^* -gal. S_2^* halmazból hagyjuk el azokat a párokat, amelyekben a tagok különbsége kisebb, mint n_1 . S_2^* Sidon-tulajdonsága miatt az elemeiből alkotott párok tagjainak különbsége mind különböző, így kevesebb, mint n_1 olyan pár lehet benne, amelyek különbsége kisebb, mint n_1 . Ebből következik, hogy biztosan kevesebb, mint $2n_1$ elemet hagyunk el. A módosított S_2^* -ot jelölje S_2 . Vegyük észre, hogy az $[1, n_1 + 2n_2]$ intervallumból hozzávetőleg $\sqrt{n_1} + \sqrt{n_2} - 2n_1$ elemet választottunk ki. Mivel $n_2 \gg n_1$, ez nagyságrendileg $\sqrt{n_2}$ elemet jelent.

Először azt szeretnénk látni, hogy $n = n_1 + 2n_2$ esetén a $\sqrt{n_2}$ elem valóban legalább annyi, mint amennyit a feladat állít, azaz teljesül a következő egyenlőtlenség:

$$A(n_1 + 2n_2) \approx \sqrt{n_2} > \left(\frac{1}{\sqrt{2}} - \varepsilon\right)\sqrt{n_1 + 2n_2}$$

Mivel feltettük, hogy $n_2 \gg n_1$, így $n_1 + 2n_2 \approx 2n_2$, amiből következik, hogy $\sqrt{n_1 + 2n_2} \approx \sqrt{2n_2}$. Ezt kihasználva:

$$\sqrt{n_2} > \left(\frac{1}{\sqrt{2}} - \varepsilon\right)\sqrt{2n_2}$$

$$\sqrt{n_2} > \frac{\sqrt{2n_2}}{\sqrt{2}} - \varepsilon\sqrt{2n_2}$$

$$\sqrt{n_2} > \sqrt{n_2} - \varepsilon\sqrt{2n_2}$$

Azt is feltettük, hogy $\varepsilon > 0$, amiből következik, hogy a jobb oldalon $\sqrt{n_2}$ értékét mindig egy valóban pozitív számmal csökkentjük, vagyis az egyenlőtlenség teljesül.

Ezenkívül azt kellene látnunk, hogy ezekre az elemekre teljesül a Sidon-tulajdonság, vagyis Sidon-sorozatot alkotnak. Azt tudjuk, hogy S_1 -re és S_2 -re külön-külön teljesül a Sidon-tulajdonság, azt kellene látni, hogy $S_1 \cup S_2$ -re is teljesül. Legyen $k_1 < k_2 < k_3 < k_4$ az $S_1 \cup S_2$ négy különböző eleme. Azt kell belátni, hogy $k_1 + k_4 \neq k_2 + k_3$, azaz

$$(3.6.2) \quad k_4 - k_3 \neq k_2 - k_1$$

Első eset: Ha $k_1, k_2, k_3, k_4 \in S_1$, akkor teljesül (3.6.2), mert S_1 Sidon. Ugyanígy ha $k_1, k_2, k_3, k_4 \in S_2$, akkor is teljesül (3.6.2), mert S_2 is Sidon.

Második eset: Legyen $k_1, k_2, k_3 \in S_1$ és $k_4 \in S_2$. Ekkor teljesül, hogy $k_4 - k_3 > n_2 > k_2 - k_1$, vagyis igaz (3.6.2).

Harmadik eset: Legyen $k_1, k_2 \in S_1$ és $k_3, k_4 \in S_2$. Ekkor $k_2 - k_1 \in [1, n]$. Mivel S_2 -t úgy készítettük, hogy ne legyen benne olyan elempár, amelyben a tagok különbsége az $[1, n]$

intervallumba esik, ezért biztos, hogy (3.6.2) teljesül.

Negyedik eset: Legyen $k_1 \in S_1$ és $k_2, k_3, k_4 \in S_2$. Ekkor igaz, hogy $k_2 - k_1 > n_2 > k_4 - k_3$, így (3.6.2) biztosan teljesül.

Ez a négy eset az összes lehetőséget tartalmazza. A négy esetet megvizsgálva beláttuk, hogy az $S_1 \cup S_2$ -re valóban teljesül a Sidon-tulajdonság.

Ezután ismételjük meg ugyanezt az eljárást: válasszunk egy n_3 -at, amely jóval nagyobb, mint $n_1 + 2n_2$. Az $[n_1 + 2n_2 + 1, n_1 + 2n_2 + n_3]$ intervallumból ne válasszunk ki semmit, majd az $[n_1 + 2n_2 + n_3 + 1, n_1 + 2n_2 + 2n_3]$ intervallumból válasszunk ki egy $\sqrt{n_3}$ elemű Sidon-halmazt. Hagyjuk el S_3 -ból azokat az elempárokat, amelyekben a tagok különbsége kisebb, mint $n_1 + 2n_2$, az így újonnan hozzávett elemeket jelölje S_3 . Így az $[1, n_1 + 2n_2 + 2n_3]$ intervallumból kiválasztottunk körülbelül $\sqrt{n_1} + \sqrt{n_2} - 2n_1 + \sqrt{n_3} - 2(n_1 - 2n_2)$ elemet. Mivel $n_3 \gg n_2$, ez hozzávetőleg $\sqrt{n_3}$ elem. Az előzőekhez hasonlóan belátható, hogy az $S_1 \cup S_2 \cup S_3$ is Sidon tulajdonságú. Ezt tovább folytatva kapunk egy végtelen Sidon-sorozatot, amelyre igaz (3.6.1).

Azt már a véges Sidon-sorozatok vizsgálatából tudjuk, hogy $A(n)$ semmilyen n -re nem lehet sokkal nagyobb, mint $\sqrt{n}$, ezzel a feladattal pedig beláttuk, hogy $A(n)$ végtelen sokszor nagyon közel lehet $\sqrt{n}$ -hez. A következő tétel azt állítja, hogy ez nem lesz igaz minden n -re, mert biztos, hogy $A(n)$ végtelen sokszor jóval kisebb lesz, mint $\sqrt{n}$. Ennek bizonyítása a *Számelmélet* tankönyvben lévő bizonyítás részletezése [11].

3.6.3. Tétel. Legyen A végtelen Sidon-sorozat. Ekkor szükségképpen igazak A -ra a következők:

- (a) $\liminf_{n \rightarrow \infty} \frac{A(n)}{\sqrt{n}} = 0$
- (b) $\liminf_{n \rightarrow \infty} \frac{A(n)}{\sqrt{n/\log n}} < \infty$, ahol $\log n$ az n szám természetes alapú logaritmus.

3.6.4. Megjegyzés. Vegyük észre, hogy (b)-ből következik (a). A (b) azt jelenti, hogy létezik $c > 0$ konstans úgy, hogy végtelen sok n -re teljesül a következő:

$$\frac{A(n)}{\sqrt{n/\log n}} \leq c$$

Ezekre az n -ekre:

$$A(n) \leq c \frac{\sqrt{n}}{\sqrt{\log n}}$$

$$\frac{A(n)}{\sqrt{n}} \leq c \frac{1}{\sqrt{\log n}}$$

Ennek a jobb oldala n tart végtelen esetén nullához tart. Ebből az következik, hogy teljesül az (a).

