Eötvös Loránd Tudományegyetem
Természettudományi Kar

Sidon-sorozatok

Bsc Szakdolgozat

Készítette: Vida Péter
ELTE TTK
Alkalmazott matematikus
BSc

Témavezető: Gyarmati Katalin
Egyetemi docens
ELTE TTK
Algebra és
Számelmélet Tanszék

Budapest, 2017

Tartalomjegyzék

Köszönetnyilvánítás

Szeretném megköszönni a témavezetőmnek, Gyarmati Katalinnak, hogy elvállalta a konzulensi teendőket, minden kérdésben tudott segíteni, és ösztönzött a saját eredmények elérésére.

Továbbá szeretném megköszönni a barátnőmnek, a családomnak a támogatást, és azt, hogy mindig mellettem álltak munkám során.

1. fejezet

Bevezetés

1.1. Sidon-sorozat fogalma

1.1.1. Definíció. *Sidon-sorozatnak vagy Sidon-halmaznak nevezzük természetes számoknak egy $A = \{a_0, a_1, a_2 \dots\}$ véges vagy végtelen sorozatát, ha az A elemeiből képzett valamennyi kéttagú $a_i + a_j$ $(i \leq j)$ összeg különböző.*

Az első definícióban szereplő Sidon halmaz fogalma először Sidon Simonnak, a Fourier-sorokra vonatkozó vizsgálatai közben merült fel az 1930-as években. Az alábbiakban először véges Sidon-sorozatokkal foglalkozunk, nevezzük ezeket röviden S-sorozatnak.

A 2 hatványai például S-sorozatot alkotnak, de a későbbiekben láthatjuk, hogy megadhatók ennél sűrűbb S-sorozatok is.

1.2. Felső becslések az elemszámra

Ebben a fejezetben véges Sidon halmazok elemszámára adunk becsléseket [3] alapján.
Jelöljük az n-nél nem nagyobb elemekből álló S-sorozatok elemszámának a maximumát $s(n)$-nel, és legyen

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

egy $s = s(n)$ elemű S-sorozat. Ekkor az $a_i + a_j$ összegek mind különbözők, nem nagyobbak $2n$ -nél és számuk $\binom{s}{2} + s = \binom{s+1}{2}$ (az $i = j$ esetet nem zárjuk ki)

Tehát

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

$$\frac{(s+1)s}{2} \leq 2n$$

$$s^2 + s \leq 4n \text{ , innen mivel } s > 0$$

$$s^2 < 4n$$

amiből

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

adódik.

Mindjárt lényegesen jobb becslést kapunk, ha meggondoljuk az alábbit:

1.2.1. Tétel. *Egy sorozat akkor és csak akkor S-sorozat, ha az elemeiből képzett különbségek mind különbözőek.*

Bizonyítás:

Ha $\{a_1, a_2, \ldots a_s\}$ S-sorozat, akkor $\forall\ i, j, k, l \in \mathbb{N}$ -re:

$$a_i + a_j \neq a_k + a_l$$

$$\Downarrow$$

$$a_j - a_l \neq a_k - a_i$$

A fordított irány: $\forall i, j, k, l \in \mathbb{N}$ -re:

$$a_i - a_j \neq a_k - a_l$$

$$\Downarrow$$

$$a_i + a_l \neq a_k + a_j$$

Így a különbségek száma $\binom{s}{2}$, és ezek egyike sem nagyobb n-nél, tehát a becslésünk az alábbiként módosul:

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

$$s(s-1) \leq 2n$$

$$s^2 - s \leq 2n$$

$$(s - \tfrac{1}{2})^2 - \tfrac{1}{4} \leq 2n$$

$$(s - \tfrac{1}{2})^2 \leq 2n + \tfrac{1}{4}$$

$$s - \tfrac{1}{2} \leq \sqrt{2n + \tfrac{1}{4}}$$

$$s \leq \sqrt{2n + \tfrac{1}{4}} + \tfrac{1}{2}$$

1.3. A becslés további javítása

Kicsit más eszközöket használva, eltüntethetjük azt a $\sqrt{2}$ -es szorzótényezőt tényezőt is. Nézzük az alábbi tételt, melyet Erdős Pál és Turán Pál bizonyított [4] :

1.3.1. Tétel. *(Erdős - Turán) Egy n-nél nem nagyobb elemekből álló S-sorozat elemszámának a maximumára:*

$$s(n) < \sqrt{n} + \sqrt[4]{n} + 1.$$

A bizonyítás egy s-sel összefüggő összeg két különböző megbecslésén alapul. Az S-sorozatoknak ismét azt a meghatározását fogjuk használni, hogy a tagok közti különbségek mind-mind különböznek.
Egy később alkalmasan megválasztott t egésszel toljunk végig egy $t-1$ hosszúságú intervallumot a $[0, n]$ intervallumon, tehát nézzük a:

