Eötvös Loránd Tudományegyetem
Matematika Intézet

Indruck Balázs

Számtani sorozatok az egész számok részhalmazaiban

Matematikus MSc Szakdolgozat

Témavezető:
Gyarmati Katalin, egyetemi docens

ELTE Algebra és Számelmélet Tanszék

Budapest, 2020

Köszönetnyilvánítás

Ezúton szeretném megköszönni a témavezetőmnek, Gyarmati Katalin tanárnőnek a közös munkát és azt a rengeteg segítséget, amit a szakdolgozat írása közben és az egyetemi tanulmányaim alatt kaptam tőle.

Kivonat

A szakdolgozatban a kombinatorikus számelmélet azon kérdéskörét járjuk körül, hogy mely feltételek biztosíthatják azt, hogy az egész számok egy, a feltételekkel rendelkező részhalmaza minden esetben tartalmaz egy adott hosszúságú számtani sorozatot.

Bemutatásra kerül Roth tétele bizonyítással együtt, majd olyan halmazkonstrukciókat vizsgálunk, melyek nem tartalmaznak háromtagú számtani sorozatokat.

Végül nagy vonalakban ismertetjük Szemerédi híres tételét k-hosszú számtani sorozatokról és a Green-Tao tételt.

Tartalomjegyzék

1. Bevezetés

Legyenek k és d pozitív egész számok. Egy k hosszúságú, d differenciájú számtani sorozaton az n, $n+d$, $n+2d$, $\ldots$, $n+(k-1)d$ számokból álló halmazt értjük, ahol n tetszőleges egész szám.

A kombinatorikus számelmélet egyik központi kérdése, hogy milyen feltételeknek kell teljesülnie az egész számok egy tetszőleges részhalmazára ahhoz, hogy az mindenképpen tartalmazzon k-hosszú számtani sorozatot valamilyen $k \in \mathbb{N}$ számra.

Az első ilyen jellegű eredmény *van der Waerdentől* [1] származik:

1.1. Tétel (van der Waerden, 1927.)**.** *Legyenek h és k pozitív egész számok. Bárhogyan is particionáljuk az egész számok halmazát h darab C_1, $\ldots$, C_h részhalmazra, az egyik részhalmaz ezek közül mindenképpen tartalmaz k-hosszú számtani sorozatot.*

Van der Waerden tétele a Ramsey-elmélet eredményei közé is tartozik, hiszen ha a particionálásra úgy tekintünk, mint az egész számok színezésére h színnel, akkor a tétel szerint bármely színezésnél létezik k hosszúságú egyszínű számtani sorozat.

Az 1.1 Tétel véges változata, amelyben minden halmaz véges elemszámú a következő:

1.2. Tétel (van der Waerden – véges változat)**.** *Legyenek h és k pozitív egész számok. Ekkor létezik olyan $N(h,k)$ szám, hogy ha $N \geq N(h,k)$ pozitív egész és az $\{1,2,\ldots,N\}$ halmazt h darab részhalmazra particionáljuk, akkor legalább az egyik részhalmaz tartalmaz k-hosszú számtani sorozatot.*

1.1. Definíció. Legyen A az egész számok tetszőleges részhalmaza. Az A halmaz Banach felső sűrűségén (vagy egyszerűen csak felső sűrűségén) az alábbi mennyiséget érjük:

$$D^*(A) = \limsup_{N\to\infty} \frac{|A \cap \{1,2,\ldots,N\}|}{N}.$$

Erdős Pál és *Turán Pál* 1936-ban fogalmazták meg azt a sejtést, miszerint ha az egész számok egy tetszőleges részhalmaza pozitív felső sűrűségű, akkor a halmaz tartalmaz tetszőlegesen hosszú számtani sorozatot. Ebből a sejtésből nyilvánvalóan következik a van der Waerden-tétel. Valóban, a felső sűrűség additív, így

$$D^*\left(\bigcup_{i=1}^{m} A_i\right) \leq \sum_{i=1}^{m} D^*(A_i),$$

ahol $A_i \subseteq \mathbb{Z}$, $i = 1, \ldots, m$ tetszőleges halmazok. Így ha $\mathbb{Z}$-t h részhalmazra particionáljuk, akkor

$$1 = D^*\left(\bigcup_{i=1}^{h} A_i\right) \leq \sum_{i=1}^{h} D^*(A_i),$$

vagyis ekkor valamelyik részhalmaz felső sűrűsége legalább $1/h > 0$.

Fogalmazzuk meg az Erdős-Turán-sejtést pontosan:

1.1. Sejtés (Erdős, Turán)**.** *Legyen $A \subseteq \mathbb{Z}$ egy tetszőleges halmaz, amire $D^*(A) > 0$. Ekkor A tartalmaz k-hosszú számtani sorozatot minden $k \geq 3$ egész számra.*

Ebből az is következik, hogy minden pozitív felső sűrűségű halmaz tartalmaz végtelen sok k-hosszú számtani sorozatot minden k-ra, hiszen a k-elemű számtani sorozatot törölve a halmazból ismét pozitív felső sűrűségű halmazhoz jutunk. A fenti sejtést átfogalmazhatjuk az alább látható módon is. A következőkben $[N]$ jelöli az $\{1,2,\ldots,N\}$ halmazt.

1.2. Sejtés (Erdős, Turán – második változat)**.** *Legyen $k \geq 3$ egész szám, valamint legyen $0 < \delta \leq 1$. Ekkor létezik olyan $N(k,\delta)$ pozitív egész szám, hogy minden $N \geq N(k,\delta)$ esetén ha $A \subseteq [N]$ és $|A| \geq \delta N$, akkor A tartalmaz k-hosszú számtani sorozatot.*

A fentihez hasonlóan most is be lehet látni, hogy ebből a véges változatból következik a véges van der Waerden-tétel.

1.1. Állítás. *Az 1.1 Sejtés és az 1.2 Sejtés állítása ekvivalens.*

Bizonyítás. Nyilvánvalóan az 1.2 Sejtésből következik az 1.1 Sejtés, így nézzük a másik irányt! Tegyük fel, hogy igaz az 1.1 Sejtés állítása, de az 1.2 Sejtés valamilyen $k \geq 3$ és $\delta \in (0,1]$ esetén mégsem teljesül. Más szóval akármilyen pozitív egész N számra létezik olyan $A \subseteq [N]$, $|A| \geq \delta N$ halmaz, amire A nem tartalmaz k-hosszú számtani sorozatot.

Legyen $N_1 = 1$, $b_1 = 0$, valamint vezessük be a következő jelöléseket:

$$N_i := b_{i-1} + N_{i-1}, \quad b_i := b_{i-1} + N_{i-1} + N_i + 1, \tag{1.1}$$

ahol $i \geq 2$.

Ekkor pozitív egész számok olyan növekvő sorozatát kapjuk, melyre $1 = N_1 \leq N_2 < < N_3 < \ldots$, valamint olyan halmazok A_1, A_2, A_3, $\ldots$ sorozatát, melyre $A_i \subseteq [N_i]$, $|A_i| \geq \geq \delta N_i$ minden i-re és egyik A_i halmaz sem tartalmaz k-hosszú számtani sorozatot.

Legyen most $\tilde{A}_i = A_i + b_i$. Ekkor nyilvánvalóan az $\tilde{A}_i$ halmazok közül egyik sem tartalmaz k-hosszú számtani sorozatot, továbbá, ha $A_i \subseteq [1, \ldots, N_i]$, akkor az $N_i := b_{i-1} + N_{i-1}$ és a $b_i := b_{i-1} + N_{i-1} + N_i + 1 = 2N_i + 1$ konstrukciója miatt $\tilde{A}_i \subseteq [2N_i + 2, \ldots, 3N_i + 1]$. Ekkor szintén az előbbi konstrukció miatt ha $\tilde{A}_i \subseteq [2N_i + 2, \ldots, 3N_i + 1]$, akkor $\tilde{A}_{i+1} \subseteq [2N_{i+1} + 2, \ldots, 3N_{i+1} + 1] = [6N_i + 4, \ldots, 9N_i + 4]$, így emiatt az $\tilde{A}_i$ halmazok diszjunktak.

Legyen $A = \cup_i \tilde{A}_i$. Ekkor A sem tartalmaz k-hosszú számtani sorozatot, hiszen az egyes intervallumok vég- és kezdőpontjai mindig több, mint kétszeres távolságra vannak egymástól.

Tudjuk még, hogy $b_i \leq 3N_i$ minden $i \geq 1$-re. Továbbá,

$$\frac{|A \cap [b_i + N_i]|}{b_i + N_i} \geq \frac{|\tilde{A}_i \cap [b_i + 1, b_i + N_i]|}{4N_i} \geq \frac{\delta N_i}{4N_i} = \frac{\delta}{4}.$$

Ebből következik, hogy A felső sűrűsége legalább $\delta/4 > 0$, de a konstrukció miatt A nem tartalmaz számtani sorozatot így ellentmondásra jutottunk, amivel beláttuk az állítást. □

A fenti Erdős-Turán-sejtésről később kiderült, hogy a bizonyítása nagyon nehéz probléma. A legegyszerűbb $k = 3$ esetet először *K. F. Roth*-nak sikerült belátnia 1953-ban, a következő fejezetben ezzel részletesen foglalkozunk.

2. Roth tétele

Ebben a szakaszban rátérünk Roth [3] tételére és annak bizonyítására. Ez a fejezet a [2] és a [4] cikkek alapján készült el, a bizonyításnál a [4]-ben leírtakat követjük. A definíciókhoz a jelöléseket az [5]-ből és a [6]-ból vettük. Roth tétele a következőképpen szól:

2.1. Tétel (Roth)**.** *Legyen $A \subseteq \mathbb{Z}$ az egész számok olyan részhalmaza, ami pozitív felső sűrűségű. Ekkor A tartalmaz háromtagú számtani sorozatot.*

Az 1.2 Sejtéssel analóg módon most is ki lehet mondani egy véges változatot:

2.2. Tétel (Roth, véges változat)**.** *Minden $0 < \delta \leq 1$ számhoz létezik olyan $N_0(\delta)$, hogy minden $N \geq N_0$ esetén, ha $A \subseteq \{1,2,\ldots,N\}$, $|A| \geq \delta N$, akkor A tartalmaz háromtagú számtani sorozatot.*

Roth azonban egy erősebb tételt bizonyított, mint amit az Erdős-Turán-sejtés $k = 3$ esetén állít. Legyen N pozitív egész szám, valamint $a_k(N) = \frac{1}{N} \max\{|A| : A \subseteq [N], A$ nem tartalmaz k-hosszú számtani sorozatot$\}$. Az Erdős-Turán-sejtés azt jelenti, hogy $k \geq 3$-ra

$$a_k(N) \to 0, \text{ amint } N \to \infty.$$

Most már kimondhatjuk Roth tételének kvantitatív változatát is.

2.3. Tétel (Roth, kvantitatív változat)**.** *Legyen $N \geq 3$ egész szám. Ekkor*

$$a_3(N) \ll \frac{1}{\log\log N},$$

ahol a log *a kettes alapú logaritmust jelöli.*

Tehát Roth tételének kvantitatív változata becslést is ad arra, hogy milyen gyorsan tűnik el $a_3(N)$.

