-

A Kombinatorikus számelmélet néhány problémájáról

MTA doktori értekezés tézisei

Hegyvári Norbert

2017

0.1. Bevezetés

Az "Additív kombinatorika" találó elnevezést néhány éve Terence Tao honosította meg, és ahogy B. Green írja egy recenziójában: *"Well one might say that additive combinatorics is a marriage of number theory, harmonic analysis, combinatorics, and ideas from ergodic theory, which aims to understand very simple systems: the operations of addition and multiplication and how they interact."*.

Fermat és Lagrange kora óta, tehát az 1600 évek közepe óta a számelmélet egyik centrális kérdése, hogy egy adott struktura bizonyos részhalmazának elemeiből képzett összegek mennyire és hogyan töltik ki a strukturát. Ez a természetes kérdés az additív analogonja annak, hogy a prímek multiplikatív módon felépítik a természetes számok halmazát.

A nevezetes eredmények közül említsünk meg kettőt: a Fermat által sejtett és Lagrange négy-négyzetszám tételt, vagy a Cauchy által vizsgált problémát; a kvadratikus maradékok (a 0−val kiegészítve) másodrendű bázist alkotnak, s mely kérdésnek az általánosítása vezetett a jól ismert Cauchy-Davenport tételhez.

A kombinatorikus számelmélet klasszikus kérdése, hogy bizonyos halmazokban milyen szabályos struktura *különösképpen* számtani sorozat van. Ezek közül talán a leghíresebb a Szemerédi tétel, amelyik pozitív felső sűrűségű sorozatokban igazolja tetszőleges hosszú számtani sorozatok létezését.

Ezen kívül fontos kérdés összeghalmazokban keresni hosszú számtani sorozatokat. Itt a probléma kezelhetősége erősen eltér, attól függően, hogy hány tagú összegeket képzünk.

Az **Elért erdemények** paragrafusban felsoroltak követik az értekezésem fejezeteinek a sorrendjét, kiemelve az általam fontosnak vélt tételeket. Az Irodalomjegyzékben külön feltüntettem, hogy melyek azok a cikkek, amelyekre az értekezésem alapját képezi.

0.2. Az értekezésben foglalt eredmények előzményei

1. Hilbert kockákról

A manapság ismert legrégebbi Ramsey-típusú eredményt D. Hilbert fogalmazta meg 1892−ben egész együtthatós racionális törtfüggvények irredu-

cibilitását vizsgálva (közel 25 évvel korábban, mint Schur nevezetes "$x + y = z$" tételét). Egy $m-$dimenziós affin kocka – vagy Hilbert tiszteletére $m-$dimeziós Hilbert kocka – alatt a

$$H = H(a_0, a_1, a_2, \ldots, a_m) = \{a_0 + \sum_{i=1}^{m} \varepsilon_i a_i : \varepsilon_i \in \{0, 1\}\}$$

halmazt értjük. Az a_i elemeket a kocka éleinek szokás nevezni, H elemszámát a kocka méretének nevezzük. Nyilván $|H| \leq 2^m$.

Hilbert nevezetes tétele $[HI]$ így hangzik:

Tétel*(Hilbert, 1892) Legyenek m és r pozitív egészek. Ekkor a természetes számok bármely $r-$színezése esetén létezik olyan $H(a_0, a_1, a_2, \ldots, a_m)$ affin kocka, melynek elemei azonos színűek.*

1969−ben Szemerédi e fenti tétel effektív-sűrűségi változatát bizonyította be.

Tétel*(Szemerédi) Legyen $A \subseteq \mathbb{N}$, melyre $\eta := \underline{d}(A) > 0$. Ekkor van olyan $\beta > 0$ valós szám, hogy bármely $n > n_0(\eta)$ esetén $A \cap [1, n]$ tartalmaz egy $\beta \log\log n$ dimenziójú Hilbert kockát.*

(lásd pl. [GRS])

Jelölje $\mathcal{Q}$ a négyzetszámok sorozatát, $\mathcal{P}$ a prímek sorozatát. T.C. Brown, Erdős és A. Freedman [BEF90] vetette fel azt a kérdést, hogy vajon a prímszámok illetve a négyzetszámok halmaza tartalmaz-e tetszőleges dimenziójú Hilbert kockát? E kérdés nyitva maradt, számos számítógép által talált példa ismert csak.

Meg kell említeni Bergelson szép tételeit ([Be85], [Be97], amelyben pozitív felső sűrűségű A sorozatok $D(A)$ különbség sorozatának erős struktúra tulajdonságát biztosítja; $D(A)$ tartalmaz $B + B + \cdots + B$ ($k-$tagú) összeghalmazt, ahol B végtelen halmaz, ill. $D(A)$ tartalmaz végtelen általánosított részhalmaz- összeg (szorzat) halmazokat. Bergelson bizonyításai ergodikusak; az ú.n. "Fürstenberg átviteli elvet" használja.

2. Ramsey típusú additív kérdések.

2.1 A következő probléma ugyancsak kapsolódik mind a Ramsey-típusú, mind a Hilbert kockák problémaköréhez. 1968-ban Raimi [Ra68] topologikus eszközökkel igazolta a következő tételt:

Tétel*(Raimi) Létezik egy $E \subseteq \mathbb{N}$ halmaz úgy, hogy bármely $r \in \mathbb{N}$ egészre a természetes számok bármely r színezése esetén létezik egy színosztály, jelöljük D_i-vel ($i \in \{1, 2, \ldots, r\}$) és egy $k \in \mathbb{N}$ melyre $(D_i+k) \cap E$ és a $(D_i+k) \setminus E$ halmazok végtelen számosságúak.*

E tételre szép összefoglaló munkájában [Hin79] N. Hindman adott egy új, kombinatorikus bizonyítást.

2.2 Sárközy vizsgálta a következő kérdést: ha vesszük a prímszámoknak $1/k$ relatív sűrűségű részeit, igaz-e, hogy ezek közül bármelyik aszimptotikus bázis lesz, és ha ez igaz, mi a rendeknek $H(k)$-val jelölt szuprémuma (amennyiben ez is létezik)? Megmutatta, hogy $H(k) \ll k^4$, és $H(k) \gg k \log\log k$. Ezt később Ramaré és Ruzsa ([RR01]) javította $H(k) \asymp k \log\log k$-ra. Ők a sorozatok egy általánosabb osztályára bizonyítottak tételeket, (de pl. a négyzetszámokra nem).

E kérdésekkel kapcsolatosan Sárközy vetette fel a következő Ramsey-típusú problémát: "Igazolható, hogy van olyan $t = t(k)$, hogy ha a négyzetszámokat k-színnel megszínezzük, minden elég nagy természetes szám előáll legfeljebb t egyszínű négyzetszám összegeként. Határozzuk meg ezen $t(k)$ minimális értékét!" Hasonló problémát tűzött ki a prímszámok sorozatára is.

3. Megszorított összegekről

3.1 1962-ben Erdős vezette be egészek sorozatának teljességét. Egy pozitív egészekből álló végtelen sorozatot *teljesnek* nevezett, ha minden elég nagy természetes szám előáll különböző $A-$beli elemek összegeként. $A-$t *részteljesnek* nevezte, ha egy végtelen számtani sorozat elemei állnak elő különböző $A-$beli elemek összegeként. Ez a Waring problémától abban különbözik, hogy egy elemet csak egyszer használhatunk, ám az összeadandók számára nem teszünk feltevést.

Erdős sejtette, hogy az $a_{n+1}/a_n \to 1$ (amint $n \to \infty$) elégséges egy sorozat részteljeségéhez. Azonban 1960-ban J. W. S. Cassels mutatott olyan sorozatot, melyre $a_{n+1} - a_n = o(a_n^{1/2+\varepsilon})$ és nem részteljes.