Bizonyítás. (A 3.6.3. tétel bizonyítása) Legyen A egy tetszőleges végtelen Sidon-sorozat, N egy elég nagy természetes szám. Jelölje A_i azt, hogy az A -nak hány eleme van a $T_i = [(i-1)N+1, iN]$ intervallumban. A korábbi jelölést használva ekkor

$$(3.6.3) \quad A_i = A(iN) - A((i-1)N), \text{ ahol } i = 1, 2, \dots, N$$

T_i -n belül bármely két elem különbsége kisebb, mint N , azaz maximum $N-1$ különböző különbség van, és a Sidon-tulajdonság miatt nem állhat elő egy különbség egynél többször, így

$$(3.6.4) \quad \sum_{i=1}^N \binom{A_i}{2} < N$$

A bal oldalt kifejtve:

$$\sum_{i=1}^N \binom{A_i}{2} = \sum_{i=1}^N \frac{A_i!}{2(A_i-2)!} = \sum_{i=1}^N \frac{A_i(A_i-1)}{2}$$

Amiből (3.6.4) miatt:

$$(3.6.5) \quad \sum_{i=1}^N A_i(A_i-1) < 2N$$

Mivel $A_i \neq 0$ esetén $A_i \geq 1$, ezért $A_i \geq \frac{1}{2}(A_i+1)$, így:

$$(3.6.6) \quad \sum_{i=1}^N A_i(A_i-1) \geq \sum_{i=1}^N \frac{1}{2}(A_i+1)(A_i-1) = \frac{1}{2} \sum_{i=1}^N (A_i^2 - 1)$$

(3.6.6) $A_i = 0$ esetén triviálisan teljesül. (3.6.5)-ből és (3.6.6)-ból következik hogy:

$$\frac{1}{2} \sum_{i=1}^N (A_i^2 - 1) < 2N$$

$$\sum_{i=1}^N (A_i^2 - 1) < 4N$$

$$\left(\sum_{i=1}^N A_i^2 \right) - N < 4N$$

$$(3.6.7) \quad \sum_{i=1}^N A_i^2 < 5N$$

Legyen $S = \sum_{i=1}^N \frac{A_i}{\sqrt{i}}$. Ezt az összeget szeretnénk két oldalról becsülni. A felső becsléshez használjuk a Cauchy-Bunyakovszkij egyenlőtlenséget, (3.6.7)-et és azt, hogy $\sum_{i=1}^N \frac{1}{i} \leq \log N + 1$:

$$(3.6.8) \quad S \leq \sqrt{\sum_{i=1}^N A_i^2 \sum_{i=1}^N \frac{1}{i}} < \sqrt{5N(\log N + 1)}$$

Az alsó becsléshez használjuk (3.6.3)-at és az Abel-féle átrendezést:

$$(3.6.9) \quad S = \sum_{i=1}^N \frac{A(iN) - A((i-1)N)}{\sqrt{i}} > \sum_{i=1}^{N-1} A(iN) \left(\frac{1}{\sqrt{i}} - \frac{1}{\sqrt{i+1}} \right)$$

Ezt tovább becsülhetjük alulról, használva a következőt:

$$\begin{aligned} \left(\frac{1}{\sqrt{i}} - \frac{1}{\sqrt{i+1}} \right) &= \frac{\sqrt{i+1} - \sqrt{i}}{\sqrt{i}\sqrt{i+1}} = \frac{(\sqrt{i+1} - \sqrt{i})(\sqrt{i+1} + \sqrt{i})}{\sqrt{i}\sqrt{i+1}(\sqrt{i+1} + \sqrt{i})} = \frac{1}{i\sqrt{i+1} + (i+1)\sqrt{i}} \geq \\ &\geq \frac{1}{2(i+1)\sqrt{i}} \end{aligned}$$

mert $i\sqrt{i+1} \leq (i+1)\sqrt{i}$ teljesül minden i -re.

Ezzel folytatva (3.6.9)-et azt kapjuk, hogy:

$$S > \sum_{i=1}^{N-1} \frac{A(iN)}{2(i+1)\sqrt{i}}$$

Tehát S -et alulról és felülről is becsültük, vagyis (3.6.8)-ból és (3.6.9)-ből következően:

$$(3.6.10) \quad \sum_{i=1}^{N-1} \frac{A(iN)}{2(i+1)\sqrt{i}} < S \leq \sqrt{5N(\log N + 1)}$$

Tegyük fel, hogy a tétel állítása nem igaz, vagyis minden $c > 0$ -ra:

$$(3.6.11) \quad A(iN) > c\sqrt{\frac{iN}{\log(iN)}}, \text{ ha } i = 1, 2, \dots, N$$

Vessük össze (3.6.11)-et a (3.6.10) bal oldalával, majd használjuk fel, hogy a szummában $\log iN < \log N^2$ mindig teljesül:

$$S > c \sum_{i=1}^{N-1} \frac{\sqrt{iN}}{2(i+1)\sqrt{i}\sqrt{\log(iN)}} > c \sum_{i=1}^{N-1} \frac{\sqrt{N}}{2(i+1)\sqrt{\log(N^2)}} =$$

$$= \frac{c\sqrt{N}}{\sqrt{8\log N}} \sum_{i=1}^{N-1} \frac{1}{i+1} \approx \frac{c\sqrt{N}\log N}{\sqrt{8}\sqrt{\log N}} = \frac{c}{\sqrt{8}}\sqrt{N\log N}$$

Ebből (3.6.10) a (3.6.11) mellett:

$$\frac{c}{\sqrt{8}}\sqrt{N\log N} < S < \sqrt{5N(\log N + 1)}$$

ami $c > \sqrt{40}$ esetén ellentmond (3.6.10) jobb oldalának, szóval ha $c > \sqrt{40}$, akkor (3.6.11) nem lehet igaz. Mivel ellentmondásra jutottunk, a tétel állítása igaz.

3.7. Vegyes feladatok

A következő két feladat érdekes kérdéseket tárgyal a Sidon-tulajdonsághoz hasonló tulajdonsággal rendelkező sorozatokkal kapcsolatban.

3.7.1. Feladat. Mutassuk meg, hogy létezik egészeknek olyan $a_1 < a_2 < \dots$ végtelen sorozata, hogy a 0-n kívül minden egész szám egyértelműen írható fel $a_i - a_j$ alakban.

Megoldás. Vegyük észre, hogy ha $a_i - a_j = k$, akkor $a_j - a_i = -k$, tehát elég arra figyelni, hogy minden pozitív egész szám előálljon két tag különbségeként. Konstruáljunk megfelelő sorozatot. Először vegyünk két egész számot, amelyeknek a különbsége 1. Ezután vegyünk hozzá két egészt úgy, hogy egyiknek se legyen semelyik korábbi taggal a különbsége 1, és a két új tag különbsége legyen 2. Ezt folytathatjuk a végtelenségig. Egy általános lépés a következő: egy lépésben mindig két újabb tagot veszünk hozzá a sorozatunkhoz úgy, hogy elég nagyok legyenek ahhoz, hogy a korábbi tagokkal ne jöhessen létre már meglévő különbség, illetve a két új tag különbsége legyen a legkisebb pozitív egész, amely eddig nem állt elő különbségként. Mivel ezt a lépést végtelenszer meg tudjuk ismételni, valóban egy megfelelő végtelen sorozatot fogunk kapni.

A következő feladat is Erdős egyik felvetett kérdésén alapul, a bizonyítás Erdős és Freud eredménye [8].

Jelölés. Továbbra is $A(n)$ jelöli az A sorozat elemszámát az $[1, n]$ intervallumon, $B(n)$ pedig a B sorozat elemszámát az $[1, n]$ intervallumon.

