Számtani sorozatokat nem tartalmazó halmazok

2022. augusztus-november

Füredi Erik

ELTE TTK-Matematika BSc 2. év

e-mail: erikfuredi@gmail.com

Témavezető: Pach Péter Pál tudományos főmunkatárs (BME)

MTA-BME Lendület Aritmetikai Kombinatorika Kutatócsoport

1. Új eredmények

Legyen $r_k(\mathbb{Z}_m^n)$ a $\mathbb{Z}_m^n$ csoport legnagyobb, k hosszú számtani sorozatot nem tartalmazó részhalmazainak mérete. A dolgozat $r_k(\mathbb{Z}_m^n)$ értékével foglalkozik az $m = p$ páratlan prím feltétellel néhány speciális esetben.

Az általam elért új eredmények főképp a felső becsléshez kapcsolódnak:

- $r_p(\mathbb{Z}_p^3) \leq p^3 - 2p^2 + p - \frac{1}{2} + \frac{4p-2-\sqrt{8p^6-20p^5+17p^4-12p^3+20p^2-16p+4}}{2p^2}$ (5. tétel), ennek következménye, hogy $r_p(\mathbb{Z}_p^3) \leq p^3 - 2p^2 - (\sqrt{2}-1)p + 2$ (5.a tétel), illetve konkrét becslések kis p-kre.
- Az 5. tétel bizonyításának általánosításából $3 \leq k \leq p$ esetén $r_k(\mathbb{Z}_p^{n+1}) \leq p(r_k(\mathbb{Z}_p^n)) - \frac{r_k(\mathbb{Z}_p^n)}{p^n} + \frac{1}{2} - \frac{\sqrt{4r_k(\mathbb{Z}_p^n)^2+p^{2n}-4r_k(\mathbb{Z}_p^n)p^n-4r_k(\mathbb{Z}_p^n)^2p^{n+1}+4r_k(\mathbb{Z}_p^n)p^{2n+1}}}{2p^n}$ (k és n pozitív egész számok), ez a 6. tétel.
- $r_5(\mathbb{Z}_5^3) < 74$ és $r_7(\mathbb{Z}_7^3) < 243$ (3. és 4. becslés), mindkettő 1-gyel jobb az 5. tételből adódó becslésnél.
- Végül Kovács Benedek $r_p(\mathbb{Z}_p^3)$-re vonatkozó alsó becslésének befejezésén pontosabb számolással aprót erősítettem $r_p(\mathbb{Z}_p^3) \geq (p-1)^3 + p - 2\sqrt{p} + O(1)$-ről, ahol a hibatag inkább negatívnak tűnt, $r_p(\mathbb{Z}_p^3) > (p-1)^3 + p - 2\sqrt{p}$-re (4. tétel).

A dolgozat tartalmaz a témában mások által elért új eredményeket is:

- A kéziratukat Pach Péter Pálon keresztül REU-s csapatunk rendelkezésére bocsátó Christian Elsholtz és Jacob Führer belátták, hogy $r_p(\mathbb{Z}_p^3) \geq (p-1)^3 + \frac{p-1}{2}$.
- Kovács Benedek programmal talált $r_5(\mathbb{Z}_5^3) \geq 70$-et és $r_7(\mathbb{Z}_7^3) \geq 225$-öt bizonyító (szimmetrikus) konstrukciói (1. és 2. becslés).

2. Előszó

2022 júliusában részt vettem egy nyári REU-ban (erről: https://coge.elte.hu/reu22.html) az ELTE-n, ahol csapatom a „Számtani sorozatokat tartalmazó és nem tartalmazó halmazok" témát kutatta. Témavezetőnk Pach Péter Pál volt, akit két alkalommal Sándor Csaba helyettesített. Csapattársaim Kovács Benedek, Simon Dániel és Velich Nóra voltak. Számtani sorozatokat nem tartalmazó halmazokkal foglalkoztunk, erről a témáról szól ezen munka is. Annak oka, hogy egyedül írtam ezen TDK-pályamunkát az, hogy két csapattársam is már befejezte a mesterszakot, Kovács Benedek az ELTE-n, Simon Dániel a Cambridge-i egyetemen, és a harmadik csapattársam, Velich Nóra is külföldön, a Cambridge-i egyetemen folytatja tanulmányait. A kutatás során Pach Péter Pálon keresztül megkaptuk Christian Elsholtz és Jakob Führer „Maximal m-progression free-sets in $\mathbb{Z}_m^n$" című kéziratát, amely a kutatás során és ezen munka írásánál is felhasználásra került. Köszönöm nekik kéziratuk rendelkezésre bocsátását. Köszönöm Sándor Csabának, hogy felhívta a figyelmet $r_p(\mathbb{Z}_p^2) = (p-1)^2$ és $r_p(\mathbb{Z}_p^3) \geq (p-1)^3 + 1$ bizonyításának elmondásával ezen esetekre és $r_p(\mathbb{Z}_p^3)$ egyes speciális eseteire. Köszönöm Kovács Benedek segítségét. Köszönöm Pach Péter Pál segítségét.

3. Bevezetés

Az írásban a következő definícióval kapott számok kiszámításával illetve becslésével foglalkozunk.
Definíció: $r_k(\mathbb{Z}_m^n)$ jelöli $\mathbb{Z}_m^n$ legnagyobb k hosszú számtani sorozatot nem tartalmazó részhalmazainak elemszámát.

Megjegyezzük, hogy $r_k(\mathbb{Z}_m^n)$ vizsgálata csak $k, m \geq 3$-ra érdekes.
Ezen írás azon esettel foglalkozik, amikor $m = p$ prímszám, ezen belül is főképp $r_p(\mathbb{Z}_p^3)$-bel.

Néhány ismert eredmény az $m = p$ esetben ([3] alapján):

- $r_p(\mathbb{Z}_p^n) \geq (p-1)^n$ ugyanis $[0, p-2]^n$ nem tartalmaz p hosszú számtani sorozatot. (Ennek oka, hogy p hosszú számtani sorozatban az i. koordináták (számjegyek) vagy megegyeznek vagy páronként különbözők minden $1 \leq i \leq n$-re és a páronként különbözés itt nem lehetséges, az egyforma koordináták pedig csak egy tagot adnak.)
- $p \geq 3$ prímekre Frankl, Graham és Rödl eredménye ([5]), hogy $r_p(\mathbb{Z}_p^{2p}) \geq p(p-1)^{2p-1}$.
- Elsholtz és Pach egy általánosabb eredményéből ([4]) adott $k, p \geq 3$ esetén $\alpha_{k,p} := \lim_{n\to\infty} r_k(\mathbb{Z}_p^n)^{\frac{1}{n}}$ létezik és szuprémum, így adott n melletti konstrukcióból az alsó korlát n-edik gyökét véve $\alpha_{k,p}$-re kapunk alsó becslést. Ez mutatja a kis n-eknél adott alsó korlátok hasznosságát.

A következőkben használjuk, hogy $\mathbb{Z}_p^n$ izomorf $AG(n,p)$-vel. $\mathbb{Z}_m^n = \mathbb{Z}_p^n$ elemeit pontoknak hívjuk, p hosszú számtani sorozatok elemei (pontjai) egy egyenesre esnek. Ha $p-1$ pont egy egyenesre esik, az is ekvivalens azzal, hogy a megfelelő elemek $p-1$ hosszú számtani sorozatot alkotnak, sőt ez még $(p-2)$-re is teljesül. A $\mathbb{Z}_p^n$-nel izomorf $AG(n,p)$-ben $AG(2,p)$-vel izomorf részhalmazokat síkoknak, az $AG(n-1,p)$-vel izomorf részhalmazokat hipersíkoknak nevezzük, ezen elnevezésekkel illetjük $\mathbb{Z}_p^n$ nekik megfelelő részeit is. $AG(2,p)$-ben két egyenes vagy párhuzamos vagy van közös pontjuk. Az $m = p$ eset szabályosabb, mint az általános, az egyenesek, amelyek egy számtani sorozatot alkotó elemekből állnak, pontosan p elemet (pontot) tartalmaznak és minden pont összes egyenese ugyanannyi pontot tartalmaz (léteznek p rendű affin geometriák). A geometriai szemléletet használjuk alapvetően a későbbiekben, egyenesekként tekintünk a számtani sorozatokra és egyes bizonyításokban illeszkedéseket számolunk.

$k = 3$ esetén ha $m = 3$, 4 vagy 5, akkor három elem (pont) pontosan akkor alkot számtani sorozatot, hogyha egy egyenesre esnek, utóbbi elegendő előbbihez.

Ezen műben az egy dologra vonatkozó becsléseket becslésnek, az általánosabbakat tételnek hívjuk. Az új állításoknál feltüntetjük, hogy ki(k)től származnak. $\lfloor x \rfloor$ az x szám egészrészét, (x,y) az x és y legnagyobb közös osztóját jelöli. Koordinátákat szögletes zárójel közé írunk. Konstrukciókat bemutató ábrákon pontot négyzet középpontjában lévő körlap jelöl.

A következő, 4. fejezet a $\mathbb{Z}_p^2$-beli $k = p$ és $k = p-1$ esetekről szól, amelyekre ismert a pontos érték, egy-egy p-ben másodfokú normált polinom. Ezután $r_p(\mathbb{Z}_p^3)$ becsléséről szól az 5., leghosszabb fejezet ismert és új alsó és felső becslésekkel, amelyek legpontosabb normált harmadfokú polinomjai közt p^2-es nagyságrendű a különbség, az általános becsléseket $p = 5$-re és $p = 7$-re konstrukcióval és felső becsléssel erősítve. Végül a 6. fejezetben az $r_p(\mathbb{Z}_p^3)$-re vonatkozó felső becslés módszerének általánosítása $r_k(\mathbb{Z}_p^{n+1})$-re $r_k(\mathbb{Z}_p^n)$ függvényében felső korlátot ad.