Erdős sűrűségi feltételt is sejtett; ha $A \subseteq \mathbb{N}$ egy olyan végtelen halmaz melyre egy alkalmas $c > 0$ konstanssal $A(n) > c\sqrt{n}$ teljesül, akkor az A részteljes. Belátható, hogy a $c\sqrt{n}$ az elméleti határ. [EP62]-ben Erdős egy gyengébb állítást igazolt:

Tétel*(Erdős62):*
Ha $A \subseteq \mathbb{N}$, egy végtelen halmaz, akkor van olyan $c > 0$, hogy ha $A(n) > cn^{(\sqrt{5}-1)/2}$, akkor az A részteljes.
További javítást Folkman ért el.

3.2 Természetesen létezik nagyon ritka (exponenciális növekedésű) teljes sorozat; az $Y_0 = \{p^n : n = 0, 1, \dots\}$, ahol $p \in \mathbb{N}_{>1}$ akkor és csak akkor teljes, ha $p = 2$. Egy kissé sűrűbb sorozat az $Y = \{p^n q^m : n, m = 0, 1, \dots\}$, ahol $1 < p, q \in \mathbb{N}$. Erdős plauzibilis sejtése az volt, hogy Y akkor és csak akkor teljes, ha $(p, q) = 1$.
1959-ben Birch [B59] igazolta Erdős e sejtését. Néhány évvel később J.W. Cassels [Ca60] bizonyított egy általánosabb tételt, amiből következett Birch tétele.

Tétel*(Cassels,1960):*
Legyen $A \subseteq \mathbb{N}$, és tegyük fel, hogy

$$\lim_{n\to\infty} \frac{A(2n) - A(n)}{\log\log n} = \infty.$$

Továbbá tegyük fel, hogy bármely θ valósra, $(0 < \theta < 1)$ $\sum_{i=1}^{\infty} \|a_i\theta\| = \infty$.
Ekkor A teljes.

Mindazonáltal – ahogy H. Davenport megjegyezte – létezik Erdős sejtésének egy erősebb változata, ami nem következik Cassels tételéből: Bármely $p, q > 1$ egészekre, melyekre $(p, q) = 1$ létezik, $K = K(p, q)$ úgy, hogy az $Y_K = \{p^n q^m : n = 0, 1, \dots\ 0 \le m \le K\}$, sorozat is teljes.

Ezen erősebb változat is kiolvasható Birch ′59-es cikkéből. Erdős erről ezt írja:

"Of course the exact value of $K(p, q)$ is not known and no doubt will be very difficult to determine."

3.3 A fentiekkel rokon kérdés Burr és Erdős problémája a megszorított összeg halmaz sűrűségéről.

Jelölje a $h-$szoros összeghalmazt és a $h-$szoros megszorított összeghalmazt

$$hA = \{a_1 + \cdots + a_h : a_1, \dots, a_h \in A\},$$

$$h \times A = \{a_1 + \cdots + a_h : a_1, \dots, a_h \in A; a_i \neq a_j, \text{ ha } i \neq j\}.$$

Erdős több helyen is kérdezi (lásd pl. [EG80] 52.o.):

"Legyen $A \subseteq \mathbb{N}$ amelyik egy $h-$ad rendű bázis. Igaz-e, hogy ekkor

$$\underline{d}(h \times A) > 0?"$$

Ugyancsak ők ketten vetették fel ([E98]), hogy ha egy A halmaz $k-$ad rendű bázis, igaz-e, hogy az A *különböző* elemeiből képzett legfeljebb k tagú összegek alkotta sorozat hézaga korlátos? Formálisan ha $ord(A) = k$, igaz-e, hogy

$$\Delta(A \cup (2 \times A) \cup \cdots \cup (k \times A)) < \infty?$$

4. Expander és lefedő polinomokról

4.1 A jól ismert Cauchy-Davenport tétel szerint, ha A, B a $\mathbb{Z}_p$ csoport részhalmazai, és $A + B \neq \mathbb{Z}_p$, akkor $|A + B| \geq |A| + |B| - 1$, továbbá a becslés éles; t.i. ha A, B közös differenciájú számtani sorozatok, akkor $|A + B| = |A| + |B| - 1$.

Ebből fakadóan az a kérdés merülhet fel, hogy mi mondható két- ill. többváltozós polinomok értékeinek a halmazáról?

A számítástudományban, a gráfelméletben, a kódelméletben és számos más helyen is fontos szerepet játszanak az olyan rendszerek, melyek *nagyító tulajdonsággal* rendelkeznek.

Kérdezhető tehát, hogy mely f polinomok nagyítják ki a tárgyhalmazukat, azaz mikor igaz, hogy bármely $A, B \subseteq \mathbb{Z}_p$, $|A| \asymp |B|$ halmazokra teljesül, hogy

$$f(A, B) := \{f(a, b) : a \in A; b \in B\}$$

lényegesen nagyobb, mint $|A|$. Könnyen látható, hogy $f(x, y) = x + y$, továbbá pl $g(x, y) = x \cdot y$ nem ilyenek. Erdős és Szemerédi híres tétele (és annak lényeges javításai) mutatják, hogy *egyszerre* azért nem lehet mindkettő "kicsi".

Az összeg-szorzat becslések a háromváltozós $f(x, y, z) = xy + z$ polinom expander tulajdonságát biztosítják. Valóban, Bourgain-Katz-Tao (később mások is javítva a c értékét) igazolták, hogy ha $\delta > 0$, akkor ha $p > p(\delta)$ és $A \subseteq \mathbb{F}_p$, melyre $p^\delta < |A| < p^{1-\delta}$, akkor létezik $c = c(\delta)$, hogy vagy $|AA|$, vagy $|A + A| \gg |A|^{1+c}$.

Ebből a Ruzsa-Plünnecke egyenlőtlenség segítségével azt kapjuk, hogy $|AA + A| \gg |A|^{1+c/2}$, azaz az $f(x, y, z) = xy + z$ polinom valóban expander tulajdonságú. Tehát az "erős kérdés" az lehet, vannak-e, és milyenek a *kétváltozós* expander polinomok?

Az első explicit *kétváltozós* expander polinom Bourgain-től származik [Bou05]:

Tétel *(Bourgain) Legyen* $B(x,y) = x^2 + xy$. *Ha* $p^\varepsilon < |A| \asymp |B| < p^{1-\varepsilon}$ *akkor* $|B(A,B)|/|A| > p^\gamma$, *ahol* $\gamma = \gamma(\varepsilon)$ *pozitív.*

Bourgain eredeti bizonyításában a γ értéke implicit.

4.2 Sárközy vizsgálta ([S05]), hogy prímtestben milyen feltételek mellett oldható meg az $x + y = zu; x \in A; y \in B; z \in Z; u \in D$ összeg-szorzat egyenlet. Megmutatta, hogy ha $A, B, C, D \subseteq \mathbb{F}_p$, és $|A||B||C||D| > p^3$, akkor van megoldás. Ebből számos szép alkalmazás is levezethető.

E tétel azt is kiadja, hogy ha $A, B, C, D \subseteq \mathbb{F}_p$, és $|A||B||C||D| > p^3$, akkor a négyváltozós $F(x,y,z,u) := x + y + zu$ polinom értékeinek a halmaza $\mathbb{F}_p$, azaz $F(A,B,C,D) = \mathbb{F}_p$.

Az ilyen típusú polinomokat nevezhetjük lefedő polinomoknak. I. Shkredov megmutatta, hogy a $B(x,y)$ Bourgain függvényre $|B(A,B)| \geq (p-1) - \frac{40p^{5/2}}{|A||B|}$, azaz ha pl. $|A|, |B| > p^{3/4+\delta}$, $\delta > 0$, akkor $B(A,B)$ majdnem minden elemet lefed. Számos nyitott kérdés kapcsolódik e témakörhöz.

Valós testben más a helyzet; Elekes és Rónyai [ER00] egy szép (és mély) cikkükben feltételt adtak arra, hogy egy $T(x,y)$ függvény esetén mikor teljesül, hogy $|T(A,B)| \leq Cn$. E feltételt C, n megszorított tulajdonságnak nevezik, ahol $|A| = |B| = n$. Ebben a cikkben található teszt a következő: legyen $q_1(x,y) := \frac{\partial T/\partial x}{\partial T/\partial y}$. Ha a $q_2(x,y) := \frac{\partial^2(\log|q_1(x,y)|)}{\partial x \partial y}$ függvény nem azonosan nulla, akkor $|T(A,B)|/n \to \infty$, amint $n \to \infty$.

