Eötvös Loránd Tudományegyetem
Természettudományi Kar

Dolecsek Máté

Matematikus MSc

Véges halmazok additív és multiplikatív felbontása F_p-ben

Szakdolgozat

Témavezető:

Gyarmati Katalin egyetemi docens, Sárközy András Professor Emeritus

Algebra és Számelmélet Tanszék

Budapest, 2015

Köszönetnyilvánítás

Ezúton szeretnék köszönetet mondani témavezetőimnek, Gyarmati Katalinnak és Sárközy Andrásnak az érdekes témafelvetésért, a konzultációkért és a sok segítségért, ami nélkül ez a szakdolgozat nem készülhetett volna el.

Tartalomjegyzék

Bevezető

A következő definíciókat 1948-ban H. H. Ostmann vezette be és vizsgálta őket a nem negatív egész számok körében.

Definíció: Legyen G egy additív félcsoport és A, B_1,...,B_k részhalmazai G-nek , úgy hogy $|B_i| \geq 2 \ \forall i = 1, 2, ..., k$. Ha $A = B_1 + B_2 + ... + B_k$ akkor azt mondjuk, hogy ez egy additív k-felbontása A-nak, ha pedig $A = B_1 * B_2 * ... * B_k$, akkor ezt A egy multiplikatív k-felbontásának nevezzük.

Definíció: Egy nemnegatív egészekből álló véges, vagy végtelen C halmazt reducibilisnek nevezünk, ha létezik additív 2-felbontása, azaz $C = A + B$, ahol $|A| \geq 2$ $|B| \geq 2$. Ha nem létezik ilyen felbontás, akkor C-t primitívnek nevezzük.

Számos szép eredmény született végtelen halmazok esetében, majd Sárközy András elkezdte vizsgálni a véges esetet is a modulo p (p prím) maradékosztályok additív, illetve multiplikatív csoportjában. Alon, Granville és Ubis bizonyították, hogy F_p-nek kevesebb, mint $(1,9602)^{p+o(p)}$ darab reducibilis részhalmaza van. A szakdolgozat ebbe a témakörbe ad betekintést főleg Gyarmati Katalin és Sárközy András munkásságán keresztül.

1. Primitív halmazok F_p-ben

1.1. Tétel (K. Gyarmati, A. Sárközy): Legyen $A = \{a_1, ..., a_t\} \subset F_p$. Tegyük fel, hogy léteznek olyan $1 \leq i < j \leq t$ indexek, hogy

$$a_i + a_j - a_k \notin A \quad \forall \text{k-ra, melyre } 1 \leq k \leq t \text{ és } k \neq i, k \neq j \tag{1.1}$$

és

$$a_i - a_j + a_k \notin A \quad \forall \text{k-ra, melyre } 1 \leq k \leq t \text{ és } k \neq j. \tag{1.2}$$

Ekkor A primitív.

Bizonyítás: Tegyük fel indirekt, hogy A teljesíti a feltételeket, de nem irreducibilis, azaz léteznek $B \subset F_p$ és $C \subset F_p$ részhalmazok, hogy

$$A = B + C, \quad |B| \geq 2, \quad |C| \geq 2. \tag{1.3}$$

Vagyis $a_i \in A$ és $a_j \in A$ elemekre (1.3) szerint létezik $b_u \in B$, $b_v \in B$, $c_x \in C$, $c_y \in C$, hogy

$$a_i = b_u + c_x \tag{1.4}$$

és

$$a_j = b_v + c_y. \tag{1.5}$$

Két eset lehetséges.

1. eset: Tegyük fel, hogy $b_u \neq b_v$ és $c_x \neq c_y$. Ekkor (1.3), (1.4) és (1.5) miatt

$$a_i + a_j = (b_u + c_x) + (b_v + c_y) = (b_u + c_y) + (b_v + c_x) = a_r + a_s \tag{1.6}$$

$a_r \in A$, $a_s \in A$. $c_x \neq c_y$ és (1.4) miatt $a_i \neq a_r$, illetve $b_u \neq b_v$ és (1.5) miatt $a_j \neq a_r$, vagyis (1.6)-ból kapjuk, hogy $a_i + a_j - a_r = a_s \in A$, ami ellentmond a feltételnek.

2. eset: Tegyük fel, hogy

$$b_u = b_v. \tag{1.7}$$

Ekkor (1.5) a következő alakban írható $a_j = b_u + c_y$. Mivel $|B| \geq 2$, így létezik $b \in B$ hogy

$$b \neq b_u. \tag{1.8}$$

Tehát (1.3) miatt

$$a_p = b + c_x \in A \tag{1.9}$$

és

$$a_q = b + c_y \in A. \tag{1.10}$$

(1.4), (1.5), (1.7), (1.9) és (1.10)-ből következik, hogy

$$a_i - a_j = (b_u - b_v) + (c_x - c_y) = c_x - c_y = a_p - a_q$$

ezért

$$a_i - a_j + a_q = a_p \in A \tag{1.11}$$

ahol (1.5), (1.7), (1.8) és (1.10) miatt

$$a_q = b + c_y \neq b_u + c_y = b_v + c_y = a_j. \tag{1.12}$$

Ekkor (1.11) ellentmond (1.2)-nek. A $c_x = c_y$ eset hasonló gondolatmenettel bizonyítható. □

1.2. Következmény: Ha $p = 4k + 1$ alakú prím és $A \subset F_p$, melyre $A = \{0, 1\} \cup \{a \in F_p : (\frac{a}{p}) = 1, (\frac{a-1}{p}) = -1, a \neq -1, a \neq 2\}$, akkor A primitív.

Bizonyítás: Az A halmaz konstrukciója miatt $0 \in A$ és $1 \in A$. Megmutatjuk, hogy az (1.1) tétel feltételei teljesülnek az $a_i = 0$ és $a_j = 1$ választásokkal, vagyis

$$1 - a_k \notin A, \forall a_k \neq 0, 1 \tag{1.13}$$

és

$$a_k - 1 \notin A, \forall a_k \neq 1. \tag{1.14}$$

Nézzük először (1.13)-t. Ha $a_k \in A$ és $a_k \neq 0$ és $a_k \neq 1$, akkor $(\frac{a_k}{p}) = 1$ és $(\frac{a_k-1}{p}) = -1$. Mivel $p = 4k + 1$ alakú prím, így

$$(\tfrac{1-a_k}{p}) = (\tfrac{-1}{p})(\tfrac{1-a_k}{p}) = (\tfrac{a_k-1}{p}) = -1.$$

Így az A definíciójából következik, hogy $1 - a_k \in A$ akkor áll fenn, ha $1 - a_k = 0$, vagy $1 - a_k = 1$, vagyis $a_k = 1$, vagy $a_k = 0$. De feltettük, hogy $a_k \neq 0, 1$, ezért (1.13) teljesül.
Nézzük (1.14)-t. Ha $a_k \in A$ és $a_k \neq 1$, akkor vagy $(\frac{a_k-1}{p}) = -1$, vagyis

$-1 + a_k \notin A$ vagy $a_k = 0$, ezért $-1 + a_k = -1$, ami megint azt jelenti, hogy teljesül a feltétel. □

1.3. Következmény: Ha $A = \{x_1, x_2, ..., x_t\} \subset F_p$ egy Sidon sorozat, akkor A primitív. (Egy $A = \{x_1, x_2, ..., x_t\}$ sorozat Sidon-sorozat, ha az $a_i + a_j$ összegek különbözőek minden $1 \leq i < j \leq t$ esetén)

Bizonyítás: Ha $|A| = 1$, vagy $|A| = 2$, akkor A primitív. Ha $|A| > 2$, akkor a_i-t és a_j-t az (1.1) tételben válasszuk úgy, hogy $a_i = a_1$ és $a_j = a_2$. Ekkor az (1.1) tételben leírt (1.1) és (1.2) feltételek teljesülnek a Sidon-sorozat definíciója miatt. □

1.4. Tétel (K. Gyarmati, A. Sárközy): Ha $A \subset F_p$ és

$$A = \{0\} \cup A_0, \text{ ahol } A_0 \subset (\tfrac{p}{3}, \tfrac{2p}{3}) \tag{1.15}$$

és

$$|A| > 4, \tag{1.16}$$

akkor A primitív.