4. $r_p(\mathbb{Z}_p^2)$ és $r_{p-1}(\mathbb{Z}_p^2)$

$r_p(\mathbb{Z}_p^1) = p-1$ triviális. $r_p(\mathbb{Z}_p^2) \geq (p-1)^2$ a $[0,p-2]^2$ konstrukcióból. Itt $r_p(\mathbb{Z}_p^2) = (p-1)^2$ teljesül, ezt Jamison bizonyította ([7]) és tőle függetlenül Brouwer és Schrijver is bizonyították ([1]). $AG(2,p)$-re vonatkozó állításként $r_p(\mathbb{Z}_p^2) = (p-1)^2$-hez elég belátni, hogy $2p-1$-nél kevesebb pontra van olyan egyenes $\mathbb{Z}_p^2$-ben, amely nem tartalmaz pontot közülük. A következőkben az 1. tételig [6]-ot követjük.

Definíció: $AG(2,p)$ pontjainak egy részhalmaza s-szeresen lefogó ponthalmaz, hogyha minden egyenesről legalább s pontot tartalmaz.

Egy általánosabb tétel prímekre vonatkozó alesete mutatja, hogy 1-szeresen lefogó ponthalmaz elemszáma legalább $2p-1$, amiből $r_p(\mathbb{Z}_p^2) = (p-1)^2$, emellett azt is, hogy 2-szeresen lefogó ponthalmaz elemszáma legalább $3p-1$:

1. Tétel (A. Blokhuis)**.** *Ha $(s,p) = 1$ és p prím, az $AG(2,p)$ affin sík bármely s-szeresen lefogó ponthalmaza legalább $(s+1)p-1$ elemű.*

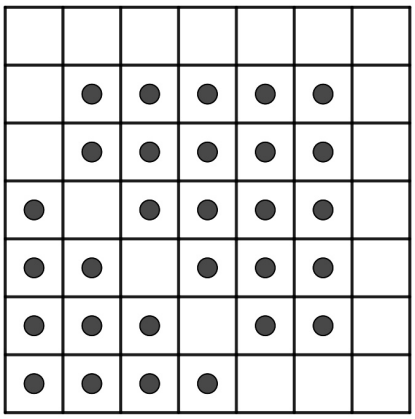
A tételt itt nem bizonyítjuk, [6]-ban szereplő indirekt bizonyítása egy, a(z elvileg s-szeresen lefogó) pontok koordinátáiból képzett kétváltozós polinomot, az úgynevezett Rédei-polinomot használja ($r_p(\mathbb{Z}_p^2) = (p-1)^2$-nek ismert más polinomos bizonyítása is).

A tételből minden 2-szeresen lefogó ponthalmaz legalább $3p-1$ pontból áll, hiszen $p-1$ egy egyenesen lévő pontnak megfelelő elemek $p-1$ hosszú számtani sorozatatot alkotnak és viszont, $r_{p-1}(\mathbb{Z}_p^2) \leq p^2 - 3p + 1$. Itt $p \geq 3$ esetén egyenlőség van, amit $r_p(\mathbb{Z}_p^3)$ becslésénél a $p = 5$ és $p = 7$ esetekben használni fogunk. Konstrukció $p^2 - 3p + 1$ pontra, amelyekből nincs $p-1$ egy egyenesen, a konstrukció az összes pontot (elemet) tartalmazza az alább ki nem zártakon kívül:

- Az utolsó sort és oszlopot ($y = p-1$ illetve $x = p-1$ egyenletűeket) elhagyjuk. Így minden egyenesről legalább 2 pontot elhagyunk az elhagyottakkal párhuzamos, tőlük eltérő egyenesek és a $(p-1, p-1)$-en átmenő egyenesek kivételével. Ez $2p-1$ pont elhagyása.
- Az $x + y \equiv -3 \pmod{p}$ egyenletű egyenes maradék $p-2$ pontját is elhagyjuk. Eddig három egymást metsző egyenest hagytunk el, a kettő metszéspontján átmenő, a harmadikkal párhuzamos három egyenest kell még kizárni (amelyeken $p-1$ pont maradt).
- Végül elhagyjuk a $[p-2, 0]$ és $[0, p-2]$ pontokat, amelyekkel az említett három, $x+y \equiv -2 \pmod{p}$, $x = p-2$ illetve $y = p-2$ egyenletű egyeneseken sem marad $(p-2)$-nél több pont.

Összesen $(2p-1) + (p-2) + 2 = 3p-1$ pont elég volt minden egyenesről legalább kettő pont elhagyásához.

Ábra $p = 7$-re az így kapott 29 pontú halmazról, amelyben nincs 6 pont egy egyenesen (nincs 6 hosszú számtani sorozat):



1. ábra

p páratlan prímekre $r_p(\mathbb{Z}_p^2)$ és $r_{p-1}(\mathbb{Z}_p^2)$ is p másodfokú egy főegyütthatójú polinomja. Kérdéses, hogy több dimenzióra is igaz-e hasonló, $r_p(\mathbb{Z}_p^n)$ felírható-e p polinomjaként, ha már $(p-1)^n$ és $(p-1)p^{n-1}$ közé esik (utóbbi p^{n-1} párhuzamos egyenest nézve triviális).

5. $r_p(\mathbb{Z}_p^3)$ becslése

Ebben a fejezetben alsó becsléseknél konstrukciókat, felső becsléseknél az előző fejezet $r_p(\mathbb{Z}_p^2) = p^2 - 2p + 1$ és $r_{p-1}(\mathbb{Z}_p^2) = p^2 - 3p + 1$ állításait alkalmazó becsléseket mutatunk be.

5.1. Az eddig ismert korlátok

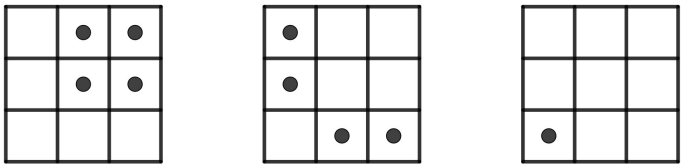
Mivel $[0, p-2]^3$ nem tartalmaz teljes egyenest, $r_p(\mathbb{Z}_p^3) \geq (p-1)^3$. Ezt $p \geq 3$-ra eggyel meg lehet javítani:

2. Tétel.
p páratlan prímre $r_p(\mathbb{Z}_p^3) \geq (p-1)^3 + 1$.

Bizonyítás:
Konstrukció: Az első $p-1$ síkról (ahol a z-koordináta legfeljebb $p-2$) két-két nem párhuzamos egyenest hagyunk el, a $z = c$ síkon két, $[0, 0, c]$ ponton átmenő egyenes ($0 \leq c \leq p-2$) összesen $2p-1$ pontját úgy, hogy mind a $p+1$, állandó z-koordinátájú egyenesre lehetséges meredekség előforduljon a $2p-2$ elhagyott egyenes közt, míg az utolsón a $[0, 0, p-1]$ pontot tesszük be. Ez $2p - 2 \geq p + 1$ miatt lehetséges.

Ekkor p pont egy egyenesen csak mind a p síkról egy-egy pontot, így $[0, 0, p-1]$-et tartalmazva lehet (egy síkon két metsző egyenes minden egyenesről tartalmaz pontot). A $[0, 0, p-1]$-en átmenő egyenesekből az $x = 0 = y$ egyenletű többi pontját elhagytuk, a többi egyenese a $z = 0$ síkra levetítve $[0, 0, 0]$-n átmenő, a síkban maradó $p+1$ egyenes valamelyike lesz. Minden ilyen egyenessel párhuzamos egyenes van az első $p-1$ sík $2p-2 (\geq p+1)$ elhagyott egyenese közt, ez pedig az ilyen vetületű egyenesekből pontelhagyással jár a vetülettel párhuzamos egyenest elhagyó síkon (az elhagyás síkján erről az elhagyott egyenesről kellene pont). ■

A tétel következménye az első nemtriviális $p = 3$ esetben, hogy $r_3(\mathbb{Z}_3^3) \geq 9$, egy konstrukciót az ábra mutat.



2. ábra (Sorra a $z = 0$, $z = 1$ és $z = 2$ síkokkal vett metszet)

A következő tétel alapján $r_3(\mathbb{Z}_3^3) \leq 10$. Mint a következő 5.2. alfejezetből kiderül, 10 pontú konstrukció nem lehetséges, így $r_3(\mathbb{Z}_3^3) = 9$. Az ennél nagyobb p-kre már nem ismert $r_p(\mathbb{Z}_p^3)$ pontos értéke.

Teszünk egy kis kitérőt. $p = 3$-ra $r_3(\mathbb{Z}_3^n)$ pontos értéke nemcsak $n = 3$-ra, hanem $n = 6$-ig

is ismert. $r_3(\mathbb{Z}_3^4) = 20$-at Pellegrino 1971-ben bizonyította. Ennek [2]-beli bizonyításánál a 21-es konstrukció kizárásának módszere hasonlít a későbbi felső becslésekére, $r_3(\mathbb{Z}_3^3) = 9$-et és a párhuzamos hipersíkokon lévő pontpárok illetve ponthármasok darabszámát használja, utóbbihoz segít, hogy $p = 3$ miatt 3 pont nem lehet egy egyenesen, így bármely három pont (és síkjuk) ugyanannyi 3-dimenziós hipersíkban szerepel együtt. Emellett ([4] alapján) $r_3(\mathbb{Z}_3^5) = 45$ és $r_3(\mathbb{Z}_3^6) = 112$ ismert, utóbbit Potechin látta be számítógép segítségét is felhasználva.

Ezután a felső becsléssel folytatjuk.