5. Struktúra tételek Heisenberg csoportokban

Gill, Helfgott munkája nyomán, ha $SL_n(\mathbb{Z}_p)$ csoportnak egy elég nagy részhalmazát választjuk, akkor a hármas szorzat nagyobb az eredeti halmaz méreténél; az előző fejezetek szóhasználattal élve a $SL_n(\mathbb{Z}_p)$ csoport "nagy" halmazaira az $F(x,y,z) = xyz$ polinom expander. Egy későbbi Babai-Nikolov-Pyber tételből azt is tudjuk, hogy ha $A \subseteq SL_2(\mathbb{Z}_p)$, $|A^2| > |A|^{1+\epsilon}$, amennyiben $|A| > p^{2+\delta}$.

Felmerül a kérdés, hogy az ilyen Lie típusú, nem kommutatív csoportoknál milyen *struktura tulajdonságot* tudunk felismerni szorzathalmazokban. Általános halmazok szorzathalmazairól ilyen csoportokban keveset tudunk.

Legyen p prímszám, $\mathbb{F}_p$ jelölje a prímtestet. Jelöljük H_n a $(n+2)\times(n+2)$ felső háromszög mátrixok azon lineáris csoportját, melynek elemei

$$[\underline{x},\underline{y},z]=\begin{pmatrix}1 & \underline{x} & z\\ 0 & I_n & {}^t\underline{y}\\ 0 & 0 & 1\end{pmatrix},$$

ahol $\underline{x}=(x_1,x_2,\ldots,x_n)$, $\underline{y}=(y_1,y_2,\ldots,y_n)$, $x_i,y_i,z\in\mathbb{F}$, $i=1,2,\ldots,n$, I_n az $n\times n$-es egység mátrix. Nyilván $|H_n|=p^{2n+1}$; a H_n-beli szorzási szabály:

$$[\underline{x},\underline{y},z][\underline{x}',\underline{y}',z']=[\underline{x}+\underline{x}',\underline{y}+\underline{y}',\langle\underline{x},\underline{y}'\rangle+z+z'],$$

ahol $\langle\cdot,\cdot\rangle$ a skalárszorzatot jelenti, azaz $\langle\underline{x},\underline{y}\rangle=\sum_{i=1}^{n}x_iy_i$.

E csoport nem kommutatív, $2-$nilpotens, ami azt jelenti, hogy bármely $a_1,a_2,a_3\in H$ elemere $[[a_1;a_2];a_3]=[0,0,0]=1_H$, ahol $[u;v]$ két elem kommutátora $[u;v]=uvu^{-1}v^{-1}$.

0.3. Vizsgálati módszerek

A bizonyítások során különböző, a kombinatorikus számelméletben használt módszerek voltak a segítségemre. Felhasználtam nem konstruktív bizonyítási ötletet, összeghalmazokra vonatkozó eredményeket, a halmazrendszerek kombinatorikájának tételét (az. ú.n. "sunflower lemma"-t, melyet manapság sokan használnak; tudomásom szerint viszont előttem csak Erdős-Sárközy használta egy kissé más probléma kezelésére). Illeszkedési tételeket (a ma ugyancsak sokat használt, Vinh-től származó becslést is az elsők között használtuk), véges testeken értelmezett diszkrét Fourier transzformációt és további kombinatorikus módszereket.

0.4. Elért eredmények

0.4.1. Hilbert kockákról

Definíció: *Legyen A a pozitív egésze egy végtelen sorozata és legyen*

$H_A(n) = \max\{m : A \cap [1,n]$ *tartalmaz egy* $H(a_0, a_1, a_2, \ldots, a_m)$ *Hilbert kockát*$\}$

Jegyezzük meg, hogy a következőkben – ha ezt külön nem jelezzük – elfajuló Hilbert kockákat is megengedünk (tehát olyanokat ahol megengedjük egy $x = \sum_{i=1}^{m} \varepsilon_i a_i$ többször is reprezantálva lehessen)

$H_A(n)$ értékére egy 1999-es cikkemben adtam becslést ([H97]). Bizonyítottam, hogy

Tétel (Hegyvári) *Létezik olyan $A \subseteq \mathbb{N}$, $\underline{d}(A) > 0$ és melyre $n \in \mathbb{N}$ esetén*

$$H_A(n) < c\sqrt{\log n \log\log n},$$

ahol $c = 6/\log(5/4)$.

A tétel bizonyítása nem konstruktív. Másfelől megmutattam, hogy legfeljebb csak a $\log\log n$ tényező hagyható el.

Propozíció (Hegyvári) *Legyen A a természetes számok egy soroazta, melyben $Pr(a \in A) = p$. Ekkor 1 valószínűséggel*

$$H_A(n) > c_p\sqrt{\log n}$$

2014-ben Conlon, Fox és Sudakov igazolta [CFS14], hogy van olyan (véletlen) sorozat $A \subseteq \mathbb{N}$, $\underline{d}(A) > 0$ és melyre $n \in \mathbb{N}$ esetén $H_A(n) \ll \sqrt{\log n}$.

Könnyű látni, hogy a fent említett Szemerédi-kocka tétel ritkább soroaztokra is igaz. Nevezetesen a $\underline{d}(A) > 0$ feltétel gyengíthető: amennyiben $A(n) \gg n^{4/5}$ akkor

$$H_A(n) \gg \log \frac{\log n}{\log(n/A(n))}.$$

[He04] cikkemben megmutattam, hogy

Tétel (Hegyvári) *Létezik olyan $A \subseteq [1,n]$, melyre $|A| \geq r_3(n)/3$ és melyre*

$$H_A(n) \ll \log\log n,$$

ahol $r_3(n)$ jelöli annak az $[1,n]$-beli maximális elemszámú halmaznak a méretét, amelyik nem tartalmaz (nem triviális) számtani sorozatot, H pedig Hilbert kockát jelöl.

Behrend a $r_3(n)$-re történt nevezetes becslésével tehát kapjuk a következőt:

Következmény: *Bármely c számra $(1/2 < c < 1)$ van olyan $A \subseteq [1,n]$, melyre $|A| > \frac{n}{e^{(\log n)^c}}$, és melyre*

$$\frac{11}{10}(1 + o(1)\log\log n) \leq H_A(n) \leq \frac{1}{\log 2}\log\log n.$$

Vizsgáltam Hilbert-kockával kapcsolatos lefedési tételt is.

Egy adott struktúrában (itt $\mathbb{F}_p$ a struktúra) egy 1 kezdőpontú multiplikatív Hilbert-kocka analóg módon definiálható (ekkor az irodalomban $FP(\cdot)$ a jelölés); legyen $X \subseteq \mathbb{F}_p$ értelmezzük X által indukált multiplikatív Hilbert-kockát a

$$FP(X) := \{\prod_{x\in Y} x : \{\emptyset\} \neq Y \subseteq X\}$$

halmazzal.

$\mathbb{F}_p$-beli sűrű halmazokban található Hibert kockákkal kapcsolatos tételek az additív eredmények közvetlen következményei: Legyen ugyanis g egy primitív gyök modulo p, és írjuk $\mathbb{Z}_p^*$ elemeit $a = g^b$ alakba. A $\mathbb{Z}_p^*$ egy X részhalmazára jelölje $indX := \{y : g^y \in X\}$.

Ekkor könnyen látható, hogy $FP(A)$ egy multiplikatív Hilbert-kocka pontosan akkor, amikor $indFP(A)$ egy (0 kezdőpontú) additív Hilbert-kocka.