2.1. *Megjegyzés.* A 2.3 Tételben a felső korlátot az évek során sikerült javítania Szemerédinek [7], Heath-Brownnak [8], Bourgainnek [9], [10] és Sandersnek [11], [12]. A jelenlegi legjobb eredmény Bloomtól [13] származik, mely szerint

$$a_3(N) \ll \frac{(\log\log N)^4}{\log N}.$$

A továbbiakban a cél, hogy ismertessük Roth tételének bizonyítását. Ám mielőtt ezt megtennénk, szükségünk lesz néhány további definícióra és eredményre.

$\mathbb{Z}_N$-nel fogjuk jelölni a mod N maradékosztályokat. Ha x, y, z természetes számok és $x + y = 2z$, akkor ezek a számok egy 3-hosszú számtani sorozatot alkotnak. Ahelyett azonban, hogy megszámolnánk az A-ban ezeket a számtani sorozatokat, először azokat az A-beli x, y és z számhármasokat fogjuk megszámolni, melyek kielégítik az előbbi egyenletet $\mathbb{Z}_N$-ben. Bár a $\mathbb{Z}_N$-beli megoldás nem feltétlenül lesz számtani sorozat $\mathbb{Z}$-ben is (a megoldás "körbeérhet"), de ezáltal használhatjuk a diszkrét Fourier–analízis eszköztárát.

Jelöljük χ-vel azt a $\mathbb{Z}_N \to \mathbb{C}$-be képező additív karaktert, melyre $\chi(t) := \exp(2\pi it/N)$. Ekkor $t \in \{0,1,\ldots,N-1\}$ esetén $\chi(t)$ értékei az N-edik egységgyököket adják, így $|\chi(t)| = 1$ minden ilyen t-re. A konjugáltra pedig igaz a $\chi(-t) = \overline{\chi(t)}$ egyenlőség.

Nagyon sokszor fel fogjuk még használni a következő egyszerű, de rendkívül fontos azonosságot.

2.1. Állítás. *Ha* $\chi(t) = \exp(2\pi it/N)$, *akkor*

$$\sum_{m\in\mathbb{Z}_N} \chi(mt) = \begin{cases} 0, & \text{ha } t \neq 0 \\ N, & \text{ha } t = 0. \end{cases} \tag{2.1}$$

Bizonyítás. Legyen

$$S = \chi(0t) + \chi(1t) + \ldots + \chi((N-1)t) = 1 + \chi(t) + \ldots + \chi((N-1)t).$$

Ennek mindkét oldalát balról $\chi(t)$-vel szorozva azt kapjuk, hogy

$$\chi(t)S = \chi(t) + \ldots + \chi((N-1)t) + 1 = S,$$

amiből vagy $S = 0$ vagy $\chi(t) = 1$ következik. Az utóbbi esetben $\chi(t)$ definíciója miatt $\chi(t) = 1$ akkor és csak akkor, ha $t = 0 \pmod N$. Ekkor viszont a fenti összeg pontosan N, így beláttuk az állítást. □

2.1. Definíció (Fourier-transzformáció)**.** Legyen adott az $f : \mathbb{Z}_N \to \mathbb{C}$ leképezés. Az f függvény $\widehat{f}$ Fourier transzformáltját a következőképpen értelmezzük:

$$\widehat{f}(m) := \sum_{x\in\mathbb{Z}_N} f(x)\chi(-xm). \tag{2.2}$$

Az $\widehat{f}(m)$ értékeket Fourier-együtthatóknak is szokás nevezni.

A Fourier transzformált a Roth-tétel bizonyítása szempontjából sok hasznos tulajdonsággal rendelkezik. Most felsoroljuk azokat a tulajdonságokat, melyekre szükségünk lesz a későbbiekben.

2.4. Tétel. *Legyen $f : \mathbb{Z}_N \to \mathbb{C}$. Ekkor az $\widehat{f}$ Fourier transzformáltra igazak a következők:*

1. *Inverziós formula. Minden $x \in \mathbb{Z}_N$ esetén*

$$f(x) = \frac{1}{N} \sum_{m \in \mathbb{Z}_N} \widehat{f}(m)\chi(xm). \tag{2.3}$$

2. *Pontonkénti becslés. Minden $m \in \mathbb{Z}_N$-re*

$$|\widehat{f}(m)| \leq \sum_{x \in \mathbb{Z}_N} |f(x)|. \tag{2.4}$$

3. *Plancherel-azonosság.*

$$\sum_{x \in \mathbb{Z}_N} |f(x)|^2 = \frac{1}{N} \sum_{m \in \mathbb{Z}_N} |\widehat{f}(m)|^2. \tag{2.5}$$

4. *Konvolúciós azonosság. Ha f,$g : \mathbb{Z}_N \to \mathbb{C}$ függvények, akkor legyen ezek konvolúciója*

$$(f * g)(x) := \sum_{y \in \mathbb{Z}_N} f(y)\overline{g(y-x)}. \tag{2.6}$$

   Ekkor minden $m \in \mathbb{Z}_N$-re

$$(\widehat{f * g})(m) = \widehat{f}(m)\overline{\widehat{g}(m)}. \tag{2.7}$$

Bizonyítás. 1. A 2.1 Állítás felhasználásával a következőt kapjuk:

$$\begin{aligned} \frac{1}{N} \sum_{m \in \mathbb{Z}_N} \widehat{f}(m)\chi(xm) &= \frac{1}{N} \sum_{m,y \in \mathbb{Z}_N} f(y)\chi(-ym)\chi(xm) \\ &= \frac{1}{N} \sum_{y \in \mathbb{Z}_N} f(y) \sum_{m \in \mathbb{Z}_N} \chi(m(x-y)) \\ &= f(x). \end{aligned} \tag{2.8}$$

2. A háromszög-egyenlőtlenséget felhasználva

$$|\widehat{f}(m)| \leq \sum_{x\in\mathbb{Z}_N} |f(x)||\chi(-xm)| = \sum_{x\in\mathbb{Z}_N} |f(x)|. \tag{2.9}$$

3. Ismét a 2.1 Állítást, a Fourier transzformált definícióját, valamint a komplex számok abszolútértéke és konjugáltja közti összefüggést felhasználva

$$\begin{aligned}\sum_{m\in\mathbb{Z}_N} |\widehat{f}(m)|^2 &= \sum_{m,x,y\in\mathbb{Z}_N} f(x)\chi(-xm)\overline{f(y)\chi(-ym)} \\ &= \sum_{x,y\in\mathbb{Z}_N} f(x)\overline{f(y)} \sum_{m\in\mathbb{Z}_N} \chi(m(y-x)) \\ &= N\sum_{x\in\mathbb{Z}_N} |f(x)|^2.\end{aligned} \tag{2.10}$$

4. A definícióból kiindulva

$$\begin{aligned}(\widehat{f*g})(m) &= \sum_{x\in\mathbb{Z}_N} (f*g)(x)\chi(-xm) \\ &= \sum_{x,y\in\mathbb{Z}_N} f(y)\overline{g(y-x)}\chi(-xm+ym-ym) \\ &= \sum_{x,y\in\mathbb{Z}_N} f(y)\chi(-ym)\overline{g(y-x)}\chi((y-x)m) \\ &= \sum_{x,y\in\mathbb{Z}_N} f(y)\chi(-ym)\overline{g(y-x)\chi(-(y-x)m)} \\ &= \sum_{y\in\mathbb{Z}_N} f(y)\chi(-ym) \sum_{(y-x)=z\in\mathbb{Z}_N} \overline{g(z)\chi(-zm)} \\ &= \widehat{f}(m)\overline{\widehat{g}(m)}.\end{aligned} \tag{2.11}$$

□

Az additív kombinatorikában bevett jelölés szerint legyen egy A halmaz $A(x)$ karakterisztikus függvénye az

$$A(x) = \begin{cases} 0, & \text{ha } x \notin A \\ 1, & \text{ha } x \in A. \end{cases}$$

Kizárólag a tétel bizonyítása közben $[N]$ nem az eddigi $\{1,2,\ldots,N\}$ halmazt fogja jelölni, hanem a $\{0,1,\ldots,N-1\}$-et, de ez semmilyen megkötést nem jelent.

Technikai okok miatt szeretnénk még feltenni, hogy az N páratlan. Ez nem okoz gondot, mert ha N páros, akkor A sűrűsége $[N+1]$-ben csak elhanyagolható mértékben különbözik az A $[N]$-beli sűrűségétől, feltéve, hogy N megfelelően nagy. Nevezetesen az új δ' sűrűségre teljesül az $(1-\frac{1}{N})\delta < (1-\frac{1}{N+1})\delta = \delta' < \delta$ egyenlőtlenség.

2.1. Roth tételének bizonyítása – bevezetés

A fenti jelölésekkel Roth tételének bizonyítása a következőképpen zajlik. A bizonyítás egy algoritmus. Tegyük fel indirekt, hogy $A \subseteq [N]$, $|A| = \delta N$ és A nem tartalmaz 3-hosszú számtani sorozatot.

Az algoritmus első lépésében két eset állhat elő: vagy az A halmaz "megfelelően véletlen" vagy az A nem "megfelelően véletlen".

Jelölje $\widehat{A}(m)$ az $A(x)$ karakterisztikus függvény Fourier transzformáltját az $m \in \mathbb{Z}_N$ helyen. Ha az $|\widehat{A}(m)|$ értékek "kicsik" minden $m \neq 0$-ra és az N elegendően nagy – később meghatározzuk ezt pontosan –, akkor A-ban sok háromtagú számtani sorozatot találhatunk az A-beli sorozatok számának becslésével. Ez egyenértékű azzal, hogy az A halmaz "megfelelően véletlen". Tehát ekkor ellentmondásra jutottunk, hiszen feltettük, hogy A-ban nem létezik 3-tagú számtani sorozat, de mégis találtunk ilyet.

Másrészről, ha az N elegendően nagy, de az első esetben nem teljesül a becslés egy feltétele, vagy ha az A halmaz nem "megfelelően véletlen", akkor találhatunk egy hosszú P számtani sorozatot úgy, hogy az A sűrűsége P-ben nagyobb, mint az $[N]$-ben, vagyis

$$|A \cap P| \geq (\delta + \varepsilon')|P|,$$

valamilyen $\varepsilon' > 0$-ra, ami csak δ-tól függ.

Legyen $A' = A \cap P$ és alkalmazzuk az algoritmust erre a halmazra és P-re. Mivel $A' \subseteq \subseteq A$, ezért a feltevés szerint A' sem tartalmaz háromtagú számtani sorozatot. Az eljárást ismételve az algoritmus minden lépésében egy olyan halmazt kapunk, aminek a sűrűsége az adott iterációban szereplő számtani sorozaton szigorúan nagyobb, mint az előző iterációban. Meg lehet mutatni, hogy ha A nem tartalmaz háromtagú számtani sorozatot, akkor kell lennie egy olyan $\tilde{P}$ számtani sorozatnak, amin A sűrűsége nagyobb, mint 1. Ez nyilvánvalóan nem lehetséges, ezért az algoritmus véges sok lépésben befejeződik: eljutunk egy olyan $\tilde{P}$ számtani sorozathoz és egy olyan $\tilde{A} = A \cap \tilde{P} \subseteq A$ halmazhoz, aminek

a Fourier transzformált értékei már kicsik. De ekkor a fentiek szerint ebben már találhatunk 3-hosszú számtani sorozatokat, ami ellentmond a feltevésnek, hogy az A-ban nem létezik ilyen. Ahhoz, hogy ez a gondolatmenet működjön, meg kell számolni a szükséges iterációk számát ahhoz, hogy eljussunk a $\tilde{P}$ sorozatig és meg kell mutatni, hogy a kapott $P \supseteq P_1 \supseteq \ldots \supseteq \tilde{P}$ részsorozatokban nem hagytunk el túl sok elemet az eljárás közben (a végeredményként kapott számtani sorozatnak nem szabad az üres halmaznak lenni).