Bizonyítás: Tegyük fel, hogy A teljesíti az (1.15) feltételt, de reducibilis, vagyis léteznek $B \subset F_p$ és $C \subset F_p$ részhalmazok, hogy

$$A = B + C, \text{hogy } |B| \geq 2 \text{ és } |C| \geq 2. \tag{1.17}$$

Mivel $0 \in A$, ezért (1.16) miatt létezik $b_0 \in B$ és $c_0 \in C$, hogy

$$0 = b_0 + c_0.$$

Legyen $B' = B + \{-b_0\}$ és $C' = C + \{-c_0\}$ és így $0 \in B'$ és $0 \in C'$. Ezért (1.17) miatt

$$B' + C' = B + C = A, \quad |B'| = |B| \geq 2, \quad |C'| = |C| \geq 2. \tag{1.18}$$

Legyen $B' = \{0, b'_1, b'_2, ...b'_r\}$ és $C' = \{0, c'_1, c'_2, ..., c'_s\}$, ahol

$$0 < b'_1 < b'_2 < ... < b'_r < p \quad \text{és} \quad 0 < c'_1 < c'_2 < ... < c'_s < p, \tag{1.19}$$

és $r \geq 1$, $s \geq 1$, illetve (1.16) és (1.18) miatt

$$(r+1)(s+1) = |B'||C'| \geq |A| > 4.$$

Ebből következik, hogy

$$r \geq 2, \tag{1.20}$$

vagy $s \geq 2$ teljesül. Feltehetjük, hogy (1.20) teljesül. Ekkor (1.18) és (1.19)-ből azt kapjuk, hogy

$$b'_i = b'_i + 0 \in B' + C' = A,\ 0 < b'_i < p \tag{1.21}$$

$i = 1, 2, ...r$ esetén és

$$c'_1 = c'_1 + 0 \in B' + C' = A,\ 0 < c'_1 < p. \tag{1.22}$$

Az A konstrukciója miatt (1.21) és (1.22)-ből következik, hogy

$$\frac{2p}{3} < b'_i + c'_1 < \frac{4p}{3}, \tag{1.23}$$

és (1.18) miatt pedig

$$b'_i + c'_1 \in B' + C' = A. \tag{1.24}$$

De szintén A konstrukciójából adódik, hogy csak egy elem van a $(\frac{2p}{3}, \frac{4p}{3})$ intervallumban, nevezetesen p, de ekkor (1.23) és (1.24)-ből

$$b'_i + c'_1 = 0 \quad i = 1, 2, ..., r.$$

Vagyis (1.20)-ból $i = 1$ és $i = 2$-re kapjuk, hogy

$$b'_1 + c'_1 = b'_2 + c'_1,$$

tehát $b'_1 = b'_2$, ami ellentmond (1.19)-nek. □

1.5. Tétel (K. Gyarmati, A. Sárközy): Legyen $A \subset F_p$ és $d \in F_p^*$-re az $a - a' = d,\ a, a' \in A$ megoldás számát jelölje $f(A, d)$. Ha

$$\max_{d \in F_p^*} f(A, d) < |A|^{\frac{1}{2}}, \tag{1.25}$$

akkor A primitív.

Bizonyítás: Tegyük fel, hogy léteznek olyan $B \subset F_p$ és $C \subset F_p$ halmazok, hogy

$$A = B + C \text{ és } |B| \geq 2, |C| \geq 2 \tag{1.26}$$

fennáll. Feltehetjük, hogy

$$|B| \geq |C|. \tag{1.27}$$

(1.26) és (1.27)-ből kapjuk, hogy

$$|A| = |B + C| \leq |((b, c) : b \in B, c \in C)| = |B||C| \leq |B|^2,$$

így

$$|A|^{\frac{1}{2}} \leq |B|. \tag{1.28}$$

(1.25) és (1.28)-ból következik, hogy

$$\max_{d \in F_p^*} f(A, d) < |B|. \tag{1.29}$$

Legyen c és c' két C-beli különböző elem. Így (1.26) miatt minden $b \in B$-re $a = b + c \in A$ és $a' = b + c' \in A$. Erre az (a, a') párra, kapjuk, hogy

$$a - a' = (b + c) - (b + c') = c - c' \tag{1.30}$$

és különböző b-re különböző megoldásokat kapunk. Vagyis az (1.30) megoldások száma legalább akkora, mint a B halmaz elemszáma:

$$f(A, c - c') \geq |B|. \tag{1.31}$$

$c \neq c'$-re $c - c' \neq 0$, így (1.30) ellentmond (1.29)-nek. □

1.6. Tétel (K. Gyarmati, A. Sárközy): Ha k_0 elég nagy és k olyan pozitív egész, hogy

$$k_0 < k < \tfrac{1}{2} p^{\frac{1}{4}}, \tag{1.32}$$

akkor létezik egy $A \subset F_p$, hogy

$$|A| = k^2, \tag{1.33}$$

$$\max_{d \in F_p^*} f(A, d) = |A|^{\frac{1}{2}} \tag{1.34}$$

és A reducibilis.

Bizonyítás: Legyen $m = 2k^2$. Az $\{1, 2, ..., N\}$ halmazból kiválasztható maximális Sidon sorozat számossága $(1 + o(1))N^{\frac{1}{2}}$. Ezért elég nagy k-ra létezik egy Sidon-sorozat

$$B = \{b_1, b_2, ..., b_k\} \subset \{1, 2, ..., m - 1\} \text{ és } |B| = k (= (\tfrac{m}{2})^{\frac{1}{2}}). \tag{1.35}$$

Legyen $C = \{c_1, c_2, ..., c_k\} = \{2mb_1, 2mb_2, ...2mb_k\}$ és

$$A = B + C. \tag{1.36}$$

Ekkor A reducibilis és minden $a \in A$ a következő alakban írható

$$a = b_i + c_j = b_i + 2mb_j, \quad i, j \in \{1, 2, ..., k\} \tag{1.37}$$

és (1.32) miatt

$$0 < b_i < m, \quad 0 < b_j < m \quad \text{és}$$

$$0 < b_i + 2mb_j < m + 2m(m-1) < 2m^2 = 8k^4 < \tfrac{p}{2}. \tag{1.38}$$

(1.37) és (1.38) egyértelműen meghatározzák b_i-t és c_j-t , ezért

$$|A| = |B + C| = |B||C| = k^2 \tag{1.39}$$

és ez bizonyítja (1.33)-t. Legyen $d \in F_p^*$ olyan, hogy $f(A, d) > 0$, vagyis létezik $a, a' \in A$, hogy $a - a' = d$. Legyen a és a' (1.37) alakú. Ekkor

$$d = a - a' = (b_{i_1} - b_{i_2}) + 2m(b_{j_1} - b_{j_2}) = u + 2mv, \tag{1.40}$$

ahol

$$0 \leq |b_{i_1} - b_{i_2}| = |u| < m \tag{1.41}$$

és

$$0 \leq |b_{j_1} - b_{j_2}| = |v| < m \tag{1.42}$$

és (1.32) miatt

$$|d| \leq |u| + |2mv| < m + 2m(m-1) < 2m^2 = 8k^4 < \tfrac{p}{2}. \tag{1.43}$$

(1.41), (1.42) és (1.43) miatt d u-t és v-t (1.40)-ben egyértelműen meghatározza. Ha $u = b_{i_1} - b_{i_2} \neq 0$ és $v = b_{j_1} - b_{j_2} \neq 0$ akkor B Sidon tulajdonsága miatt az (u, v) pár a b_{i_1}, b_{i_2}, b_{j_1}, b_{j_2} elemeket és így az a és a' elemeket is egyértelműen meghatározza, így $f(A, d) = 1$. Ha $u = b_{i_1} - b_{i_2} = 0$ és $v = b_{j_1} - b_{j_2} \neq 0$, akkor $i = i_1$-t k módon választhatjuk meg, míg v a j-t és j_1-t egyértelműen meghatározza, ezért (1.39) miatt

$$f(A, d) = k = |A|^{\frac{1}{2}}. \tag{1.44}$$

Hasonlóan, ha $u \neq 0$ és $v = 0$, akkor $j = j_1$-t is k módon választhatjuk meg, míg i_1 és i_2 megint egyértelműen meghatározott, vagyis (1.44) megint teljesül és ez bizonyítja (1.36)-t is. □

2. Az előző 3 kritérium összehasonlítása

Jelölje F_1, F_2 és F_3 azon F_p-beli halmazokat, melyek kielégítik az 1.1, 1.4 és 1.5 tétel feltételeit és jelölje L_1, L_2 és L_3 a legnagyobb részhalmazt, mely az F_1, F_2 és F_3-hoz tartozik.