[He09]-ben igazoltam a következő összeg-szorzat típusú lefedési tételt:

Tétel (Hegyvári) *Legyen $A \subseteq \mathbb{F}_p$, $|A| > 2$, és legyen $q(x) = 1 + u_1 x + \cdots + u_D x^D$ egy nem-konstans polinom. Jelölje továbbá $Q = [q(r) : r \in \mathbb{F}_p]$ az értékeinek multihalmazát.*

Ekkor létezik olyan B multi-részhalmaza Q-nak és egy $c_1 > 0$ konstans melyre

$$|B| < c_1 \log\frac{\log p/D}{log|A|} + 2D + 3$$

és

$$FP(B)_{mult} * A := \sum_{h \in FP_{mult}(B)} h \cdot A = \mathbb{F}_p.$$

Bizonyos halmazokon vett karakterösszegek mostanában igen intenzíven vizsgált területe az additív kombinatorikának.

Egy $f : \mathbb{F}_p \mapsto \mathbb{C}$ függvény (additív) diszkrét Fourier tarnszformáltján az $\widehat{f(r)} := \sum_{x \in \mathbb{F}_p} f(x) e_p f(rx)$. Egy multiplikatív karakterrel vett összeg pedig a $\widetilde{f(u)} := \sum_{x \in \mathbb{F}_p^*} f(x)\chi_u(x)$ jelöli, ahol $\chi_u(x) = e^{\frac{2\pi i ind x \cdot u}{p-1}}$.

Ismert, hogy "nem túl nagy" halmazokhoz van olyan frekvencia, amin felvett karakterösszeg "nagy". Montgomery igazolta (lásd pl.[Ga10]-ben), hogy ha $U \subseteq \mathbb{F}_p$ egy tetszőleges halmaz és $A \subseteq U$ olyan részhalmaza, melyre $|A| < B \log p,\ B > 0$, akkor valamely $c = c(B)$ konstanssal $\max_{r \neq 0} |\widehat{A}(r)| \geq c|A|$.

Mintegy kontraszként említsük meg Ajtai (et al) [AI90] eredményét, miszerint van olyan $T \subseteq \mathbb{Z}_m$, melyre $|T| = O(\log m (\log^* m)^{c' \log^* m})$ $c' > 0$ és $\max_{r \neq 0} |\widehat{T}(r)| \leq O(|T|/\log^* m)$ ($\log^* m$ a multi-iterált logaritmus).

Az alább vizsgált kérdésekben néhány olyan erdeményemet említem, ami árnyalja a fenti jelenséget; megvizsgáltam Hilbert kockákon definiált Dirichlet karakterek értékét.

Szükségünk lesz Hilbert kockák fogalmának a kiterjesztésére:

1. Definíció. *Az r-ed rendű Hilbert kockán a*

$$H_r(x_0, a_1, a_2, \ldots, a_d) = \Big\{ x_0 + \sum_{1 \leq i \leq d} \varepsilon_i a_i \Big\} \quad \varepsilon_i \in \{0, 1, \ldots, r\}. \tag{1}$$

halmazt értjük.(Amint $r = 1$, ez a szokásos Hilbert kocka).

Legyen $\Delta, 0 < \Delta \leq 1$ valós paraméter. Azt mondjuk, hogy $H =: H_r(x_0, a_1, a_2, \ldots, a_d)$ $\Delta-$degenerált, ha $\frac{\log_{r+1}|H|}{d} = \Delta$. (Ha $\Delta = 1$, akkor $|H| = (r+1)^d$ és így a fenti kockának az elemei mind különbözőek és ekkor nem degenerált kockáról beszélünk).

Elsőként megemlíteném a következő tételt ([HE16]):

Tétel (Hegyvári) *Legyen $\Delta \in (0, 1]$, $r > 1$, $r \in \mathbb{N}$ és legyen $H_r(x_0, a_1 < a_2 < \cdots < a_d)$ egy tetszőleges Δ-degenerált Hilbert kocka. Ekkor*

$$\sum_{\chi} \Big| \sum_{h \in H} \chi(h) \Big| \gg \begin{cases} \sqrt{p}|H|^{3/2 - \gamma_r/2} & |H| < p^{2/3} \\ p^{3/2}|H|^{-\gamma_r/2} & |H| \geq p^{2/3} \end{cases}$$

ahol $\gamma_r = \frac{\log_{r+1}(2r+1)}{\Delta}$.

E tétel becslésénél szükségünk volt Hilbert kockák multiplikatív energiájának becslésére.

Emlékeztetnénk, hogy egy $A, B \subseteq \mathbb{F}_p$ halmazpár additív energiáján a $E_\times(A,B) := |\{(a_1,a_2,b_1,b_2) \in A\times A\times B\times B : a_1\cdot b_1 = a_2\cdot b_2\}|$ értéket értjük.

E vonatkozásban a következő eredmény vezetett a fenti tételre:

Propozíció (Hegyvári) *Legyen* $\Delta \in (0,1];\ r>1,\ r\in\mathbb{N}$, *legyen továbbá* $H = H_r(x_0, a_1 < a_2 < \cdots < a_d)$ *egy* Δ*-degenerált Hilbert kocka. Ekkor*

$$E_\times(H) \ll \begin{cases} |H|^{\gamma_r} p & |H| < p^{2/3} \\ \frac{|H|^{3+\gamma_r}}{p} & |H| \geq p^{2/3} \end{cases} \tag{2}$$

ahol $\gamma_r = \frac{\log_{r+1}(2r+1)}{\Delta}$.

Jegyezzük meg, hogy a fenti becslés nem triviális, ha H "nem túl degenerált" (Δ közel van 1-hez). Például, ha $|H| \asymp p^{2/3}$, r "nagy",akkor $|H|^{\gamma_r}p$ közel van $|H|^{5/2}$-hez, ami $|H|^3$-nél (a triviális becslésnél) jobb.

Itt természetesen merül fel az a kérdés, hogy mit lehet mondani *multiplikatív Hilbert kockák* additív energiájáról. A multiplikatív Hilbert kocka definíciója analóg az additívéhez, a teljesség kedvéért definiáljuk:

2. Definíció. *Multiplikatív Hilbert kocka alatt a*

$$H^\times(x_0, a_1, a_2, \ldots, a_d) = \Big\{ x_0 \cdot \prod_{1\leq i\leq d} a_i^{\varepsilon_i} \Big\} \quad \varepsilon_i \in \{0,1\}$$

halmazt értjük.

Tehát a régebbi jelöléssel élve $H^\times(x_0, a_1, a_2, \ldots, a_d) = x_0 FP(x_0, a_1, a_2, \ldots, a_d)$. Ezzel kapcsolatosan igazoltam a következőt:

Propozíció (Hegyvári) *Legyen* $H^\times := H^\times(x_0, a_1, a_2, \ldots, a_d) \subseteq \mathbb{F}_p^*;\ |H^\times| = p^\alpha;\ \alpha > \frac{13}{18}$ *egy multiplikatív Hilbert kocka,* $H_2^\times = H_2^\times(x_0, a_1, a_2, \ldots, a_d)$. *Ekkor*

$$E_+(H^\times) \ll |H^\times|^3 \Big(\frac{|H_2^\times|}{p}\Big)^{1/5}.$$

Következményeként kapjuk:

Következmény (Hegyvári) *Legyen* $H^\times := H^\times := H^\times(x_0, a_1, a_2, \dots, a_d) \subseteq \mathbb{F}_p^*$; $|H^\times| = p^\alpha$; $\alpha > \frac{13}{18}$ *egy multiplikatív Hilbert kocka és tegyük fel, hogy* $|H_2^\times| \ll |H^\times|^{1+\varepsilon}$ $(\varepsilon > 0)$. *Ekkor*

$$E_+(H^\times) \ll |H^\times|^{3-\delta}$$

ahol $\delta = \frac{1-\alpha(1+\varepsilon)}{5\alpha}$.