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

intervallumokat. Az S-sorozat egyes intervallumokba eső elemeinek a száma legyen: $A_1, A_2, \ldots, A_{n+t}$.
Minden egyes a_i t darab egymást követő intervallumban van benne, ezért:

$$\sum_{i=0}^{n+t} A_i = ts$$

Most az $(a_i, a_j), i > j$ párokat számoljuk össze, megint annyiszor, ahány intervallumban benne vannak. Ezeknek az összesített számát jelöljük D-vel. Ekkor egyrészt nyilván:

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

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

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

A D-re nyert két összefüggést, hogyha összehasonlítjuk, akkor:

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

A bal oldalon lévő második összegről már beláttuk korábban, hogy ts -sel egyenlő. Az elsőre alkalmazva a számtani és négyzetes közép közti egyenlőtlenséget:

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

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

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

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 $t = \sqrt[4]{n^3}+1$ választás mellett lesz a jobb oldal első tagja kisebb, mint $\frac{1}{2}\sqrt[4]{n}$, a négyzetögykjel alatti kifejezés pedig kisebb lesz, mint $\sqrt{n}+\frac{1}{2}\sqrt[4]{n}+\frac{1}{2}$ négyzeténél.

Ezzel a bizonyítani kívánt egyenlőtlenséget kaptuk.

2. fejezet

Sidon-sorozatok konstrukciója

2.1. Konstrukció (mod $p(p-1)$)

Az alábbiakban, Erdős Pál által bizonyított tételt használjuk [3] :

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

Véve egy g primitív gyököt modulo p, legyen a_i az :

$$x \equiv i \pmod{p-1}$$

$$x \equiv g^i \pmod{p}$$

Szimultán kongruencia-rendszer legkisebb nemnegatív megoldása (mod $p^2 - p$).

Azt kell megmutatni, hogy az:

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

kongruencia, vagy átrendezve az:

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

kongruencia csak a triviális módon teljesül. Ez más szóval azt jelenti, hogy 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 a

$$c \equiv i + j \pmod{p - 1}$$

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

kongruenciapár egyidejű teljesülésével. Az első kongruencia átírható

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

alakba, hiszen:

$$c \equiv \mathrm{i} + \mathrm{j} \pmod{p-1}$$

$$\Rightarrow c = i + j + k(p-1) \text{ , ahol k egész.}$$

$$\Rightarrow g^c = g^{i+j+k(p-1)} =$$

$$= g^i \; g^j \; g^{k(p-1)} = g^i \; g^j \; g^{(p-1)^k}$$

innen az Euler-Fermat tétel alapján:

$$g^{p-1} \equiv 1 \pmod{p}$$

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

A másodfokú egyenlet gyökei és együtthatói közötti összefüggés szerint a g^i és g^j maradékosztályok modulo p az:

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

kongruenciának a megoldásai. A fokszámtétel miatt egy másodfokú kongruenciának legfeljebb 2 gyöke van, így p prím volta miatt egyértelműen meghatározott a gyökpárja, és így az i, j pár is egyértelmű. Tehát a megkonstruált a_i-k Sidon-sorozatot alkotnak.

2.2. Konstrukció (mod $\frac{p(p-1)}{2}$)

Ebben a fejezetben saját eredményeimet ismertetem. Az előző konstrukciót kicsit módosítom. Így ugyan valamivel ritkább Sidon-sorozatot kapok, de még mindig $c\sqrt{m}$ nagyságrendűt, ahol a modulusunk $m = \frac{p(p-1)}{2}$. Ebben a konstrukcióban a modulust módosítjuk $p(p-1)$-ről $\frac{p(p-1)}{2}$-re.

Nézzük, definiáljuk a következőképp a Sidon-sorozat elemeit:

$$a_i \equiv g^{2i} \pmod{p}$$

$$a_i \equiv i \pmod{\tfrac{p-1}{2}}$$

ahol : $1 \leq i \leq \frac{p-1}{2}$
Tegyük fel, hogy ez nem Sidon. Ekkor az alábbi teljesül :

$$a_i + a_j = a_k + a_l \text{ Valamely } i, j, k, l \in \mathbb{Z}$$

Ebből következik, hogy:

$$g^{2i} + g^{2j} \equiv g^{2k} + g^{2l} \pmod{p} \text{ és:}$$

$$i + j \equiv k + l \pmod{\tfrac{p(p-1)}{2}}$$

Innen azt kapjuk, hogy :

$$i + j = k + l + \tfrac{t(p-1)}{2}$$

$$\Downarrow$$

$$g^{i+j} = g^{k+l+\frac{t(p-1)}{2}}$$

Innen négyzetre emeléssel kapjuk, hogy:

$$g^{2i+2j} = g^{2k+2l+t(p-1)}$$

$$g^{2i+2j} = g^{2k+2l} g^{t(p-1)}$$

Viszont az Euler-Fermat tétel alapján tudjuk, hogy :

$$g^{t(p-1)} \equiv 1 \pmod{p}$$

Mert g primitív gyök volt. Tehát:

$$g^{2i+2j} = g^{2k+2l} \pmod{p}$$

$$\Downarrow$$

$$g^{2i}g^{2j} \equiv g^{2k}g^{2l} \pmod{p}$$

Innen pedig hasonlóan az előző konstrukcióban leírtakhoz:$\{g^{2i}, g^{2j}\}$ és $\{g^{2k}, g^{2l}\}$ ugyanannak a másodfokú kongruenciának a gyökei, tehát:

$$g^{2i} \equiv g^{2j} \text{ és } g^{2k} \equiv g^{2l} \pmod{p} \text{ vagy fordítva.}$$