2.1. Tétel (K. Gyarmati, A. Sárközy):
1,

$$|F_1| \geq 2^{\frac{p}{2}-O(1)} \tag{2.1}$$

és

$$L_1 = \tfrac{p}{2} + O(1) \tag{2.2}$$

2,

$$|F_2| = 2^{\frac{p}{3}+O(1)} \tag{2.3}$$

és

$$L_2 = \tfrac{p}{3} + O(1) \tag{2.4}$$

3,

$$|F_3| \leq \exp((1+o(1))p^{\frac{2}{3}}\log p) \tag{2.5}$$

és

$$L_3 \leq (1+o(1))p^{\frac{2}{3}} \tag{2.6}$$

Bizonyítás: 1, Legyen

$$B = \{b : -\tfrac{p-3}{2} \leq b \leq \tfrac{p-3}{2},\ \ 2|b,\ \ b \neq 0, 2\}.$$

Legyen $A_0 \subset B$ és vegyük az $A = A_0 \cup \{0, 1\}$ halmazt. Belátjuk, hogy az A halmaz az $a_i = 1$ és az $a_j = 0$ választással kielégíti az (1.1) és (1.2) feltételeket, vagyis $A \in F_1$. Tehát azt kell belátni, hogy

$$1 - a \notin A, \text{ha } \ a \in A \ \text{ és } \ a \neq 0, 1, \tag{2.7}$$

illetve

$$1 + a \notin A, \text{ha } \ a \in A \ \text{ és } \ a \neq 0. \tag{2.8}$$

Ha $a \in A$, $a \neq 0, 1$ $a \in A_0 \subset B$ akkor

$$-\tfrac{p-1}{2} \le 1-a, 1+a \le \tfrac{p-1}{2}$$

és a páros, így $1-a$ és $1+a$ páratlan, ezért nem elemei A_0-nak, így (2.7) és (2.8) következik. Ha $a=1$, akkor $a+1=2$, de ez se eleme A_0-nak így (2.8) ismét fennáll. Mivel $|B| = \frac{p}{2} - O(1)$, ezért $A_0 \subset B$ halmaz $2^{\frac{p}{2}-O(1)}$ módon választható ki, így (2.1) teljesül, mert $A = A_0 \cup \{0,1\}$. Legyen $A_0 = B$. Így $A = B \cup \{0,1\} \in F_1$, ez pedig ad egy alsó becslést L_1-re, vagyis

$$L_1 \ge \tfrac{p}{2} + O(1). \tag{2.9}$$

A felső becsléshez legyen a_i és a_j rögzített és jelöljük az 1.1 tétel feltételeit kielégítő halmazt A-val. Ekkor (1.2) miatt minden $c, d \in F_p$ párra, melyre $a_i + a_j - c = d$ fennáll, csak az egyik tartozhat A-ba. Legfeljebb $\frac{p+1}{2}$ ilyen pár van (beleszámítva a (c,d) párt is) és F_p minden eleme egy párhoz tartozik. Ezért $|A|$ legfeljebb $\frac{p+1}{2} + 2 = \frac{p}{2} + O(1)$ és így $L_1 \le \frac{p}{2} + O(1)$ is teljesül, ami (2.9)-cel együtt bizonyítja (2.2)-t.

2, Az (1.15) feltételt kielégítő A-k száma megegyezik azon $A_0 \subset F_p$ halmazok számával, melyre $A_0 \subset (\frac{p}{3}, \frac{2p}{3})$ fennáll, vagyis ezek száma

$$2^{\frac{2p}{3}-\frac{p}{3}+O(1)} = 2^{\frac{p}{3}-O(1)}$$

és a maximális elemszámra:

$$|A| \le |\{0\}| + |A_0| \le 1 + |\{a : \tfrac{p}{3} \le a < \tfrac{2p}{3}\}| = \tfrac{p}{3} + O(1)$$

Ebből a kettőből következik (2.3)-t és (2.4)-t.

3, Ha $A \in F_3$ akkor (1.25) teljesül, tehát

$$\sum_{d \in F_p^*} f(A,d) < \sum_{d \in F_p^*} |A|^{\frac{1}{2}} = (p-1)|A|^{\frac{1}{2}}. \tag{2.10}$$

De

$$\sum_{d \in F_p^*} f(A,d) = \sum_{d \in F_p^*} |((a,a') : a,a' \in A, a-a' = d)| =$$

$$= |\{(a,a') : a,a' \in A, a \ne a'\}| = |A|(|A|-1). \tag{2.11}$$

(2.10) és (2.11)- ből kapjuk, hogy

$$|A|^{\frac{1}{2}}(|A|-1) < p-1. \tag{2.12}$$

Tegyük fel (2.6)-tal ellentétben, hogy létezik $\epsilon > 0$, hogy végtelen sok prímre létezik $A \in F_3$, hogy

$$|A| > (1+\epsilon)p^{\frac{2}{3}}. \tag{2.13}$$

(2.12) és (2.13)-ból következik, hogy

$$(1+\epsilon)^{\frac{1}{2}}p^{\frac{1}{3}}((1+\epsilon)p^{\frac{2}{3}}-1) < p-1,$$

amiből

$$(1+\epsilon)^{\frac{3}{2}} - \frac{(1+\epsilon)^{\frac{1}{2}}}{p^{\frac{2}{3}}} < 1 - \frac{1}{p} \tag{2.14}$$

következik. De $p \to \infty$ esetén a baloldal határértéke $(1+\epsilon)^{\frac{3}{2}} > 1$, míg a jobboldal határértéke 1, így elég nagy p-re a (2.14) egyenlőtlenség nem teljesülhet és ez az ellentmondás bizonyítja (2.6)-t. (2.6)-ból következik, hogy

$$|F_3| \leq |\{A : A \subset F_p, |A| \leq L_3\}| = \sum_{k=1}^{L_3} \binom{p}{L_3} \leq$$

$$\leq p\binom{p}{L_3} = p^{L_3+1} = exp((1+o(1))p^{\frac{2}{3}}logp)$$

és ez bizonyítja (2.5)-t. □

2.2 Állítás: Elég nagy p-re az 1.1, 1.4 és 1.5 tételek függetlenek, vagyis található olyan $A \subset F_p$ halmaz, ami a három tétel közül egynek a feltételeit teljesíti, de egy másik tétel feltételeit ezek közül nem teljesíti.

Bizonyítás: Létezik sok olyan A Sidon-sorozat, hogy $A \subset (0, \frac{p}{3}$ és $|A| > 1$. Ezek a halmazok eleget tesznek az 1.5 tétel feltételeinek, de nem elégítik ki az 1.4 tétel feltételeit.

Kimutatható, hogy majdnem minden $A \subset F_p$ halmaz, melyre $|A| = [\frac{1}{2}n^{\frac{2}{3}}]$ teljesül, eleget tesz a következő egyenlőtlenségnek

$$2 \leq f(A,d) < |A|^{\frac{1}{2}} \quad \forall d \in F_p^*,$$

egy ilyen halmaz eleget tesz az 1.5 tétel feltételeinek, de nem tesz eleget az 1.1 tétel feltételeinek.