3. Tétel.
$r_p(\mathbb{Z}_p^3) \leq p^3 - 2p^2 + 1$ *minden* p *prímre.*

Bizonyítás ([3] és [8] nyomán):
Mivel $(p-2)p^2 < p^3-2p^2+1$, ha létezik p hosszú számtani sorozatot, teljes egyenest nem tartalmazó konstrukció több mint $p^3 - 2p^2 + 1$ ponttal, akkor p^2 párhuzamos egyenes valamelyikéről pontosan $p-1$ pontot tartalmazna. Ezen egyenest $p+1 = \frac{p^3-p}{p^2-p}$ sík tartalmazza, ugyanis $\mathbb{Z}_p^3$ többi eleme pontosan egy síkon szerepel az egyenes pontjaival együtt. Ekkor az ezen egyenest tartalmazó $p+1$ síkon az egyenes $p-1$ pontján kívül legfeljebb $r_p(\mathbb{Z}_p^2)-(p-1) = (p-1)^2-(p-1)$ pont lehet, összesen pedig $(p+1)((p-1)^2-(p-1))+(p-1) = p^3-2p^2+1$ db pont, amelyből az állítás következik. ■

Összességében tehát megkaptuk, hogy p páratlan prímszámra $p^3 - 3p^2 + 3p = (p-1)^3 + 1 \leq r_p(\mathbb{Z}_p^3) \leq p^3 - 2p^2 + 1$. Eszerint $r_p(\mathbb{Z}_p^3)$ p^3-ös nagyságrendű, és a felső és az alsó korlát különbsége p^2-es nagyságrendű. A következőkben kicsit javítunk az alsó és a felső becsléseken, de a különbség p^2-es nagyságrendje nem változik.

5.2. Új becslések

Elsholtz és Führer kéziratuk ([3]) alapján $[0, p-2]^3$-hoz képest csak az utolsó két sík pontjainak megváltoztatásával konstrukciót adva belátták, hogy
$r_p(\mathbb{Z}_p^3) \geq (p-1)^3 + \frac{p-1}{2}$.
Ennek ismeretében [3] $r_7(\mathbb{Z}_7^3)$-re adott alsó becslésének konstrukciójából is ötletet merítve csapattársam, Kovács Benedek a soron következő konstrukcióval tovább javította az alsó korlátot ugyancsak az utolsó két síkot használva $(p-1)^3 + p - 2\sqrt{p} + O(1)$-re. Ezen minimálisat javítottam a következő bizonyítás $t+s < 2\sqrt{p}$-ről szóló befejezésével, vagyis $\lfloor\sqrt{p}\rfloor + \lfloor\frac{p}{\lfloor\sqrt{p}\rfloor}\rfloor < 2\sqrt{p}$ bizonyításával $p > 3$-ra (a hibatag durvább becslésnél negatív):

4. Tétel (Kovács B., Füredi E.)**.**
$r_p(\mathbb{Z}_p^3) > (p-1)^3 + p - 2\sqrt{p}$ *minden* p *prímszámra.*

Bizonyítás:
$p = 2$-re és 3-ra $r_2(\mathbb{Z}_2^3) = 1 > 1 + 2 - 2\sqrt{2} \approx 0,17$ és $r_3(\mathbb{Z}_3^3) = 9 > 8 + 3 - 2\sqrt{3} \approx 7,54$.

Ezután $p \geq 5$-re konstrukciót adunk. Legyen $\lfloor \sqrt{p} \rfloor = s$ és $\lfloor \frac{p}{\lfloor \sqrt{p} \rfloor} \rfloor = \lfloor \frac{p}{s} \rfloor = t$. Ekkor $p \geq 5$-re $1 < s < \frac{p}{2}$, így s és t is 1-nél nagyobb és p-nél kisebb egész szám.

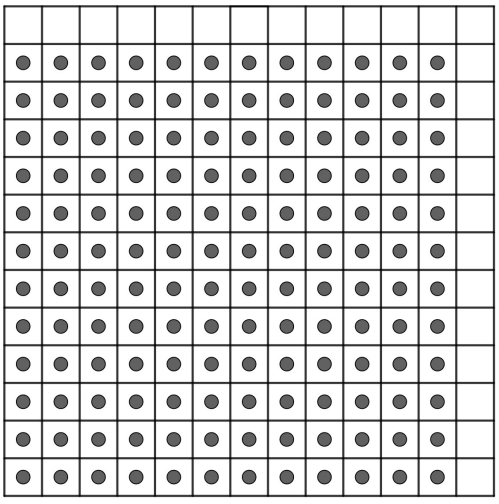
Konstrukció:

- A $z = 0$, $z = 1$, …, $z = p - 3$ egyenletű síkokon a $[0, p-2] \times [0, p-2] \times [0, p-3]$-beli pontokat tartjuk meg, vagyis mind a $p - 2$ síkon az utolsó sort és oszlopot hagyjuk el, mindegyiken $(p-1)^2$ pont van.

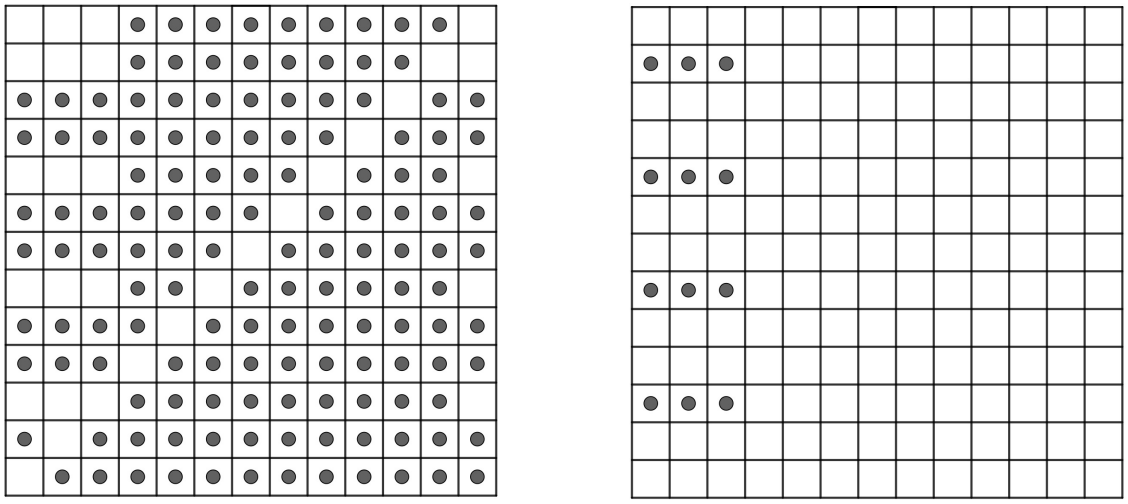
- A $z = p-2$ síkon $p+ts+t+s-1$ pontot hagyunk el a p^2-ből az alábbiak szerint. Elhagyjuk az $x = y$ egyenletű átló p pontját és az $y = s - 1$, $y = 2s - 1$, …, $y = ts - 1$ egyenletet kielégítő vízszintes egyenesek 0, 1, …, $s - 1$ x-koordinátájú pontjait, vagyis az „alulról” $s.$, $2s.$, …, $ts.$ sorok első s pontját, összesen ts pontot, amelyből az $[s-1, s-1, p-2]$-t már számoltuk egyszer. Végül elhagyjuk az előbb elhagyott ts pont sorainak illetve oszlopainak az $x = p - 1$ illetve $y = p - 1$ egyenletű utolsó oszloppal illetve sorral vett metszetét, a $[p-1, js-1, p-2]$ illetve $[i, p-1, p-2]$ koordinátájú pontokat, ahol $0 \leq i \leq s-1$, $1 \leq j \leq t$ és $i, j \in \mathbb{Z}$, összesen $t + s$ pontot, amelyeknek a korábban felsoroltakkal nincs metszetük ($ts < p$ miatt).

- A $z = p - 1$ síkon csak ts pontot tartunk meg, olyanokat, amelyek $z = p - 2$ síkra vett vetületeit ott elhagytuk, az $[i, js - 1, p - 2]$ koordinátájú pontokat, ahol $0 \leq i \leq s - 1$, $1 \leq j \leq t$ és $i, j \in \mathbb{Z}$.

(Példaként íme a leírt konstrukció $p = 13$-ra, az egyik ábrán az első tizeneggyel megegyező, utána pedig az utolsó két sík (itt $s = 3$ és $t = 4$, 1734 pontot tartalmaz a konstrukció):



3. ábra



4. ábra)

A konstrukció jó minden $p \geq 5$ prímszámra, ugyanis ha lenne p pontja, amely egyenest (számtani sorozatot) alkot, akkor ezek x-, y- és z-koordinátáira is teljesül, hogy a $\{0, \ldots, p-1\}$ halmazon vagy egyenletesen oszlanak el vagy mind a p pontra azonos az adott koordináta. Állandó z-koordináta mellett $z = 0, 1, \ldots, p-3$ esetén a $[0, p-2]^2$-beli x- és y-koordinátájú pontok nem adnak egyenest és $z = p-1$ esetén $ts < p$ miatt az utolsó síkon nincs is elég pont egy egyeneshez. A $z = p-2$ síkon az $x = y$ egyenesről nincs pont, így csak a vele párhuzamos egyenesek jöhetnek szóba teljes egyenesként, de azok mindegyikére a leírt ts elhagyott pont és az $y = p-1$ egyenesről elhagyott további s pont valamelyike rajta van. $y = x$, $y = x+1$, $\ldots y = x+s-1$ egyenesek esetén az $y = s-1$ egyenessel közös pont, $y = x+s$, $y = x+s+1$, $\ldots y = x+2s-1$ egyenesek esetén az $y = 2s-1$ egyenessel közös pont, $\ldots$, $y = x+(t-1)s$, $y = x+(t-1)s+1$, $\ldots y = x+ts-1$ egyenesek esetén az $y = ts-1$ egyenessel közös pont, végül az $y = x+ts$, $\ldots$, $y = x+p-1$ egyenletű egyenesek esetén pedig az $y = p-1$ egyenletű egyenessel közös pont van kihagyva a konstrukcióból.