Tehát ebből az következik, hogy:

$$2i \equiv 2k \pmod{(p-1)}$$

$$\Downarrow$$

$$i \equiv k \pmod{\tfrac{p-1}{2}}$$

Ebből pedig ellentmondásra jutunk, mert :

$$a_i = a_k \quad a_j = a_l \text{ vagy pedig fordítva.}$$

Tehát ez valóban Sidon-sorozat lesz. Nézzük meg mennyire "erős" : a modulusunk : $m = \frac{p(p-1)}{2}$, elemszáma $\frac{p-1}{2}$, ez körülbelül $\frac{\sqrt{m}}{\sqrt{2}}$. Tehát ez a konstrukció rosszabb, mint az eredeti, viszont jobb lesz a következőben tárgyalt mod p^2 -es konstrukciónál, mely Erdős Páltól származik.

2.3. Konstrukció (mod p^2)

Nézzük Erdős Pálnak [2] a következő konstrukcióját, amely elemszámát tekintve kicsit gyengébb lesz az előző konstrukciónál.

Legyen $\mathcal{A} = \{\ a + p\ r_p(a^2) : 0 \leq a \leq \frac{p-1}{2}\ \}$, ahol r_p a p-vel vett osztási maradék.

1. Állítás. *$\mathcal{A} \subseteq \mathbb{Z}_{p^2}$ halmaz Sidon.*

Bizonyítás: nézzük ennek a halmaznak az elemeit:

$$\mathcal{A} = \{\ 0; 1 + p\ r_p\ (1^2)\ ;\ 2 + p\ r_p\ (2^2)\ ;\ \ldots;\ \tfrac{p-1}{2} + p\ r_p\ ((\tfrac{p-1}{2})^{\,2})\ \}$$

Ezek p-vel osztva mind különböző maradékot adnak. $|\mathcal{A}| = \frac{p+1}{2}$

$$\mathcal{A} \subseteq [\ 0; \tfrac{p-1}{2} + p\ (p-1)\ ] \text{ és } \mathcal{A} \subseteq [\ 0; p^2 - 1\ ]$$

Tegyük fel, hogy $\mathcal{A}$ nem Sidon halmaz, azaz $\exists\ 0 \leq a, b, c, d \leq \frac{p-1}{2}$ amelyre:

$$a + p\ r_p(a^2) + b + p\ r_p(b^2) = c + p\ r_p(c^2) + d + p\ r_p(d^2).$$

Ekkor:

$$a + p\ r_p(a^2) + b + p\ r_p(b^2) \equiv c + p\ r_p(c^2) + d + p\ r_p(d^2) \pmod{p}$$

$$\Downarrow$$

$$a + b \equiv c + d \pmod{p}$$

Mivel:

$$0 \leq a + b \leq p - 1 \text{ és } 0 \leq c + d \leq p - 1$$

$$\Downarrow$$

$$a + b = c + d$$

$$\Downarrow$$

$$p\ r_p(a^2) + p\ r_p(b^2) = p\ r_p(c^2) + p\ r_p(d^2)$$

$$\Downarrow$$

$$r_p(a^2) + r_p(b^2) = r_p(c^2) + r_p(d^2)$$
$$\Downarrow$$
$$a^2 + b^2 \equiv c^2 + d^2 \pmod{p}$$

Mivel:

$$a + b = c + d \Rightarrow (a+b)^2 = (c+d)^2$$
$$a^2 + b^2 \equiv c^2 + d^2 \pmod{p}$$
$$(a+b)^2 \equiv (c+d)^2 \pmod{p}$$

A két kongruencia különbsége: $\Rightarrow 2ab \equiv 2cd \pmod{p} \Rightarrow ab \equiv cd \pmod{p}$

$$A = a + b \equiv c + d \pmod{p}$$
$$B = ab \equiv cd \pmod{p}$$

Vegyük az:

$$X^2 - AX - B \equiv 0 \pmod{p}$$

Ennek megoldása {a;b} és {c;d} is. Viszont a fokszámtételből adódóan ennek a két megoldásnak egyenlőnek kell lennie, így ellentmondásra jutottunk.

2.4. Konstrukció (mod $p^2(p-1)$)

Ebben a fejezetben megpróbálom a 2.1. fejezetbeli konstrukciót prímhatványra általánosítani. Ez sikerült is, azonban sajnos a konstruált Sidon-sorozat nagyságrendje köbgyökös. Nézzük akkor a konstrukciót:

Legyen g primitív gyök (mod m), ekkor g hatványai a redukált maradékrendszert adják (mod m). Láttuk, hogy ekkor az:

$$a_i \equiv g^i \pmod{p}$$
$$a_i \equiv i \pmod{p-1}$$

konstrukció Sidon-sorozatot ad meg. Tudjuk, hogy primitív gyök akkor létezik, ha $m = 2, 4, p^\alpha, 2p^\alpha$ alakú.