3.7.2. Feladat. A természetes számok két végtelen részsorozatát, A -t és B -t akkor nevezzük jó sorozatpárnak, ha az $a + b$ ($a \in A, b \in B$) összegek mind különbözőek. (Például ilyen, ha egy végtelen Sidon-sorozatot kettévágunk.) Adjunk meg egy jó sorozatpárt, amelynél minden n -re $A(n) > c\sqrt{n}$ és $B(n) > c\sqrt{n}$ valamely $c > 0$ konstansra.

Megoldás. Az A sorozat legyen olyan, hogy tartalmazza azokat a számokat, amelyek kettes számrendszerbeli alakjában az egyesektől kezdődően tekintve minden páros helyen 0 áll, a B sorozat pedig olyan, hogy tartalmazza azokat, amelyek kettes számrendszerbeli alakjában szintén az egyesektől kezdődően nézve minden páratlan helyen 0 áll. Azt szeretnénk belátni, hogy ekkor teljesül egyrészt a feltétel az elemszámokra, másrészt az, hogy az $a + b$ ($a \in A, b \in B$) összegek mind különbözőek.

Vegyük észre, hogy $a + b$ -nek a kettes számrendszerbeli alakjában pontosan akkor fog 0 szerepelni, ha azon a helyen a -ban és b -ben is 0 szerepel, mivel az A és a B sorozat meghatározásakor kizártuk azt, hogy a és b kettes számrendszerbeli alakjában ugyanazon a helyen egyszerre szerepeljen 1-es. Tegyük fel, hogy létezik $a_1, a_2 \in A$ és $b_1, b_2 \in B$ úgy, hogy $a_1 + b_1 = a_2 + b_2$, azaz a kettes számrendszerbeli alakjukban minden helyiértéken ugyanaz a szám áll. Ha az összegben páros helyiértéken 1 áll, akkor b_i -ben azon a helyen 1-nek kell állnia, ha az összegben 0 van ott, akkor b_i -ben is annak kell lennie. Ugyanez igaz páratlan helyiértékre is, csak fordítva. Tehát az összeg egyértelműen meghatározza a_i -t és b_i -t, vagyis $a_1 + b_1 = a_2 + b_2$ csak úgy teljesülhet, ha $a_1 = a_2$ és $b_1 = b_2$. Vagyis valóban minden $a + b$ összeg különböző lesz.

Azt kell még belátni, hogy az elemszámok az $[1, n]$ intervallumon valóban meghaladják a $c\sqrt{n}$ -et. Az A és a B sorozat tagjaira is igaz, hogy kettes számrendszerben felírt alakjukban a számjegyek egyik fele 0, a másik fele pedig tetszőlegesen 0 vagy 1. Ebből már következik, hogy $A(n)$ és $B(n)$ is $\sqrt{n}$ nagyságrendű, tehát alkalmas c -vel mindkettőre teljesülni fog, hogy legalább $c\sqrt{n}$. A legjobb c meghatározásához vegyük észre, hogy ha n csupa egyesből áll, azaz $n = 2^k - 1$, akkor az n előtt sokáig 1-es az első számjegy, ami azt jelenti, hogy vagy A -nak, vagy B -nek n előtt sokáig nincsen tagja. A k paritásától függ, hogy melyiknek. Tehát az $n = 2^k - 1$ értékek adják a lerosszabb eseteket. Ebben az esetben n kettes számrendszerben felírva k jegyű. Először számoljuk össze az A tagjait n -ig, azaz azokat, amelyekben a páros helyeken 0 áll. Ha k páros, akkor $k/2$ helyen van mindenképp 0, ha k páratlan, akkor $(k-1)/2$ helyen. A maradék helyekre szabadon választhatunk a két lehetőség közül, így összesen $2^{\lfloor \frac{k}{2} \rfloor}$ ilyen szám van. Azt szeretnénk látni, hogy alkalmas $c > 0$ -ra $2^{\lfloor \frac{k}{2} \rfloor} > c\sqrt{2^k - 1}$. Ha k páros, akkor $c < 1$ esetén, ha pedig k páratlan, akkor $c < \frac{1}{\sqrt{2}}$ esetén teljesül a feltétel az elemszámra. Hasonlóan gondolkodhatunk, ha a B tagjait szeretnénk megszámolni. Ha k páros, akkor $k/2$ helyen van mindenképp 0, ha páratlan, akkor $(k+1)/2$ helyen. A többi helyre szabadon választható 0 vagy 1, így összesen $2^{\lceil \frac{k}{2} \rceil}$ ilyen szám van. Azt szeretnénk látni, hogy alkalmas $c > 0$ -ra $2^{\lceil \frac{k}{2} \rceil} > c\sqrt{2^k - 1}$. Ez páros k esetén akkor teljesül, ha $c < 1$, páratlan k esetén pedig akkor, ha $c < \sqrt{2}$. Legyen $c = 0,5$. Ekkor a megadott A és B megfelelő sorozatpárt alkot.

4. fejezet

Csupa különböző összegű sorozatok

4.1. Csupa különböző összeg

A definíció, az alapvető kérdés és az egyszerű alsó becslés elhangzott Erdős 1993-as előadásában az Eötvös Napon [6]. Ezekből fogunk kiindulni a fejezet tárgyalása során.

4.1.1. Definíció (*Csupa különböző összegű sorozat*). Az egész számoknak egy $a_1 < a_2 < \dots < a_k \leq n$ sorozatát csupa különböző összegű sorozatnak nevezzük, ha az összes

$$(4.1.1) \quad \sum_{j=1}^k \varepsilon_j a_j$$

alakú részösszeg különböző, ahol $\varepsilon_j = 0$ vagy 1 . (Azaz ha a sorozat bárhány tagját összeadva mindig különböző eredményt kapunk.)

4.1.2. Kérdés (*Alapvető kérdés*). Legfeljebb hány eleme lehet annak a csupa különböző összegű sorozatnak, amelynek minden eleme az $[1, n]$ intervallumba esik?

A következőkben erre az elemszámmra szeretnénk minél jobb felső becslést adni.

4.2. Felső becslés az elemszámmra

Jelölés. A továbbiakban legyen az $[1, n]$ intervallumon vett csupa különböző összegű sorozat elemszáma k .

4.2.1. Egyszerű alsó becslés. A sorozat tagjainak válasszuk a kettő hatványait. Ebben az esetben a sorozat tagjaira biztosan teljesül (4.1.1), mert minden szám egyértelműen áll elő kettőhatványok összegeként. Ekkor $k = \lfloor \log_2 n \rfloor + 1$.

Felmerül a kérdés: Vajon ez a maximális k ? Biztosan nem, mert $n = 2^{21}$ -re létezik egy sűrűbb sorozat, amelyre $k = \lfloor \log_2 n \rfloor + 2$ [5]. Az ismeretlen, hogy ezt lehet-e még tovább növelni, de Erdős megmutatta, hogy sokkal biztosan nem. Erről szól a következő tétel, amely Erdős és Leo Moser eredménye [3].