Végül ebben a pargrafusban megemlíteném Montgomery kérdéséhez kapcsolódó ereményemet:

Tétel (Hegyvári) *Legyen* $H(x_0, a_1 < a_2 < \cdots < a_d)$ *egy tetszőleges nem-degenerált Hilbert kocka. Ekkor bármely* $\xi \in \mathbb{F}_p^*$ *frekvenciához létezik* $H' \subseteq H$, *melyre* $|H'| \gg e^{c\sqrt{\log |H|}}$ *és melyre teljesül*

$$|\widehat{H'}(\xi)| \gg |H'|.$$

Hilbert kockákról; Brown-Erdős-Freedman problémájáról

Ebben a paragrafusban T.C. Brown, Erdős és A. Freedman problémájához kapcsolódva nevezetes sorozatokban található Hilbert kockák dimenzióját vizsgáljuk. Jelölje mint az előző paragrafusban $\mathcal{Q}$ a négyzetszámok sorozatát, $\mathcal{P}$ a prímek sorozatát.

Sárközyvel a következő eredményeket találtuk ([HS99]):

Tétel (Hegyvári-Sárközy)

$$H_{\mathcal{P}}(N) \ll \log N.$$

Továbbá a négyzetszámokra

Tétel (Hegyvári-Sárközy)

$$H_{\mathcal{Q}}(N) < 48\sqrt[3]{\log N}.$$

Eredményeinket később többen javították (lásd pl. [W04], [DE12],[DE15]). Megemlíteném, hogy egy érdekes számítástudományi kapcsolata is van tételünknek. Woods ([W04]) vizsgálta a következő kérdést: tekintve azt a Boole-hálozatot amelyik teszteli egy prímszám $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$ bináris jegyeit, akkor mennyi az "AND" (input) és "OR" (output) kapuk száma? A szerző becslést nyer ezek számára, (ami egyébként a fenti tételünk javításából kapható).

Hilbert kockákról; Bergelson egy problémájáról

Egy pozitív felsősűrűségű $A \subseteq \mathbb{N}$ sorozat kétszer iterált különbség sorozata (azaz a $D(D(A)) = A - A + A - A$) nagyon jól strukturált; ez a tény fontos szerepet játszott a Freiman-Ruzsa tétel bizonyításában. Természetesen adódik a kérdés, hogy iterálás nélkül, tehát a $D(A) = A - A$ sorozat mennyire jól strukturált?

1985-ben Bergelson megmutatta, hogy ha egy $A \subseteq \mathbb{N}$ sorozatra $\overline{d}(A) > 0$, akkor bármely $k \in \mathbb{N}$ számhoz létezik egy *végtelen* B sorozat, melyre $A - A \supseteq B + B + \cdots + B = kB$.

Bizonyításában a Fürstenberg által kidolgozott egodelméleti módszerek játszottak szerepet. Később ezt az eredményt élesebb formában – ugyancsak ergodelméleti módszerekkel – javította; társszerzőkkel megmutatta, hogy $A - A$ (a fenti feltételek mellett) általánosított számtani és geometriai sorozatot is tartalmaz.

Ruzsa Imrével – Følner tételének felhasználásával igazoltuk a következő tételt ([HR16]):

Tétel (Hegyvári-Ruzsa) *Legyen A a természetes számok egy olyan sorozata, melyre $\overline{d}(A) > 0$. Legyen $f : \mathbb{N}_+ \to \mathbb{N}_+$ egy tetszőleges függvény. Ekkor létezik egy végtelen C halmaz, melyre $A - A \supseteq FS_f(C) \cup FP(C)$, ahol*

$$FS_f(C) := \Big\{ \sum_{c_i \in X} w_i c_i : X \subseteq C,\ |X| < \infty;\ w_i \in [1, f(i)] \cap \mathbb{N} \Big\},$$

$$FP(C) := \Big\{ \prod_{c_i \in X} c_i : X \subseteq C;\ X \neq \emptyset,\ |X| < \infty \Big\}.$$

0.4.2. Ramsey típusú additív kérdések

Két Ramsey típusú kérdést tárgyalok.

Az első a Raimi-Hindman tétel nagymértékű álatlánosítását adja (He05]):

Tétel (Hegyvári) *Legyen $A \subseteq \mathbb{N}$ az egészek olyan sorozata, melyre valamely pozitív γ irracionálisra a $[0,1)$ intervallumban a $\{\langle \gamma x \rangle : x \in A\}$ halmaz sűrű.*

Legyen $r \in \mathbb{N}$ és legyenek $\alpha_1, \alpha_2, \ldots, \alpha_r$ olyan pozitív valósak, melyekre $\sum_{i=1}^{r} \alpha_i = 1$.

Ekkor létezik a természetes számok $\mathbb{N} = \bigcup_{i=1}^{r} E_i$ olyan partíciója, melyere.

(1) bármely $i \in \{1, 2, \ldots, r\}$ esetén $d(E_i) = \alpha_i$,

(2) bármely $t \in N$ és bármely az A halmaz $A = \bigcup_{j=1}^{t} F_j$ $t-$színezése esetén

van olyan $m \in \{1, 2, \ldots, t\}$ és végtelen $\{x_n\}_{n=1}^{\infty}$ $\mathbb{N}$-beli sorozat úgy, hogy bármely $h \in FS(\{x_n\}_{n=1}^{\infty})$ részösszegre és bármely $i \in \{1, 2, \ldots, r\}$ indexekre,

$$(F_m + h) \cap E_i$$

végtelen halmaz.

Tehát ebben a tételben nem csak egy E halmaz és komplementere metsz bele végtelen halmazzal az egyik partícióba, hanem tetszőleges számú és előre adott sűrűségű halmazzal tudjuk biztosítani egy Hilbert kocka összes eltoltjával ezt. A Raimi-Hindman tétel az $r = 2$, és az $\{x_n\}_{n=1}^{\infty}$ végtelen sorozat helyet egy $k \in \mathbb{N}$ speciális esetben kapható meg.

A másik additív-Ramsey típusú és a Sárközy által felvetett kérdésekre talált eredmények leírására definiáljuk egy A sorozat K színezésének a rendjét:

Definició:

Legyen $A \subseteq \mathbb{N}$, vegyük ennek egy K színezését (K-partícióját), és gyűjtsük a sorozat egyszínű elemeit részhalmazokba. Azaz

$$A = \bigcup_{1 \le i \le K} A_i,$$

tehát, ahol A_i-ben az A halmaz i-edik színnel színezett elemei kerülnek. Legyen $U = \{A_1, \ldots, A_K\}$, és jelölje $ord(U)$ azt a legkisebb h számot, amelyre

igaz, hogy minden elég nagy n számhoz van olyan i, $1 \leq i \leq K$, hogy az n szám előáll legfeljebb h A_i-beli elem összegeként. Végül legyen

$$ord_K(A) := \sup\{ord(U) : U \text{ egy } K \text{ színezése } A-\text{nak}\}.$$

Jelölje $\mathcal{Q}$ a négyzetszámok halmazát, $\mathcal{P}$ pedig a prímekét. E kérdéskörben a következő eredményeket sikerült elérni ([HH07]):

Tétel (Hegyvári-Hennecart) *Legyen $K \in \mathbb{N}$. Ekkor*

$$(e^{\gamma} + o(1))K \log\log K \leq ord_K(\mathcal{P}) \leq 1500K^3.$$

Tétel (Hegyvári-Hennecart) *Legyen $K \in \mathbb{N}$. Ekkor*

$$K \exp\big((\log 2 + o(1))\frac{\log K}{\log\log K}\big) \leq ord_K(\mathcal{Q}) \leq 10^9(K \log K)^5.$$

Ezeket az eredményeket P. Akhilesh, D. S. Ramana, O. Ramaré ([AR14], [RR12]) és G. Chen [Ch16] tovább javították.