2.2. *Megjegyzés.* Bár a fenti algoritmus bemenetében az $[N] = \{0,1,\ldots N-1\}$ alakú és az $A \subseteq [N]$ halmazok szerepelnek, utána pedig áttérünk a $P \subseteq [N]$ *számtani sorozatra* (ami nem feltétlenül $\{0,1,\ldots,|P|-1\}$ alakú) és az $A' = A \cap P$ halmazra, ez semmilyen megkötést nem jelent. Technikailag ugyanis a P számtani sorozatot azonosíthatjuk $[|P|]$-vel abban az értelemben, hogy P elemei és a $\{0,1,\ldots,|P|-1\}$ halmaz között kölcsönösen egyértelmű megfeleltetést létesítünk. Ha a P differenciája d, akkor az új differencia 1 lesz, P elemei pedig szomszédos elemek lesznek az új halmazban – végső soron normáljuk a differenciát és amennyiben szükséges "eltoljuk" a számtani sorozat elemeit úgy, hogy azok a $\{0,1,\ldots,|P|-1\}$ számoknak feleljenek meg. Ekkor természetesen az $A' = A \cap$ $\cap P$ elemeit is hozzárendelhetjük a nekik megfelelő elemeknek, így tényleg az algoritmus eredeti bemenetével megegyező alakú halmazokat kapunk a következő iterációban is.

2.2. Egy halmaz véletlenségének jellemzése

A Fourier transzformált segítségével megszámolhatjuk az

$$x + y \equiv 2z \pmod{N}$$

kongruencia megoldásszámát, ahol $x, y, z \in A$. Jelöljük ezt a megoldásszámot Q_0-val. Ekkor felhasználva a 2.1 Állítást, illetve a Fourier transzformált definícióját az $f(x) = = A(x)$ karakterisztikus függvénnyel, azt kapjuk, hogy

$$Q_0 = \sum_{x\in A}\sum_{y\in A}\sum_{z\in A}\frac{1}{N}\sum_{m\in\mathbb{Z}_N}\chi(-(x+y-2z)m) = \frac{1}{N}\sum_{m\in\mathbb{Z}_N}\widehat{A}(m)^2\widehat{A}(-2m). \tag{2.12}$$

Ha felhasználjuk, hogy $\widehat{A}(0) = |A| = \delta N$, akkor

$$Q_0 = \delta^3 N^2 + \frac{1}{N}\sum_{m=1}^{N-1}\widehat{A}(m)^2\widehat{A}(-2m).$$

A fenti egyenlet "főegyüttható́jára", $\delta^3 N^2$-re a következőképpen is gondolhatunk. Ez a szám nem más, mint az $x + y \equiv 2z \pmod N$ egyenlet várható megoldásszáma abban az esetben, ha az A halmaz egy véletlen részhalmaza $[N]$-nek. Tegyük fel, hogy annak a valószínűsége, hogy egy adott $a \in [N]$ elem A-ban van minden ilyen a-ra egymástól függetlenül δ. Ha tetszőlegesen választunk egy x-et és egy z-t az A-ból, akkor ezt $\delta^2 N^2$ módon tehetjük meg, mert $|A| = \delta N$. De ekkor egy konkrét x-re és z-re ha y-t úgy definiáljuk, hogy $y \equiv 2z - x \pmod N$, akkor annak a valószínűsége, hogy ez az y elem A-ban van, nem más, mint $\delta = |A|N^{-1}$. Ezért, ha A egyenletesen oszlik el a $\{0,1,\dots,N-1\}$ számokon, akkor arra számítunk, hogy A-ban sok számtani sorozatot találunk mod N.

Vegyük észre, hogy ha $|\widehat{A}(m)| \le \varepsilon N$ minden $m \neq 0$-ra, akkor a Plancherel formulát felhasználva

$$\frac{1}{N}\left|\sum_{m=1}^{N-1} \widehat{A}(m)^2 \widehat{A}(-2m)\right| \le \max_{m\neq 0} |\widehat{A}(-2m)| \frac{1}{N}\sum_{m=0}^{N-1} |\widehat{A}(m)|^2 \le \varepsilon N \sum_{m=0}^{N-1} |A(m)|^2 = \varepsilon\delta N^2,$$

ezért

$$Q_0 \ge \delta^3 N^2 - \varepsilon\delta N^2.$$

Tehát a bevezetett ε számmal meg tudjuk mérni, hogy az A halmaz a fenti értelemben mennyire közel áll ahhoz, hogy véletlen legyen.

2.2. Definíció. Azt mondjuk, hogy az A halmaz ε-egyenletes eloszlású (vagy megfelelően véletlen), ha

$$|\widehat{A}(m)| \le \varepsilon N$$

minden $m = 1,\dots,N-1$-re.

2.3. Az ε-egyenletes eloszlású halmazok esete

A fentiekből nyilvánvaló, hogy ha például $\varepsilon < \delta^2/2$ és A ε-egyenletes, akkor $Q_0 \ge \delta^3 N^2/2$, tehát A legalább $\delta^3 N^2/2$ háromtagú számtani sorozatot tartalmaz (mod N), beleértve a triviális $x = y = z$ sorozatokat is.

Azonban egy $\mathbb{Z}_N$-beli megoldás nem feltétlenül lesz számtani sorozat $\mathbb{Z}$-ben is (pl. $N = 9$ esetén $x = 6$, $z = 8$, $y = 1(= 10)$), így ezeket meg kell különböztetni. Jelöljük Q-val az $x + y = 2z$ megoldásszámát $\mathbb{Z}$-ben, ahol $x, y, z \in A$. Ahhoz, hogy a 3-hosszú számtani

sorozatokat csak $\mathbb{Z}$-ben számoljuk, legyen $B := A \cap [N/3,\ 2N/3)$. Ha most $x, z \in B$ és $y \in A$ akkor a fenti egyenlet bármely $\mathbb{Z}_N$-beli megoldása számtani sorozat lesz $\mathbb{Z}$-ben is.

Amikor az A halmaz ε-egyenletes, akkor az előző (2.12) egyenletből kiindulva direkt módon is megmutatható, hogy A-ban létezik 3-tagú számtani sorozat.

2.5. Tétel. *Ha A ε-egyenletes úgy, hogy $\varepsilon \le \delta^2/8$ és $|B| \ge \frac{\delta}{4}N$, akkor $Q \ge \delta^3 N^2/32$ és A tartalmaz háromtagú számtani sorozatot, ha N elég nagy.*

Bizonyítás. A (2.12)-höz hasonlóan azt írhatjuk, hogy

$$Q \ge \frac{1}{N} \sum_{m \in \mathbb{Z}_N} \widehat{B}(m)\widehat{A}(m)\widehat{B}(-2m) = \delta|B|^2 + \frac{1}{N}\sum_{m=1}^{N-1} \widehat{B}(m)\widehat{A}(m)\widehat{B}(-2m).$$

Felhasználva a Cauchy-Schwarz-egyenlőtlenséget, a Plancherel-azonosságot, valamint, hogy N páratlan, ezért 2 invertálható mod N,

$$\begin{aligned}
\left|\sum_{m=1}^{N-1} \widehat{B}(m)\widehat{A}(m)\widehat{B}(-2m)\right| &\le \max_{m\neq 0}|\widehat{A}(m)| \sum_{m=0}^{N-1} |\widehat{B}(m)||\widehat{B}(-2m)| \\
&\le \varepsilon N \left(\sum_m |\widehat{B}(m)|^2\right)^{1/2} \left(\sum_m |\widehat{B}(-2m)|^2\right)^{1/2} \\
&= \varepsilon N \sum_m |\widehat{B}(m)|^2 \\
&= \varepsilon N^2 \sum_m B(x) \\
&\le \varepsilon N^2 |B|.
\end{aligned} \tag{2.13}$$

Ha most felhasználjuk, hogy $\varepsilon \le \delta^2/8$ és $|B| \ge \frac{\delta}{4}N$, akkor

$$Q \ge \frac{1}{2}\delta|B|^2 \ge \delta^3 N^2/32.$$

Ezzel beláttuk az állítás első felét.

Mivel a Q-ból nem zártuk ki a triviális $x = y = z$ számtani sorozatokat, ezért ezek számát még le kell vonni. De ezekből összesen annyi van, mint A elemszáma, azaz $|A| = \delta N$. Így a nem triviális 3-hosszú számtani sorozatok száma A-ban legalább

$$\delta^3 N^2/32 - \delta N, \tag{2.14}$$

ami pozitív, ha N megfelelően nagy. Konkrétan $N > 32/\delta^2$-re igaz az állítás. □

Foglaljuk össze, hogy hol tartunk most. A fenti tétel feltételei szerint a következőt mondhatjuk.

2.2. Állítás. *Legyen $A \subseteq \{0,1,\dots,N-1\}$ és $|A| = \delta N$. Ha A-ban nincs háromtagú számtani sorozat, akkor a következők egyike áll fent:*

1. *A nem ε-egyenletes semmilyen $\varepsilon \leq \delta^2/8$-ra.*
2. *$N \leq 32/\delta^2$.*
3. *$|B| < \frac{\delta}{4}N$. Ebben az esetben létezik olyan $\mathbb{Z}$-beli P (számtani) sorozat, amire $|P| \geq$ $\geq N/3$ és*
$$|A \cap P| \geq (\delta + \delta/8)|P|.$$

Bizonyítás. Az első két állítás egyszerűen a fenti tétel feltételeinek megfordítása. A harmadik állítás pedig azért igaz, mert $|A| = \delta N$ és ha $|B| < \frac{\delta}{4}N$, akkor az $A \setminus B$ két részintervallumára

$$\max\{|A \cap [0, N/3)|, |A \cap [2N/3, N)|\} \geq 3\delta N/8 = 9\delta/8 \cdot (N/3).$$

□

Tehát, ha $0 < \delta \leq 1$ akkor létezik olyan $N_0(\delta)$ küszöbindex, hogy minden $N > N_0(\delta)$ esetén, ha $A \subseteq \{0,1,\dots,N-1\}$ és $|A| = \delta N$, akkor A tartalmaz háromtagú számtani sorozatot, feltéve, hogy A ε-egyenletes és $|B| \geq \frac{\delta}{4}N$, így ebben az esetben igaz a Roth-tétel.

Ha viszont $|B| < \frac{\delta}{4}N$, akkor a fenti lemma szerint létezik olyan P sorozat, amin A sűrűsége növekedett, így P-vel és $A \cap P$-vel elkezdhetjük a fent leírt algoritmus következő iterációját és megismételhetjük az eddigi gondolatmenetet.

Tehát már csak azt az esetet kell kezelnünk, amikor A nem ε-egyenletes. Ez következik most.

2.4. A nem ε-egyenletes eloszlású halmazok esete

Meg fogjuk vizsgálni azt az esetet, amikor az A halmaz rendelkezik nagy Fourier-együtthatóval, azaz valamilyen $m \neq 0$-ra $|\widehat{A}(m)| > \frac{\delta^2}{8}N$ a fentiek szerint.

2.3. Definíció. Azt mondjuk, hogy a $\mathbb{Z}_N$-beli P számtani sorozat nem átfedő, ha a P-beli közös differencia d és P hossza L, akkor $dL < N$.