Vegyük a következő halmazt

$$A = \{0\} \cup \{a : \tfrac{p}{3} < a < \tfrac{2p}{3}\}.$$

Elég nagy p-re ez a halmaz eleget tesz az 1.4 tétel feltételeinek. Ugyanakkor, ha $a_i,\ a_j \in A$, akkor $-a_i \in A$, mert A minden elemének az ellentettjét is tartalmazza. Ha most az 1.1 tételbeli $a_k = -a_i$ elemet vesszük a_k-nak, akkor

$$a_i - a_j + a_k = a_i - a_j - a_i = -a_j \in A$$

teljesül, vagyis erre a halmazra az 1.1 tétel (1.1) feltétele nem teljesül. □

3. Adott részhalmazt tartalmazó primitív halmaz létezése

3.1 Tétel (K. Gyarmati, A. Sárközy): Legyen

$$p > 39 \tag{3.2}$$

egy prím és legyen $A \subset F_p$, hogy

$$|A| < \tfrac{1}{3} p^{\frac{2}{5}}. \tag{3.3}$$

Ekkor van olyan $x \in F_p \setminus A$ elem, hogy az $A \cup \{x\}$ halmaz primitív.

Bizonyítás: Nevezzünk egy $x \in F_p$ elemet jónak, ha $x \notin A$ és $A \cup \{x\}$ primitív, egyébként nevezzük az x-et rossznak. Azt kell megmutatni, hogy legalább egy jó elem van vagyis, hogy a rossz elemek száma kevesebb, mint p. Egy $x \in F_p$ rossz, ha

$$x \in A, \tag{3.4}$$

vagy

$$x \notin A \text{ és } A \cup \{x\} \text{ reducibilis.} \tag{3.5}$$

Jelölje B a (3.5)-t kielégítő elemek halmazát. Azt kell megmutatni, hogy

$$|A| + |B| < p. \tag{3.6}$$

A következőkben B méretét becsüljük. Ha x kielégíti (3.5)-t, akkor léteznek olyan $C, D \subset F_p$ halmazok, hogy

$$A \cup \{x\} = C + D, |C| \geq 2, |D| \geq 2; \tag{3.7}$$

feltehetjük, hogy

$$|C| \leq |D|. \tag{3.8}$$

Ekkor létezik $c_0 \in C$ és $d_0 \in D$, hogy

$$c_0 + d_0 = x. \tag{3.9}$$

(3.7)-ből következik, hogy létezik

$$c_1 \in C, \quad c_0 \neq c_1. \tag{3.10}$$

és

$$d_1 \in D, \quad d_0 \neq d_1. \tag{3.11}$$

Először tegyük fel, hogy

$$|A| \leq 3. \tag{3.12}$$

(3.9), (3.10) és (3.11)-ből következik, hogy

$$x \neq c_0 + d_1 = a_1 \in A, \tag{3.13}$$

$$x \neq c_1 + d_0 = a_2 \in A \tag{3.14}$$

és

$$c_1 + d_1 \in A \cup \{x\},$$

vagyis

$$c_1 + d_1 = a_3 \in A, \tag{3.15}$$

vagy

$$c_1 + d_1 = x. \tag{3.16}$$

Ha (3.15) teljesül akkor (3.9), (3.13) és (3.14) miatt kapjuk, hogy

$$a_1 + a_2 = (c_0 + d_1) + (c_1 + d_0) = (c_0 + d_0) + (c_1 + d_1) = x + a_3,$$

így

$$a_1 + a_2 - a_3 = x, \tag{3.17}$$

míg ha (3.16) teljesül, akkor (3.9), (3.13) és (3.14) miatt

$$a_1 + a_2 = (c_0 + d_1) + (c_1 + d_0) = (c_0 + d_0) + (c_1 + d_1) = 2x,$$

így

$$\tfrac{a_1+a_2}{2} = x \tag{3.18}$$

teljesül. (3.17)-ben az (a_1, a_2, a_3) hármasok száma legfeljebb $|A|^3$, míg (3.18)-ban az (a_1, a_2) párok száma $|A|^2$, így (3.12) miatt az x lehetséges értékeinek száma:

$$|B| \leq |A|^3 + |A|^2 \leq 27 + 9 = 36, \tag{3.19}$$

ugyanakkor (3.2), (3.12) és (3.19)-ből következik, hogy

$$|A| + |B| \leq 3 + 36 = 39$$

és (3.6) következik ebből és (3.2)-ből.

Maradt az az eset, amikor

$$|A| \geq 4. \tag{3.20}$$

Minden $d \in D$-re kapjuk, hogy

$$(d + c_1) - (d + c_0) = c_1 - c_0 (\neq 0 \text{ (3.10) miatt}).$$

$A' = A \cup \{x\}$, (3.7)-ből kapjuk, hogy $d + c_0 \in A'$ és $d + c_1 \in A'$, így $a'_0 = d + c_0$, $a'_1 = d + c_1$ és $e = c_1 - c_0$ jelölésekkel

$$a'_1 - a'_0 = (d + c_1) - (d + c_0) = c_1 - c_0 = f, \quad a'_0, a'_1 \in A \tag{3.21}$$

Ennek a megoldás halmaznak az elemszámát $f(A', f)$-vel jelöltük és minden $d \in D$ egy megoldást határoz meg, így

$$f(A', f) \geq |D|$$

adódik. (3.21)-ben az $a'_0 = x$, vagy $a'_1 = x$ értékektől eltekintve (3.21) megoldásai megoldásai az

$$a'_1 - a'_0 = f, \quad a'_0, a'_1 \in A$$

egyenletnek is és így ennek az egyenletnek legalább

$$f(A, f) \geq f(A', f) - 2 \geq |D| - 2 \tag{3.22}$$

megoldása van. Legyen F azon $f \in F_p^*$ elemek halmaza, amelyek eleget tesznek (3.22)-nek. (2.11)-hez hasonlóan kiszámolható, hogy

$$\sum_{f \in F_p^*} f(A, f) = |A|^2 - |A|. \tag{3.23}$$

Másrészt F definíciója miatt

$$\sum_{f \in F_p^*} f(A, f) \geq \sum_{f \in F} f(A, f) \geq \sum_{f \in F} (|C| - 2) = |F|(|D| - 2).$$

Ebből (3.7), (3.8) és (3.20) miatt

$$\sum_{f \in F_p^*} f(A, f) \geq |F|(|A \cup \{x\}|^{\frac{1}{2}} - 2) = |F|(|A| + 1)^{\frac{1}{2}} - 2) \geq$$

$$\geq |F|((|A| + 1)^{\frac{1}{2}} - 2\frac{(|A| + 1)^{\frac{1}{2}}}{5^{\frac{1}{2}}}) = (1 - \frac{2}{5^{\frac{1}{2}}})|F|(|A| + 1)^{\frac{1}{2}} > \frac{1}{10}|F||A|^{\frac{1}{2}}. \tag{3.24}$$

(3.23) és (3.24)-ből következik, hogy

$$|F| < 10(|A|^{\frac{3}{2}} - |A|^{\frac{1}{2}}). \tag{3.25}$$

Ha c_1 és d_0 olyan elemek F_p-ben, melyek megjelennek (3.9)-ben és (3.10)-ben, akkor (3.7), (3.9) és (3.10) miatt kapjuk, hogy $c_1 + d_0 = a \in A$. Ekkor (3.9) miatt

$$x = c_0 + d_0 = (d_0 + c_1) - (c_1 - c_0) = a - f \in B,$$

ahol $a \in A$ és $f \in F$. Itt a-hoz legfeljebb $|A|$ érték és f-hez legfeljebb $|F|$ érték tartozik, így a B elemszáma

$$|B| \leq |A||F|. \tag{3.26}$$

(3.3), (3.25) és (3.26) miatt

$$|A| + |B| \leq |A| + |A||F| < |A| + 10|A|^{\frac{5}{2}} < 11|A|^{\frac{5}{2}} < \frac{11}{3^{\frac{5}{2}}}p < p$$

Ez bizonyítja (3.6)-t $|A| \geq 4$-re is. □

A következő tételhez előbb egy lemmát bizonyítunk be.