4.2.2. Tétel. Tegyük fel, hogy az $1 \leq a_1 < a_2 < \dots < a_k \leq n$ egész számok közül akárhány különbözőnek az összege mind különböző értéket ad. Ekkor:

$$(4.2.1) \quad k \leq \log_2 n + \log_2 \log_2 n + 1$$

Sőt, $n > 8$ -ra:

$$(4.2.2) \quad k \leq \log_2 n + \frac{\log_2 \log_2 n}{2} + 2$$

Bizonyítás. A feltétel szerint a sorozatunkban k elem van. Ebből a k különböző a_i -ből képezzünk összegeket, jelöljük ezeket u_j -vel. Minden a_i vagy bekerül egy adott összegbe, vagy nem. Ebből következik, hogy 2^k különböző u_j összeg képezhető. Ezek közül a legkisebb az üres összeg, a legnagyobb pedig az összes a_i -nek az összege. Biztos, hogy $u_j \in [0, nk - 1] = I$. Mivel az összes u_j különböző és az I intervallumban nk egész szám van, teljesülni fog, hogy:

$$2^k \leq nk$$

Vegyük mindkét oldal kettes alapú logaritmusát:

$$\log_2 2^k \leq \log_2 nk$$

A logaritmus azonosságait használva ekkor:

$$(4.2.3) \quad k \leq \log_2 n + \log_2 k$$

Abból, hogy $k \leq n$, következik, hogy $\log_2 k \leq \log_2 n$. Ezt összevetve (4.2.3)-mal azt kapjuk, hogy:

$$k \leq \log_2 n + \log_2 n$$

$$k \leq 2 \log_2 n$$

Ismét vegyük mindkét oldal kettes alapú logaritmusát, majd használjuk a logaritmus azonosságait:

$$\log_2 k \leq \log_2(2 \log_2 n)$$

$$\log_2 k \leq \log_2 2 + \log_2 \log_2 n$$

$$(4.2.4) \quad \log_2 k \leq \log_2 \log_2 n + 1$$

(4.2.3)-ből és (4.2.4)-ből az következik, hogy:

$$k \leq \log_2 n + \log_2 \log_2 n + 1$$

Ezzel (4.2.1) egyenlőtlenséget beláttuk.

(4.2.2) egyenlőtlenség felső becslése nagy n -re jobb, mert kisebb. Ennek bizonyításához sejtjük meg, hogy az u_j összegek az I intervallumban nem egyenletesen helyezkednek el, hanem a legtöbb közülük az átlag közelében csoportosul. Ezt szeretnénk valahogyan megmutatni. Vezessünk be egy X valószínűségi változót, és a továbbiakban jelölje P a valószínűséget, E a várható értéket és D a szórást. Az X a 2^k darab u_j mindegyikét 2^{-k} valószínűséggel veszi fel, azaz minden j -re:

$$P(X = u_j) = 2^{-k}$$

Írjuk fel a Csebisev-egyenlőtlenséget X -re:

$$P(|X - E(X)| > cD(X)) < \frac{1}{c^2}$$

Mit fejez ki az egyenlőtlenség? Azt, hogy az u_j értékek kevesebb, mint c^{-2} -szerese esik az $E(X)$ középpontú, $2cD(X)$ hosszúságú intervallumon kívülre. Ebből következik, hogy az u_j értékek $(1 - c^{-2})$ -szerese esik ennek az intervallumnak a belsejébe. Szeretnénk alkalmazni a bizonyítás első felében használt gondolatmenetet azoknak az u_j -knek a számára, amelyek biztosan beleesnek az intervallumba. Ha $Z = \sum_{i=1}^k a_i$, akkor $E(X) = Z/2$, mert az u_j összegeket össze lehet úgy párosítani, hogy a párok összege pont Z legyen. Vezessük be az ξ_i , $i = 1, \dots, k$ valószínűségi változókat. Minden ξ_i $1/2$ - $1/2$ eséllyel veszi fel az a_i , illetve a 0 értéket. A ξ_i -k függetlenek és $\sum_{i=1}^k \xi_i = X$. Ekkor:

$$D^2(X) = \sum_{i=1}^k D^2(\xi_i) = \frac{1}{4} \sum_{i=1}^k a_i^2 < \frac{kn^2}{4}$$

Megint írjuk fel a Csebisev egyenlőtlenséget X -re, legyen $c = 2$:

$$P\left(\left|X - \frac{Z}{2}\right| > 2\frac{n\sqrt{k}}{2}\right) < \frac{1}{4}$$

Azaz a 2^k darab u_j legalább $\frac{3}{4}$ része a $\frac{Z}{2}$ középpontú, $2n\sqrt{k}$ hosszúságú intervallumba esik. Ebből következik, hogy:

$$\frac{3}{4}2^k \leq 2n\sqrt{k}$$

$$2^k \leq \frac{8}{3}n\sqrt{k}$$

Vegyük mindkét oldal kettes alapú logaritmusát és alkalmazzuk a logaritmus azonosságait:

$$(4.2.5) \quad k \leq \log_2 n + \frac{\log_2 k}{2} + \log_2 \frac{8}{3}$$

Ebből $n > 8$ esetén következik, hogy:

$$k \leq 2\log_2 n$$

Ebből logaritmust véve következik, hogy:

$$(4.2.6) \quad \log_2 k \leq 1 + \log_2 \log_2 n$$

(4.2.5)-öt és (4.2.6)-ot összevetve:

$$k \leq \log_2 n + \frac{\log_2 \log_2 n + 1}{2} + \log_2 \frac{8}{3} < \log_2 n + \frac{\log_2 \log_2 n}{2} + 2$$

Ezzel a (4.2.2) egyenlőtlenséget is beláttuk.

4.3. Vegyes feladatok

A következő három feladatban olyan érdekes kérdéseket fogunk megvizsgálni, amelyek hasonlítanak a csupa különböző sorozatok problémájához, de a feltételeink kissé eltérőek lesznek. Az első feladatban nem azt tesszük fel, hogy a sorozat tagjaiból alkotott minden részletösszeg különböző, hanem azt, hogy egyik részletösszeg sem adja a sorozat valamely tagját eredményül. A sorozat tagjai továbbra is az $[1, n]$ intervallumból kerülnek ki, illetve az elemszám továbbra is k .

4.3.1. Feladat. Mennyi k maximuma n függvényében, ha egyik a_i sem áll elő csupa különböző (és egynél több) a_j összegeként?

Megoldás. Vegyük észre, hogy az $[n/2, n]$ intervallum egészeire igaz a feltétel, azaz egyik intervallumbeli egész sem áll elő csupa különböző, másik intervallumbeli egész összegeként, hiszen ha már csak kettőt is összeadunk ezek közül, n -nél nagyobb számot kapunk. Az $[n/2, n]$ intervallumban $\lfloor n/2 \rfloor + 1$ egész van, így ezzel a konstrukcióval egy $\lfloor n/2 \rfloor + 1$ elemszámú megfelelő sorozatot készítettünk.

Azt állítjuk, hogy $\lfloor n/2 \rfloor + 1$ -nél több elemet nem választhatunk ki úgy, hogy a megadott feltételek teljesüljenek. Vegyünk egy, a feltételt teljesítő tetszőleges sorozatot, jelöljük A -val, és jelölje a_k a legnagyobb elemét. Azt szeretnénk belátni, hogy ennek a sorozatnak legfeljebb $\lfloor n/2 \rfloor + 1$ eleme lehet. Mivel a_k a legnagyobb elem, csak nála kisebb elemek lehetnek az A sorozat további tagjai. Írjuk fel a_k -t minden lehetséges módon két szám összegeként. Ez a felírás függ a_k paritásától. Az első esetben legyen $a_k = 2u$ páros.

$$1 + (2u - 1)$$

$$2 + (2u - 2)$$

...

$$u + u$$

Vegyük észre, hogy a feltétel miatt ekkor az $1, 2, \dots, 2u$ számokból legalább $u - 1$ kimarad a sorozatból, ezért legfeljebb $u + 1$ lesz bevehető.