Egy nem átfedő $\mathbb{Z}_N$-beli számtani sorozat felírható két $\mathbb{Z}$-beli számtani sorozat diszjunkt uniójaként.

2.1. Lemma. *Tegyük fel, hogy B' egy nem átfedő $\mathbb{Z}_N$-beli számtani sorozat, amin A sűrűsége $\delta + \varepsilon'$. Ekkor létezik olyan $\mathbb{Z}$-beli P számtani sorozat, aminek a hossza legalább $\frac{1}{2}\varepsilon'|B'|$ és A sűrűsége P-n legalább $\delta + \frac{1}{2}\varepsilon'$.*

Bizonyítás. A feltétel szerint B' felírható $B' = P_1 \cup P_2$ alakban, ahol P_1 és P_2 már mindketten $\mathbb{Z}$-beli számtani sorozatok. Tegyük fel, hogy $|P_1| \leq |P_2|$. Ha $|P_1| \leq (1/2)\varepsilon'|B'|$, akkor

$$\begin{aligned} |A \cap P_2| &\geq |A \cap B'| - |P_1| \\ &\geq (\delta + \varepsilon')|B'| - \frac{1}{2}\varepsilon'|B'| \\ &= (\delta + \frac{1}{2}\varepsilon')|B'| \geq (\delta + \frac{1}{2}\varepsilon')|P_2|. \end{aligned} \tag{2.15}$$

Másrészről, ha $|P_1| > (1/2)\varepsilon'|B'|$, akkor P_1 és P_2 elemszáma is legalább $(1/2)\varepsilon'|B'|$. Mivel A sűrűsége B'-n $\delta + \varepsilon'$, ezért A sűrűsége vagy P_1-en vagy P_2-n is $\delta + \varepsilon'$. Valóban, tegyük fel indirekt, hogy

$$|A \cap P_1| < (\delta + \varepsilon')|P_1|, \quad |A \cap P_2| < (\delta + \varepsilon')|P_2|.$$

Ekkor

$$\begin{aligned} \delta + \varepsilon' = \frac{|A \cap B|}{|B|} = \frac{|A \cap P_1| + |A \cap P_2|}{|P_1| + |P_2|} &< \frac{(\delta + \varepsilon')|P_1| + (\delta + \varepsilon')|P_2|}{|P_1| + |P_2|} \\ = (\delta + \varepsilon')\frac{|P_1| + |P_2|}{|P_1| + |P_2|} &= \delta + \varepsilon', \end{aligned} \tag{2.16}$$

ami ellentmondás a szigorú egyenlőtlenség miatt. □

2.2. Lemma. *Tegyük fel, hogy $|\widehat{A}(m)| > \varepsilon N$ valamilyen $m \neq 0$-ra. Ekkor létezik egy olyan nem átfedő B' számtani sorozat, aminek hossza $|B'| \geq \sqrt{N}/8$, valamint $|A \cap B'| \geq (\delta + \varepsilon/4)|B'|$.*

A 2.2 Lemma bizonyításához szükségünk lesz olyan függvényekre, melyeknek az átlaga 0. Ehhez vezessük be az úgynevezett egyensúly függvényt, amit $f(x) := A(x) - \delta$ jelöl.

2.3. Állítás. *Az f egyensúly függvény a következő tulajdonságokkal rendelkezik.*

1. $\sum_x f(x) = 0$.
2. $\widehat{f}(m) = \widehat{A}(m)$ *minden* $m \neq 0$*-ra és* $\widehat{f}(0) = 0$.

Bizonyítás. A definícióból kiindulva

$$\sum_x f(x) = \sum_x (A(x) - \delta) = |A| - \delta N = 0.$$

Továbbá, ha $m \neq 0$, akkor

$$\widehat{f}(m) = \sum_x f(x)\chi(-xm) = \sum_x A(x)\chi(-xm) - \delta \sum_x \chi(-xm) = \widehat{A}(m),$$

Ha pedig $m = 0$, akkor

$$\widehat{f}(0) = \sum_x f(x) = 0.$$

□

A 2.2 Lemma bizonyítása. Először vegyük észre, hogy $B' = B + x$-et írva igaz az

$$|A \cap (B + x)| \geq (\delta + \frac{1}{4}\varepsilon)|B| \Longleftrightarrow \sum_y f(y)B(y - x) \geq \frac{1}{4}\varepsilon|B|.$$

Valóban, nyilván $|B| = |B'|$ és $b + x = y \in |A \cap (B + x)|$ pontosan akkor igaz, ha $f(y) = A(y) - \delta = 1 - \delta$, $B(y - x) = 1$. Továbbá a szummában összesen $-\delta|B|$ kerül levonásra.

Ezután két lépés szerint fogunk eljárni.

1. Megmutatjuk, hogy bármely $1 \leq m \leq N - 1$-re létezik egy nem átfedő B számtani sorozat, melynek hossza legalább $\sqrt{N}/8$ és

$$|\widehat{B}(m)| \geq \frac{1}{2}|B|.$$

2. Végül az előző lépés felhasználásával megmutatjuk, hogy egy megfelelő x-re a lemmában szereplő B' sorozat a B sorozat x-szel való eltolásával jön létre, azaz igaz a

$$\sum_y f(y)B(y-x) \geq \frac{1}{4}\varepsilon|B|.$$

Ebből a két lépésből nyilvánvalóan következik az állítás a fenti azonosság szerint.

Az első lépéshez legyen m fix és tekintsük a következő ponthalmazok egyikét:

$$\{(0,0),(1,m),(2,2m),\ldots,(N-1,(N-1)m)\} \subseteq \mathbb{Z}_N^2$$

vagy

$$\{(N-1,0),(N-2,m),(2,2m),\ldots,(0,(N-1)m)\} \subseteq \mathbb{Z}_N^2.$$

Ha a $[0,N-1]^2 = \mathbb{Z}_N^2$-et kevesebb, mint N, mondjuk $\lceil\sqrt{N}-1\rceil^2$ egyenlő méretű négyzetre particionáljuk, akkor a skatulyaelv szerint a fenti N-elemű ponthalmazból biztosan lesz két olyan pont, amelyek egy négyzetbe esnek. Vagyis létezik olyan $0 \leq l < k \leq N-1$ egész szám, hogy $k-l \leq \sqrt{N}$ és $m(k-l) \leq \sqrt{N}$, ha mod N tekintjük a pontok koordinátáit.

Legyen $d = k-l$. Legyen továbbá $B = \{\ldots,-2d,-d,0,d,2d,\ldots\}$ az számtani sorozat, melynek hossza $|B| = \lfloor\sqrt{N}/(2\pi)\rfloor$ és differenciája d. A konstrukció miatt B hossza legalább $\sqrt{N}/8$ és B nyilván nem átfedő, mert $d|B| < N$.

Már csak azt kell megmutatni, hogy $|\widehat{B}(m)|$ legalább $\frac{1}{2}|B|$.

$$\begin{aligned} |\widehat{B}(m) - |B|| &= \left|\sum_x (B(x)\chi(-xm) - B(x))\right| \\ &\leq \sum_{x\in B} |\chi(-xm)-1| \\ &\leq \sum_{|t|\leq|B|/2} |\chi(-tdm)-1| \\ &\leq |B| \cdot \max_{|t|\leq|B|/2} |\chi(-tdm)-1|. \end{aligned} \tag{2.17}$$

B konstrukciója miatt $m(k-l) = md \leq \sqrt{N}$, $|t| \leq |B|/2$, így $|-tdm| \leq \frac{|B|}{2}\sqrt{N} = \frac{\lfloor\sqrt{N}/(2\pi)\rfloor}{2}\sqrt{N} \leq N/(4\pi)$.

Definíció szerint $\chi(s) = \chi(-tdm)$ egy olyan N-edik egységgyök, melynek értéke csak a $-tdm/N$ törtrészétől függ. Továbbá a komplex egységkört vizsgálva egy ismert eredmény,

hogy $|e^{2\pi i\alpha} - 1| \leq 2\pi|\alpha|$, ahol $\alpha \in \mathbb{R}$. Ebből következik, hogy bármely t-re $|\chi(-tdm) - -1| \leq 2\pi \cdot |-tdm/N| \leq 2\pi\frac{N/(4\pi)}{N} = 1/2$. Tehát azt kaptuk, hogy

$$|\widehat{B}(m) - |B|| \leq \frac{1}{2}|B|,$$

így valóban $|\widehat{B}(m)| \geq \frac{1}{2}|B|$.

A következő lépésben szeretnénk tehát megmutatni, hogy egy megfelelően választott x értékre igaz a

$$\sum_y f(y)B(y-x) \geq \frac{1}{4}\varepsilon|B|.$$

Ehhez fel fogjuk használni a (2.4) pontonkénti becslést és a (2.7) konvolúciós azonosságot is. Legyen

$$G(x) := \sum_y f(y)B(y-x) = \sum_y f(y)\overline{B(y-x)} = (f * B)(x).$$

Felhasználva a pontonkénti becslést és konvolúciós azonosságot, a 2.3 Állítást, valamint a $|\widehat{B}(m)|$-re adott alsó becslést és azt, hogy A nem ε-egyenletes, igaz, hogy

$$\sum_x |G(x)| \geq |\widehat{G}(m)| = |\widehat{f}(m)||\widehat{B}(m)| = |\widehat{A}(m)||\widehat{B}(m)| \geq \varepsilon N\frac{|B|}{2},$$

ahol a feltevés szerint $r \neq 0$.

Az f-hez hasonlóan G átlagértéke is 0, mert

$$\sum_x G(x) = \sum_{x,y} f(y)B(y-x) = \sum_y f(y)\sum_x B(y-x) = |B| \cdot \sum_y f(y) = 0.$$

A fenti becsléshez hozzáadva ezt a 0-összegű kifejezést, a

$$\sum_x (|G(x)| + G(x)) \geq \varepsilon N\frac{|B|}{2} (> 0)$$

egyenlőtlenséghez jutunk. Itt a bal oldalon olyan tagokat összegzünk, melyekben egy szám és ugyanennek a számnak az abszolútértéke szerepel. Vagyis minden tag vagy 0 vagy $2G(x)$ lesz, amennyiben $G(x)$ pozitív. A jobb oldalon viszont egy szigorúan pozitív szám szerepel, ezért létezik olyan x, melyre $|G(x)| + G(x) \geq \frac{1}{2}\varepsilon|B|$, hiszen a szummában N tagot adunk össze. Ebből viszont az következik, hogy erre az x-re $G(x) \geq \frac{1}{4}\varepsilon|B|$, tehát találtunk olyan x-et, ami kielégíti a kívánt feltételeket. □

Ha egyesítjük a 2.1 Lemma és a 2.2 Lemma eredményeit, akkor a következőt kapjuk.

2.4. Állítás. *Tegyük fel, hogy* $|\widehat{A}(m)| > \varepsilon N$ *valamilyen* $m \neq 0$*-ra. Ekkor létezik olyan* $\mathbb{Z}$*-beli* P *számtani sorozat, aminek a hossza legalább* $\frac{1}{16}\varepsilon\sqrt{N}$ *és* A *sűrűsége* P*-n*

$$\frac{|A \cap P|}{|P|} \geq (\delta + \frac{1}{8}\varepsilon).$$

2.5. A bizonyítás befejezése

Most már minden eszköz rendelkezésünkre áll ahhoz, hogy befejezzük Roth tételének a bizonyítását, de ehhez előbb még vessük össze a 2.2 és a 2.4 Állítás eredményeit. Ekkor a következőt fogalmazhatjuk meg.