0.4.3. Megszorított összegekről

Idézzük fel, ha $X = \{x_1 < x_2 < \dots\} \subseteq \mathbb{N}$, jelölje X aszimptotikus hézagát (a következőkben röviden X hézagát) $\Delta(X)$, azaz legyen

$$\Delta(X) := \limsup_{i\to\infty}(x_{i+1} - x_i).$$

Megmutattuk, hogy a $k = 2$ kivételével a Burr-Erdős sejtés hamis ([HHP2]):

Tétel (Hegyvári-Hennecart-Plagne) *1. Ha $ord(A) = 2$, akkor*

$$\Delta(A \cup (2 \times A)) \leq 2.$$

2. Legyen $h \geq 3$. Ekkor létezik olyan $A \subseteq \mathbb{N}$, hogy $ord(A) = h$, ám

$$\Delta(A \cup (2 \times A) \cup \dots \cup (h \times A)) = \infty.$$

Becsléseket kaptunk az összeghalmaz és az összeghalmaz sűrűségeinek a kapcsolatáról. Pontosabban igazoltuk ([HHP]):

Tétel (Hegyvári-Hennecart-Plagne) *Legyen $A \subseteq \mathbb{N}$ és tegyük fel, hogy valamely $h \in \mathbb{N}$ egészre $\underline{d}(hA) > 0$ teljesül. Ekkor*

$$\underline{d}(h \times A) \geq \frac{1}{h^h e^{\pi\sqrt{2h/3}}} \underline{d}(hA).$$

További természetes sejtés az, hogy a $\{\Delta(h \times A)\}_{h \geq 1}$ sorozat monoton csökkenő. E kérdés még nyitva maradt, mindazonáltal sikerült bizonyítani, hogy ha van olyan véges h melyre a hézag h-nál nem nagyobb, akkor egy legalább $1/h$ alsó sűrűségű indexhalmazon valóban nem növekszik a hézag.

Az alábbiakban igazoltuk a következő tételt:

Tétel (Hegyvári-Hennecart-Plagne) *Legyen $A \subseteq \mathbb{N}$ és legyen h az a legkisebb természetes szám, melyre $\Delta(h \times A)$ véges. Ekkor létezik egy index sorozat*

$$h = h_0 < h_1 < \cdots < h_j \ldots$$

melyre $2 \leq h_{j+1} - h_j \leq h + 1$, $(j \geq 1)$ és

$$\Delta(h_{j+1} \times A) \leq \Delta(h_j \times A).$$

E tétel bizonyításában felhasználjuk az Erdős-Radó ú.n. delta-rendszerekre vonatkozó tételét.

E témakörben jól alkalmazható ez a kombinatorikus halmazelméleti eredmény, amit – tudomásunk szerint – előttünk csak Erdős és Sárközy használták egy részösszeghalmazok probléma megoldására. Később e módszert aztán többen alkalmazták.

0.4.4. Expander és lefedő polinomokról

Idézzük fel, hogy egy 2 változós polinomot mikor nevezünk expander polinomnak:

Legyen p prímszám és legyen $f : \mathbb{F}_p^2 \to \mathbb{F}_p$ egy 2 változós polinom. Nevezzük az f-et *expander függvénynek*, ha bármely α, $0 < \alpha < 1$ értékre létezik $\epsilon = \epsilon(\alpha) > 0$ pozitív valós szám, melyre

$$|f(A, B)| \gg p^{\alpha+\epsilon}$$

amennyiben $|A| \asymp |B| \asymp p^\alpha$.

Mint említettük az első explicit expander polinom Bourgain-től származott, ineffektív $\epsilon(\alpha)$ expanziós mértékkel.

Sikerült expander polinomok egy végtelen osztályát megmutatni, bizonyos tartományon effektív expanziós mértékkel ([HH09]).

Tétel (Hegyvári-Hennecart) *Legyen $k \geq 1$ és f, g egész együtthatós egyváltozós polinomok. Legyen továbbá F $F : \mathbb{Z}^2 \mapsto \mathbb{Z}$ függvény, amelyik*

$$F(x, y) = f(x) + x^k g(y).$$

Tegyük fel, hogy $f(x)$ és x^k affin függetlenek. Ekkor F expander.

(Az f és g függvényeket affin függetleneknek nevezzük, ha nincs olyan $(u, v) \in \mathbb{Z}^2$, hogy $f(x) = uh(x) + v$ vagy $h(x) = uf(x) + v$ teljesül. Az összefüggők könnyen láthatóan nem expanderek.)

Az expanzió mértékére a következő tétel igaz:

Tétel (Hegyvári-Hennecart) *Legyen F az előbbi tételben definiált polinom és tegyük fel, hogy $\alpha > 1/2$.*

Ekkor bármely $A, B \subseteq \mathbb{F}_p$ halmazpárra, melyekre $|A| \asymp |B| \asymp p^\alpha$, az expanzió mértéke

$$|F(A, B)| \gg |A|^{1+\frac{\min\{2\alpha-1;2-2\alpha\}}{2}}.$$

Bevezettük az ú.n. teljes expander fogalmát: Legyen I a $[0, 1]$ intervallum részhalmaza (általában részintervalluma). $F-$et I szerinti teljes expandernek nevezzük, amennyiben

$$|F(A, B)| \geq cp^{\min\{1;2\alpha\}}$$

teljesül minden olyan halmazpárra, amelyre $|A|, |B| \asymp p^\alpha$ és $\alpha \in I$.

Például I. Shkredov igazolta, hogy Bourgain függvénye az $I = (3/4, 1)$ szerint teljes expander. A következőben megmutattuk, hogy itt a $3/4$ nem cserélhető le $1/2$-re, pontosabban a következő tételt igazoltuk:

Tétel (Hegyvári-Hennecart)

1. Legyen $k \geq 2$ egész, $u \in \mathbb{Z}$ és $F(x, y) = x^{2k}+ux^k+x^k y = x^k(x^k+y+u)$. Ekkor bármely α, $0 < \alpha \leq 1/2$ esetén F $\{\alpha\}$ szerint nem teljes expander.

2. Legyen $f(x)$ és $g(y)$ két nem konstans polinom és legyen $F(x, y) = f(x)(f(x) + g(y))$. Ekkor F nem teljes expander $\{1/2\}$ szerint.

E tételek effektív bizonyításában a Weil tétele mellett Erdős "szorzat tételének" Tenenbaum-tól származó változata segített.

Sárközy vizsgálta ([S05]), hogy prímtestben milyen feltételek mellett oldható meg az $x+y=zu; x\in A; y\in B; z\in Z; u\in D$ összeg-szorzat egyenlet. Megmutatta, hogy ha $A,B,C,D\subseteq\mathbb{F}_p$, és $|A||B||C||D|>p^3$, akkor van megoldás. Ebből számos szép alkalmazás is levezethető.

E tételből az is leolvasható, hogy ha $A,B,C,D\subseteq\mathbb{F}_p$, és $|A||B||C||D|>p^3$, akkor a négyváltozós $F(x,y,z,u):=x+y+zu$ polinom értékeinek a halmaza $\mathbb{F}_p$, azaz $F(A,B,C,D)=\mathbb{F}_p$. Az ilyen típusú polinomokat nevezthetjük lefedő polinomoknak. A tétel éles. Meglepő módon, ha az általánosabb $F(x,y,z,u):=x+y+g(z,u)$ polinomot vizsgáljuk, $g(u,v)$ nem konstans polinom, akkor a fenti feltétel gyengíthető. Például igaz a

Tétel (Hegyvári-Hennecart) *Legyenek $F_1(x,y)=xy+x^2h_1(y)$ és $F_2(x,y)=x^2y+xh_2(y)$, ($h_i(y)\in\mathbb{Z}[y]$; $i=1,2$ nem zérus polinomok). Ekkor léteznek $0<\delta,\delta'<1$ valósak úgy, hogy bármely p prímre és $A,B,C,D\subseteq\mathbb{F}_p$ halmazokra, melyekre*

$$|C|>p^{1/2-\delta},\quad |D|>p^{1/2-\delta}\quad |A||B|>p^{2-\delta'},$$

teljesül, a $G(x,y,u,v)=x+y+F_i(u,v)$ lefedő polinom.