Kérdés: vajon tudunk-e alkotni Sidon-sorozatot, ha p helyett p^α -t veszünk modulusnak, tehát az:

$$a_i \equiv g^i \pmod{p^\alpha}$$

$$a_i \equiv i \pmod{p(p-1)}$$

rendszerrel akarjuk a konstrukciót megvalósítani, ahol $i = 1, 2, , \ldots \varphi(p^\alpha) - 1$

Szakdolgozatomban az $\alpha = 2$ esetet vizsgálom. A kínai maradéktételt alkalmazva látjuk, hogy az:

$$x \equiv g^i \pmod{p^2}$$

$$x \equiv i \pmod{p(p-1)}$$

szimultán kongruenciarendszernek akkor van megoldása, ha :

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

Ezért definiáljuk I -t a következőképpen:

$$I = \{i : \quad i \equiv g^i \pmod{p},\ 0 \leq i \leq p(p-1)\}$$

$\forall i \in I$-re definiáljuk a_i -t úgy, hogy :

$$a_i \equiv g^i \pmod{p^2}$$

$$a_i \equiv i \pmod{p(p-1)}$$

Tudjuk, hogy a Kínai maradéktétel miatt biztosan létezik ilyen a_i.

Lássuk be akkor, hogy ezzel a konstrukcióval valóban Sidon-sorozatot alkottunk. Tegyük fel indirekten, hogy nem. Ekkor:

$$a_i + a_j = a_k + a_l$$
$$\Downarrow$$

$$a_i + a_j \equiv a_k + a_l \pmod{p^2}\ \text{, illetve:}$$

$$a_i + a_j \equiv a_k + a_l \pmod{p(p-1)}$$

$$\Downarrow$$

$$g^i + g^j \equiv g^k + g^l \pmod{p^2}, \text{ és:}$$

$$i + j \equiv k + l \pmod{p(p-1)}$$

$$\Downarrow$$

$$g^i + g^j \equiv g^k + g^l \pmod{p^2}$$

$$g^{i+j} \equiv g^{k+l} \pmod{p^2}$$

g^i, g^j illetve g^k, g^l az :

$$X^2 - AX + B \equiv 0 \pmod{p^2}$$

másodfokú kongruenciának a megoldásai. A fokszámtétel miatt tudjuk, hogy a fenti kongruenciának legfeljebb 2 megoldása van mod p.

Legyen ez d_1 és d_2. $\Rightarrow$ $p|d_1^2 - Ad_1 + B$

$$\Downarrow$$

$$X \equiv d_1 + mp \pmod{p^2} \text{ , ahol } m \in \mathbb{Z}$$

Ezt behelyettesítve a másodfokú kongruenciába kapjuk, hogy:

$$(d_1 + mp)^2 - A(d_1 + mp) + B \equiv 0 \pmod{p^2}$$

$$\Downarrow$$

$$(d_1)^2 + 2mpd_1 + m^2p^2 - Ad_1 - Amp + B \equiv 0 \pmod{p^2}$$

$$\Downarrow$$

$$\underbrace{(d_1)^2 - Ad_1 + B}_{t_1 p} + p(2md_1 - Am) \equiv 0 \pmod{p^2}$$

$$\Downarrow t_1 \text{ adott}$$

$$t_1 p + pm(2d_1 - A) \equiv 0 \pmod{p^2}$$

$$\Downarrow p \text{ -vel egyszerűsítve}$$

$$t_1 + m(2d_1 - A) \equiv 0 \pmod{p}$$

Itt két esetre választhatjuk szét. Első eset:

$$2d_1 - A \not\equiv 0 \bmod (p)$$

Ebben az esetben m egyértelműen adott mod p, mivel a:

$$t_1 + m(2d_1 - A) \equiv 0 \pmod{p}$$

lineáris kongruenciának egy megoldása van m-ben modulo p.

Tehát $X^2 - AX + B$-nek két darab gyöke van modulo p^2.

g^i, g^j is gyöke $X^2 - AX + B$ -nek, és g^k, g^l is gyöke $X^2 - AX + B$ - nek.

$$\{g^i, g^j\} \equiv \{g^k, g^l\} \pmod{p^2}$$

$$\{i, j\} \equiv \{k, l\} \pmod{p(p-1)}$$

$$a_i \equiv g^i \pmod{p^2} \text{ , és } a_i \equiv i \pmod{p(p-1)}$$

$$\Downarrow$$

$$\{a_i, a_j\} \equiv \{a_k, a_l\} \pmod{p^2(p-1)}$$

A második esetben, ha

$$2d_1 - A \equiv 0 \text{ (mod } p)$$

akkor

$$t_1 + m(2d_1 - A) \equiv 0 \pmod{p}$$

miatt:

$$t_1 \equiv 0 \pmod{p}$$

is teljesül.