2.5. Állítás. *Legyen* $A \subseteq \{0,1,\ldots,N-1\}$, $|A| = \delta N$ *és* $N > 32/\delta^2$*. Ekkor* A *vagy tartalmaz nemtriviális háromtagú* $\mathbb{Z}$*-beli számtani sorozatot, vagy létezik egy olyan* $\mathbb{Z}$*-beli* P *számtani sorozat, aminek a hossza* $|P| \geq \frac{1}{128}\delta^2\sqrt{N}$ *és*

$$|A \cap P| \geq (\delta + \frac{1}{64}\delta^2)|P|.$$

Roth tételének a bizonyítása. A fenti állítás szerint tegyük tehát fel, hogy $A \subseteq [N]$, $|A| = \delta N$, $N > 32/\delta^2$ és indirekt, A nem tartalmaz nemtriviális háromtagú $\mathbb{Z}$-beli számtani sorozatot. Megmutatjuk, hogy elég nagy N esetén ekkor ellentmondásra jutunk.

Jelölje $P_1 \subseteq \{0,1,\ldots,N-1\}$ a 2.5 Állítás szerinti számtani sorozatot, valamint legyen $N_1 := |P_1| \geq \frac{1}{128}\delta^2\sqrt{N}$. Azonosítsuk P_1-et a $P_1 \backsimeq \{0,1,\ldots,N_1-1\}$ halmazzal és A_1-et az $A_1 \backsimeq A \cap P_1$ halmazzal egyszerűen P_1 elemeinek növekvő sorrendje szerinti megfeleltetéssel. Mivel feltettük, hogy A nem tartalmaz nemtriviális háromtagú számtani sorozatot, ezért A_1 sem tartalmaz ilyet. Továbbá tudjuk, hogy $|A_1| = \delta_1 N_1$ és $\delta_1 \geq (\delta + \frac{1}{64}\delta^2)$.

Ha most megismételjük az eljárást az A_1 és P_1 halmazokkal, akkor kapunk egy P_2 számtani sorozatot és egy $A_2 \backsimeq A_1 \cap P_2$ részhalmazt, ahol A_2 sűrűsége P_2-ben $\delta_2 \geq (\delta_1 + \frac{1}{64}\delta_1^2)$ és A_2 sem tartalmaz nemtriviális háromtagú számtani sorozatot.

Folytatva az eljárást P_k számtani sorozatok, valamint δ_k sűrűségű A_k részhalmazok olyan sorozatát kapjuk, melyre

$$N_k \geq \frac{\delta_{k-1}^2}{128}\sqrt{N_{k-1}}, \quad \delta_k \geq \delta_{k-1} + \frac{\delta_{k-1}^2}{64}.$$

Mivel

$$\delta_2 \geq \delta_1 + \frac{\delta_1^2}{64} \geq \delta + \frac{\delta^2}{64} + \frac{1}{64}\left(\delta + \frac{\delta^2}{64}\right)^2 = \delta + 2\frac{\delta^2}{64} + \frac{\delta^3}{64 \cdot 32} + \left(\frac{1}{64}\right)^3 \delta^4 \geq \delta + 2\frac{\delta^2}{64},$$

ezért ebből indukcióval látható, hogy

$$\delta_k \geq \delta + k\frac{\delta^2}{64}.$$

$k = \frac{64}{\delta}$ lépés után egy olyan $A_k \subseteq \{0,1,\ldots,N_k - 1\}$ halmazhoz érkezünk, amelynek a sűrűsége $\delta_k \geq \delta + \delta = 2\delta$. Mivel

$$\delta_k \geq \delta_{k-1} + \frac{\delta_{k-1}^2}{64},$$

ezért ebbe $k' > 64/\delta$ esetén 2δ-t helyettesítve azt kapjuk, hogy

$$\delta_{k'} \geq 2\delta + k'\frac{(2\delta)^2}{64}.$$

Ezért további $64/(2\delta)$ iteráció után a sűrűség 2δ-ról 4δ-ra változik.

Általánosan tehát a sűrűség legalább $2^l\delta$-ra változik nem több, mint $\frac{64}{\delta}(1 + \frac{1}{2} + \frac{1}{4} + + \ldots + \frac{1}{2^{l-1}})$ lépés alatt. Az a-t elegendően nagynak választva azt látjuk, hogy a sűrűség 1 fölé emelkedik nem több, mint $(128/\delta)$ véges sok lépésben, ami ellentmondás, feltéve, hogy a kapott sorozatnak van legalább egy eleme.

Tehát már csak azt kell ellenőrizni, hogy ennyi lépés alatt nem hagyunk el túl sok elemet az egyes P_k sorozatok elkészítése közben. Az első lépés után $N_1 \geq \frac{1}{128}\delta^2\sqrt{N}$ és k lépés után $N_k \geq \frac{\delta_{k-1}^2}{128}\sqrt{N_{k-1}}$. Felhasználva ezt, illetve a δ_k-ra vonatkozó rekurzív összefüggést, azt látjuk, hogy k lépés után a kapott sorozat hossza legalább $\frac{1}{128^2}\delta^4 N^{1/2^k}$.

Azt kell megmutatni, hogy $k = \frac{128}{\delta}$ lépés esetén $\frac{1}{128^2}\delta^4 N^{1/2^k} \geq 1$, azaz $N^{1/2^k} \geq 2^{14}\delta^{-4}$. Ha vesszük mindkét oldal logaritmusát, akkor

$$\log N \geq (14\log 2 + 4\log\delta^{-1})2^{128/\delta}.$$

Egy egyszerű logaritmusos egyenletrendezésből könnyen látszik, hogy

$$14\log 2 + 4\log\delta^{-1} \leq 2^{4/\delta}$$

minden $\delta \in (0,1]$ esetén teljesül. Tehát ahhoz, hogy elérjük a fenti ellentmondást, elég, ha $N \geq \exp\exp(132 \cdot \delta^{-1}\log 2)$, amivel megkaptuk a tételben állított $N(\delta)$ küszöbindexet és ezzel igazoltuk Roth tételét. □

2.3. *Megjegyzés.* A bizonyításból az is látszik, hogy ha $0 < \delta \leq 1$, $|A| \geq \delta N$ és A nem tartalmaz háromtagú számtani sorozatot, akkor

$$N < \exp\exp(132 \cdot \delta^{-1} \log 2),$$

amiből

$$\delta < \frac{132 \log 2}{\log\log N}.$$

Emiatt a korábban bevezetett $a_3(N)$-re is beláttuk, hogy igaz az

$$a_3(N) \ll \frac{1}{\log\log N}.$$

3. Számtani sorozatot nem tartalmazó halmazok

Ebben a szakaszban olyan halmazkonstrukciókat tekintünk át, amelyek nem tartalmaznak számtani sorozatokat. Előbb a Roth-tételből kiindulva ismertetésre kerül Behrend konstrukciója, majd olyan halmazokat vizsgálunk, melyek négyzetszámokból állnak és nem tartalmaznak háromtagú számtani sorozatokat. Végül ez utóbbi problémához kapcsolódóan bemutatunk egy eredményt n-edik hatványokból álló, számtani sorozat nélküli halmazokra. Ez a fejezet a [15] és [16] cikkek alapján készült.

3.1. Behrend konstrukciója

Roth tételének kvantitatív változata szerint (2.3 Tétel) $a_3(N) \ll \frac{1}{\log\log N}$ egy felső korlát, így természetesen adódik az a kérdés, hogy ez a felső korlát meddig javítható. Szeretnénk alsó korlátot adni az $|A|/N$ értékére, ahol $A \subseteq [N]$ maximális méretű, ami nem tartalmaz 3-hosszú számtani sorozatot. A jelenlegi legjobb ilyen jellegű eredmény Behrendtől [14] származik.

3.1. Tétel (Behrend, 1946.)**.** *Legyen N pozitív egész szám. Ekkor létezik olyan $A \subseteq [N]$ részhalmaz, amire teljesül, hogy $\frac{|A|}{N} \geq \exp(-c\sqrt{\log N})$ és A nem tartalmaz 3-hosszú számtani sorozatot.*

Összevetve Behrend tételét a 2.1 Megjegyzéssel, azt láthatjuk, hogy az $|A|/N$ értékekre adott alsó és felső korlát között még nagy a távolság, így ennek javítása továbbra is nyitott probléma.

Behrend tételének bizonyításánál a [15]-ben leírtakat követjük.

Bizonyítás. Behrend konstrukciója azon a megfigyelésen alapul, hogy egy egyenes egy gömböt legfeljebb 2 pontban metszhet el.

Tekintsük az $x = (x_1, x_2, \ldots, x_n) \in [1, M]^n$ alakú pontokat. Nyilvánvalóan M^n darab ilyen pont létezik és minden egyes pontra az $r^2 = x_1^2 + \ldots + x_n^2$ szám egész értékű az $[n, nM^2]$ intervallumban. Így a skatulyaelv szerint létezik olyan r sugarú $S_n(M)$ gömb, ami legalább

$$|S_n(M)| \geq \left\lceil \frac{M^n}{nM^2 - n + 1} \right\rceil \geq \frac{M^n}{n(M^2 - 1)} > \frac{M^{n-2}}{n}$$

pontot tartalmaz.

Szeretnénk $S_n(M)$ pontjait egész számokhoz rendelni. Definiáljuk a $P : \mathbb{Z}^n \to \mathbb{Z}$ függvényt a következőképpen.

$$P(x) := \frac{1}{2M} \sum_{i=1}^{n} x_i (2M)^i.$$

A fenti függvény több hasznos tulajdonsággal is rendelkezik.

1. P egész értékű.
2. $1 \leq P(x) \leq (2M)^n$ minden $x \in [1, M]^n$-re.
3. P lineáris.
4. P injektív az $[1, M]^n$-en.
5. $P(z) - P(y) = P(y) - P(x) \Longrightarrow z - y = y - x$ minden $x, y, z \in [1, M]^n$-re.

Az 1. tulajdonság nyilvánvaló, hiszen a szumma minden tagja tartalmazza a $2M$ faktort.

A 2. tulajdonság azért igaz, mert az egyes összeadandók szigorúan növekvők az egyes x_i koordinátákban. Emiatt azt kapjuk, hogy

$$\begin{aligned} 1 \leq \frac{(2M)^n - 1}{(2M) - 1} = P((1,1,\ldots,1)) \leq P(x) \leq P((M, M, \ldots, M)) &= \frac{1}{2M} \sum_{i=1}^{n} M(2M)^i \\ = M \sum_{i=0}^{n-1} (2M)^i = M \frac{(2M)^n - 1}{2M - 1} &\leq M \frac{(2M)^n}{M} = (2M)^n. \end{aligned}$$

A 3. tulajdonság ugyancsak P definíciójából következik. Legyen $x, y \in \mathbb{Z}^n$ és $a, b \in \mathbb{Z}$, ekkor

$$\begin{aligned} P(ax + by) &= \frac{1}{2M} \sum_{i=1}^{n} (ax_i + by_i)(2M)^i \\ &= a \left(\frac{1}{2M} \sum_{i=1}^{n} x_i (2M)^i \right) + b \left(\frac{1}{2M} \sum_{i=1}^{n} y_i (2M)^i \right) = aP(x) + bP(y). \end{aligned}$$

A 4. és 5. tulajdonság igazolásához szükségünk lesz a következő lemmára.