Ezek alapján ellentmondást okozó teljes egyenes pontjainak z-koordinátája pontonként más. Van pont az utolsó síkról is. Ha az x-koordináta állandó lenne a p db pontra (ami az utolsó sík alapján csak 0, 1, $\ldots$, $s-1$ lehet), az y-koordináta is az, ugyanis az $y = p-1$ síkról nincs pont $x < s$ feltétellel. Ugyanakkor a $z = p-1$ és $z = p-2$ síkon nincs egy-egy olyan pont, amelyekre az x- és y-koordináta is megegyezik. Így az x-koordináta is pontonként más lenne teljes egyenesen. A teljes egyenesen lenne olyan pont, amelynek $p-1$ az x-koordinátája, ilyen csak $z = p-2$ feltétellel lehet. Ekkor viszont a $z = p-1$ és $z = p-2$ síkokon lévő pontoknak más lenne az y-koordinátája, így az összes y-koordináta is különböző kell legyen a teljes egyenesen (p elemű számtani sorozatban). Így lenne az $y = p-1$ síkról is pont, de csak a $z = p-2$ síkról lehet, ahonnan $p-1$ x-koordinátájú pont van. Ebből a $[p-1, p-1, p-2]$ pont rajta lenne a teljes egyenesen, de nem a konstrukció pontja, ellentmondást kaptunk. A konstrukció helyességét bebizonyítottuk.

Összesen $(p-1)^2 \cdot (p-2) + (p^2-p-ts-t-s+1) + ts = p^3 - 3p^2 + 4p - 1 - t - s = (p-1)^3 + p - (t+s)$ pontú a konstrukció. Belátjuk, hogy $t+s < 2\sqrt{p}$.
$s = \lfloor \sqrt{p} \rfloor$ miatt mivel egy prímszám nem négyzetszám, $s < \sqrt{p} < s+1$ és $s^2 < p < (s+1)^2$.
$p \neq s(s+2)$ mivel s nem osztója a p prímnek, így $s^2 < p < s^2 + 2s$ is teljesül. $t = \lfloor \frac{p}{s} \rfloor$ és $ts \neq p$ miatt $ts < p < (t+1)s$. Mivel az s^2 és $s(s+2)$ közé eső p nagyobb ts-nél és kisebb

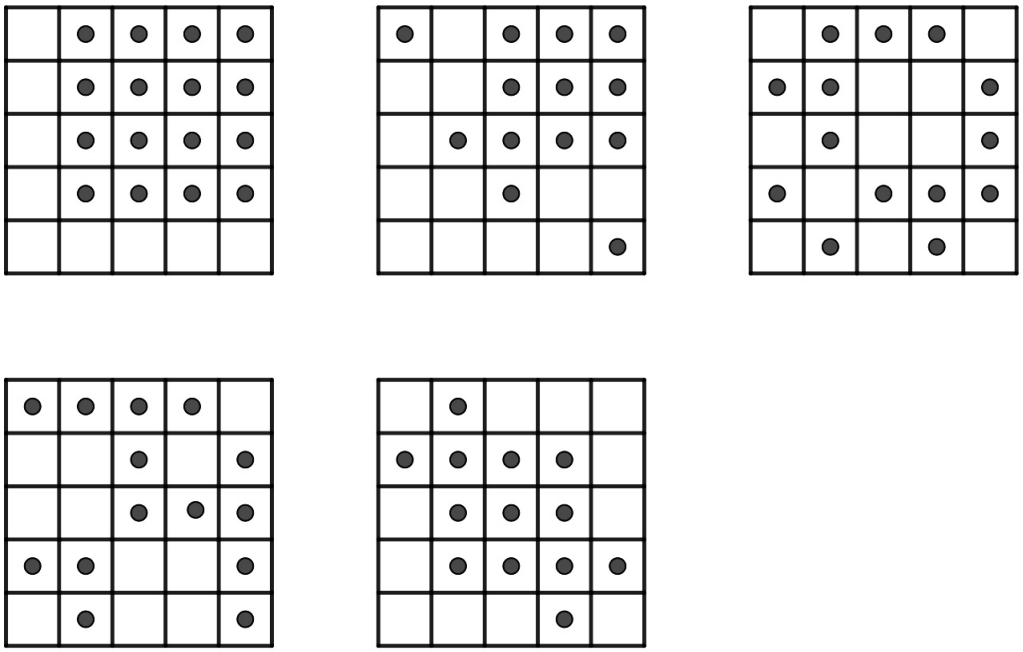
$(t+1)s$-nél, $t=s$ vagy $t=s+1$. Ha $t=s$, akkor $t+s=2s=2\lfloor\sqrt{p}\rfloor<2\sqrt{p}$. Ha pedig $t=s+1$, akkor $ts=s(s+1)<p$, így mivel p egész szám, $(s+0,5)^2=s(s+1)+0,25<p$ is teljesül. Ebből $\frac{t+s}{2}=s+0,5<\sqrt{p}$, tehát $t+s<2\sqrt{p}$ ekkor is. Így a $p\geq 5$ esetben a teljes egyenest nem tartalmazó konstrukció $(p-1)^3+p-(t+s)$ ponttal több mint $(p-1)^3+p-2\sqrt{p}$ pontú, vagyis $r_p(\mathbb{Z}_p^3)>(p-1)^3+p-2\sqrt{p}$ minden p prímszámra, a 3-nál nagyobb prímekre is teljesül. ■

Kis p-kre $p=13$-ig a $(p-1)^3+\frac{p-1}{2}$, nagyobbakra $p=17$-től a $(p-1)^3+p-2\sqrt{p}$ alsó korlát a pontosabb.

A következő konstrukciókat Kovács Benedek találta program segítségével.

1. Becslés (Kovács B.)**.**
$r_5(\mathbb{Z}_5^3)\geq 70$.

(Az állítás szerepel a [3]-as kéziratban is, de csak 69-es konstrukciót mutatnak.)
Bizonyítás:
70-es konstrukció teljes egyenes (5 elemű számtani sorozat) nélkül:

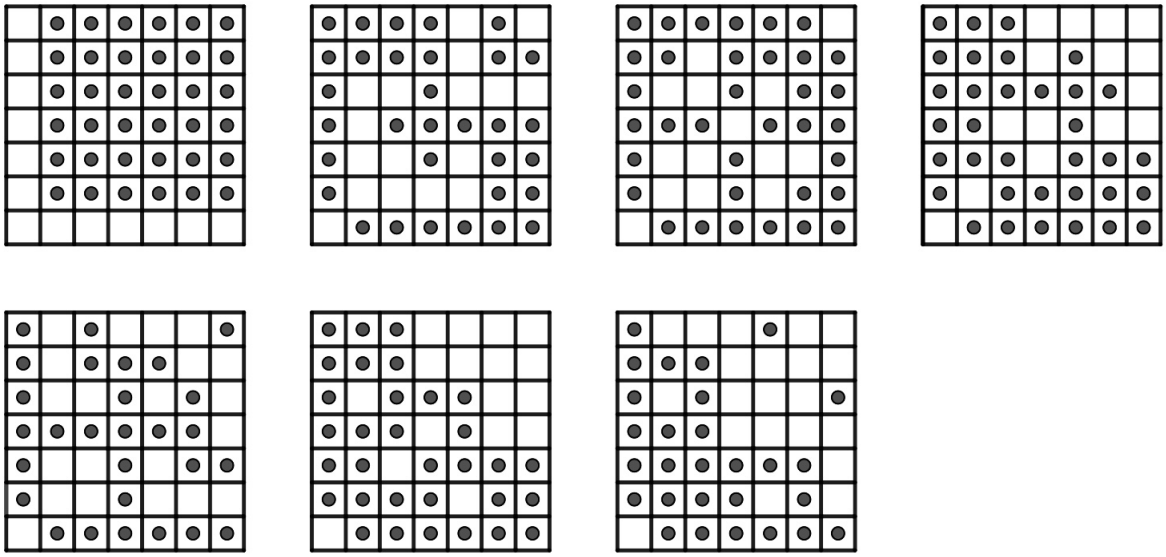


5. ábra (Sorra felül a $z=0$, $z=1$, $z=2$ síkokkal, alul a $z=3$ és $z=4$ síkokkal vett metszet)

A konstrukció érdekessége, hogy $[a,b,c]$ tartalmazása esetén tartalmazza $[b,a,c]$-t és $[-a,b-c,-c]$-t is, ezek alapján 8-at osztó elemszámú csoportokba rendezhetők a pontok, melyek elemei közt $[a,b,c]$-t $[b,a,c]$-re vagy $[-a,b-c,-c]$-re váltva „átjárás" van. Felderítésre vár, hogy van-e valami könnyen ellenőrizhető feltétel (pl. kevés tagból álló háromváltozós polinom, ami náluk 0), amely pontosan a 70-es konstrukció pontjaira (elemeire) teljesül.

2. Becslés (Kovács B.)**.**
$r_7(\mathbb{Z}_7^3) \geq 225$

Bizonyítás:
225-ös konstrukció teljes egyenes (7 hosszú számtani sorozat) nélkül (felül a $z = 0$, $z = 1$, $z = 2$ és $z = 3$ síkokkal, alul a $z = 4$, $z = 5$ és $z = 6$ síkokkal közös metszet):



6. ábra

A konstrukció tükrös az $x = y$, $x = z$ és $y = z$ síkokra (vagyis adott koordinátahármasnál az összes ilyen pont benne van vagy egy sem), ami nem véletlen, ugyanis a program kifejezetten az ilyen szabályosabb ponthalmazokat vizsgálta. Ugyanakkor $r_5(\mathbb{Z}_5^3)$ alsó becslésénél csak az előző 70 pontúnál kevesebb pontú ilyen típusú konstrukciót talált a program.

A felső becslés javítása saját eredményem:

5. Tétel (Füredi E.)**.**
Minden p páratlan prímre $r_p(\mathbb{Z}_p^3) \leq p^3 - 2p^2 + p - \frac{1}{2} + \frac{4p-2-\sqrt{8p^6-20p^5+17p^4-12p^3+20p^2-16p+4}}{2p^2}$.