A második esetben legyen $a_k = 2u + 1$ páratlan. Ekkor a lehetséges kéttagú összegek a következők lesznek:

$$1 + (2u)$$

$$2 + (2u - 1)$$

...

$$u + (u + 1)$$

Ebben az esetben az $1, 2, \dots, 2u + 1$ számokból legalább u kimarad a sorozatból, ezért legfeljebb $u + 1$ lesz bevehető. Tehát mindkét esetben igaz, hogy legfeljebb $\lfloor a_k/2 \rfloor + 1$ elem lehet benne az A sorozatban. Mivel $a_k \leq n$, ezért:

$$\lfloor a_k/2 \rfloor + 1 \leq \lfloor n/2 \rfloor + 1$$

Ezzel beláttuk, hogy az adott feltétel mellett k maximuma n függvényében $\lfloor n/2 \rfloor + 1$.

4.3.2. Feladat. A második feladatban azt vizsgáljuk, hogy egy t szám hányféleképpen állhat elő egymás után következő a_i -k összegeként. Legyen $L(k)$ a $t = a_i + a_{i+1} + \dots + a_j$ egyenlet

megoldásszámának maximuma, ahol a maximumot az összes lehetséges a_i rendszerre és t -re vesszük. Igazoljuk, hogy $L(k) = \lceil k/2 \rceil$.

Megoldás. A feladat átfogalmazása: Vegyünk egy fix k -t, majd k darab tetszőleges egészt növekvő sorrendben ($a_1 < a_2 < \dots < a_k$). Készítsük el ezekből az összes olyan összeget, amelyekben egymás utáni indexű tagok szerepelnek: $a_1, a_2, \dots, a_k, a_1 + a_2, \dots, a_{k-i} + a_k, \dots, a_1 + a_2 + \dots + a_k$. Mutassuk meg, hogy ezek közül maximum $\lceil k/2 \rceil$ darab összeg lehet egyenlő t -vel, ha az a_i számokat szabadon megválaszthatjuk.

Egy konstrukciót fogunk mutatni arra, hogy meg tudunk adni úgy k darab növekvő számot, hogy $L(k) = \lceil k/2 \rceil$. Először mutassunk egy példát $k = 10$ -re, amit majd később általánosítunk. Vegyünk $10/2 = 5$ növekvő számot úgy, hogy a legkisebb legyen nagyobb 5-nél:

$$a_1 = 8, a_2 = 9, a_3 = 10, a_4 = 11, a_5 = 12$$

Folytassuk a sorozatot a következőképpen:

$$a_6 = a_1 + a_2 = 17$$

$$a_7 = a_3 + a_4 = 21$$

$$a_8 = a_5 + a_6 = 29$$

$$a_9 = a_7 + a_8 = 50$$

Vegyünk észre, hogy a_{10} -et már nem tudjuk így megadni, de válasszunk egy a_9 -nél nagyobb számot. Legyen $a_{10} = 52$. Ekkor a következő öt összeg egyenlő lesz, hiszen ennek megfelelően határoztuk meg a sorozat tagjait:

$$(4.3.1) \quad 50 = a_1 + a_2 + a_3 + a_4 + a_5 = a_3 + a_4 + a_5 + a_6 = a_5 + a_6 + a_7 = a_7 + a_8 = a_9$$

Ezzel megadtunk 10 számot növekvő sorrendben úgy, hogy $L(10) = 5$.

Ezt a konstrukciót írjuk fel általánosan. Legyen $\lceil k/2 \rceil = f$, és vegyünk egy $p > f$ számot. Legyen $a_1 = p + 1, a_2 = p + 2, \dots, a_f = p + f$ (ez f darab szám növekvő sorrendben) és $t = a_1 + a_2 + \dots + a_f$ az az összeg, amelyet szeretnénk összesen f -szer előállítani különböző egymás utáni indexű számokból. Vegyünk hozzá további számokat a meglévő $a_1, \dots, a_f$ számokhoz a következő módon: $a_{f+1} = a_1 + a_2, a_{f+2} = a_3 + a_4$ és így tovább, egészen addig, amíg k darab számunk nem lesz. Ekkor $t = a_1 + \dots + a_f = a_3 + a_4 + \dots + a_f + a_{f+1} = \dots$

Általános alakban legyen $a_{f+j} = a_{2j-1} + a_{2j}$, ha $j \leq f-1$, azaz amíg el nem érjük a k darab tagot a sorozatban. Ha k páros, akkor a $a_k (= a_{2f})$ bármely $a_{k-1} (= a_{2f-1})$ -nél nagyobb szám lehet.

Ellenőrizni kell, hogy az így kiválasztott k darab szám valóban minden esetben növekvő sorrendben áll, és valóban $\lceil k/2 \rceil$ -féleképpen lehet belőlük előállítani t -t. Növekvőek lesznek, mert az elején $a_1, \dots, a_f$ számokat növekvőnek választottuk, továbbá $a_f < a_{f+1}$, mert $a_f = p + f < p + 1 + p + 2 = 2p + 3 = a_1 + a_2 = a_{f+1}$. A nagyobb indexűekre pedig szintén teljesül, mert $a_u < a_v$ esetén, ahol $f < u < v \leq 2f-1$, mindig teljesül, hogy a kisebb tag két korábbi kisebb indexű tagnak az összege, míg a nagyobb tag két korábbi nagyobb indexű tagnak az összege. Valóban $\lceil k/2 \rceil$ -féleképpen lehet belőlük előállítani t -t: először f különböző elem összegeként állítottuk elő, utána $f-1$ különböző elem összegeként és így tovább, mindig 1-gyel csökken a tagok száma az összegben (lásd a (4.3.1) képletet). Így összesen f -szer állítottuk elő t -t, de tudjuk, hogy $f = \lceil k/2 \rceil$.

Ezek után azt is meg kell mutatnunk, hogy sem ezekre az a_i -kre, sem más a_i sorozat tagjaiból nem tudunk többféleképpen előállítani egy számot egymás utáni indexű a_i -k összegeként. Legyen a sorozatunk $a_1 < a_2 < \dots < a_k$, és vegyük ehhez a legjobban kiválasztott t -t. Használjunk fel két fontos észrevételt. Az első: minden t -t előállító összeg tagjainak a darabszáma különbözik. Ez könnyen látható abból, hogy egymás utáni indexű tagokat kellett vennünk, és ha elhagyunk egy legelső tagot, akkor csak az összesnél nagyobbat vehetünk hozzá a darabszám kiegyenlítése végett, de ekkor az összeg mindenképp nagyobb lesz. A második: minden t -t előállító összeg utolsó tagja különbözik. Ha lenne kettő, amelyeknek az utolsó tagjuk ugyanaz, akkor azok elé ugyanazokat a tagokat kellene bevenni sorban az összegbe ahhoz, hogy a t -t kapjuk, így pedig ezek ugyanazt az összeget adják. Vegyük most t -nek azt az előállítását, amelyben az utolsó tag a lehető legkisebb, ennek a tagnak legyen az indexe q . Ha $q > f = \lceil k/2 \rceil$, akkor legfeljebb $k - (q-1)$ összeg lehet, hiszen csak a_q -nál nagyobb tagok lehetnek utolsó elemek, mert a_q volt a lehető legkisebb utolsó elem. Mivel $k - (q-1) \leq k - f \leq f$, ezért ebből látjuk, hogy ha $q > f$, akkor legfeljebb $f = \lceil k/2 \rceil$ előállítása lehet a t -nek. Ha $q \leq f$, akkor vegyük észre, hogy t előállítása abban az esetben áll a legtöbb tagból, amikor az utolsó elem a lehető legkisebb, ezért az előállítás legfeljebb q tagú lehet. Ebből következik, hogy legfeljebb q különböző előállítása lehet t -nek, de azt feltettük, hogy $q \leq f$, tehát ebben az esetben is megkaptuk a keresett maximumot.