3.1. Lemma. *Legyen $x \in (-2M,2M)^n$. Ekkor $P(x) = 0$ akkor és csak akkor, ha $x = 0$.*

Bizonyítás. Ha $x = 0$, akkor nyilvánvalóan $P(x) = 0$ a P definíciójából. Így tegyük fel (indirekt), hogy $P(x) = 0$, de $x \neq 0$. Ebben az esetben létezik olyan legkisebb j koordináta, amire $x_j \neq 0$. Így

$$P(x) = \frac{1}{2M} \sum_{i=1}^{n} x_i (2M)^i = \frac{1}{2M} \sum_{i=j}^{n} x_i (2M)^i = 0,$$

és ebből az következik, hogy

$$-x_j = \sum_{i=j+1}^{n} x_i (2M)^{i-j} = 2M \sum_{i=0}^{n-(j+1)} x_{i+(j+1)} (2M)^i = 2M \cdot k,$$

ahol k egész szám. De a feltevésünk szerint $0 < |x_j| < 2M$, amiből $0 < k < 1$ és így ellentmondásra jutottunk. Tehát $x = 0$, amivel a lemmát beláttuk. □

A lemma segítségével most már igazolni tudjuk a 4. és 5. tulajdonságokat is.

A 4. tulajdonsághoz tegyük fel, hogy $P(x) = P(y)$ teljesül valamilyen $x, y \in [1, M]^n$-re. Ekkor $0 = P(x) - P(y) = P(x - y)$ a linearitás miatt, és mivel $x - y \in (-M, M)^n \subseteq (-2M,2M)^n$, ebből a lemma szerint $x - y = 0$, azaz $x = y$ következik. Tehát P injektív.

Végül az 5. tulajdonsághoz tegyük fel, hogy $P(z) - P(y) = P(y) - P(x)$ teljesül valamilyen $x, y, z \in [1, M]^n$-re. Ekkor

$$P(z) - 2P(y) + P(x) = P(z - 2y + x) = 0,$$

és látható, hogy $z - 2y + x \in (-2M,2M)^n$. Így ismét a lemma miatt $z - 2y + x = 0$, azaz $z - y = y - x$, amit be kellett látni.

Legyen most $n = \lceil \sqrt{\log N} \rceil$, $M = \lfloor N^{1/n}/2 \rfloor$ és $A := P(S_n(M))$. Ekkor $A \subseteq [1, (2M)^n] \subseteq \subseteq [1, N]$, mert P egész értékeket vesz fel az $[1, (2M)^n]$-ből és $|A| = |S_n(M)|$, mert P injektív.

Végül észrevehetjük, hogy A nem tartalmaz 3-hosszú számtani sorozatot, mert az 5. tulajdonság szerint minden nem triviális A-beli 3-tagú számtani sorozat megfelel egy ugyanilyen számtani sorozatnak S-ben. Ez viszont nem lehetséges, mert ez azt feltételezné, hogy az x, y, z pontok kollineárisak, de egy egyenes az Euklideszi gömböt legfeljebb 2 pontban metszheti el.

Már csak azt kell belátni, hogy A elegendően nagy, feltéve, hogy N elég nagy.

$$\begin{aligned}\frac{|A|}{N} = \frac{|S|}{N} &\geq \frac{M^{n-2}}{nN} = \frac{\lfloor N^{1/n}/2 \rfloor^{n-2}}{nN} \geq \frac{(N^{1/n}/e)^{n-2}}{nN} = e^{2-n} \cdot N^{-2/n} \cdot \frac{1}{n} \\ &= e^{2-\lceil\sqrt{\log N}\rceil} \cdot N^{(-2/\lceil\sqrt{\log N}\rceil)} \cdot \frac{1}{\lceil\sqrt{\log N}\rceil} \\ &\geq e^{2-(\sqrt{\log N}+1)} \cdot N^{(-2/\sqrt{\log N})} \cdot \frac{1}{\sqrt{\log N}+1} \\ &\geq e^{1-\sqrt{\log N}} \cdot e^{(-2\log N/\sqrt{\log N})} \cdot e^{-1-\sqrt{\log N}} = e^{-4\sqrt{\log N}}.\end{aligned}$$

Így A valóban teljesíti a tétel feltételeit. □

3.2. Négyzetszámokból álló halmazok számtani sorozat nélkül

A fentiekben az első N egész részhalmazai között kerestünk 3-hosszú számtani sorozatokat, most pedig áttérünk egy hasonló problémára: az első N négyzetszámból álló halmaz részhalmazait fogjuk vizsgálni. Jelölje $Q(N)$ a maximális elemszámát azoknak az $A \subseteq \{1^2,2^2,\dots,N^2\}$ halmazoknak, melyek nem tartalmaznak 3-hosszú számtani sorozatot. Jelenleg is megoldatlan a következő kérdés:

3.1. Probléma. $Q(N) = o(N)$?

Bár a fenti kérdésre nem ismert a válasz, az alábbiakban megmutatjuk, hogy amennyiben $Q(N)/N$ a 0-hoz tart, az nem történhet "túl gyorsan", mert megadható egy elég nagy elemszámú A halmaz minden N-re, ami nem tartalmaz 3-hosszú számtani sorozatot. A következő tétel Gyarmati Katalintól és Ruzsa Imrétől [16] származik.

3.2. Tétel (Gyarmati, Ruzsa)**.** *Minden elég nagy N egész számra létezik olyan $A \subseteq \{1,2,\dots,N\}$ halmaz, hogy az*

$$x^2 + y^2 = 2z^2$$

egyenletnek nincs megoldása a triviális megoldásokon ($x = y = z$) kívül, ha $x, y, z \in A$, továbbá

$$|A| > cN/\sqrt{\log\log N}$$

teljesül valamilyen pozitív c konstansra.

A fenti tételt több lemma segítségével bizonyítjuk. Az

$$x^2 + y^2 = 2z^2 \tag{3.1}$$

egyenlet megoldását *primitívnek* nevezzük, ha x, y, z relatív prímek. Nyilvánvalóan minden megoldás $x = dx'$, $y = dy'$, $z = dz'$ alakban írható, ahol $d = \text{lnko}(x, y, z)$ és x', y', z' primitív megoldások. Az (x', y', z') primitív megoldást az (x, y, z) megoldásból származtatott megoldásnak nevezzük.

3.2. Lemma. *Ha x, y, z primitív megoldása a (3.1)-nek, akkor x és y kizárólag $p \equiv \pm$ $\pm 1 \pmod 8$, míg z kizárólag $p \equiv 1 \pmod 4$ alakú prímek szorzatából áll.*

Bizonyítás. Először belátjuk, hogy amennyiben x, y, z primitív megoldás, akkor a $p = 2$ egyiknek sem lehet osztója. Induljunk ki először a $2 \mid x$ esetből. Mivel $x^2 = 2z^2 - y^2$ és $2z^2$ páros, ebből következik a $2 \mid y$ oszthatóság is. De ha $2 \mid x$ és $2 \mid y$, akkor $4 \mid x^2$ és $4 \mid y^2$, így speciálisan $4 \mid 2z^2$ is igaz, amiből $2 \mid z^2$, vagyis $2 \mid z$ következik. Ez viszont ellentmond annak, hogy az x, y, z primitív megoldás.

Szimmetria okok miatt ugyanez a gondolatmenet érvényes akkor is, ha a $2 \mid y$ osztha-tóságból indulunk ki.

Tegyük fel most, hogy $2 \mid z$. Mivel $2z^2 = x^2 + y^2$ és x, y, z primitív megoldások, ezért x és y nem lehetnek páros számok, továbbá a paritásuknak meg kell egyezniük, így mindkettő páratlan. Tehát $2z^2 = (2k+1)^2 + (2l+1)^2$ teljesül valamilyen $k, l \in \mathbb{Z}$ számokra. Ekkor viszont a zárójeleket felbontva és kettővel osztva a $z^2 = 2k^2 + 2k + 2l^2 + + 2l + 1$ egyenletet kapjuk, ami ellentmondás, hiszen z páros a feltétel szerint, a jobb oldalon viszont páratlan szám szerepel. Beláttuk tehát, hogy $p > 2$ páratlan prím.

Legyen most $p > 2$ prím és tegyük fel először, hogy $p \mid x$. Ekkor a (3.1)-et átírva a $2z^2 \equiv \equiv y^2 \pmod{p}$ kongruenciát kapjuk. Ekkor azt állítjuk, hogy $p \nmid z$. Valóban, ha p osztaná z-t, valamint a kiindulási feltétel szerint x-et, akkor osztaná y-t is, ami ellentmond annak, hogy x, y, z primitív megoldás. Mivel a p nem osztja a z-t, ezért létezik z^{-1} multiplikatív inverze mod p. Ekkor

$$2z^2 \equiv y^2 \pmod{p},$$

amit jobbról $(z^2)^{-1}$-zel szorozva a

$$2 \equiv (yz^{-1})^2 \pmod{p}$$

kongruenciát kapjuk. Ez pontosan akkor oldható meg, ha a 2 kvadratikus maradék mod p, azaz

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{ha} \quad p \equiv \pm 1 \pmod{8}, \\ -1 & \text{ha} \quad p \equiv \pm 3 \pmod{8}. \end{cases}$$

Tehát x-re és szimmetria okok miatt y-ra beláttuk az állítást.

A fenti gondolatmenet szerint tudunk elindulni akkor is, ha feltesszük, hogy p osztója z-nek. Ekkor a $0 \equiv x^2 + y^2 \pmod{p}$ egyenletet kapjuk. Itt ha $p \mid x$ vagy $p \mid y$, akkor p osztója mindhárom számnak, ami ellentmond a primitív megoldásnak. Emiatt ismét a fentiek szerint, létezik x^{-1} (y-ra ugyanígy). Most a

$$-x^2 \equiv y^2 \pmod{p}$$

egyenletet szorozva $(x^2)^{-1}$-zel azt kapjuk, hogy

$$-1 \equiv (yx^{-1})^2 \pmod{p}.$$

Ez pontosan akkor oldható meg, ha -1 kvadratikus maradék mod p, azaz

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{ha} \quad p \equiv 1 \pmod 4, \\ -1 & \text{ha} \quad p \equiv -1 \pmod 4. \end{cases}$$

Ezzel beláttuk a lemmát. □

Vezessük be a következő jelölést. Ha j olyan egész szám, amire $1 \leq j \leq 7$, akkor legyen $\nu_j(n)$ az n azon prímosztóinak száma multiplicitásokkal számolva, melyekre $p \equiv j \bmod 8$. A $\nu_j(n)$ függvények teljesen additív számelméleti függvények, azaz minden $a, b \in \mathbb{Z}$ esetén $\nu_j(ab) = \nu_j(a) + \nu_j(b)$.