Bizonyítás:
A bizonyítás $r_p(\mathbb{Z}_p^2) = (p-1)^2$-en alapul. Tegyük fel, hogy létezik konstrukció teljes egyenes nélkül h ponttal, ahol $h \geq (p-1)^3$. Számoljuk össze az összes pontpár-sík párt, ahol a pontpár rajta van a síkon.
Minden pontpár (egyenese) $p+1$ síkon van rajta, így pontpáronként összeadva $\binom{h}{2}(p+1)$-et kapunk. Síkonként összeadáshoz nézzük, hogy p párhuzamos síkra mennyi lehet az összeg legfeljebb. Minden síkra legfeljebb $r_p(\mathbb{Z}_p^2) = (p-1)^2$ pont juthat. Ha van két sík ennél kevesebb ponttal, a nem-több pontú síkról a másikra áttéve egy pontot a pontpárok száma nőne a felső korlátot meg nem sértve, $y \geq x > 0$ esetén $\binom{y}{2}+\binom{x}{2} < \binom{y+1}{2}+\binom{x-1}{2}$. Ezzel a maximális pontpár darabszám összeg csak $p-1$ db $(p-1)^2$ pontú síkkal lehet minden síkon legfeljebb $r_p(\mathbb{Z}_p^2)$

ponttal ($h \geq (p-1)^3$-et használjuk). Ez a maximális összeg $(p-1)\binom{(p-1)^2}{2} + \binom{h-(p-1)^3}{2}$. Mivel p^2+p+1 db iránya van az egyeneseknek $\mathbb{Z}_p^3$-ben és ugyanennyi a rájuk merőleges síkoknak, p párhuzamos síkból p^2+p+1 db van. Ezzel a kapott felső becslés síkonként összeadva a rajtuk lévő pontpárok számát a pontpáronként kapott pontos értékkel összehasonlítva az alábbit adja:

$$\binom{h}{2}(p+1) \leq (p^2+p+1)\Big((p-1)\binom{(p-1)^2}{2} + \binom{h-(p-1)^3}{2}\Big).$$

2-vel felszorozva, kifejtve és rendezve az alábbit kapjuk:

$$h^2p^2 + h(-2p^5+4p^4-2p^3+p^2-4p+2) + (p^8-4p^7+6p^6-5p^5+5p^4-6p^3+4p^2-p) \geq 0.$$

Ebből h-ra kapunk egy másodfokú egyenletet, amelynek gyökeire a bal oldal 0, a két gyök közt negatív, máshol pozitív. Vagyis $|h - \frac{2p^5-4p^4+2p^3-p^2+4p-2}{2p^2}| < \frac{\sqrt{8p^6-20p^5+17p^4-12p^3+20p^2-16p+4}}{2p^2}$ esetén ellentmondást kapunk. Ha pedig egy ezt teljesítő $(p-1)^3$-nél nem kisebb h egész számra ily módon kizárjuk a konstrukció lehetőségét, minden nagyobb pozitív egész számra is kizárjuk, mert abból pontokat elhagyva ennyi pontú teljes egyenes nélküli konstrukciót kapnánk.
$\frac{\sqrt{8p^6-20p^5+17p^4-12p^3+20p^2-16p+4}}{p^2} = \frac{\sqrt{p^6+(7p^6-20p^5)+(17p^4-12p^3)+(20p^2-16p)+4}}{p^2} > \frac{\sqrt{p^6}}{p^2} = p > 1$, így a h számára kizárt intervallum hossza $p \geq 3$ mellett 1-nél nagyobb, esik bele pozitív egész szám, például $\lfloor \frac{2p^5-4p^4+2p^3-p^2+4p-2-\sqrt{8p^6-20p^5+17p^4-12p^3+20p^2-16p+4}}{2p^2} \rfloor + 1$. Ez a szám $p \geq 3$ (prímszám) esetén nagyobb $(p-1)^3$-nél, ilyen sok pontra már nem létezhet konstrukció számításaink alapján. Ugyanis $\frac{2p^5-4p^4+2p^3-p^2+4p-2-\sqrt{8p^6-20p^5+17p^4-12p^3+20p^2-16p+4}}{2p^2} > p^3 - 3p^2+3p-1$, hiszen $p > 3$-ra $\frac{2p^5-4p^4+2p^3-p^2+(4p-2)-\sqrt{8p^6+(-20p^5+17p^4)+(-12p^3+20p^2)+(-16p+4)}}{2p^2} > \frac{2p^5-4p^4+2p^3-p^2-\sqrt{8p^6}}{2p^2} > p^3-2p^2-p-\frac{1}{2} > p^3-3p^2+3p-1$, míg $p=3$-ra
$\frac{2p^5-4p^4+2p^3-p^2+4p-2-\sqrt{8p^6-20p^5+17p^4-12p^3+20p^2-16p+4}}{2p^2} = \frac{217-\sqrt{2161}}{18} \approx 9,47 > 8 = (p-1)^3$.

Ebből adódik az állítás, $r_p(\mathbb{Z}_p^3) \leq p^3-2p^2+p-\frac{1}{2}+\frac{4p-2-\sqrt{8p^6-20p^5+17p^4-12p^3+20p^2-16p+4}}{2p^2}$ minden p páratlan prímszámra. ■

A gyök alatt p^6 nagyságrendű szám áll, így lényegében p-vel arányos a javítás az $r_p(\mathbb{Z}_p^3) \leq p^3-2p^2+1$ egyenlőtlenséghez képest. A tétel gyengített változata, amely ezt jobban mutatja, a következő:

5.a Tétel (Füredi E.)
Minden p páratlan prímre $r_p(\mathbb{Z}_p^3) \leq p^3-2p^2-(\sqrt{2}-1)p+2$.

Bizonyítás:
Az állítás következik az előző tételből és abból, hogy $p^3-2p^2-(\sqrt{2}-1)p+2 > p^3-2p^2+p-\frac{1}{2}+\frac{4p-2-\sqrt{8p^6-20p^5+17p^4-12p^3+20p^2-16p+4}}{2p^2}$. Utóbbi ekvivalens
$\frac{-2\sqrt{2}p^3+4p^2}{2p^2} > \frac{-p^2+4p-2-\sqrt{8p^6-20p^5+17p^4-12p^3+20p^2-16p+4}}{2p^2}$-tel, ami pedig felszorozva és rendezve $\sqrt{8p^6-20p^5+17p^4-12p^3+20p^2-16p+4} > 2\sqrt{2}p^3-5p^2+4p-2$-tel, pozitív bal és jobb oldal miatt négyzetre emelve majd rendezve $20(\sqrt{2}-1)p^5-(8+16\sqrt{2})p^4+(28+8\sqrt{2})p^3-16p^2 > 0$-val ekvivalens. Utóbbi $p \geq 5$-re teljesül $20(\sqrt{2}-1)p^5-(8+16\sqrt{2})p^4 > 0$ és $(28+8\sqrt{2})p^3-16p^2 > 0$ miatt és konkrétan $p=3$-ra is teljesül. Ennélfogva az állítás valóban következik az előzőből, annak gyengített változata. ■

A következő táblázat mutatja, hogy mi jön ki az 5. tételből kis páratlan prímekre felhasználva, hogy $r_p(\mathbb{Z}_p^3)$ egész szám.

p	$p^3 - 2p^2 + p - \frac{1}{2} + \frac{4p-2-\sqrt{8p^6-20p^5+17p^4-12p^3+20p^2-16p+4}}{2p^2}$	következmény
3	$\frac{217-\sqrt{2161}}{18} \approx 9,47$	$r_3(\mathbb{Z}_3^3) \leq 9$
5	$\frac{3993-\sqrt{72049}}{50} \approx 74,49$	$r_5(\mathbb{Z}_5^3) \leq 74$
7	$\frac{24673-\sqrt{642625}}{98} \approx 243,59$	$r_7(\mathbb{Z}_7^3) \leq 243$
11	$\frac{266121-\sqrt{11186641}}{242} \approx 1085,85$	$r_{11}(\mathbb{Z}_{11}^3) \leq 1085$
13	$\frac{632617-\sqrt{31650961}}{338} \approx 1855,003$	$r_{13}(\mathbb{Z}_{13}^3) \leq 1855$
17	$\frac{2515233-\sqrt{166069825}}{578} \approx 4329,32$	$r_{17}(\mathbb{Z}_{17}^3) \leq 4329$
19	$\frac{4444345-\sqrt{328985137}}{722} \approx 6130,48$	$r_{19}(\mathbb{Z}_{19}^3) \leq 6130$

Vagyis ezzel láttuk be $r_3(\mathbb{Z}_3^3) = 9$-et. Az 5. tétel már $p = 3$-ra is erősebb az eddig ismert 3. tételnél.

5.3. A felső becslés javítása a $p = 5$ és $p = 7$ esetekben

A következőkben 1-gyel javítunk a $p = 5$ és $p = 7$ esetekben kapott felső becsléseken. Mindkét bizonyításnál a síkonként adott számú pontokat tartalmazó párhuzamos síkok eloszlását és a $p - 1$ pontú egyeneseket tartalmazó síkokat vizsgáljuk.

3. Becslés (Füredi E.)**.**
$r_5(\mathbb{Z}_5^3) < 74$.

Bizonyítás:
$r_5(\mathbb{Z}_5^3) < 75$ az előző rész alapján. Tegyük fel, hogy létezik 74 pontú konstrukció teljes egyenes nélkül. Nézzük meg, hogy hány pont lehet egy síkon. Minden síkon legfeljebb $r_5(\mathbb{Z}_5^2) = 16$ pont lehet, így legalább $74 - 4 \cdot 16 = 10$ pontnak kell lennie bármely síkon (a négy vele párhuzamos sík pontjainak összesített darabszáma alapján). Emellett bármely a konstrukcióból 4 pontot tartalmazó egyenesre az egyenest tartalmazó 6 síkra a rajtuk lévő pontok darabszámát összeadva a 74 pont közül csak az egyenes 4 pontját számoltuk hatszor, a többit egyszer, így a 6 síkon a pontok darabszámának összege 94. Ez legfeljebb 16 pontú síkok mellett $94 = 6 \cdot 16 - 2$ miatt csak legalább 14 pontú síkok mellett lehetséges, 4 pontú egyenes csak 14-16 pontú síkokon lehet. Ugyanakkor $r_4(\mathbb{Z}_5^2) = 11$ miatt 12-13 pontú sík is tartalmazna 4 pontú egyenest, így ilyenek nem lehetnek a konstrukcióban, csak 10, 11, 14, 15 és 16 pontú síkok.