Továbbá megmutattam, hogy ha azt az egyenletet vizsgáljuk, melyre $a+b=h$, $h\in H$ és e H halmaz jól strukturált, ugyancsak gyengíthető a fenti feltétel (egy általánosabb tétel speciális esete) ([HE12]):

Tétel (Hegyvári) *Legyen $A,B\subseteq\mathbb{F}_p$, és $H<\mathbb{F}_p^*$ egy multiplikatív részcsoportja, melyre $|H|=p^\beta$. Ekkor az*

$$a+b=h;\ (a,b,h)\in A\times B\times H$$

megoldható, amennyiben

$$|A||B||H|^2>p^{\frac{9+5\beta}{4}}.$$

Ez tehát a $0<\beta<\frac{3}{5}$ értékekre jobb eredményt ad.

A fenti tételek az adott halmazok (multiplikatív) energiájának, és bizonyos Multilineáris exponenciális összegek eloszlásától függenek.

Vinogradov egy szép (és gyakran alkalmazható) tétele arról informál, hogyan oszlik el az $A \cdot B \bmod p$.

Vinogradov tételének szép általánosítása (amelynek bizonyítása az additív kombinatorika számos tételét ötvözi) Bourgain-től és Garaev-től származik és amelyik háromtényezős, tehát egy

$$|S(r)| = |\sum_{x=1}^{p}\sum_{y=1}^{p}\sum_{z=1}^{p} v(x)\varrho(y)\vartheta(z)(e(xyz)|$$

exponenciális összeg abszolút értékére ad felső becslést.

Tetszőleges tényezőkre Bourgain a következő (nem explicit konstansokat tartalmazó) becslést adta ([B09b]):

Tétel (Bourgain) *Létezik olyan $C > 1$ konstans, hogy bármely $0 < \delta < 1$, és $r \in \mathbb{N},\ r > C/\delta$, esetén, ha $A_1, A_2, \ldots, A_r \subseteq \mathbb{F}_p$, $|A_i| > p^{\delta}$, $1 \leq i \leq r$, és p elég nagy prím, akkor*

$$\Big|\sum_{x_1 \in A_1, \ldots, x_r \in A_r} e(x_1 x_2 \cdots x_r)\Big| < p^{-\delta'}|A_1||A_2|\cdots|A_r|,$$

ahol $\delta' > C^{-r}$.

Várható, hogy ha a halmazok strukturájáról további feltételeket kötünk ki, több információt nyerünk erről az összegről. Valóban, ha az n számú halmaz közül kettőről valamely additív strukturát tételezünk fel, és e halmazok elemszámára vonatkozó feltételt is szabunk, egy élesebb és kvantitatív becslést is kaphatunk.

A halmazok additív tulajdonságait felhasználva következtethetünk a karakterösszegeink a nagyságára.

Itt a következő eredményem említeném meg ([HE12]):

Tétel (Hegyvári) *Legyen $\varepsilon > 0$, c_1, c_2 pozitív valós számok, $p > p(\varepsilon, c_1, c_2)$, prímszám, $A_1, A_2, A_3, \ldots A_n \subseteq \mathbb{F}_p, n \geq 3$. Tegyük fel, hogy $i = 2, 3$ esetén $|A_i| \geq c_i\sqrt{p} > 0$, továbbá, hogy*

$$|A_i - A_i| \leq 8c_i^2|A_i|, \tag{4.4.1}$$

és

$$0 < \alpha \leq \frac{\ln\{|A_1|/(|A_2||A_3|)^{13/8+\varepsilon}\}}{2\ln p} + 5/8. \tag{4.4.2}$$

Ekkor

$$|S| := \Big| \sum_{x_1 \in A_1, x_2 \in A_2, \ldots, x_n \in A_n} e(x_1 \cdots x_n) \Big| < p^{-\alpha} \cdot \prod_{i=1}^{n} |A_i|.$$

E tételből leolvashatjuk:

Következmény:
Legyen $|A_2|, |A_3| \asymp \sqrt{p}$, $|A_1| > p^{\eta}$, $\eta > 3/8$ *és tegyük fel* (4.4.1)*-t. Ekkor*

$$|S| := \Big| \sum_{x_1 \in A_1, x_2 \in A_2, \ldots, x_n \in A_n} e(x_1 \cdots x_n) \Big| < p^{-\alpha} \cdot \prod_{i=1}^{n} |A_i|,$$

ahol $0 < \alpha < \frac{\ln |A_1|}{2 \ln p} - \frac{3}{16}$.

0.4.5. Struktúra tételek Heisenberg csoportokban

E pontban prímtest feletti Heisenberg csoport ú.n. tégláinak szorzathalmazára mondunk ki struktúra tételeket. Az irodalomban az általános Lie-típusú csoportok bizonyos halmazainak szorzathalmazai expander tulajdonsága ismert. Struktúra tételek nem ismertek.

Legyen $A \subseteq H_n$ és e halmaz vetületei az egyes koordinátákra $X_1, X_2, \ldots, X_n$, $Y_1, Y_2, \ldots, Y_n$ és Z, azaz $[\underline{x}, \underline{y}, z] \in A$, $\underline{x} = (x_1, x_2, \ldots, x_n), \underline{y} = (y_1, y_2, \ldots, y_n)$, akkor és csak akkor, ha $x_i \in X_i$, $y_i \in Y_i$, $i = 1, \ldots, n$, $z \in Z$.

E részhalmazt téglának nevezünk, ha

$$A = [\underline{X}, \underline{Y}, Z] := \{[\underline{x}, \underline{y}, z] \text{ úgy, hogy } \underline{x} \in \underline{X},\ \underline{y} \in \underline{Y},\ z \in Z\}$$

ahol $\underline{X} = X_1 \times \cdots \times X_n$ és $\underline{Y} = Y_1 \times \cdots \times Y_n$ bármely nem üres $X_i, Y_i \subset \mathbb{F}_p^*$ részhalmazokkal.

Az n dimenziós esetben a következő struktúra tétel igaz ([HH13]):

Tétel (Hegyvári, Hennecart) *Bármely pozitív* $\varepsilon > 0$ *számhoz található olyan* n_0 *index, melyre ha* $n \geq n_0$, $B \subseteq H_n$ *egy tégla és*

$$|B| > |H_n|^{3/4+\varepsilon}$$

akkor létezik egy nem triviális G részcsoport H_n-ben, nevezetesen $[\underline{0}, \underline{0}, \mathbb{F}_p]$ úgy, hogy $B \cdot B$ legalább $|B|/p$ mellékosztályt tartalmaz modulo G.

E tétel bizonyításában a fő lépés diszkrét Fourier analízis használatával történi, amit pl. [He09]-ben is jól lehetett használni.

Másfelöl igaz a következő:

Propozíció (Hegyvári, Hennecart) *Bármely n természetes és p prímszámhoz létezik $B \subseteq H_n$ tégla úgy, hogy*

$$|B| \geq \frac{\sqrt{p}}{4(2n)^n}|H_n|^{1/2}$$

és a $B \cdot B$-ben található mellékosztályok csak a H_n triviális részcsoportja szerinti mellékosztályok.

Irodalomjegyzék

Az értekezés alapját képező cikkek listája:

[H97] N. Hegyvári, On the dimension of the Hilbert cubes. J. Number Theory 77 (1999), no. 2, 326–330.

[HS99] N. Hegyvári, A. Sárközy, On Hilbert cubes in certain sets. Ramanujan J. 3 (1999), no. 3, 303–314.

[He00] N. Hegyvári, On the representation of integers as sums of distinct terms from a fixed set Acta Arith. 92.2 2000. 99-104

[HN] N. Hegyvári, Note on difference sets in $\mathbb{Z}^n$ (Period. Math. Hungar. Vol 44 (2), 2002, pp. 183-185

[He04] N. Hegyvári, On Combinatorial Cubes, The Ramanujan Journal, 2004, Volume 8, Issue 3, pp 303-307

[He05] N. Hegyvári, On intersecting properties of partitions of integers, Combin. Probab. Comput. (14) 03, (2005), 319-323

[HH07] N. Hegyvári, F. Hennecart, On Monochromatic sums of squares and primes, Journal of Number Theory, Volume 124, Issue 2, 2007, Pages 314-324

[He08] N. Hegyvári, Additive Structure of Difference Sets, seminar Advanced Courses in Mathematics CRM Barcelona, Thematic Seminars Chapter 4 p 253-265

[He08c] N. Hegyvári, IP sets, Hilbert cubes, Publ. Math. Debrecen 72/1-2 (2008), 45-53

[He08b] N. Hegyvári, On additive and multiplicative Hilbert cubes Journal of Combinatorial Theory, Series A 115 (2008) 354-360

[He09] N. Hegyvári,On sum-product bases, Ramanujan J. (2009) 19:p 1-8

[HH13] N. Hegyvári, F. Hennecart, A structure result for bricks in Heisenberg groups (with F. Hennecart), Journal of Number Theory 133 (2013) 2999-3006

[HR16] N. Hegyvári, I.Z. Ruzsa, Additive Structure of Difference Sets and a Theorem of Følner, Australasian J. of Combinatorics Volume 64(3) (2016), Pages 437-443

[HH09] N. Hegyvári, F. Hennecart, Explicit Constructions of Extractors and Expanders Acta Arith. 140 (2009), 233-249.