3.2 Lemma: Legyen $p \geq 3$ egy prím és $A \subset F_p$. Tegyük fel, hogy léteznek $u, v \in F_p$ elemek, hogy

$$u \notin A + A, \;\; v \notin A - A \;\text{ és }\; \tfrac{3v+u}{2} \notin A \tag{3.27}$$

teljesül. Ekkor A-hoz hozzáadva legfeljebb két elemet $F_p \setminus A$-ból egy olyan B halmazt kapunk, amely primitív.

Bizonyítás: Legyen $A = \{a_1, a_2, ...a_s\}$. Legyen u, v olyan mint (3.27)-ben és legyen

$$a_{s+1} = \tfrac{u+v}{2} \text{ és } a_{s+2} = \tfrac{u-v}{2}.$$

Ekkor (3.27) miatt

$$a_{s+1} + a_{s+2} = u \notin A + A,$$

$$a_{s+1} - a_{s+2} = v \notin A - A,$$

$$2a_{s+1} - a_{s+2} = \tfrac{3v+u}{2} \notin A,$$

vagyis

$$a_{s+1} + a_{s+2} - a_k \notin A, \text{ ha } 1 \leq k \leq s$$

és

$$a_{s+1} - a_{s+2} + a_k \notin A, \text{ ha } 1 \leq k \leq s+1$$

Így az (1.1) tételből $i = s+1$ és $j = s+2$ választással adódik, hogy az $A \cup \{a_{s+1}, a_{s+2}\}$ halmaz primitív.

3.3 Tétel (K. Gyarmati, A. Sárközy): Legyen $p \geq 3$ egy prím és $A \subset F_p$. Ekkor kitörölve legfeljebb $\left[\frac{3+\sqrt{5}}{2}\frac{|A|^2}{p}\right]$ elemet A-ból és legfeljebb két elemet hozzáadva $F_p \setminus A$-hoz keletkezik egy B halmaz, mely primitív.

Bizonyítás: Ha $|A| \geq \frac{3-\sqrt{5}}{2}p$, akkor $\left[\frac{3+\sqrt{5}}{2}\frac{|A|^2}{p}\right] \geq |A|$ és elvéve $|A| - 1$ elemet A-ból olyan halmazt kapunk, ami csak egy elemet tartalmaz, vagyis a kapott halmaz irreducibilis.
Tegyük fel, hogy

$$|A| < \frac{3-\sqrt{5}}{2}p. \tag{3.28}$$

Először azt bizonyítjuk, hogy létezik $A' \subset A$ és egy $u \in F_p$ elem, hogy

$$u \notin A' + A' \text{ és } |A'| \geq |A| - \frac{|A|^2}{p}. \tag{3.29}$$

Legyen $d \in F_p$-re

$$h(A,d) = |\{(a,a') : a + a' = d, a, a' \in A\}|.$$

Ekkor

$$\sum_{d \in F_p} h(A,d) = \sum_{d \in F_p} \sum_{a,a' \in A, a+a'=d} 1 = \sum_{a,a' \in A} 1 = |A|^2.$$

Másrészről pedig

$$p \min_{d \in F_p} h(A,d) \leq \sum_{d \in F_p} h(A,d) = |A|^2,$$

azaz

$$\min_{d \in F_p} h(A,d) \leq \frac{|A|^2}{p}. \tag{3.30}$$

Legyen $u \in F_p$ olyan elem, hogy

$$h(A,u) = \min_{d \in F_p} h(A,d) = t. \tag{3.31}$$

és (a_1, a'_1), (a_2, a'_2),..., (a_t, a'_t) az

$$a + a' = u \quad a, a' \in A$$

egyenlet megoldásai. (3.30) és (3.31) miatt

$$t = h(A, u) \leq \frac{|A|^2}{p}.$$

Az $A' = A \setminus \{a_1, a_2, ..., a_t\}$ halmazon az $a + a' = u$ egyenlet nem oldható meg, így

$$u \notin A' + A'.$$

Ez bizonyítja (3.29)-t. Vegyünk egy olyan halmazt és egy olyan $u \in F_p$ elemet, mely teljesíti (3.29)-t. Azt bizonyítjuk, hogy létezik egy $A'' \subset A'$ halmaz és egy $v \in F_p$ elem, hogy

$$v \notin A'' - A'', \quad \frac{u+3v}{2} \notin A'' \tag{3.32}$$

és

$$|A''| \geq |A'| - \frac{1+\sqrt{5}}{2}\frac{|A|^2}{p} \geq |A| - \frac{3+\sqrt{5}}{2}\frac{|A|^2}{p}. \tag{3.33}$$

Mivel $A'' \subset A'$, ezért (3.29) miatt

$$u \notin A'' + A'' \tag{3.34}$$

teljesül. Legyen $f(A', d)$, mint az 1.5 tételben és legyen $G = \{v \in F_p : \frac{u+3v}{2} \in A'\}$. Mivel u rögzített, így

$$|G| \leq |A'| \leq |A| \tag{3.35}$$

teljesül. Továbbá

$$\sum_{d \in F_p \setminus G} f(A', d) = \sum_{d \in F_p \setminus G} \sum_{a, a' \in A,\ a - a' = d} 1 \leq$$

$$\leq \sum_{d \in F_p} \sum_{a, a' \in A,\ a - a' = d} 1 = \sum_{a, a' \in A} 1 = |A'|^2 \leq |A|^2. \tag{3.36}$$

De (3.35) és (3.36) miatt

$$(p - |A|) \min_{d \in F_p \setminus G} f(A', d) \leq (p - |G|) \min_{d \in F_p \setminus G} f(A', d) \leq \sum_{d \in F_p \setminus G} f(A', d) \leq |A|^2.$$

(3.37)

(3.28) és (3.37)-ből következik, hogy

$$\min_{d\in F_p\setminus G} f(A',d) \le \frac{|A|^2}{p-|A|} \le \frac{|A|^2}{p-\frac{3-\sqrt{5}}{2}p} \le \frac{1+\sqrt{5}}{2}\frac{|A|^2}{p}. \tag{3.38}$$

Legyen $v \in F_p \setminus G$ egy olyan elem, melyre

$$f(A',v) = \min_{d\in F_p\setminus G} f(A',d) = s \tag{3.39}$$

és (b_1, b'_1), (b_2, b'_2),..., (b_s, b'_s) a

$$b - b' = v \quad b, b' \in A$$

egyenlet megoldásai. (3.38) és (3.39) miatt

$$s = f(A',v) \le \tfrac{1+\sqrt{5}}{2}\tfrac{|A|^2}{p} \tag{3.40}$$

Az

$$A'' = A' \setminus \{b_1, b_2, ..., b_s\} \tag{3.41}$$

halmazon a $b - b' = v$ egyenlet nem oldható meg, így

$$v \notin A'' + A'' \tag{3.42}$$

$v \in F_p \setminus G$ és a G definíciója miatt $\frac{u+3v}{2} \notin A'$. Mivel $A'' \subseteq A'$ azt kapjuk, hogy

$$\tfrac{u+3v}{2} \notin A''. \tag{3.43}$$

Tehát (3.32) és (3.33) következik (3.40), (3.41), (3.42) és (3.43)-ból. Így $A'' \subset A$ egy olyan halmaz és $u, v \in F_p$ olyan elemek, melyekre

$$u \notin A'' + A'', \;\; v \notin A'' - A'', \;\; \tfrac{u+3v}{2} \notin A'' \text{ és } \; |A''| \ge |A| - \tfrac{3+\sqrt{5}}{2}\tfrac{|A|^2}{p}.$$

A 3.2 lemmát használva adódik, hogy legfeljebb két elemet hozzá adva A''-hoz $F_p \setminus A''$-ból egy primitív halmazt kapunk.

4. Összeghalmazok elemszámára vonatkozó alsó és felső becslés

4.1 Tétel (Cauchy-Davenport-Chowla tétel): Legyen p prím, $A, B \in F_p$, $|A| = k > 0$, $|B| = l > 0$. Ekkor

$$|A + B| \geq min(p, k + r - 1) \tag{4.1}$$

1. bizonyítás: Legyen p rögzített és tegyük fel, hogy van olyan A és B, amelyre (4.1) nem igaz és nevezzük rossznak az ilyen halmazpárokat. Tekintsünk egy olyan A, B rossz halmazpárt, melyre $|B| = l$ a lehető legkisebb.