Nézzük meg akkor ezt az esetet, ha mindkettő teljesül:

$$X^2 + AX + B \equiv 0 \pmod{p^2}$$

$$t_1 p = d_1^2 - Ad_1 + B \equiv 0 \pmod{p^2}$$

$$2d_1 - A \equiv 0 \pmod{p} \Rightarrow d_1 \equiv \tfrac{A}{2} \pmod{p}$$

$$\Downarrow$$

$$\tfrac{A^2}{4} - \tfrac{A^2}{2} + B \equiv 0 \pmod{p}$$

$$\Downarrow$$

$$-\tfrac{A^2}{4} + B \equiv 0 \pmod{p}$$

$$\Downarrow$$

$$B \equiv \tfrac{A^2}{4} \pmod{p}$$

Viszont a gyökök és együtthatók közötti összefüggés alapján tudjuk, hogy ebben a másodfokú kongruenciában:

$$d_1^2 - Ad_1 + B \equiv 0 \pmod{p^2}$$

$$A \equiv g^i + g^j \text{ illetve } B \equiv g^i g^j \pmod{p^2}$$

Ezeket behelyettesítve:

$$g^{i+j} \equiv \tfrac{(g^i+g^j)^2}{4} \pmod{p^2}$$

$$\Downarrow$$

$$4g^{i+j} \equiv g^{2i} + g^{2j} + 2g^{i+j} \pmod{p^2}$$

$$\Downarrow$$

$$(g^i - g^j)^2 \equiv 0 \pmod{p^2}$$

$$\Downarrow$$

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

Itt felhasználjuk a következő lemmát:

1. Lemma. $(a, m) = 1$ *esetén:*

$$a^x \equiv a^y \quad (mod\ m)$$

pontosan akkor teljesül, ha:

$$x \equiv y \quad (mod\ \mathrm{ord}_m(a))$$

ahol $\mathrm{ord}_m(a)$ *az* a *elem rendje modulo* m*.*

A fenti lemma alapján :

$$i \equiv j \pmod{\mathrm{ord}_p(g)} \tag{1}$$

De mennyi $\mathrm{ord}_p(g)$? Mivel g primitív gyök (mod p^2), ezért az Euler-Fermat tétel miatt:

$$g^x \equiv g^{x+(p-1)} \equiv g^{x+2(p-1)} \equiv \cdots \equiv g^{x+(p-1)} \equiv g^{x+(p-1)(p-1)} \pmod{p}$$

Mivel $g^0, g^1, \ldots, g^{p-1(p-1)}$ redukált maradékrendszer (mod p^2), ezért $g^0, g^1, \ldots, g^{p-1}$ -nek is redukált maradékrendszert kell adnia (mod p).

Vagyis $\mathrm{ord}_p(g) = p - 1$.

Innen tehát:

$$i \equiv j \pmod{p-1} \tag{2}$$

Másrészt az I halmaz definiciója miatt:

$$g^i \equiv i \text{ és } g^j \equiv j \pmod{p}$$

és mivel:

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

így:

$$i \equiv j \pmod{p} \tag{3}$$

Tehát (2) és (3) alapján:

$$i \equiv j \pmod{p(p-1)} \text{ azaz } i = j$$

Tehát készen vagyunk, a konstruált halmazunk valóban Sidon-sorozat. De vajon mekkora $|I|$?

Becsüljük meg $|I|$ -t , azaz az $I = \{i : \ i \equiv g^i \ \ (p) \mid 0 \leq i \leq p(p-1)\}$ halmaz elemszámát.

$$i \equiv g^i \pmod{p} \quad 0 \leq i \leq p(p-1)$$

g^i p-vel vett maradéka i-nek a $p-1$ -es maradékától függ:

$$g^{p-1}, g^{2(p-1)}, g^{3(p-1)}, \ldots, \equiv 1 \pmod{p}$$

ugyanis az Euler-Fermat tétel miatt:

$$g^{p-1} \equiv 1 \pmod{p}$$

$$\Downarrow$$

$$(g^{p-1})^k \equiv 1^k \pmod{p}$$

$$\Downarrow$$

$$g^{k(p-1)} \equiv 1 \pmod{p}$$

$i, i+p-1, i+2(p-1), \ldots$ -re :

$$g^i \equiv g^{i+p-1} \equiv g^{i+2(p-1)} \equiv \ldots$$

Itt $i, i+(p-1), i+2(p-1), \ldots, i+(p-1)p-1)$ teljes maradékrendszert alkot modulo p. Másrészt $\forall j \in \{i, i+p-1, \ldots\}$ esetén g^j modulo p vett maradéka ugyanaz.

Ezek alapján pontosan egy olyan $i^* \in \{i, i+(p-1), i+2(p-1), \ldots, i+(p-1)p-1)\}$ létezik, amelyre :

$$g^{i^*} \equiv i^* \pmod{p}$$

$$\{0, p-1, 2(p-1), \ldots, \} \leftarrow 1 \text{ darab } i^* \text{ van benne}$$

$$\{1, 1+(p-1), 1+2(p-1), \ldots, \} \leftarrow 1 \text{ darab } i^* \text{ van benne}$$

$$\{2, 2+(p-1), 2+2(p-1), \ldots, \} \leftarrow 1 \text{ darab } i^* \text{ van benne}$$

$$\vdots$$

$$\{p-2, p-2+(p-1), p-2+2(p-1), \ldots, \} \leftarrow 1 \text{ darab } i^* \text{ van benne}$$

Tehát $|I| = p-1$. Viszont ez nagyon kevés elemszámú konstrukció lesz, kb. a mohó algoritmussal megegyező méretű, mert a konstruált Sidon halmaz mérete körülbelül köbgyöke a modulusnak.