3.3. Lemma. *Legyenek az x, y, z számok a (3.1) egyenlet megoldásai. Legyenek továbbá $x = dx'$, $y = dy'$, $z = dz'$, ahol $d = \text{lnko}(x, y, z)$ és így az (x', y', z') a származtatott megoldások. Ekkor*

$$\begin{aligned} \nu_5(x) - \nu_5(z) &= -\nu_5(z') \\ \nu_7(x) - \nu_7(z) &= \nu_7(x'). \end{aligned} \tag{3.2}$$

Bizonyítás. Valóban, az előző lemma szerint $\nu_5(x) = \nu_5(d) + \nu_5(x') = \nu_5(d)$, valamint $\nu_5(z) = \nu_5(d) + \nu_5(z')$. Kivonással megkapjuk (3.2) első egyenlőségét. Hasonlóan $\nu_7(x) = = \nu_7(d) + \nu_7(x')$ és $\nu_7(z) = \nu_7(d) + \nu_7(z') = \nu_7(d)$. Ismét kivonással megkapjuk (3.2) második egyenlőségét. □

Most bevezetünk egy újabb teljesen additív függvényt a következő jelöléssel:

$$\rho(n) = \nu_5(n) - \nu_7(n).$$

3.4. Lemma. *Legyen A az egész számok olyan részhalmaza, melyre $\rho(n) = k$ teljesül minden $n \in A$ esetén. Legyen $(x, y, z) \in A^3$ a (3.1) egyenlet A-beli megoldása, amiből a származtatott megoldás (x', y', z'). Ekkor az x', y', z' számok kizárólag $p \equiv 1 \pmod 8$ alakú prímek szorzatából állnak.*

Bizonyítás. (3.2) második egyenletéből kivonva az első egyenletet azt kapjuk, hogy

$$\rho(z) - \rho(x) = \nu_7(x') + \nu_5(z'),$$

x és y szimmetriája miatt pedig azt kapjuk, hogy

$$\rho(z) - \rho(y) = \nu_7(y') + \nu_5(z').$$

Mivel a feltevés szerint $\rho(n) = k$ minden $n \in A$-ra, ezért mindkét egyenlet bal oldala 0, a jobb oldalon pedig nemnegatív egész számok összege szerepel, ami csak úgy lehet igaz, ha a jobb oldalon is minden tag eltűnik. A 3.2 Lemma miatt x' és y' csak ± 1 lehet (mod 8), de most azt kaptuk, hogy $\nu_7(x') = \nu_7(y') = 0$, tehát valóban csak az $x', y' \equiv 1 \pmod 8$ eset marad. Hasonlóan a 3.2 Lemma miatt z' csak 1 és 5 lehet (mod 8), de $\nu_5(z') = 0$, így csak a $z' \equiv 1 \pmod 8$ lehetőség marad. □

3.5. Lemma. *Legyen (x, y, z) primitív megoldása (3.1)-nek úgy, hogy $x > z > y$. Ekkor léteznek olyan pozitív egész u és v számok, melyek relatív prímek, ellentétes paritásúak, valamint*

$$\begin{aligned} x &= u^2 - v^2 + 2uv \\ y &= |u^2 - v^2 - 2uv| \\ z &= u^2 + v^2. \end{aligned}$$

Bizonyítás. A 3.2 Lemma bizonyításában láttuk, hogy x, y és z mindegyike páratlan. Ha átírjuk a (3.1) egyenletet a következő alakba

$$\left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 = z^2,$$

akkor alkalmazhatjuk a Pitagoraszi számhármasok megoldására vonatkozó tételt. □

Legyen most $W \subseteq \mathbb{N}^2$ olyan (u, v) számpárok halmaza, amelyek generálják a 3.5 Lemmában szereplő (x, y, z) megoldásokat, feltéve, hogy x, y és z mindegyike kizárólag $p \equiv 1 \pmod 8$ alakú prímek szorzata.

3.6. Lemma.

$$|W \cap [1, N]^2| = O(N^2 (\log N)^{-3/2}).$$

Bizonyítás. Legyen u fix és

$$W_u := \{v : 1 \leq v \leq N, (u, v) \in W\}.$$

Először $|W_u|$ értékét becsüljük.

Legyen p páratlan prím, amire $p \not\equiv 1{,}3 \pmod 8$. Megmutatjuk, hogy bizonyos maradékosztályok modulo p nincsenek benne W_u-ban.

Ha $p \mid u$, akkor a 0 maradékosztály nincs benne W_u-ban, mivel u és v relatív prímek a 3.5 Lemma szerint.

Nézzük azt az esetet, amikor $p \nmid u$, $p \equiv 5 \pmod 8$. Jelöljük i-vel az

$$i^2 \equiv -1 \pmod p$$

kongruencia megoldását. Az a feltevés, hogy $p \nmid z = u^2 + v^2$ átírható a

$$v \not\equiv \pm iu \pmod p$$

alakba, ami két maradékosztály kizárását jelenti.

Tegyük most fel, hogy $p \nmid u$, $p \equiv 7 \pmod 8$. Legyen i az

$$i^2 \equiv 2 \pmod p$$

megoldása. Az a feltevés, hogy

$$p \nmid x = u^2 - v^2 + 2uv = 2u^2 - (u - v)^2$$

azt jelenti, hogy

$$v \not\equiv (\pm i + 1)u \pmod p,$$

ami szintén két maradékosztályt zár ki.

Végül, ha

$$p \nmid \pm y = u^2 - v^2 - 2uv = 2u^2 - (u + v)^2,$$

akkor

$$v \not\equiv (\pm i - 1)u \pmod p,$$

ami ismét két maradékosztályt zár ki a lehetőségek közül. Nyilvánvalóan ez utóbbi négy maradékosztály különböző, így összesen $1 + 2 + 4 = 7$ maradékosztályt zártunk ki.

Felhasználva egy szita becslést, amely a Brun-szitából következik (ez a [17] könyvben olvasható, mint 2.2 Tétel), azt kapjuk, hogy

$$|W_u| < c_1 N \prod_{p|u} \left(1-\frac{1}{p}\right) \prod_{p\nmid u, p\equiv 5 \pmod 8, p<\sqrt{N}} \left(1-\frac{2}{p}\right) \prod_{p\nmid u, p\equiv 7 \pmod 8, p<\sqrt{N}} \left(1-\frac{4}{p}\right)$$
$$\leq c_1 N f(u) \prod_{p\equiv 5 \pmod 8, p<\sqrt{N}} \left(1-\frac{2}{p}\right) \prod_{p\equiv 7 \pmod 8, p<\sqrt{N}} \left(1-\frac{4}{p}\right),$$

ahol

$$f(u) = \prod_{p|u, p\equiv 5 \pmod 8} \frac{p-1}{p-2} \prod_{p|u, p\equiv 7 \pmod 8} \frac{p-1}{p-4}.$$

Ha most felhasználjuk Dirichlet számtani sorozatokra vonatkozó tételét, akkor

$$\sum_{p\leq x, p\equiv j \pmod 8} \frac{1}{p} = \frac{1}{4}\log\log x + O(1)$$

és itt $j=5$ és $j=7$ esetén azt kapjuk, hogy

$$|W_u| < c_2 f(u) N (\log N)^{-3/2}.$$

Az $f(u)$ függvény nem korlátos, de a számtani közepe igen, így

$$\sum_{u\leq N} f(u) < c_3 N.$$

Ez utóbbi egyenlőtlenség multiplikatív függvények összegére való becslésből következik, ami a [18] könyv 2.11 Következményében olvasható. Végül a fenti eredményeket összevetve kész a lemma bizonyítása. □

3.7. Lemma.

$$\sum_{(u,v)\in W} \frac{1}{u^2+v^2} < \infty.$$

Bizonyítás. Ez az előző lemmából következik parciális összegzéssel. □

3.8. Lemma (Heilbronn–Rohrbach–egyenlőtlenség, [19] és [20])**.** *Legyen V pozitív egész számok halmaza és legyen B azon pozitív egészek halmaza, melyek nem oszthatók V egyetlen elemével sem. Ekkor B-nek van aszimptotikus sűrűsége és ez legalább*

$$\prod_{v\in V} \left(1-\frac{1}{v}\right).$$

Most már minden eredmény ismertetésre került, amire szükségünk van, így rátérhetünk a tétel bizonyítására.

A 3.2 Tétel bizonyítása. Legyen B azon egész számok halmaza, melyek nem oszthatók egyetlen $u^2 + v^2$ alakú számmal sem, ahol $(u, v) \in W$. Az előző lemma szerint ekkor B-nek pozitív aszimptotikus sűrűsége van, jelöljük ezt c_3-mal. Legyen most

$$A_k = \{n \in B : n \leq N, \rho(n) = k\}$$

egy megfelelő k számmal. Ekkor két dolgot állítunk.

1. A (3.1) egyenletnek nem létezik nem triviális megoldása semelyik A_k-ban.

2. Egy megfelelő N-től függ k értékre

$$|A_k| > cN/\sqrt{\log\log N}.$$

Ebből a két tulajdonságból nyilvánvalóan következik a tétel.

Az első tulajdonság igazolásához tegyük fel indirekt, hogy létezik x, y, z megoldás primitív x', y', z' származtatott megoldással. Ekkor a 3.4 Lemma miatt x', y' és z' kizárólag $\equiv 1 \pmod 8$ alakú prímek szorzata. Így ezeket valamilyen $(u, v) \in W$ generálja és ekkor

$$u^2 + v^2 = z' \mid z \in A_k \subset B,$$

ami ellentmond B definíciójának.

A második állítás igazolásához a Turán–Kubilius–egyenlőtlenséget [21] használjuk fel, ami például a [18] könyv 3.2 alfejezetében is olvasható, mint 3.1 Tétel. Eszerint

$$\sum_{n=1}^{N}(\rho(n) - m)^2 < c_4 N \sum_{p^k \leq N} p^{-k}\rho(p^k)^2 < c_5 N \log\log N,$$

ahol

$$m = \sum_{p \leq N} \rho(p)/p.$$

Nevezetesen, egy megfelelően választott c_6 konstanssal kevesebb, mint $(c_3/2)N$ egész van N-ig úgy, hogy

$$|\rho(n) - m| \geq c_6\sqrt{\log\log N}.$$

Hagyjuk el ezeket a számokat B-ből. Ekkor több, mint $(c_3/2)N$ szám van N-ig a megmaradók közül B-ben és a legfeljebb $2c_6\sqrt{\log\log N}$ darab lehetséges $\rho(n)$ érték közül legalább egy $cN/\sqrt{\log\log N}$-szer fog szerepelni. □

3.3. n-edik hatványokból álló halmazok számtani sorozat nélkül

Az előző fejezetben az első N négyzetszámból álló halmaz olyan részhalmazait vizsgáltunk, melyek nem tartalmaznak háromtagú számtani sorozatokat. A 3.2 Tétel szerint minden elég nagy N egész számra létezik olyan $A \subseteq \{1,2,\ldots,N\}$ részhalmaz, hogy az

$$x^2 + y^2 = 2z^2$$

egyenletnek nincsen megoldása a triviális megoldásokon ($x = y = z$) kívül, ha $x, y, z \in A$, továbbá

$$|A| > cN/\sqrt{\log\log N}$$

teljesül valamilyen pozitív c konstansra.

Egy természetesen adódó kérdés, hogy mi történik akkor, ha mondjuk köbszámokból vagy akár általánosan, n-edik hatványokból álló halmazokat vizsgálunk, ahol $n > 2$ egész szám. Szeretnénk minél nagyobb olyan $A \subseteq \{1,2,\ldots,N\}$ részhalmazt adni, amelyre az

$$x^n + y^n = 2z^n$$

egyenletnek nem létezik megoldása a triviális megoldásokon ($x = y = z$) kívül, ha $x, y, z \in$ $\in A$ és $n > 2$, $n \in \mathbb{N}$.

Erre a problémára pedig egy nagyon pozitív eredményt tudunk mutatni. Ha az A részhalmaz a fenti alakú, akkor A tetszőlegesen nagy lehet, mégsem lesz soha megoldása az előbbi egyenletnek. Igaz ugyanis a következő tétel, amit Darmon és Merel bizonyítottak be [22]-ben.