5 párhuzamos síkon az a pontok síkonkénti eloszlása 5-féle lehet, sorrendben 16-16-16-16-10, 16-16-16-15-11, 16-16-14-14-14, 16-15-15-14-14 és 15-15-15-15-14. Ezek darabszámát sorra a, b, c, d és e-vel jelölve, mivel $31 \cdot 5$ síkunk van,

$$a + b + c + d + e = 31. \tag{1}$$

Emellett a pontpárok darabszámát is megszámoljuk síkonként, öt párhuzamos síkra az összeg rendre 525, 520, 513, 512 és 511 a korábbi sorrendben. Mivel minden pontpár 6 síkon van rajta, ebből $525a + 520b + 513c + 512d + 511e = 6 \cdot \binom{74}{2} = 16206$.
Ezt (1) 525-szöröséből levonva megkapjuk, hogy

$$5b + 12c + 13d + 14e = 69. \tag{2}$$

A két egyenletből, mivel az ismeretlenek darabszámként természetes számok, minden esetet meg lehet kapni, a például legalább 19, mert $b + c + d + e \leq 12$ a második egyenletből. Szerencsére csupán 11 eset van a párhuzamos síkok 5-féle eloszlásának konstrukcióbeli a-b-c-d-e eloszlására, nevezetesen: 19-11-0-0-1, 20-9-2-0-0, 22-6-0-3-0, 22-6-1-1-1, 23-4-3-1-0, 24-3-1-0-3, 24-3-0-2-2, 25-1-1-4-0, 25-1-2-2-1, 25-1-3-0-2 és 26-0-0-1-4. Ugyanakkor nekünk lényegesebb a síkonkénti pontszámeloszlás a 16, 15, 14, 11 és 10 pontot tartalmazó síkok közt, amely viszont a párhuzamos síkok 5-féle eloszlásának eloszlásából számolható, itt csak 7 eset van, mert az előző 11 eset közül pl. a 8., 9. és 10. ugyanazt adja, ugyanis a 16-15-15-14-14 eloszlás 16-16-14-14-14 és a 15-15-15-15-14 eloszlások átlaga. A 7 eset sorra 109-15-1-11-19, 111-9-6-9-20,109-12-6-6-22,111-6-11-4-23,107-15-6-3-24,109-9-11-1-25 és 105-18-6-0-26.

Térjünk vissza a 4 pontú egyenesekre, bármelyik 6 síkjára 94 a pontok darabszámának összege, ami csak 16-16-16-16-16-14 és 16-16-16-16-15-15 eloszlással lehetséges. Jelölje rendre A, B illetve C a 4 pontú egyenesek illeszkedései darabszámának összegét 16, 15 illetve 14 pontú síkokra. Ekkor $A - 2B - 5C = 0$ teljesül, ugyanis a bal oldalt megkaphatjuk úgy is, hogy egyenesenként nézzük azon síkokat, amelyeken rajta vannak és ezek hozzájárulását összegezzük. Síkjai alapján mindkét típusú 4 pontú egyenes 0-val járul hozzá a bal oldalhoz. Ezután síkonként számolva jutunk ellentmondáshoz a bal oldal pozitivitását bizonyítva az alábbi lemma segítségével.

Lemma. 5 *pontú egyenest nem tartalmazó* 16 *pontú síkon legalább* 12 *db* 4 *pontú egyenes van, míg* 15 *pontú síkon legfeljebb* 15*,* 14 *pontú síkon pedig legfeljebb* 14 *db* 4 *pontú egyenes van.*

A lemma bizonyítása: 15 és 14 pontú síkokon minden pontra (a 15 illetve 14 közül) legfeljebb 4 darab 4 pontú egyenes megy át. Ugyanis a 6 egyenesen a pontok összege 20 illetve 19, amibe 5 darab 4 pontú egyenes nem fér bele, mert a hatodikon is van legalább egy pont. Így a pontokon átlagosan legfeljebb 4 darab 4 pontú egyenes megy át, tehát a pontok számánál több 4 pontú egyenes nem lehet.

16 pontú síknál jelölje rendre x_1, x_2, x_3 illetve x_4 az 1, 2, 3 illetve 4 pontú egyenesek számát. Ekkor az egyenesekre a pontok számát összeadva minden pontot hatszor számolunk, így $x_1 + 2x_2 + 3x_3 + 4x_4 = 96$. Minden pontpárt egyszer számolunk, ebből $x_2 + 3x_3 + 6x_4 = \binom{16}{2} = 120$. Utóbbiból előbbit kivonva $-x_1 - x_2 + 2x_4 = 24$, így $2x_4 \geq 24$, $x_4 \geq 12$, a lemma ezen állítását is beláttuk. (Megjegyzés: csak az alsó becslésnél állhat egyenlőség pl. két nem párhuzamos egyenest elhagyva, az egy pontot sem tartalmazó egyeneseket x_0-lal jelölve $x_0 + x_1 + \cdots + x_4 = 30$ egyenletet is használva 14 illetve 15 pontnál 11-re illetve 13-ra leszorítható a maximum, ezekre pedig Kovács Benedek számítógéppel talált konstrukciókat.) ■

A lemma alapján a 16, 15 illetve 14 pontú síkok egyenként legalább 12-vel, -30-cal illetve -70-nel járulnak hozzá $A - 2B - 5C$-hez. Az ebből kapott alsó becslést mutatja a következő táblázat:

16, 15, 14, 11 és 10 pontú síkok darabszáma	$A-2B-5C$ alsó becslése
109-15-1-11-19	788
111-9-6-9-20	642
109-12-6-6-22	528
111-6-11-4-23	382
107-15-6-3-24	414
109-9-11-1-25	268
105-18-6-0-26	300

Így $A-2B-5C$ nem lehet 0, ami ellentmondást jelent. A 74 pontú konstrukció lehetlenségét és vele az állítást beláttuk. ■

A bizonyítás során kihasználtuk a viszonylag kis számokat az esetek végignézésével, ugyanakkor hasonló módon a pontok és $p-1$ pontú egyenesek síkonkénti eloszlását nagyobb prím és konstrukció esetén is lehet nézni. A következő bizonyítással 1-gyel javítjuk az $r_7(\mathbb{Z}_7^3)<244$ becslést is.

4. Becslés (Füredi E.)**.**
$r_7(\mathbb{Z}_7^3)<243$.

Bizonyítás:
A bizonyítás menete hasonlít az előzőhöz, indirekten bizonyítjuk a konstrukció lehetetlenségét $p-1$ pontú egyeneseket tartalmazó síkok vizsgálatával.
Tegyük fel, hogy létezik 243 pontú konstrukció, amelyben nincs 7 pont egy egyenesen. Ekkor minden sík legfeljebb $(7-1)^2=36$ pontot tartalmazhat és legalább $243-6\cdot 36=27$-et tartalmaznia kell. A konstrukcióban létezik pontosan 6 kiválasztott pontot tartalmazó egyenes, ugyanis ilyen nélkül a 100 kihagyott pont bármelyikét hozzávehetnénk, amit korábbi eredményünk tilt. Egy 6 kiválasztott pontot tartalmazó egyenesre a 8 őt tartalmazó síkon a pontokat összeadva minden pont egyszer szerepel, kivéve ez a 6, amelyek 8-szor, így a 8 síkra a pontok számának összege 285. Ez $36\cdot 8-3$, így a 8 darab 6 pontú egyenest tartalmazó síkra a pontok darabszámának minimuma 33. Tehát a konstrukció létezése esetén bármely 6 pontú egyenest tartalmazó síkon a pontok száma legalább 33. Ugyanakkor $r_{p-1}(\mathbb{Z}_p^2)=p^2-3p+1$ miatt $p=7$-re $r_6(\mathbb{Z}_7^2)=29$, így 29-nél több pontú síkon létezik 6 pont egy egyenesen. Ez kizárja a 30, 31 és 32 pontú síkok létezését. A konstrukció bármely síkján 27, 28, 29, 33, 34, 35 vagy 36 db pont van.

7 párhuzamos síkon ezek szerint a pontok számának eloszlása az alábbiak valamelyike lehet, a 14 lehetséges eloszlást egy-egy sorszámmal jelölve:

(1.) 36-36-36-36-36-36-27,
(2.) 36-36-36-36-36-35-28,
(3.) 36-36-36-36-36-34-29,
(4.) 36-36-36-36-35-35-29,
(5.) 36-36-36-36-33-33-33,
(6.) 36-36-36-35-34-33-33,

(7.) 36-36-35-35-35-33-33,
(8.) 36-36-36-34-34-34-33,
(9.) 36-36-35-35-34-34-33,
(10.) 36-35-35-35-35-34-33,
(11.) 35-35-35-35-35-35-33,
(12.) 36-36-35-34-34-34-34,
(13.) 36-35-35-35-34-34-34,
(14.) 35-35-35-35-35-34-34.

Bármely 6 pontú egyenes vagy 7 db 36 és 1 db 33, vagy 6 db 36, 1 db 35 és 1 db 36 vagy 5 db 36 és 3 db 35 pontú síkra illeszkedik. Jelöljük A-val a 6 pontú egyenesek 36 pontú síkokra illeszkedéseinek számát, B-vel a 6 pontú egyenesek 35 pontú síkokra illeszkedéseinek számát, C-vel a 6 pontú egyenesek 34 pontú síkokra illeszkedéseinek számát és D-vel a 6 pontú egyenesek 33 pontú síkokra illeszkedéseinek számát. Az előző felsorolásból a 6 pontú egyeneseket nézve megkapjuk, hogy $A = \frac{5}{3}B + \frac{13}{3}C + 7D$. Ugyanis az őt tartalmazó síkokra eső pontok száma alapján mindhárom típusba eső egyenesek ugyanannyit adnak mindkét oldalhoz. Ebből $A - \frac{5}{3}B - \frac{13}{3}C - 7D = 0$. Belátjuk, hogy ez a szám, $A - \frac{5}{3}B - \frac{13}{3}C - 7D$ csak pozitív lehet, így jutunk ellentmondásra.