A harmadik feladatban egy olyan sorozat elemszámát fogjuk megvizsgálni, amelyben semelyik két tag különbsége sem lehet négyzetszám.

4.3.3. Feladat. Tegyük fel, hogy $a_i - a_j$ nem négyzetszám minden $i \neq j$ esetén. Legyen $h(n)$ k maximuma ezen feltétel mellett. Mit tudunk mondani ekkor $h(n)$ -ről?

Megoldás. Használjuk a mohó algoritmust. Vegyük be mindig a következő lehetséges számot és zárjuk ki az összes olyat, amelynek az újonnan bevett számmal vett különbsége négyzetszám. Tehát az elején bevehetjük az 1-et, és ki kell zárunk a következőket: $1 + 1 = 2$, $1 + 4 = 5$, $1 + 9 = 10$ és így tovább. Ekkor n -ig kizárunk $\lfloor \sqrt{n-1} \rfloor$ elemet. A következő bevehető szám a 3. A kizárando elemek között lehetnek átfedések az eddig kizártakkal, de legfeljebb $\lfloor \sqrt{n-3} \rfloor$ elemet kell kizárunk. És így tovább. Amikor bevesszük az i -edik elemet, akkor $\lfloor \sqrt{n-a_i} \rfloor$ elemet kell kizárunk. Számoljuk össze, hogy k elem esetén legfeljebb hány elemet zárunk ki n -ig:

$$\sum_{i=1}^k \lfloor \sqrt{n-a_i} \rfloor \leq k(\lfloor \sqrt{n-1} \rfloor)$$

Ha a bevett és a kizárt elemek számának összege kisebb, mint n , akkor mindig tovább tud haladni a mohó algoritmus, mert lesz még olyan szám, amelyet bevehetünk. Vagyis tovább tud menni az algoritmus, ha:

$$k + k(\lfloor \sqrt{n-1} \rfloor) < n$$

$$k(1 + \lfloor \sqrt{n-1} \rfloor) < n$$

Ez biztosan teljesül, amíg $k \leq \lfloor \sqrt{n-1} \rfloor - 1$. Vagyis azt kaptuk, hogy addig biztosan nem akad el a mohó algoritmus, amíg kevesebb, mint $\lfloor \sqrt{n-1} \rfloor$ elemet választottunk be, azaz biztosan igaz lesz, hogy $h(n) \geq \lfloor \sqrt{n-1} \rfloor$.

Ennél sokkal jobb becslést is adhatunk $h(n)$ -re a következő konstrukcióval, amelyet csak megemlítünk az érdekesség kedvéért. A feltételnek megfelelő sorozatot alkotnak azok a számok, amelyek ötös számrendszerbeli alakjában az egyes helyiértéktől nézve a páratlanadik helyen 0 vagy 2 áll. Ekkor n -ig nagyjából n^c ilyen szám van, ahol $c = (1 + \log_5)/2 \approx 0,71$, vagyis elég nagy n -re teljesülni fog, hogy $h(n) \geq n^{0,71}$.

4.4. Felső becslés a reciprokösszegre

Eddig főként a csupa különböző összegű sorozatoknak, illetve a hozzájuk hasonló tulajdonságú sorozatoknak az elemszámát becsültük. Ehhez a témakörhöz kötődik egy másik Erdős-probléma is, de ez nem az elemszámmal foglalkozik, hanem a tagok reciprokának az összegével. Erdős sejtését, a 4.4.1 tételt Ryavec, Bruen és Borwein, illetve Frenkel Péter is bizonyították különböző módon [11] [9]. Bruen és Borwein bizonyítását részletezzük.

4.4.1. Tétel. Ha az $a_1 < a_2 < \dots < a_k$ pozitív egész számok közül akárhány különbözőnek az összege mind különböző értéket ad, akkor:

$$(4.4.1) \quad \sum_{i=1}^k \frac{1}{a_i} < 2$$

4.4.2. Megjegyzés. (4.4.1) jobb oldalán a 2 helyére kisebb konstans nem írható. Ez jól látszik abból, ha az a_i -knek az első k kettőhatványt választjuk. A bizonyításból fog látszani, hogy a reciprokösszeg pont akkor lesz maximális, ha $a_i = 2^{i-1}$.

Bizonyítás. A tétel feltételéből adódik, hogy bármely $1 \leq i \leq k$ esetén az $a_1, a_2, \dots, a_i$ számokból $2^i - 1$ nemüres összeg képezhető, ezek mindegyike különböző pozitív egész értéket ad eredményül. Ezért a legnagyobb lehetséges összegre mindig teljesül, hogy legalább $2^i - 1$.

$$(4.4.2) \quad a_1 + a_2 + \dots + a_i \geq 2^i - 1, \text{ ha } i = 1, 2, \dots, k$$

Legyen $b_i = 2^{i-1}$, ahol továbbra is $i = 1, 2, \dots, k$. Ekkor, ha vesszük a $b_1, b_2, \dots, b_i$ mértani sorozatot és összeadjuk az első i tagját, akkor pont azt kapjuk, hogy:

$$S_i = b_1 + b_2 + \dots + b_i = 1 \frac{2^i - 1}{2 - 1} = 2^i - 1$$

azaz (4.4.2)-t át tudjuk írni $i = 1, 2, \dots, k$ mellett a következő módon:

$$(4.4.3) \quad a_1 + a_2 + \dots + a_i \geq b_1 + b_2 + \dots + b_i$$

Elég belátni, hogy ekkor

$$(4.4.4) \quad \frac{1}{a_1} + \frac{1}{a_2} + \dots + \frac{1}{a_k} \leq \frac{1}{b_1} + \frac{1}{b_2} + \dots + \frac{1}{b_k},$$

mert

$$\frac{1}{b_1} + \frac{1}{b_2} + \dots + \frac{1}{b_k} = 1 + \frac{1}{2} + \frac{1}{4} + \dots + \frac{1}{2^{k-1}} = 2 - \frac{1}{2^{k-1}} < 2$$

Azt szeretnénk tehát megmutatni, hogy (4.4.3)-ból

$$(4.4.5) \quad 0 < a_1 < \dots < a_k \text{ és } 0 < b_1 < \dots < b_k$$

mellett mindig következik (4.4.4), ha a_i, b_i valós számok. Legyen

$$(4.4.6) \quad c_i = a_1 - b_1 + a_2 - b_2 + \dots + a_i - b_i$$

Ekkor (4.4.3)-ból következik, hogy $c_i \geq 0$. Rendezzük át (4.4.4)-et:

$$(4.4.7) \quad 0 \leq \frac{1}{b_1} - \frac{1}{a_1} + \frac{1}{b_2} - \frac{1}{a_2} + \dots + \frac{1}{b_k} - \frac{1}{a_k}$$

Azt szeretnénk látni, hogy (4.4.7) teljesül, ha igaz (4.4.5).