[HE12] N. Hegyvári, Some Remarks on Multilinear Exponential Sums with an Application, Journal of Number Theory Volume 132, Issue 1, January 2012, Pages 94-102

[HE16] N. Hegyvári, Note on character sums of Hilbert cubes, Journal of Number Theory Volume 160: pp. 526-535. (2016)

[HHP] N. Hegyvári, F. Hennecart and A. Plagne, Answer to the Burr-Erdős question on restricted addition and further results, Combinatorics, Probability and Computing, Volume 16, Issue 05, Sep 2007, pp 747-756

[HHP2] N. Hegyvári, F. Hennecart and A. Plagne, A proof of two Erdős' conjectures on restricted addition and further results, J. reine angew. Math. (Crelle) 560 (2003), 199-220

Az értekezésben foglaltakhoz kapcsolódó cikkek listája:

[AI90] M. Ajtai, H. Iwaniec, J. Komlós, J. Pintz, and E. Szemerédi: Construction of a thin set with small Fourier coefficients, Bull. London Math. Soc. **22** (1990) 583-590

[AR14] P. Akhilesh, D. S. Ramana, A chromatic version of Lagrange's four squares theorem, Monatshefte für Mathematik, May 2014

[Be85] V. Bergelson, Sets of reccurence of $\mathbb{Z}^m$-actions and properties of sets of differences, *J. London Math. Soc.* (2) 31 (1985), 295–304

[Be97]Be97 V. Bergelson, P. Erdős, N. Hindman, T. uczak, Dense difference sets and their combinatorial structure. The mathematics of Paul Erdős, I, 165-175, Algorithms Combin., 13, Springer, Berlin, 1997.

[Bou05] Bourgain, J., More on the sum-product phenomenon in prime fields and its application, Int. J. of Number Theory **1** (2005), 1–32.

[BKT04] Bourgain J., Katz N. and Tao T., A sum-product theorem in finite fields and application, Geom. Funct. Anal. 14 (2004), 27–57.

[B09b] J. Bourgain, Multilinear Exponential Sums in Prime Fields Under Optimal Entropy Condition on the Source, GAFA Vol 18 (2009) 1477-1502

[B59] B.J. Birch: Note on a problem of Erdős, Proc. Camb. Philos. Soc. 55 (1959), p. 370-373

[BEF90] T.C. Brown, P. Erdős and A. Freedman Quasi-progressions and descending waves, J. of Combinatorial Theory, Series A, Volume 53, Issue 1, 1990, Pages 81-95

[Ca60] J. W. Cassels: On the representation of integers as the sums of distinct summands taken from a fixed set, Acta Sci. Math. 21 (1960), p.111-124

[GRS] R. L. Graham, B. L. Rothschild, J. H. Spencer, Ramsey Theory, Wiley 1980

[Ch16] Guohua Chen, On monochromatic sums of squares of primes, Journal of Number Theory Volume 162 2016, Pages 180-189

[DE12] R. Dietmann and C. Elsholtz: Hilbert cubes in progression-free sets and in the set of squares, Israel J.of Math. (2012),

[DE15] R. Dietmann and C. Elsholtz: Hilbert cubes in arithmetic sets, Revista Matemática Iberoamericana, Vol 31, Issue 4, 2015, pp. 1477-1498

[CFS14] D. Conlon, J. Fox, B. Sudakov: Short Proofs of Some Extremal Results, Combinatorics, Probability and Computing, Volume 23, Issue 1 2014, pp. 8-28 DOI: http://dx.doi.org/10.1017/S0963548313000448

[ER00] G. Elekes and L. Rónyai. A combinatorial problem on polynomials and rational functions. Journal of Combinatorial Theory, Series A, 89:1–20, 2000

[EP62] P. Erdős, On the Representation of Integers as Sums of Distinct Summands taken from a Fixed Set, Acta Arithmetica , Vol. VII (1962), pp. 345-354.

[EG80] P. Erdős, R. Graham: Old a new problems and results in combinatorial number theory, Monogr. Enseign. Math. 28, (1980)

[E98] P. Erdős: Some of my new and almost new problems and results in combinatorial number theory, In Number Theory, de Gruyter, pp 169-180

[Ga10] M. Garaev: Sums and products of sets and estimates of rational trigonometric sums in fields of prime order, Russian Math. Surveys 65:4 599-658 2010

[HI] D. Hilbert, Über die irreducibilität ganzer rationaler Functionen mit ganzzahligen Koeflizienten, J. Reine Angew. Math. 110 (1982), 104-129.

[CFH] Y.G. Chen és J-H Fang and N. Hegyvári, Ont the subset sums of exponential type sequences, Acta Arithmetca 173 no.2 p.141-150

[HH12] N. Hegyvári, F. Hennecart, A Note on Freiman models in Heisenberg groups Israel Journal, 2012, Volume 189, Issue 1, pp 397-411

[HR] N. Hegyvári, G. Rauzy, On the completeness of certain sequences. Publ. Math. Debrecen 55 (1999), no. 3-4, 245–252.

[Hin79] N. Hindman: Ultrafilters and combinatorial number theory. Number theory, Carbondale 1979 (Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979), pp. 119–184, Lecture Notes in Math., 751, Springer, Berlin, 1979.

[KA] A. A. Karatsuba: An Estimate of the L_1-Norm of an Exponential Sum, *Mathematical Notes*, **64**, (3), 1998 401-404

[Ra68] R. Raimi, Translation properties of finite partitions of the positive integers, Fund. Math. 61 (1968) 253-256.

[RR01] O. Ramaré, I.Z. Ruzsa, Additive properties of dense subsets of sifted sequences, J. Théor. Nombres Bordeaux 13 (2001) p.557-581.

[RR12] D. S. Ramana, O. Ramaré, Additive energy of dense sets of primes and monochromatic sums Israel Journal of Math, (2014), Volume 199, Issue 2, pp 955-974,

[CSS] Sándor, Csaba Non-degenerate Hilbert cubes in random sets. J. Théor. Nombres Bordeaux 19 (2007), no. 1, 249-261

[S01] A. Sárközy, Unsolved problems in number theory, Period. Math. Hungar. 42 (2001), p. 17-35

[S05] Sárközy, A., On sums and products of residues modulo p, Acta Arith. 118 (2005), 403-409.

[SH08] I. Shparlinski: On the solvability of bilinear equations in finite fields, Glasgow Math. J. 2008. v. 50 p. 523-539

[SZV] Szemerédi, E.; Vu, V. H. Finite and infinite arithmetic progressions in sumsets. Ann. of Math. (2) 163 (2006), no. 1, 1–35.

[Ta14] T. Tao: Expanding Polynomials over finite fileds of large characteristic, and a regularity lemma for definable sets, Contrib. Disc. Math. Vol. 10. n. 1 p 22-98

[VI11] Vinh, L.A.; Szemeredi-Trotter type theorem and sum-product estimate in finite fields, European J. Combin. 32 (2011), 1177–1181.

[W04] Woods, Alan R. Subset sum „cubes" and the complexity of primality testing. Theoret. Comput. Sci. 322 (2004), no. 1, 203–219.