Az egyenesek után jöjjenek a síkok, nézzük, hogy egy 36, 35, 34 illetve 33 pontú síkra hány 6 pontú egyenes illeszkedik, feltéve, hogy a sík nem tartalmaz 7 pontú egyenest. Erről szól a következő lemma.

Lemma. *7 pontú egyenest nem tartalmazó 36 pontú sík legalább 18, 35 pontú legfeljebb 33, 34 pontú legfeljebb 30 és 33 pontú legfeljebb 27 db 6 pontú egyenest tartalmaz, amennyiben nem tartalmaz 7 pontú egyenest.*

A lemma bizonyítása: Jelölje a $\mathbb{Z}_7^2$-nel izomorf struktúrából x pontot tartalmazó (7 pontú egyenes néküli) sík 56 egyeneséből a 0, 1, 2, 3, 4, 5 és 6 pontúak számát rendre x_0, x_1, x_2, x_3, x_4, x_5 és x_6. Mivel összesen $7 \cdot 8 = 56$ egyenes van $\mathbb{Z}_7^2$-ben, $x_0+x_1+x_2+x_3+x_4+x_5+x_6 = 56$. Mind az x pont 8 egyenesen van rajta, így egyenesenként számolva $x_1+2x_2+3x_3+4x_4+5x_5+6x_6 = 8x$. Végül bármely két pontot az x-ből egy egyenes köti össze, így $x_2+3x_3+6x_4+10x_5+15x_6 = \binom{x}{2}$.

$x = 36$ esetén utóbbi kettőből $x_1+2x_2+3x_3+4x_4+5x_5+6x_6 = 288$ és $x_2+3x_3+6x_4+10x_5+15x_6 = 630$. A másodikból az első kétszeresét levonva $-2x_1 - 3x_2 - 3x_3 - 2x_4 + 3x_6 = 54$, így $3x_6 \geq 54$. Tehát 36 pont esetén legalább 18 db 6 pontú egyenes van. A lemma első részét beláttuk. Más esetekben a 3 egyenletet úgy használjuk, hogy az első 3-szorosához adjuk a harmadikat és levonjuk a második kétszeresét. Ekkor azt kapjuk, hogy $3x_0 + x_1 + x_4 + 3x_5 + 6x_6 = 168 - 16x + \binom{x}{2}$, vagyis $6x_6 \leq 168 - 16x + \binom{x}{2}$. $x = 35$ esetén ebből $x_6 \leq \frac{203}{6}$, $x = 34$ esetén $x_6 \leq \frac{185}{6}$ és $x = 33$ esetén $x_6 \leq 28$. Mivel x_6 egész szám, így 35-re illetve 34-re a 33-as illetve 30-as felső becslést kapjuk.

$x = 33$-ra pedig az $x_6 = 28$-as lehetőség esetén $3x_0 + x_1 + x_4 + 3x_5 = 0$ lenne, így $x_0 = x_1 = x_4 = x_5 = 0$. Ebből a 3 egyenlet $x_6 = 28$-at használva az $x_2 = -12$ és $x_3 = 40$ megoldást adja, amely nem lehetséges, x_2 természetes szám kell, hogy legyen. Így $x = 33$-ra $x_6 \neq 28$, $x_6 \leq 27$. Így a lemma állításait beláttuk. (Azt nem bizonyítottuk, de nem szükséges és nem is feltétlen igaz, hogy ilyen számú 6 pontú egyenesekkel és ponttal létezik teljes egyenest nem tartalmazó konstrukció, 36-nál 18-as létezik $[0, 5]^2$-nel.) ■

Megkaptuk, hogy $A - \frac{5}{3}B - \frac{13}{3}C - 7D = 0$ kiszámításához egy 36, 35, 34 illetve 33 pontú sík legalább 18-cal, -55-tel, -130-cal illetve -189-cel járul hozzá. Ebből kiszámítható a 7 párhuzamos síkra, hogy náluk összegezve legalább mennyi ezen hozzájárulás (a 33-nál kevesebb pontú síkokon nincs 6 pont egy egyenesen a konstrukciónkban).

Ugyanakkor a párhuzamos síkhetesek 14-féle ponteloszlásának előfordulásaira bizonyos szabályok teljesülnek. Összesen $7^2 + 7 + 1 = 57$ párhuzamos síkhetes van. Ezeknél összeadva síkonként a rajtuk lévő pontpárok számát (ami y pontú síkon $\binom{y}{2}$), minden pontpárt 8 síknál számolunk, így az 57 szám összege $8 \cdot \binom{243}{2} = 235224$. A síkonkénti pontpárok számának összege az 1., 2., ..., 14. típusú eloszlásnál rendre 4131, 4123, 4117, 4116, 4104, 4102, 4101, 4101, 4100, 4099, 4098, 4099, 4098 és 4097. $4131 \cdot 57 = 235467 = 235224 + 243$, ezen 243-as többletet kell az 1.-től eltérő ponteloszlású párhuzamos síkheteseken elvesztegetetni, a „veszteség" rendre 0, 8, 14, 15, 27, 29, 30, 30, 31, 32, 33, 32, 33 illetve 34. Tehát 57 ezek közül kikerülő szám összege 243 lesz. Ezután jöjjön egy táblázat a párhuzamos síkok ponteloszlásának 14 típusánál a v-vel jelölt „veszteségről" és az $A - \frac{5}{3}B - \frac{13}{3}C - 7D$-hez való h-val jelölt hozzájárulásról.

eloszlás	v	h
36-36-36-36-36-36-27	0	108
36-36-36-36-36-35-28	8	35
36-36-36-36-36-34-29	14	-40
36-36-36-36-35-35-29	15	-38
36-36-36-36-33-33-33	27	-495
36-36-36-35-34-33-33	29	-509
36-36-35-35-35-33-33	30	-507
36-36-36-34-34-34-33	30	-525
36-36-35-35-34-34-33	31	-523
36-35-35-35-35-34-33	32	-521
35-35-35-35-35-35-33	33	-519
36-36-35-34-34-34-34	32	-539
36-35-35-35-34-34-34	33	-537
35-35-35-35-35-34-34	34	-535

Láthatjuk, hogy $h \geq -\frac{67}{3}v + 108$ (1.-nél és 5.-nél egyenlőséggel). Mivel esetünkben 57 db párhuzamos síkhetesünknél adunk össze h-kat, melyekhez tartozó v-k összege 243, a h-k összege legalább $108 \cdot 57 - (-\frac{67}{3} \cdot 243) = 729$, nem lehet 0, így $A - \frac{5}{3}B - \frac{13}{3}C - 7D > 0$ lenne, ami ellentmondás. Az állítást bebizonyítottuk. ■

Még egyszer összefoglalva $r_p(\mathbb{Z}_p^3)$ egyjegyű páratlan prímekre kapott becsléseit, $r_3(\mathbb{Z}_3^3) = 9$, $70 \leq r_5(\mathbb{Z}_5^3) \leq 73$ és $225 \leq r_7(\mathbb{Z}_7^3) \leq 242$.

6. A felső becslés módszerének általánosítása

A következőkben $r_k(\mathbb{Z}_p^{n+1})$-re adunk becslést $r_k(\mathbb{Z}_p^n)$-ből az $n = 2$ esethez hasonlóan, p db párhuzamos n-dimenziós hipersíkon lévő pontpárok darabszámának összegével felső becslést adva. A felső korlát létezése miatt az összeg ismét akkor maximális, ha egy hipersík kivételével

mindegyiken $r_k(\mathbb{Z}_p^n)$ pont van.

6. Tétel (Füredi E.)**.**
$r_k(\mathbb{Z}_p^{n+1}) \leq p(r_k(\mathbb{Z}_p^n)) - \frac{r_k(\mathbb{Z}_p^n)}{p^n} + \frac{1}{2} - \frac{\sqrt{4r_k(\mathbb{Z}_p^n)^2 + p^{2n} - 4r_k(\mathbb{Z}_p^n)p^n - 4r_k(\mathbb{Z}_p^n)^2 p^{n+1} + 4r_k(\mathbb{Z}_p^n)p^{2n+1}}}{2p^n}$, *ahol* p *páratlan prímszám,* $3 \leq k \leq p$*,* k *és* n *pozitív egész számok.*

Bizonyítás:
Nézzünk egy w pontú k hosszú számtani sorozat nélküli konstrukciót $\mathbb{Z}_p^{n+1}$-ben. Adjuk össze az n-dimenziós hipersíkokon lévő pontpárok darabszámát. p párhuzamos hipersíkon összesen w pont van, egyiken sem lehet több $r_k(\mathbb{Z}_p^n)$-nél. Ezen feltétel mellett amennyiben $w \geq (p-1)(r_k(\mathbb{Z}_p^n))$, el lehet helyezni a pontokat a p párhuzamos hipersíkon úgy, hogy $(p-1)$ hipersíkra $r_k(\mathbb{Z}_p^n)$ esik, az utolsóra $w-(p-1)r_k(\mathbb{Z}_p^n)$ és ekkor lesz a p párhuzamos hipersíkon a pontpárok darabszámának összege maximális. Ugyanis minden hipersíkra esik pont a konstrukcióban, és ha két párhuzamos hipersíkra is $r_k(\mathbb{Z}_p^n)$-nél kevesebb pont esne, a nem több pontúról egy pontot áttéve a másikra növelhetnénk a pontpárok összesített darabszámát a p párhuzamos hipersíkon az $r_k(\mathbb{Z}_p^n)$ felső korlátot a p párhuzamos hipersík egyikén sem lépve át. Ennek oka, hogy ha $x \geq y > 0$ pont volt a két hipersíkon, $\binom{x+1}{2} + \binom{y-1}{2} > \binom{x}{2} + \binom{y}{2}$. Emellett az esetek véges száma miatt létezik maximum a pontpárok darabszámának összegére. Ebből a konstrukcióban p párhuzamos hipersíkon síkonként véve a pontpárok darabszámát, a kapott összeg legfeljebb

$$(p-1)\binom{r_k(\mathbb{Z}_p^n)}{2} + \binom{w-(p-1)r_k(\mathbb{Z}_p^n)}{2}.$$

Ehhez feltettük, hogy $w \geq (p-1)(r_k(\mathbb{Z}_p^n))$, ugyanakkor teljesül $w < (p-1)(r_k(\mathbb{Z}_p^n))$-re is, hiszen $(p-1)(r_k(\mathbb{Z}_p^n))$ pontnál p párhuzamos hipersíkra összeadva a pontpárok darabszámát minden hipersíkon legfeljebb $r_k(\mathbb{Z}_p^n)$ ponttal legfeljebb $(p-1)\binom{r_k(\mathbb{Z}_p^n)}{2} = (p-1)\binom{r_k(\mathbb{Z}_p^n)}{2} + \binom{0}{2}$-t kaphatunk összegként, kevesebb pontra kevesebbet, de $(p-1)\binom{r_k(\mathbb{Z}_p^n)}{2} + \binom{w-(p-1)r_k(\mathbb{Z}_p^n)}{2}$ legalább ennyi. (Ugyanis $\binom{u}{2}$ nemnegatív minden u egész számra.)