2.5. Sidon halmazok összetett modulus esetén

Az alábbiakban azt fogom megmutatni, hogy összetett modulus esetén optimális Sidon halmaz nem konstruálható a Kínai maradéktétel egyszerű felhasználásával. Ehhez gráfelméletet fogok alkalmazni:

2. Lemma. (Zarankiewicz [7])
Adott egy G páros gráf, aminek az egyik osztályában n, a másik osztályában m darab csúcs van. Amennyiben G nem tartalmaz $K_{s,t}$ gráfot, ahol $K_{s,t}$ a Kuratowski-féle teljes páros gráf, akkor a következő becslést adhatjuk G élszámára:

$$|E(G)| < (s-1)^{1/t}(n-t+1)m^{1-1/t} + (t-1)m$$

Például amennyiben G nem tartalmaz $K_{2,2}$ -t, akkor az élszámára az alábbi becslés adható:

$$|E(G)| < (2-1)^{1/2}(n-2+1)m^{1-1/2} + (2-1)m = (n-1)\sqrt{m} + m.$$

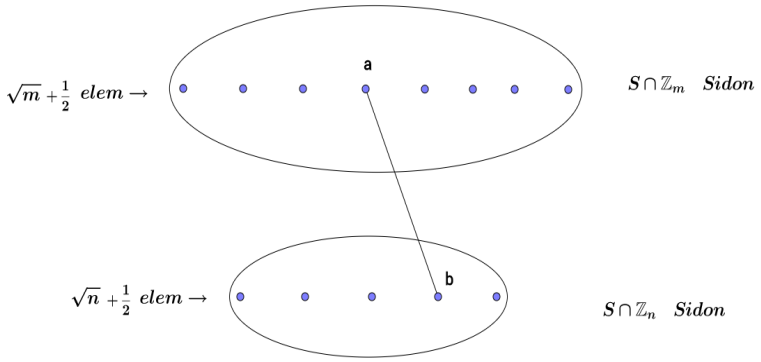
Tegyük fel, hogy $S \subseteq \mathbb{Z}_{mn}$ Sidon halmaz. Ekkor $|S| \leq \sqrt{mn} + \frac{1}{2}$. Definiáljuk $S \cap \mathbb{Z}_m$ és $S \cap \mathbb{Z}_n$ halmazokat a következőképpen:

$$S \cap \mathbb{Z}_m = \{a \in \mathbb{Z}_m : \exists s \in S \quad a \equiv s \bmod (m)\ \}$$

$$S \cap \mathbb{Z}_n = \{a \in \mathbb{Z}_n : \exists s \in S \quad a \equiv s \bmod (n)\ \}$$

2.5.1. Tétel. *Ha $S \subseteq \mathbb{Z}_{mn}$ Sidon , $S \cap \mathbb{Z}_m$ és $S \cap \mathbb{Z}_n$ is Sidon, akkor :*
$|S| \leq \sqrt[4]{m}\sqrt{n} + \sqrt{m} + 2$

Ez azért érdekes, mert a standard Sidon halmazos felső becslésnél egy nagyságrenddel jobb. Vagyis nem reménykedhetünk abban, hogy a Kínai maradéktétel egyszerű felhasználásával optimális méretű Sidon halmazt tudunk konstruálni.
Lássuk a bizonyítást: konstruáljuk az alábbi G' páros gráfot:



Ahol két pont között akkor van él, ha $\exists s \in S$ úgy, hogy :

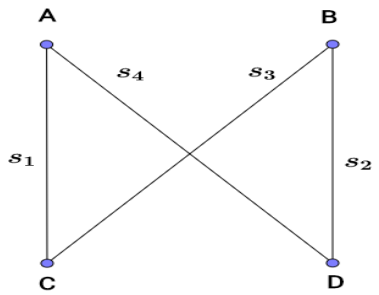
$$s \equiv a \pmod{m}$$

és

$$s \equiv b \pmod{n}$$

2. Állítás. *Ez a G' gráf nem tartalmaz $K_{2,2}$ -t.*

Bizonyítás: Tegyük fel, hogy tartalmaz, ekkor tekintsük ezt:



Az élek definíciója miatt ekkor:

$$s_1 + s_2 \equiv A + B \mod (m)$$

$$s_3 + s_4 \equiv A + B \mod (m)$$

$$\Downarrow$$

$$s_1 + s_2 \equiv s_3 + s_4 \mod (m)$$

Azaz $m|s_1 + s_2 - s_3 - s_4$.

Illetve:

$$s_1 + s_2 \equiv A + B \mod (n)$$

$$s_3 + s_4 \equiv A + B \mod (n)$$

$$\Downarrow$$

$$s_1 + s_2 \equiv s_3 + s_4 \mod (n)$$

Vagyis $n|s_1 + s_2 - s_3 - s_4$.