1. eset: Ha $k + l - 1 > p$, akkor B-ből hagyjunk el $k + l - 1 - p(< r)$ elemet és a maradék halmazt jelöljük B'-vel. Ekkor

$$|A + B'| \leq |A + B| < min(p, k + l - 1) = p = min(p, |A| + |B'| - 1),$$

vagyis az A, B' is rossz halmazpár, de $0 < |B'| < |B|$ miatt ez ellentmond $|B|$ minimalitásának.

2. eset: Tegyük fel, hogy $k + l - 1 \leq p$. $k \geq l \geq 2$, mert $k < l$ esetén A és B szerepcseréje ellentmondana $|B|$ minimalitásának, $l = 1$ esetén pedig (4.1)-ben egyenlőség áll, azaz A és B nem lenne rossz halmazpár. Mivel $l \geq 2$ és $k + l - 1 \leq p$, ezért $k < p$ is teljesül.
Feltehetjük, hogy $0 \in B$, mert B minden eleméhez ugyanazt az értéket hozzáadva $|A|$, $|B|$ és $|A + B|$ nem változik.
Legyen $b \neq 0$ tetszőleges rögzített eleme B-nek. Ekkor $A + b = \{a + b | a \in A\} \subsetneq A$, ellenkező esetben ugyanis $A + b = A$ teljesülne, és így a két oldalon álló halmazok elemeinek összege megegyezne:

$$\sum_{a \in A} a = \sum_{a \in A} (a + b) = kb + \sum_{a \in A} a, \;\; \Rightarrow \;\; kb = 0,$$

ami $k < p$ és $b \neq 0$ miatt nem lehet.
Vagyis van olyan $a_1 \in A$ és $b_1 \in B$, hogy $a_1 + b_1 \notin A$. Legyen

$$A' = A \cup \{a_1 + b | b \in B, a_1 + b \notin A\} \text{ és } B' = \{b | a_1 + b \in A\}.$$

$|A'| = k'$ és $|B'| = l'$ esetén $k' + l' = k + l$ és $0 < l' < l$, mert $0 \in B'$, de $b_1 \notin B$. Kell még, hogy $A' + B' \subseteq A + B$. Legyen $a' + b' \in A' + B'$. Ha $a' \in A$, akkor $a' + b' \in A + B$. Ha $a' = a_1 + b$, akkor

$$a' + b' = (a_1 + b) + b' = (a_1 + b') + b \in A + B,$$

hiszen B' definíciója miatt $a_1 + b' \in A$. Ezek alapján

$$|A' + B'| \leq |A + B| < min(p, k + l - 1) = k + l - 1 = k' + l' - 1 = min(p, k' + l' - 1),$$

tehát A' és B' is rossz pár és $l' < l$, ami ellentmond $|B|$ minimalitásának, vagyis a tétel igaz.□

A 2. bizonyításhoz az Alon-féle Nullstellensatz következményét használjuk. Az Alon-féle Nullstellensatz a gyűrű elméleti Hilbert-féle nullhelytétellel mutat rokonságot és így szól: F tetszőleges test, $g_i = \prod_{s \in S_i}(X_i - s)$ $i = 1, ...n$ és $S_i \subseteq F$ adottak. Ha az f polinom eltűnik a g_i-k közös gyökein, akkor $f = \sum_{i=1}^{n} h_i g_i$ és $\forall i$-re $deg h_i \leq deg f - deg g_i$. Ennek egy következménye a következő: legyen az $f(x_1, ...x_n)$ polinom egy főtagja $\alpha x_1^{t_1} x_2^{t_2} ... x_n^{t_n}$. Legyenek $S_1, ..., S_n \subseteq F$, $\forall |S_i| > t_i$, akkor f nem tűnhet el az egész $S_1 \times S_2 \times ... \times S_n$ halmazon.

2. bizonyítás: A bizonyításban az előző következményt használjuk fel.

I. eset: $k + l > p$, ekkor minden $g \in F_p$-re $|A \cap (g - B)| \neq 0$, vagyis $\exists a = g - b$, tehát $a + b = g$.

II. eset: tegyük fel, hogy $|A + B| \leq k + l - 2$. Ekkor $A + B \subseteq C$, ahol $|C| = k + l - 2$. Nézzük a következő polinomot: $\prod_{c \in C}(x + y - c) = F(x, y)$. F eltűnik az $A \times B$ halmazon és $deg\ F = (k - 1) + (l - 1)$. Kell még, hogy $x^{k-1} y^{l-1}$ együtthatója nem nulla. Ennek a tagnak az együtthatója $\binom{k+l-2}{k-1}$, ami nem nulla, mert $k + l - 2 < p$, de ez ellentmond a következménynek.□

A 4.1 egyenlőtlenség éles, ugyanis, ha $A = \{0, 1, ..., k - 1\}$ és $B = \{0, 1, ..., r - 1\}$, akkor $k + r \leq p + 1$ esetén $A + B = \{0, 1, ..., k + r - 2\}$, tehát $|A + B| = k + r - 1$ Az $A = B$ speciális estben a 4.1 egyenlőtlenség az $|A + A| \geq min(p, 2k - 1)$ becslést adja és ez is éles az $A = \{0, 1, ...k - 1\}$ halmazt véve.

4.2 Tétel (Alon, Granville, Ubis): Legyen G egy n rendű Abel-csoport és $A \subset G$ és $|A| = k \geq 2$. Ekkor

$$\#\{A + B : B \subset G\} \leq n \min_{2 \leq l \leq k} \sum_{j=0}^{n} \binom{n}{[\frac{j}{l}]} min\{2^{n-j}, 2^{[\frac{jk}{k-l+1}]}\} \qquad (4.2)$$

Bizonyítás: Egy adott B halmazból mohón válasszunk ki elemeket a következőképpen: elsőnek választunk egy $b_1 \in B$ elemet, majd $b_2 \in B$ legyen olyan, hogy maximalizálja az

$$(A + \{b_2\}) \setminus (A + \{b_1\})$$

halmazt, majd $b_3 \in B$ legyen olyan, hogy maximalizálja az

$$(A + \{b_3\}) \setminus (A + \{b_1, b_2\})$$

halmazt és így tovább. Jelöljük B_l-lel azon b_i-k halmazát, amelyre $A + \{b_1, b_2, ..., b_i\}$ legalább l elemmel többet tartalmaz, mint $A + \{b_1, b_2, ..., b_{i-1}\}$ és tegyük fel, hogy $|B_j + A| = j$. Definíció szerint

$$l|B_l| \leq |B_j + A| = j, \text{ vagyis } |B_l| \leq [\tfrac{j}{l}]$$

Így B_l-t maximum $\sum_{i \leq [\frac{j}{l}]} \binom{n}{i}$ féleképpen választhatjuk meg. $\frac{j}{l} \leq \frac{n}{2}$, ha $l \geq 2$ és így

$$\sum_{i \leq [\frac{j}{l}]} \binom{n}{i} \leq n \binom{n}{[\frac{j}{l}]}$$

Meghatározzuk, hogy adott B_l mellett $A + B$-re hány lehetőségünk van. Mivel $B_l + A \subset B + A \subset G$, ezért az ilyen $A + B$-k száma az olyan H halmazok száma, melyekre $B_l + A \subset H \subset G$ teljesül, ami 2^{n-j}.
Legyen $C = B_l + A$ és D olyan halmaz, melyre ha $d \in D$ teljesül, akkor $r(d) \geq k + 1 - l$, ahol $r(d)$ a $c - a = d$, $c \in C$, $a \in A$ egyenlet megoldásszámát jelöli. Ha $b \in B \setminus B_l$, akkor

$$r(b) = |(b + A) \cap (B_l + A)| \geq k + 1 - l$$

és így $b \in D$ teljesül. Mivel $(B \setminus B_l) \subset D$, így legfeljebb $2^{|D|}$ darab $B \setminus B_l$ halmaz van és így legfeljebb ennyi $A + B$ alakú halmaz van. Kaptuk, hogy

$$|D|(k + 1 - l) \leq \sum_{d \in G} r(d) = |A||C| = kj$$

és így $|D| \leq \frac{kj}{k+1-l}$, ebből pedig (4.2) következik.□

4.4 Tétel (I. Z. Ruzsa): Legyen G egy nem feltétlenül kommutatív csoport és A, B, C véges részhalmazai G-nek. Ekkor

$$|A||B - C| \leq |A - B||A - C|$$

teljesül.