3.3. Tétel (Darmon, Merel)**.** *Legyen az n kitevő egy tetszőleges pozitív egész szám. Ekkor az $x^n + y^n = 2z^n$ egyenletnek nem létezik nem triviális primitív megoldása, ha $n \geq 3$.*

A tétel bizonyítása a Nagy Fermat-tétel bizonyításához használt eszközökön alapul (Galois-elmélet, algebrai geometria és elliptikus görbék), ezt itt nem részletezzük.

4. Kitekintés: Szemerédi tétele és a Green-Tao tétel

Ahogy azt a dolgozat elején említettük, az Erdős-Turán sejtés általános $k \geq 4$ esetén igen nehéz problémának bizonyult. A megoldáshoz végül Szemerédi Endre jutott el, aki előbb 1969-ben $k = 4$-re [23], majd 1975-ben minden $k \geq 4$-re megoldotta a feladatot [24].

4.1. Tétel (Szemerédi)**.** *Legyen A a természetes számok tetszőleges részhalmaza, melyre*

$$\limsup_{N\to\infty} \frac{|A \cap \{1,2,\ldots,N\}|}{N} > 0.$$

Ekkor A tartalmaz k-hosszú számtani sorozatot minden $k \geq 3$-ra.

Szemerédi bizonyítása nem a Roth-tételnél bemutatott analitikus gondolatmenetet követi, hanem kombinatorikai megfontolásokat. A bizonyítás kulcsa az úgynevezett Szemerédi-féle regularitási lemma, ami egy gráfelméleti eredmény. Ez durván megfogalmazva azt mondja ki, hogy minden n csúccsal és cn^2 éllel ($0 < c \leq 1$ egy abszolút konstans) rendelkező gráfot kevés számú részgráfra tudunk particionálni, melyek "véletlen tulajdonságokkal" rendelkeznek. Az alábbiakban a [2]-beli tárgyalást követjük.

Legyen $G = (V, E)$ egy véges nem irányított gráf, melyben nincsenek hurok- és többszörös élek, valamint legyen $A, B \subseteq V$ két nem üres diszjunkt részhalmaza V-nek. Jelöljük továbbá $e(A, B)$-vel azoknak a G-beli (a, b) éleknek a számát, melyekre $a \in A$ és $b \in B$. Az (A, B) pár élsűrűségének nevezzük a

$$d(A, B) := \frac{e(A, B)}{|A||B|}$$

számot.

4.1. Definíció. Az (A, B) párt ε-regulárisnak hívjuk, ha

$$|d(A', B') - d(A, B)| < \varepsilon$$

teljesül minden $A' \subseteq A$ és $B' \subseteq B$ részhalmazra, amire $|A'| > \varepsilon|A|$ és $|B'| > \varepsilon|B|$.

Tehát egy (A, B) párt ε-regulárisnak hívunk, ha a pár mindkét tagjából egy-egy nagy részhalmazt véve a részhalmazok élsűrűsége nincs túl távol a pár élsűrűségétől. Példa ε-reguláris párra egy véletlen páros gráf, ahol p annak a valószínűsége, hogy $a \in A$, $b \in B$ esetén $(a, b) \in E(G)$. Ekkor nyilvánvalóan $p \approx d(A, B)$ és az (A, B) pár 1 valószínűséggel ε-reguláris minden $\varepsilon > 0$-ra.

4.2. Definíció. Egy G gráf V csúcshalmazának a $C_0, C_1, \ldots, C_k$ halmazokra való particionálását ε-regulárisnak nevezzük, ha

1. $|C_0| < \varepsilon |V|$,
2. $|C_1| = |C_2| = \ldots = |C_k|$,
3. $\varepsilon\binom{k}{2}$ pár kivételével minden (C_i, C_j) pár ε-reguláris, ha $1 \leq i < j \leq k$.

A fenti jelölésekkel a Szemerédi-féle regularitási lemma a következőképpen szól.

4.1. Lemma (Szemerédi-féle regularitási lemma)**.** *Legyen $0 < \varepsilon \leq 1$ és legyen l pozitív egész. Ekkor léteznek olyan $n_0(\varepsilon, l)$ és $k_0(\varepsilon, l)$ számok, hogy minden G gráfra, aminek legalább $n_0(\varepsilon, l)$ csúcsa van, létezik G csúcsainak k osztályra való ε-reguláris particionálása úgy, hogy $l \leq k \leq k_0(\varepsilon, l)$.*

A Szemerédi-tétel és a regularitási lemma bizonyítását a dolgozatban nem ismertetjük, ehhez útmutatás találhatunk az eredeti [24], illetve az összefoglaló jellegű [25] cikkben.

Szemerédi tételére később alternatív bizonyítások is születtek, melyek közül a legjelentősebbek Furstenberg és Gowers eredményei. Furstenberg ergodelméleti eszközöket alkalmazott, míg Gowers a Roth-tétel bizonyításához hasonlóan a Fourier-analízis eszköztárát vette igénybe.

Gowers bizonyítása [26] azért jelentős, mert a korábbi bizonyítások egyáltalán nem, vagy csak nagyon gyenge felső becslést adtak az $a_k(N)$ értékére.

4.2. Tétel (Gowers)**.** *Minden $N \geq 3$-ra és $k \geq 4$-re igaz az*

$$a_k(N) \ll \frac{1}{(\log\log N)^{c_k}},$$

ahol $c_k = 2^{-2^{k+9}}$ konstans.

Ugyanakkor Gowers eredménye fontos lépést tett Erdős és Turán egy másik híres sejtésének igazolása felé, amely a következőképpen szól.

4.1. Sejtés (Erdős, Turán)**.** *Legyen $A = \{n_1 < n_2 < \ldots\}$ pozitív egész számokat tartalmazó halmaz, melyre teljesül, hogy*

$$\sum_{i=1}^{\infty} \frac{1}{n_i} = \infty.$$

Ekkor A tartalmaz tetszőlegesen hosszú számtani sorozatot.

Meg lehet mutatni, hogy a 4.1 Sejtés ekvivalens azzal a feltétellel, hogy $\sum_{l=1}^{\infty} a_k(4^l)$ konvergens minden $k \geq 3$-ra (lásd [2]). Így ahhoz, hogy belássuk a 4.1 Sejtést, elég lenne igazolni, hogy $a_k(N) \ll 1/(\log N)^{1+\varepsilon}$ minden $k \geq 3$ és tetszőleges $\varepsilon > 0$ esetén.

A legjelentősebb eredményt eddig Ben Green és Terence Tao [27] érték el az $A = \mathbb{P}$ prímek halmazára, akik igazolták a következő nagyon szép tételt.

4.3. Tétel (Green, Tao)**.** *Bármely $k \geq 3$ egész esetén létezik k-hosszú prímszámokból álló számtani sorozat.*

Zárásként megjegyezzük, hogy a 4.1 Sejtés a dolgozat írásakor egy még megoldatlan probléma.

Felhasznált irodalom

Hivatkozások

[1] B. L. van der Waerden, *Beweis einer Baudetschen Vermutung.*
Nieuw. Arch. Wisk. (in German). 15 (1927): 212–216.

[2] I. D. Shkredov, *Szemerédi's theorem and problems on arithmetic progressions.*
Russian Mathematical Surveys. 61 (6): 1101-1166.

[3] K. F. Roth, *On certain sets of integers.*
Journal of the London Mathematical Society. 28 (1): 104–109.

[4] N. Lyall, *Roth's theorem, The Fourier analytic approach.*
Lecture Notes http://math.uga.edu/~lyall/REU/Roth.pdf

[5] Hegyvári Norbert, *Additív Kombinatorika.*
ISBN: 978-963-489-088-1

[6] A. Lott, *Roth's theorem on arithmetic progressions.*
BA honor's thesis, University of Rochester, 2017.

[7] E. Szemerédi, *Integer sets containing no arithmetic progressions.*
Acta Math. Hungar. 56 (1–2): 155–158.

[8] R. Heath-Brown, *Integer sets containing no arithmetic progressions.*
Journal of the London Mathematical Society. 35 (3): 385–394.

[9] J. Bourgain, *On triples in arithmetic progression.*
Geom. Funct. Anal. 9 (5): 968–984.

[10] J. Bourgain, *Roth's theorem on progressions revisited.*
Journal d'Analyse Mathématique. 104 (1): 155–192.

[11] T. Sanders, *On Roth's theorem on progressions.*
Annals of Mathematics. 174 (1): 619–636.

[12] T. Sanders, *On certain other sets of integers.*
Annals of Mathematics. 185 (1): 53–82.

[13] T. F. Bloom, *A quantitative improvement for Roth's theorem on arithmetic progressions.*
Journal of the London Mathematical Society. Second Series. 93 (3): 643–663.

[14] F. A. Behrend, *On sets of integers which contain no three terms in arithmetical progression.*
Proceedings of the National Academy of Sciences, 32 (12): 331–332.

[15] B. Gillespie, *Behrend's Construction.*
http://www.epsilonsmall.com/resources/behrends-construction/behrend.pdf

[16] K. Gyarmati, I. Z. Ruzsa, *A set of squares without arithmetic progression.*
Acta Arith. 155 (2012): 109-115.

[17] H. Halberstam, H.-E. Richert, *Sieve Methods (2nd ed.).*
Dover Publications, 2011, ISBN: 0-486-47939-0.

[18] G. Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory: Third Edition.*
Graduate Studies in Mathematics Volume: 163, 2015, ISBN: 978-0-8218-9854-3.

[19] H. A. Heilbronn, *On an inequality in the elementary theory of numbers.*
Proc. Cambridge Philos. Soc. 33 (1937), 207-209.

[20] H. Rohrbach, *Beweis einer zahlentheoretischen Ungleichung.*
J. Reine Angew. Math. 177 (1937), 153-156.

[21] J. Kubilius, *Probabilistic methods in the theory of numbers.*
Amer. Math. Soc. Translations of Math. Monographs 11 (1964).

[22] H. Darmon, L. Merel, *Winding quotients and some variants of Fermat's Last Theorem.*
Journal für die reine und angewandte Mathematik 490 (1997) 81-100.

[23] E. Szemerédi, *On sets of integers containing no four elements in arithmetic progression.*
Acta Math. Acad. Sci. Hung. 20: 89–104.

[24] E. Szemerédi, *On sets of integers containing no k elements in arithmetic progression.*
Acta Arithmetica. 27: 199–245.

[25] W. T. Gowers, *The work of Endre Szemerédi.*
https://gowers.files.wordpress.com/2013/03/szemeredi.pdf

[26] W. T. Gowers, *A new proof of Szemerédi's theorem.*
Geom. funct. anal. Vol. 11:3 (2001), 465-588.

[27] B. Green, T. Tao, *The primes contain arbitrarily long arithmetic progressions.*
Annals of Mathematics. 167 (2): 481–547.

[28] A. Sárközy, C.L. Stewart, *Irregularities of sequences relative to long arithmetic progressions.*
Analytic Number Theory Essays in Honour of Klaus Roth, edited by Chen, Gowers, Halbertstam, Schmidt and Vaughan, Cambridge University Press (2009), 389-401.

[29] A. Sárközy, C.L. Stewart, *On irregularities of distribution in shifts and dilations of integer sequences I.*
Math. Annalen 276 (1987), 353-364.

[30] A. Sárközy, C.L. Stewart, *On irregularities of distribution in shifts and dilations of integer sequences, II.*
Number Theory in Progress, edited by K. Györy, H. Iwaniec and J. Urbanowicz, Walter de Gruyter, Berlin (1999), 633–638.