Nézzük, hogy összesen hány n-dimenziós hipersík van. p párhuzamos hipersíkhoz egyértelműen találunk $\frac{p^{n+1}}{p} = p^n$ párhuzamos egyenest, amelyek előbbiekre merőlegesek. A párhuzamos egyenesek és a rájuk merőleges párhuzamos hipersíkok családjai párbaállíthatók. Mind a p^{n+1} ponton át $\frac{p^{n+1}-1}{p-1}$ egyenes megy át, így $\frac{p^{n+1}}{p} \cdot \frac{p^{n+1}-1}{p-1} = p^n \cdot \frac{p^{n+1}-1}{p-1}$ egyenesünk van, rájuk $p \cdot \frac{p^{n+1}-1}{p-1}$ hipersík jut, $\frac{p^{n+1}-1}{p-1}$ darab p párhuzamos. Ebből a hipersíkonkénti pontpárok darabszámának összege legfeljebb

$$\left(\frac{p^{n+1}-1}{p-1}\right) \cdot \left((p-1)\binom{r_k(\mathbb{Z}_p^n)}{2} + \binom{w-(p-1)r_k(\mathbb{Z}_p^n)}{2}\right). \tag{3}$$

Ugyanakkor pontpáronként számolva a hipersíkonkénti pontpárok darabszámának összegét minden pontpárt ($\binom{w}{2}$ darab) annyiszor számoltunk, ahány n-dimenziós hipersík tartalmazza a rajtuk átmenő egyenest. Minden n-dimenziós hipersík összes pontján $\frac{p^n-1}{p-1}$ darab hipersíkbeli egyenes megy át, így $p^{n-1} \cdot \frac{p^n-1}{p-1}$ egyenes van a hipersíkon. Összesen $p \cdot \frac{p^{n+1}-1}{p-1}$ hipersík van és $p^n \cdot \frac{p^{n+1}-1}{p-1}$ egyenes, így minden egyenes (illetve pontpár) $\frac{(p^{n-1} \cdot \frac{p^n-1}{p-1}) \cdot (p \cdot \frac{p^{n+1}-1}{p-1})}{p^n \cdot \frac{p^{n+1}-1}{p-1}} = \frac{p^n-1}{p-1}$ db

n-dimenziós hipersíkon van rajta. Ezzel pontpáronként számolva a hipersíkonkénti pontpárok darabszámának összege a konstrukcióra

$$\left(\frac{p^n-1}{p-1}\right)\cdot\binom{w}{2}, \tag{4}$$

ennél nem kisebb a korábbi felső becslés. A két egyenlet összevetéséből

$$\left(\frac{p^{n+1}-1}{p-1}\right)\cdot\left((p-1)\binom{r_k(\mathbb{Z}_p^n)}{2}+\binom{w-(p-1)r_k(\mathbb{Z}_p^n)}{2}\right)\geq\left(\frac{p^n-1}{p-1}\right)\cdot\binom{w}{2}.$$

$(p-1)$-gyel felszorozva

$$(p^{n+1}-1)\cdot\left((p-1)\binom{r_k(\mathbb{Z}_p^n)}{2}+\binom{w-(p-1)r_k(\mathbb{Z}_p^n)}{2}\right)\geq(p^n-1)\cdot\binom{w}{2}.$$

Ezt átrendezve és 2-vel szorozva majd $(p-1)$-gyel osztva megkapjuk, hogy

$$0\leq w^2p^n+w((p^{n+1}-1)(-2r_k(\mathbb{Z}_p^n))+(-p^n))+(p^{n+1}-1)(r_k(\mathbb{Z}_p^n)^2)p.$$

Ezen w-ben másodfokú, pozitív főegyütthatójú egyenlet alapján kapunk egy, a két gyök közé eső nyílt intervallumot, amelybe eső w-re negatív a jobb oldal. Jelölje Δ a diszkriminánst, $\Delta=(-2p^{n+1}r_k(\mathbb{Z}_p^n)+2r_k(\mathbb{Z}_p^n)-p^n)^2-4p^n(p^{n+1}-1)(r_k(\mathbb{Z}_p^n)^2)p=4r_k(\mathbb{Z}_p^n)^2+p^{2n}-4r_k(\mathbb{Z}_p^n)p^n-4r_k(\mathbb{Z}_p^n)^2p^{n+1}+4r_k(\mathbb{Z}_p^n)p^{2n+1}$.

$\frac{2p^{n+1}r_k(\mathbb{Z}_p^n)-2r_k(\mathbb{Z}_p^n)+p^n-\sqrt{\Delta}}{2p^n}<w<\frac{2p^{n+1}r_k(\mathbb{Z}_p^n)-2r_k(\mathbb{Z}_p^n)+p^n+\sqrt{\Delta}}{2p^n}$ esetén ellentmondást kapunk, ilyen egész w esetén nincs w pontú konstrukció $\mathbb{Z}_p^{n+1}$-ben k elemű számtani sorozat nélkül. Ha pedig nem létezik w pontú konstrukció, nem létezik w-nél több pontú sem, ti. tartalmazna w pontú konstrukciót. A két gyök különbsége $\frac{\sqrt{\Delta}}{p^n}=\frac{\sqrt{p^{2n}+4r_k(\mathbb{Z}_p^n)(p^{n+1}-1)(p^n-r_k(\mathbb{Z}_p^n))}}{p^n}>\frac{\sqrt{p^{2n}}}{p^n}=1$, így az 1-nél nagyobb különbség miatt létezik egész szám, amely a korlátok közé esik, a legkisebb ilyen és több pontra nincs konstrukció $\mathbb{Z}_p^{n+1}$-ben k hosszú számtani sorozat nélkül.

Így megkaptuk, hogy $r_k(\mathbb{Z}_p^{n+1})\leq\frac{2p^{n+1}r_k(\mathbb{Z}_p^n)-2r_k(\mathbb{Z}_p^n)+p^n-\sqrt{\Delta}}{2p^n}$, az utóbbi kisebb gyöknél több pontú konstrukcióra ellentmondást kaptunk. Ebből kis átírással megkapjuk a tétel állítását, $r_k(\mathbb{Z}_p^{n+1})\leq p(r_k(\mathbb{Z}_p^n))-\frac{r_k(\mathbb{Z}_p^n)}{p^n}+\frac{1}{2}-\frac{\sqrt{4r_k(\mathbb{Z}_p^n)^2+p^{2n}-4r_k(\mathbb{Z}_p^n)p^n-4r_k(\mathbb{Z}_p^n)^2p^{n+1}+4r_k(\mathbb{Z}_p^n)p^{2n+1}}}{2p^n}$. ■

Ezzel az állítással a triviális $p(r_k(\mathbb{Z}_p^n))\leq r_k(\mathbb{Z}_p^{n+1})$ becslésen javítottunk. Kis esetekben akár pontos felső becslést is kaphatunk. A $k=3$, $p=5$, $n=2$ esetben $r_3(\mathbb{Z}_5^2)=6$ alapján $r_3(\mathbb{Z}_5^3)\leq 30-\frac{6}{25}+\frac{1}{2}-\frac{\sqrt{57169}}{50}\approx 25,48$, így $r_3(\mathbb{Z}_5^3)\leq 25$. 25 pontú konstrukció 3 hosszú számtani sorozat nélkül ugyanakkor létezik, Kovács Benedek programmal talált ilyet, tehát $r_3(\mathbb{Z}_5^3)=25$.

A $k=p$ esetben $\frac{\sqrt{p^{2n}+4r_k(\mathbb{Z}_p^n)(p^{n+1}-1)(p^n-r_k(\mathbb{Z}_p^n))}}{2p^n}$ $p^{\frac{n}{2}}$-es nagyságrendjéből a felső korlát $p^{\frac{n}{2}}$-es nagyságrendűvel kisebb a triviális felső korlátnál, $p(r_k(\mathbb{Z}_p^n))$-nél, így a javítás jelentősebb a kisebb n-ekre.

7. Irodalomjegyzék

[1] A. E. Brouwer-A. Schrijver: The blocking number of an affine space. Journal of Combinatorial Theory, Series A, 24 (2): 251-253, 1978

[2] B. L. Davis-D. Maclagan: The card game set. The Mathematical Intelligencer, 25 (3): 33-40, 2003

[3] C. Elsholtz-J. Führer: Maximal m-progression free-sets in $\mathbb{Z}_m^n$. Kézirat, 2021

[4] C. Elsholtz-P. P. Pach: Caps and progression-free sets in $\mathbb{Z}_m^n$. Designs, Codes and Criptography, 88 (10): 2133-2170, 2020

[5] P. Frankl-R. L. Graham-V. Rödl: On subsets of abelian groups with no 3-term arithmetic progression. Journal of Combinatorial Theory, Series A, 45 (1): 157-161, 1987

[6] A. Gács: The Rédei Method Applied to Finite Geometry. Ph.D értekezés, ELTE, 1997

[7] R. E. Jamison: Covering finite fields with cosets of subspaces. Journal of Combinatorial Theory, Series A, 22 (3): 253-266, 1977

[8] https://mathoverflow.net/questions/229417/blocking-sets-in-three-dimensional-finite-affine-spaces