Bizonyítás: Legyenek $a \in A$, $b \in B - C$. Ezeket az (a, b) párokat fogjuk injektíven beleképezni az $(A - B) \times (A - C)$ halmazba. B elemei legyenek b_1, b_2,...,b_n. Egy adott (a, b) párhoz, nézzük azokat az $y \in B$, $c \in C$ elemeket, melyekre $b = y - c$ teljesül. Ekkor $y = b_i$ valamilyen i-re, legyen ez az i minimális és feleltessük meg az (a, b) párnak az $(a - y, a - c)$ párt. Vegyünk egy másik párt (a', b') és legyen $b' = y' - c'$. Ha

$$a - y = a' - y', \ a - c = a' - c'$$

teljesül, akkor kapjuk, hogy $y - c = y' - c'$, de y minimális volt, így $y = y'$, tehát $c = c'$ és $a = a'$, vagyis a leképezés injektív. □

4.5 Következmény: Ha $|A| = m$, $|3A| \leq \alpha m$, akkor

$$| - 2A + 2A| \leq \alpha^2 m$$

A következő tételhez előbb egy lemmát mondunk ki.

4.6 Lemma: Legyen $d \leq 2$ egész és $X_1, ...X_d$ tetszőleges halmazok, $B \subset X_1 \times ... \times X_d$ egy véges részhalmaza és legyen

$$B_i \subset X_1 \times ... \times X_{i-1} \times X_{i+1} \times ... \times X_d$$

projekció. Ekkor $|B|^{d-1} \leq \prod_{i=1}^{d} |B_i|$ teljesül.

Bizonyítás: A lemmát d-re szerinti indukcióval bizonyítjuk. $d = 2$-re az állítás nyilvánvaló. Legyenek a $\{b_1, b_2, ..., b_t\}$ elemek olyanok, amik előfordulnak, mint egy B-beli elem első koordinátája és particionáljuk a B halmazt az első koordináta szerint, tehát

$$B = B(b_1) \cup B(b_2) \cup ... \cup B(b_t),$$

ahol

$$B(b_i) = \{(b_i, x_2, x_3, ..., x_d) = b : b \in B\}$$

Az indukciós hipotézis miatt kapjuk, hogy

$$|B(b_i)|^{d-2} \leq |B(b_i)_2|...|B(b_i)_d|,$$

vagyis

$$|B(b_i)|^{\frac{d-2}{d-1}} \leq (|B(b_i)_2|...|B(b_i)_d|)^{\frac{1}{d-1}}$$

Triviális, hogy $|B(b_i)| \leq |B_1|$ is teljesül és ezért

$$|B(b_i)| \leq (|B(b_i)_2|...|B(b_i)_d|)^{\frac{1}{d-1}} |B_1|^{\frac{1}{d-1}}$$

Ezt és a Hölder-egyenlőtlenséget használva a következőt kapjuk:

$$|B| = \sum_{i=1}^{t} |B(b_i)| \leq |B_1|^{\frac{1}{d-1}} \sum_{i=1}^{t} (|B(b_i)_2|...|B(b_i)_d|)^{\frac{1}{d-1}} \leq$$

$$\leq |B_1|^{\frac{1}{d-1}} \prod_{j=2}^{d} (\sum_{i=1}^{t} (|B(b_i)_j|)^{\frac{1}{d-1}} = \prod_{j=1}^{d} |B_j|^{\frac{1}{d-1}}$$

és ez bizonyítja az állítást. □

4.7 Tétel (K. Gyarmati, M. Matolcsi, I. Z. Ruzsa): Legyenek A_1, A_2,...,A_k véges, nem üres részhalmazai egy kommutatív félcsoportnak.

$$S = A_1 + A_2 + ... + A_k, \quad S_i = A_1 + ... + A_{i-1} + A_{i+1} + ... + A_k$$

Ekkor $|S| \leq (\prod_{i=1}^{k} |S_i|)^{\frac{1}{k-1}}$.

Bizonyítás: Soroljuk fel az A_1, A_2, ...,A_k halmazok elemeit valamilyen sorrendben:

$$A_1 = \{c_{11}, c_{12}, ..., c_{1t_1}\}$$

$$A_2 = \{c_{21}, c_{22}, ..., c_{2t_2}\}$$

$$.$$

$$.$$

$$A_k = \{c_{k1}, c_{k2}, ..., c_{kt_k}\}$$

Minden $s \in S$-re nézzük azt az

$$s = c_{1i_1} + c_{2i_2} + ... + c_{ki_k} \quad (\in A_1 + ... + A_k)$$

felbontást, ahol az összeadandó tagok sorszáma a lexikografikus rendezés szerint minimális. Nézzük a következő függvényt: $f : S \longrightarrow A_1 \times ... \times A_k$,

$$f(s) = (c_{1i_1}, c_{2i_2}, ..., c_{ki_k}) \ \in \ A_1 \times ... \times A_k$$

Ez jól definiált és az S halmazt egy $B \subset A_1 \times ... \times A_k$ halmazba képezi úgy hogy, $|B| = |A_1 + ... + A_k|$ teljesül. A 4.6 lemmát a B halmazra alkalmazva kapjuk, hogy

$$|B|^{k-1} \leq |B_1||B_2|...|B_k|$$

teljesül. Ezért elég megmutatni, hogy

$$|B_j| \leq |A_1 + A_2 + ... + A_{j-1} + A_{j+1} + ...A_k|$$

Ez az egyenlőtlenség pedig következik abból, hogy a B_j-ben lévő elemek koordinátáinak összege különbözik. Valóban, tegyük fel, hogy $z \neq z' \in B_j$ elemekre

$$z = (c_{1i_1}, c_{2i_2}, ..., c_{j-1i_{j-1}}, c_{j+1i_{j+1}}, ..., c_{ki_k}),$$

$$z' = (c_{1i'_1}, c_{2i'_2}, ..., c_{j-1i'_{j-1}}, c_{j+1i'_{j+1}}, ..., c_{ki'_k}),$$

és

$$c_{1i_1} + c_{2i_2} + ... + c_{ki_k} = c_{1i'_1} + c_{2i'_2} + ... + c_{ki'_k}$$

Feltehetjük, hogy

$$(i_1, i_2, ..., i_{j-1}, i_{j+1}, ...i_k) < (i'_1, i'_2, ..., i'_{j-1}, i'_{j+1}, ...i'_k)$$

a lexikografikus rendezés szerint. $z' \in B_j$, ezért létezik egy $d \in A_j$ elem, hogy

$$(c_{1i'_1}, c_{2i'_2}, ..., c_{j-1i'_{j-1}}, d, c_{j+1i'_{j+1}}, ..., c_{ki'_k}) \in B.$$

Tehát létezik $u \in S$, hogy

$$u = c_{1i'_1} + c_{2i'_2} + ... + c_{j-1i'_{j-1}} + d + c_{j+1i'_{j+1}} + ... + c_{ki'_k},$$

és

$$f(u) = (c_{1i'_1}, c_{2i'_2}, ..., c_{j-1i'_{j-1}}, d, c_{j+1i'_{j+1}}, ..., c_{ki'_k}) \in B.$$

teljesül. Mivel $c_{1i_1} + c_{2i_2} + ... + c_{ki_k} = c_{1i'_1} + c_{2i'_2} + ... + c_{ki'_k}$, ezért

$$u = c_{1i_1} + c_{2i_2} + ... + c_{j-1i_{j-1}} + d + c_{j+1i_{j+1}} + ... + c_{ki_k}$$

is teljesül, azonban $d = c_{ji_j}$-re

$$(i_1, i_2, ..., i_{j-1}, i_j, i_{j+1}, ...i_k) < (i'_1, i'_2, ..., i'_{j-1}, i_j, i'_{j+1}, ...i'_k)$$

teljesül a lexikografikus rendezésben, de ekkor f definíciója miatt $f(u) \neq (c_{1i'_1}, c_{2i'_2}, ..., c_{j-1i'_{j-1}}, d, c_{j+1i'_{j+1}}, ..., c_{ki'_k})$, ami ellentmondás. Ezzel a tételt bizonyítottuk. □