Mivel $(m, n) = 1$ ezért:

$$mn|s_1 + s_2 - s_3 - s_4$$

azaz:

$$s_1 + s_2 \equiv s_3 + s_4 \pmod{mn}$$

Viszont itt ellentmondásra jutottunk, mert S Sidon. Tehát valóban nem tartalmaz $K_{2,2}$-t, ezért az előbb definiált gráfelméleti lemmát tudjuk alkalmazni:

$$|S| \leq |E(G')| < \sqrt[4]{m}\sqrt{n} + \sqrt{m} + 2$$

3. fejezet

További konstrukciók

Érdekes felvetés, hogy néhány nevezetes sorozat Sidon-e? Illetve ha nem, akkor milyen módosításokkal tehetjük azzá. Ebben a fejezetben ezt fogom vizsgálni.

3.1. Fibonacci sorozat Sidon-e?

A Fibonacci-számok a matematikában az egyik legismertebb másodrendben rekurzív sorozat elemei. Az első két elem 0 és 1, a további elemeket az előző kettő összegeként kapjuk. Képletben:

$$F_n = \begin{cases} 0, & \text{ha } n = 0; \\ 1, & \text{ha } n = 1; \\ F_{n-1} + F_{n-2}, & \text{ha } n > 1. \end{cases}$$

Tegyük fel, hogy $n > 1$, ekkor a Fibonacci sorozat elemei : $2, 3, 5, 8, 13 \ldots$

Tudjuk, hogy :

$$F_n = F_{n-1} + F_{n-2},$$

Adjunk hozzá mindkét oldalhoz F_n -t

$$2F_n = F_n + F_{n-1} + F_{n-2}$$

$F_{n+1} = F_n + F_{n-1}$ -et beírva:

$$F_n + F_n = F_{n+1} + F_{n-2}$$

Tehát a Fibonacci-sorozat nem Sidon. Itt vezessünk be egy új fogalmat:

3.1.1. Definíció. *Gyenge, vagy úgynevezett weak Sidon-sorozatnak nevezzük természetes számoknak egy $A = \{a_0, a_1, a_2 \dots\}$ véges sorozatát, ha az A elemeiből képzett valamennyi kéttagú $a_i + a_j$ $(i < j)$ összeg különböző.*

Azaz teljesen hasonlóan definiáljuk, mint a Sidon-sorozatokat, azzal a különbséggel, hogy az $i = j$ esetet kizárjuk.

3. Állítás. *A Fibonacci sorozat n>1 esetén gyenge Sidon sorozat.*

Bizonyítás: Először belátjuk, hogy a Fibonacci sorozat szigorúan monoton növekvő.

$$\forall \text{ n-re: } F_n \leq F_{n+1}$$

$$F_{n+1} = F_n + F_{n-1} \text{ -t helyettesítve:}$$

$$F_n \leq F_n + F_{n-1}$$

$$0 \leq F_{n-1}$$

Ez pedig teljesül, hiszen a Fibonacci sorozat minden tagja pozitív.

Tudjuk, hogy $n = 5$ -re gyenge Sidon, mert a $\{2,3,5,8,13\}$ halmaz teljesíti a feltételeket.
Tegyük fel, hogy n -re igaz, de ha F_{n+1} -et hozzávesszük, már nem lesz gyenge Sidon. Ez nem lehet, hiszen F_{n+1} csak úgy ronthatná el a gyenge Sidon tulajdonságot, ha:

$$F_{n+1} + F_j = F_k + F_l \text{ valamely } j, k, l \in N \text{ -re}$$

Viszont, mivel szigorúan monoton növő a sorozat, ezért:

$$F_{n+1} + F_j > F_n + F_{n-1}$$

Ebből következik, hogy sehogy sem állítható elő ez az összeg, tehát F_{n+1} nem rontotta el a gyenge Sidon tulajdonságait.

3.2. Sidon-sorozat megkonstruálása lineáris rekurzióval

Az előbb láthattuk, hogy bizonyos feltételek mellett, a Fibonacci-sorozat gyenge Sidon-sorozat volt. Most nézzünk egy általánosabb rekurziót, és vizsgáljuk meg, hogy mely esetekben lehet Sidon.

3.2.1. Definíció. *Egy $a_n (n \in \mathbb{N})$ sorozatra vonatkozó,*
$a_{n+k} = c_1 a_{n+k-1} + \cdots + c_k a_n$ *alakú képletet (homogén, k-adfokú) állandó együtthatós lineáris rekurziónak nevezünk, ahol k rögzített pozitív egész, a* $c_1, \ldots, c_k \quad c_k \neq 0$ *együtthatók pedig rögzített valós számok.*

A továbbiakban az $k = 2$ esetet vizsgáljuk részletesebben, azaz az :

$$a_1 = \alpha, a_2 = \beta$$

$$a_{n+2} = c_1 a_{n+1} + c_2 a_n$$

Ahol α, β, c_1, c_2 rögzített, valós számok.