Rendezzük át (4.4.7)-et (4.4.6) segítségével:

$$\begin{aligned} & \frac{1}{b_1} - \frac{1}{a_1} + \frac{1}{b_2} - \frac{1}{a_2} + \dots + \frac{1}{b_k} - \frac{1}{a_k} = \frac{a_1 - b_1}{a_1 b_1} + \frac{a_2 - b_2}{a_2 b_2} + \dots + \frac{a_k - b_k}{a_k b_k} = \\ & = \frac{c_1}{a_1 b_1} + \frac{c_2 - c_1}{a_2 b_2} + \dots + \frac{c_k - c_{k-1}}{a_k b_k} = \\ & = c_1 \left(\frac{1}{a_1 b_1} - \frac{1}{a_2 b_2} \right) + c_2 \left(\frac{1}{a_2 b_2} - \frac{1}{a_3 b_3} \right) + \dots + c_{k-1} \left(\frac{1}{a_{k-1} b_{k-1}} - \frac{1}{a_k b_k} \right) + \frac{c_k}{a_k b_k} \end{aligned}$$

Tudjuk, hogy $c_i \geq 0$, valamint (4.4.5) miatt a zárójelekben is mindig pozitív számok vannak. Ebből következik, hogy a teljes összeg is nemnegatív, azaz (4.4.7) valóban teljesül. Ezt szerettük volna belátni. Ráadásul a bizonyításból az is kiderül, hogy (4.4.4)-ben pontosan akkor van egyenlőség, ha $c_i = 0$ minden i -re, ami pedig ekvivalens azzal, hogy $a_i = b_i$ minden i -re. Ebből következik a 4.4.2. megjegyzés.

A következő feladatokban szintén sorozatok elemeinek a reciprokösszegét fogjuk megvizsgálni, de módosítunk a feltételeken. Tegyük fel, hogy bármely $i \neq j$ -re $[a_i, a_j] > n$, ahol $[a_i, a_j]$ az a_i és az a_j legkisebb közös többszörösét jelöli.

4.4.3. Feladat. Bizonyítsuk be, a következőt:

$$\sum_{i=1}^k \frac{1}{a_i} < 2$$

Megoldás. Legyen a sorozatunk a következő: $1 \leq a_1 < a_2 < \dots < a_k \leq n$, és tudjuk, hogy minden $i \neq j$ -re $[a_i, a_j] > n$ teljesül. A feltételből következik, hogy bármely m -re, amelyre $1 \leq m \leq n$ teljesül, igaz, hogy maximum egy a_i -vel osztható. Ha létezne a_i és a_j , amelyek osztják m -et, akkor ezeknek m közös többszöröse lenne, amiből következik, hogy $[a_i, a_j] \leq n$, ami ellentmondás. Ebből adódik, hogy az a_i -k többszörösei n -ig összesen nem lehetnek többen, mint n , mert akkor lenne n -ig egy olyan szám, amely több a_i -nek is többszöröse, ami ellentmondás. Tehát $\sum_{i=1}^k \lfloor \frac{n}{a_i} \rfloor \leq n$. Ebből következik az alábbi becslés:

$$n \sum_{i=1}^k \frac{1}{a_i} < n + k = n \left(1 + \frac{k}{n} \right)$$

Az első egyenlőtlenség igaz, mert ha a $\sum_{i=1}^k \lfloor \frac{n}{a_i} \rfloor \leq n$ egyenlőtlenségből elhagyjuk az

egészrészt, akkor mind a k tag értéke kevesebb, mint eggyel nő. Az egyenlőség adódik kiemeléssel. A becslésből következik, hogy

$$\sum_{i=1}^k \frac{1}{a_i} < 1 + \frac{k}{n} < 2$$

Az utolsó reláció azért igaz, mert a sorozatban biztosan n -nél kevesebb tag lesz, vagyis $\frac{k}{n} < 1$ mindig teljesül.

4.4.4. Feladat. Szeretnénk belátni, hogy ennél erősebb becslés is igaz:

$$(4.4.8) \quad \sum_{i=1}^k \frac{1}{a_i} < 1 + \frac{k}{n} < \frac{3}{2}$$

Megoldás. Ehhez az kell, hogy

$$\frac{k}{n} < \frac{1}{2}, \text{ azaz } k < \frac{n}{2},$$

ami azt jelenti, hogy 1-től n -ig kevesebb mint a számok felét tudjuk beválasztani a sorozatba úgy, hogy teljesüljön a feltétel. A sorozatunk tagjaira igaznak kell lennie, hogy bárhogyan választunk ki két számot, nem oszthatja egyik a másikat, hiszen az kell, hogy a legkisebb közös többszörösük nagyobb legyen n -nél. Ennek megmutatásához elég belátnunk az alábbi állítást:

Állítás. Ha az $1, 2, \dots, 2m$ számok közül kiválasztunk tetszőlegesen $m + 1$ darabot, akkor biztosan lesz a kiválasztott számok között két olyan, hogy egyik osztja a másikat.

Írjuk fel a számokat 1-től $2m$ -ig egy kettőhatvány és egy páratlan szám szorzataként:

$$1, 2, 3, 2^2, 5, 2 \cdot 3, 7, 2^3, 9, 2 \cdot 5, \dots$$

Ekkor mindegyik számhoz egyértelműen hozzá tudunk rendelni egy páratlan számot:

$$1 \mapsto 1; 2 \mapsto 1; 3 \mapsto 3; 2^2 \mapsto 1; 5 \mapsto 5; 2 \cdot 3 \mapsto 3; 7 \mapsto 7; 2^3 \mapsto 3; 9 \mapsto 9; 2 \cdot 5 \mapsto 5 \dots$$

Használjuk a skatulyaelvet. Legyenek a páratlan számok a skatulyák: azok a számok kerüljenek egy skatulyába, amelyekhez ugyanazt a páratlan számot rendeltük hozzá. Ekkor az egy skatulyában levő számok közül tetszőlegesen kiválasztva kettőt, az egyik osztani fogja a másikat, hiszen mindkét szám ugyanannak a páratlan számnak egy kettőhatvánnyal vett szorzata. $2m$ -ig m darab páratlan szám van, így ha $m + 1$ számot választunk ki, akkor biztosan lesz két szám ugyanabból a skatulyából. Vagyis az állítás teljesül.

Ebből következik, hogy a feladat feltételei mellett mindig teljesül, hogy $\frac{n}{2}$ -nél kevesebb számot választhatunk be a sorozatba. Emiatt igaz lesz (4.4.8).

4.5. Csupa különböző szorzatú sorozatok

Felmerülhet a kérdés, hogy mit mondhatunk el egy sorozat elemszámáról akkor, ha nem az elemekből alkotott összegekre, hanem a szorzatokra szabunk meg feltételeket. Ez szintén egy olyan problémakör, amellyel Erdős is foglalkozott [4].

4.5.1. Definíció (*Csupa különböző szorzatú sorozat*). Az egész számoknak egy $a_1 < a_2 < \dots < a_k \leq n$ sorozatát csupa különböző szorzatú sorozatnak nevezzük, ha az a_i számok közül akárhány különbözőnek a szorzata mind különböző értéket ad.

Jelölés. Legyen egy, az $[1, n]$ intervallumon vett csupa különböző szorzatú sorozat elemszáma k . A következő feladatban jelöljük k maximumát $s(n)$ -nel, és jelölje $\pi(n)$ az n -nél nem nagyobb prímek számát.

4.5.2. Feladat. Mutassuk meg, hogy $|s(n) - \pi(n)| < 2n^{2/3}$.

Megoldás. Ha vesszük a prímeket n -ig, akkor igaz lesz a feltétel, mert különböző prímek szorzata biztosan különböző, tehát $\pi(n) \leq s(n)$ biztosan teljesül. Ebből következik, hogy $|s(n) - \pi(n)| = s(n) - \pi(n)$, vagyis a következőt kell megmutatni:

$$s(n) - \pi(n) < 2n^{2/3} \Leftrightarrow s(n) < \pi(n) + 2n^{2/3}$$

Ennek megmutatásához vegyük a következő két halmazt és egy állítást:

$$C = \{ c \in \mathbb{Z} \mid 1 \leq c \leq n^{2/3} \}$$

$$D = C \cup \{ p \in \mathbb{Z} \mid p \text{ prímszám és } 1 \leq p \leq n \}$$

Állítás. n -ig minden a egész szám felírható $a = cd$ alakban, ahol $c \in C$ és $d \in D$.

Bizonyítás. Minden $t \in D$ -re $t = 1t$ jó lesz, mert $1 \in C$ mindig igaz. Ha $k \notin D$, azaz $n^{2/3} < k$ és nem prím, akkor fel lehet írni k -t $k = lm$ alakban. Ha k -nak van egy $q \geq n^{1/3}$ prímosztója, akkor:

$$\frac{k}{q} \leq \frac{k}{n^{1/3}} \leq \frac{n}{n^{1/3}} = n^{2/3}, \text{ azaz } q \in D \text{ és } \frac{k}{q} \in C \text{ teljesül.}$$

Ha k -nak minden r_i prímosztójára $r_i < n^{1/3}$, akkor vegyünk a $k = r_1 \dots r_l$ prímtényező felbontást, ahol $r_i \leq r_j$ teljesül minden $i < j$ -re. A felbontás elejéről vegyünk s prímet úgy, hogy teljesüljenek a következők: $r_1 \dots r_{s-1} < n^{1/3}$, de $r_1 \dots r_s \geq n^{1/3}$. Vegyük észre, hogy nem lehetséges az, hogy $r_1 \dots r_{s-1} < n^{1/3}$ és $r_1 \dots r_s \geq n^{2/3}$, mert ekkor $r_s > n^{1/3}$, és ezt már az előbb tárgyaltuk. Tehát $r_1 \dots r_s$ mindenképpen benne van C -ben. Ekkor:

$$r_{s+1} \dots r_l = \frac{k}{r_1 \dots r_s} \leq \frac{k}{n^{1/3}} \leq \frac{n}{n^{1/3}} = n^{2/3}, \text{ azaz } r_1 \dots r_s \in C \text{ és } r_{s+1} \dots r_l \in D \text{ teljesül.}$$

Ezzel az állítást beláttuk.

Folytassuk a feladat bizonyítását. Készítsünk egy páros gráfot. A gráf egyik csúcsosztályában legyenek a csúcsok a C halmaz elemei, a másik csúcsosztályban pedig legyenek a D halmaz elemei. Így a gráfnak $|C| + |D|$ csúcsa lesz. Az előző állítás alapján 1-től n -ig minden egésznek rögzítsük egy felírását: $a_i = c_i d_i$, ahol $c_i \in C$ és $d_i \in D$. Vegyük ezek közül azt az $s(n)$ darab egész számot, amelyeket beválaszthatunk a sorozatunkba. Akkor kössük össze c_i csúcsot a d_i csúccsal, ha a sorozatban szereplő számok rögzített szorzatai között szerepel $c_i d_i$. Így a páros gráfnak pontosan $s(n)$ éle lesz, minden kiválasztott egészhez egy él fog tartozni.

Vegyük észre, hogy $|C| + |D| \leq \pi(n) + 2n^{2/3}$, hiszen mindkét halmaz tartalmazza az egészeket 1-től $n^{2/3}$ -ig és D még a fennmaradó prímekeket is. Emiatt elég belátnunk, hogy $s(n) < |C| + |D|$.

Indirekt tegyük fel, hogy $|C| + |D| \leq s(n)$, azaz a páros gráfban az élek száma legalább annyi, mint a csúcsok száma. Ebből következik, hogy a gráfban van kör, sőt, mivel a gráf páros, van páros kör. A páros kör éleit felváltva színezzük piros és kék színűre. Ekkor a kék élek szorzata meg fog egyezni a piros élek szorzatával, és mindkettő a csúcsokban lévő számok szorzatát adja. Vagyis találtunk egy számot, amely kétféleképpen is előáll az általunk kiválasztott egészek közül valamennyinek a szorzataként. Ez ellentmond a sorozatunk feltételeinek. Ebből következik, hogy $s(n) < |C| + |D|$, amivel megmutattuk a feladat állításának helyességét.

Irodalomjegyzék

- [1] CHOWLA, SARVADAMAN. Solution of a problem of Erdős and Turán in additive-number theory. *Proc. Nat. Acad. Sci.*, 14:1–2, 1944.
- [2] CHOWLA, SARVADAMAN–BOSE, RAJ CHANDRA. Theorems in the additive theory of numbers. *Commentarii mathematici Helvetici*, 37:141–147, 1962/63.
- [3] ERDŐS PÁL. Problems and results in additive number theory. In *Colloque sur la Théorie des Nombres, Bruxelles*. 1955. 127–137.
- [4] ERDŐS PÁL. On some applications of graph theory to number theoretic problems. *Publ. Ramanujan Inst.*, 1:131–136, 1969.
- [5] ERDŐS PÁL. Some problems in additive number theory. *Amer. Math. Monthly*, 77:619–621, 1970.
- [6] ERDŐS PÁL. Előadás az Eötvös-napon. https://www.youtube.com/watch?v=mZMW_zXcSi0&ab_channel=ELTEMatematikatan%C3%A1r-klub, 1993. (Link ellenőrizve: 2025.04.26.).
- [7] ERDŐS PÁL–TURÁN PÁL. On a problem of Sidon in additive number theory and on some related problems. *Journal of the London Mathematical Society*, 16:212–215, 1941.
- [8] ERDŐS PÁL, FREUD RÓBERT. On disjoint sets of differences. *J. Number Theory*, 18(1):99–109, 1984.
- [9] FRENKEL PÉTER. Integer sets with distinct subset sums. *Proceedings of the American Mathematical Society*, 126(11):3199–3200, 1998.
- [10] FREUD RÓBERT. *Lineáris algebra*. ELTE, Eötvös Kiadó, 1996. (hivatkozott rész: 354–361).
- [11] FREUD RÓBERT–GYARMATI EDIT. *Számelmélet*. Nemzeti Tankönyvkiadó Rt., 2006. (hivatkozott szakasz: 495–517).
- [12] LINDSTRÖM, BERNT. An inequality for B_2 sequences. *Journal of Combinatorial Theory*, 6:211–212, 1969.

-
- [13] RUZSA Z. IMRE. Solving a linear equation in a set of integers I. *Acta Arithmetica*, 65:259–282, 1993.
- [14] SINGER, JAMES. A theorem in finite projective geometry and some applications to number theory. *Trans.Amer.Math.Soc.*, 43:377–385, 1938.

Alulírott Nemes-Kosteleczi Anna Róza nyilatkozom, hogy a szakdolgozatom elkészítése során az alább felsorolt feladat elvégzésére a megadott MI alapú eszközt alkalmaztam:

Feladat	Eszköz	Hely	Megjegyzés
Néhány konkrét szakirodalmi tétel megkeresése az interneten	GPT-4-turbo	[9], [12], [13], [14] szakirodalmi tételek	pontos cím és évszám alapján a MI kereste meg az interneten a teljes cikkeket, utána az eredeti szövegeket használtam

A felsoroltakon túl más MI alapú eszközt nem használtam.