Azt vizsgáljuk, hogy ha $c_1 = 1, c_2 > 1$ egész számok, akkor az:

$$a_{n+2} = a_{n+1} + c_2 a_n$$

$a_0 = 0; a_1 = 1; a_2 = 1$ rekurzióval megadott sorozat gyenge Sidon halmaz-e?

Ekkor a sorozatunk:

$$a_3 = 1 + c_2$$

$$a_4 = 1 + 2c_2$$

$$a_5 = 1 + 3c_2 + c_2^2$$

$$\vdots$$

A sorozat első 3 tagját elhagyva a kapott sorozat Sidon. Ezt szeretnénk belátni. Először belátjuk, hogy monoton növő:

$$a_n \leq a_{n+1}$$

$$a_n \leq a_n + c_2 a_{n-1}$$

$$0 \leq c_2 a_{n-1}$$

Ez pedig teljesül, mert a sorozat minden eleme pozitív, és c_2 -ről is feltettük, hogy az.
Most vizsgáljuk meg a tagok közti különbségeket, hiszen azt akarjuk belátni, hogy nem állhat elő egy szám se kétféle különbségként.

A tagok differenciáját d-vel jelölve kapjuk, hogy :

$$d(a_4; a_3) = c_2.$$

$$d(a_5; a_4) = c_2^2 + c_2$$

Ezek a különbségek c_2 -nek polinomjai lesznek, és monoton növőek, hiszen:

$$a_{n+2} - a_{n+1} = c_2 a_n > c_2 a_{n-1} = a_{n+1} - a_n$$

Tudjuk, hogy az első 4 tag Sidon-sorozatot alkot. Ha hozzáveszünk egy tagot, akkor az csak úgy ronthatja el a Sidon tulajdonságot, ha a többi taggal képzett különbsége megegyezik két, már meglévő tag különbségével.

Viszont:

$$a_{n+2} - a_{n+1} = c_2 a_n > a_n = a_n - a_0$$

Tehát ez nem lehetséges, vagyis a kapott sorozat gyenge Sidon.

Ha tovább vizsgálnánk a lineáris rekurziókat, feltéve, hogy $c_1, c_2 > 1$, akkor hasonló gondolkodással rájöhetünk, hogy itt is könnyen tudunk gyenge Sidonokat konstruálni.

3.3. Sidon-sorozat konstruálása a mohó algoritmus segítségével

A mohó algoritmus vagy greedy algoritmus az a problémamegoldó algoritmus, amely helyi optimumok megvalósításával próbálja megtalálni a globális optimumot. Főként gráfelméletben használják, előnye, hogy sok problémát megoldhatunk vele, viszont a hátránya, hogy általában nem az optimális algoritmust fogja szolgáltatni.

Legyen például $n = 100$. Egy Sidon-sorozat megszerkesztéséhez próbálkozhatunk ezzel algoritmussal, [6] amely szerint mindig kiválasztjuk a legkisebb olyan számot, amely nagyobb az előzőleg kiválasztott számoknál, és teljesíti a Sidon-tulajdonságot.

Tehát elindulunk az első tagból, jelen esetben az 1-ből majd hozzávesszük a legkisebb elemet a 2-t, hiszen így még Sidon marad. Azután folytatjuk az eljárást, a 3-mat már nem vehetjük hozzá hiszen $2 + 2 = 3 + 1$ elrontaná a Sidon-tulajdonságot. Ezt az algoritmust folytatva az:

$$1, 2, 4, 8, 13, 21, 31, 45, 66, 81, 97$$

számokat kapjuk.
Felmerül a kérdés, hogy ez lesz-e a leghosszabb Sidon-sorozat 100-ig? Erre a válasz nem, mivel az :

$$1, 3, 7, 25, 30, 41, 44, 56, 69, 76, 77, 86$$

sorozat hosszabb, lásd [6].

Így tehát ahogy említettem, mohó algoritmussal már 100-ig sem kapjuk meg az optimális, leghosszabb Sidon-sorozatot, viszont az előnye, hogy bármilyen hosszú sorozatot megszerkeszthetünk a segítségével.

Megjegyezzük, hogy a mohó algoritmussal megadott $S \subseteq \{1, 2, \dots\}$ Sidon halmaz mérete $c\sqrt[3]{n}$.

Irodalomjegyzék

[1] *C*illeruelo, J.; Ruzsa, I.; Vinuesa, C. (2010), "Generalized Sidon sets" , Advances in Mathematics, 225: 2786–2807

[2] *E*rdős, P. & Rényi, A. (1960), "Additive properties of random sequences of positive integers", Acta Arithmetica 6: 83–110

[3] *E*rdős Pál–Surányi János, Válogatott fejezetek a számelméletbol , Polygon, Szeged, 1996, 234-239.

[4] *E*rdős, P. & Turán, P. (1941), "On a problem of Sidon in additive number theory and on some related problems", J. London Math. Soc. 16: 212–215

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

[6] *h*ttps://www.ms.sapientia.ro/ kasa/BegeKasaKomb.pdf 73.

[7] *h*ttps://en.wikipedia.org/wiki/Zarankiewicz_problem