5. F_p adott részhalmazának legnagyobb reducibilis részhalmaza

Ha A Sidon-sorozat, akkor minden részsorozata is Sidon-sorozat és az 1.3 következmény miatt primitív, így A-nak nincs reducibilis részhalmaza. Van olyan Sidon-sorozat F_p-ben, melynek a számossága (1+o(1))$(\frac{p}{2})^{\frac{1}{2}}$ (ezt Erdős és Turán bizonyította) Ezért van olyan $A \subset F_p$ részhalmaz, hogy $|A| > c_1 p^{\frac{1}{2}}$ és A nem tartalmaz reducibilis részhalmazt. Ugyanakkor igaz a következő tétel:

5.1 Tétel (K. Gyarmati, A. Sárközy): Ha $A \subset F_p$ olyan részhalmaz, hogy

$$|A|^2 - |A| > p - 1, \tag{5.1}$$

akkor A tartalmaz egy M reducibilis részhalmazt, melyre a következő teljesül: ha $M = B + C$, akkor

$$|M| \geq |B| \geq \tfrac{|A|^2-|A|}{p-1}, \tag{5.2}$$

$$|B| \geq 2 \tag{5.3}$$

és

$$|C| = 2. \tag{5.4}$$

Bizonyítás: Legyen $f(A,d)$, mint az 1.5 tételben, ekkor fennáll a következő:

$$\sum_{d\in F_p^*} f(A,d) = \sum_{d\in F_p^*} |\{(a,a') : a,a' \in A, a-a' = d\}| =$$

$$= |\{(a,a') : a,a' \in A, a \neq a'\}| = |A|^2 - |A|. \tag{5.5}$$

Legyen $d_0 \in F_p^*$ olyan elem, melyre $f(A,d)$ maximális: $f(A,d_0) \geq f(A,d)$, minden $d \in F_p^*$. Ekkor (5.5)-ből kapjuk, hogy

$$|A|^2 - |A| = \sum_{d\in F_p^*} f(A,d) \leq \sum_{d\in F_p^*} f(A,d_0) = (p-1)f(A,d_0)$$

vagyis

$$\tfrac{|A|^2-|A|}{p-1} \leq f(A,d_0). \tag{5.6}$$

Legyen $B = \{a' : a', a'+d_0 \in A\}$ és $C = \{0, d_0\}$. Ekkor

$$B + C = B + \{0, d_0\} = B \cup (B + \{d_0\}) \subset A,$$

így (5.6)-ból

$$|B + C| \geq |B| = |\{a' : a', a' + d_0 \in A\}| = f(A, d_0) \geq \frac{|A|^2 - |A|}{p-1}, \quad (5.7)$$

(5.3) következik (5.1) és (5.7)-ből, illetve (5.2) is fennáll. □

6. k-primitív és k-reducibilis halmazok

Definíció: Egy $A \subset F_p$ halmazt k-primitívnek nevezünk, ha minden $B \subset F_p$ olyan halmaz primitív, melyre $D(A,B) \leq k$. ($D(A,B)$ jelöli a két halmaz szimmetrikus differenciáját)

6.1 Tétel (K. Gyarmati, A. Sárközy): Legyen $A \subset F_p$ és legyen $f(A,d)$, mint az 1.5 tételben. Ha

$$\max_{d \in F_p^*} f(A,d) < \frac{|A|^{\frac{1}{2}}}{3} \tag{6.1}$$

és $k \in N$ olyan, hogy

$$k \leq \frac{|A|^{\frac{1}{2}}}{4}, \tag{6.2}$$

akkor A k-primitív.

Bizonyítás: Azt kell megmutatni, hogy minden olyan $B \subset F_p$ halmaz primitív, melyre

$$D(A,B) \leq k \tag{6.3}$$

teljesül. Az 1.5 tétel miatt elég megmutatni, hogy

$$\max_{d \in F_p^*} f(B,d) < |B|^{\frac{1}{2}}. \tag{6.4}$$

Hogy ezt megmutassuk, egy felső becslést adunk $f(B,d)$-re, vagyis az olyan (b,b') párok számára, melyekre

$$b, b' \in B \tag{6.5}$$

és

$$b - b' = d \tag{6.6}$$

teljesül, ahol $d \in F_p^*$ rögzített. Mivel $B = (A \cap B) \cup (B \setminus A)$, ezért bármely b, b' párra, mely eleget tesz az (6.5) és (6.6) feltételeknek eleget kell tennie a következő feltételek egyikének:

$$b, b' \in A \cap B \subset A, \qquad b - b' = d, \tag{6.7}$$

$$b \in B \setminus A, \qquad b' = b - d, \tag{6.8}$$

$$b' \in B \setminus A, \qquad b = b' + d. \tag{6.9}$$

(6.1) miatt a (6.7)-t kielégítő b, b' párok száma legfeljebb

$$f(A,d) < \tfrac{1}{3}|A|^{\frac{1}{2}}.$$

Sőt a (6.8)-t kielégítő b-k száma legfeljebb

$$|B \setminus A| \leq D(A,B) \leq k$$

és b egyértelműen meghatározza a $b' = b - d$ értéket, így (6.8)-nak legfeljebb k megoldása van és ugyanígy az (6.9)-nek is legfeljebb k megoldása van. Felhasználva (6.2)-t azt kapjuk, hogy

$$f(B,d) < \tfrac{1}{3}|A|^{\frac{1}{2}} + 2k \leq \tfrac{5}{6}|A|^{\frac{1}{2}}. \tag{6.10}$$

$A \subset B \cup (A \setminus B)$-ből kapjuk, hogy

$$|A| \leq |B| + |A \setminus B| \leq |B| + D(A,B),$$

amiből (6.2) és (6.3) felhasználásával

$$|B| \geq |A| - D(A,B) \geq |A| - k \geq |A| - \tfrac{1}{4}|A|^{\frac{1}{2}} \geq |A| - \tfrac{1}{4}|A| = \tfrac{3}{4}|A|. \tag{6.11}$$

(6.10) és (6.11)-ből következik, hogy

$$f(B,d) < \tfrac{5}{6}|A|^{\frac{1}{2}} \leq \tfrac{5}{6}(\tfrac{4}{3}|B|)^{\frac{1}{2}} = (\tfrac{25}{27})^{\frac{1}{2}}|B|^{\frac{1}{2}} < |B|^{\frac{1}{2}}.$$

Ebből pedig következik (6.4). □

Következmény: Ha $A \subset F_p$ Sidon-sorozat és $|A| \geq 16$ és $k = [\frac{1}{4}|A|^{\frac{1}{2}}]$ teljesül, akkor A k-primitív.

Definíció: Ha p egy prím, akkor legyen $M(p)$ a legnagyobb olyan pozitív egész, melyre létezik k-primitív halmaz F_p-ben.

6.2 Tétel (K. Gyarmati, A. Sárközy): $p \to \infty$ esetén

$$0.0029p < M(p) < \tfrac{1}{4}p. \tag{6.12}$$

Bizonyítás: Először a felső korlátot látjuk be. Legyen $K(A) = max\{k : k \in N, A \text{ } k\text{-primitív}\}$, így

$$M(p) = \max_{A \subset F_p} K(A).$$

$K(A)$ definíciójából kapjuk, hogy minden reducibilis $A' \subset F_p$ halmazra

$$D(A, A') \geq K(A) + 1,$$

vagyis

$$D(A, A') - 1 \geq K(A).$$

Vagyis a felső korlát igazolásához azt kell megmutatni, hogy minden $A \subset F_p$ részhalmazhoz van egy A' részhalmaz, hogy

$$D(A, A') - 1 < \tfrac{1}{4}p. \tag{6.13}$$

Két esetet különböztetünk meg.

1. eset:

$$|A| > 2p^{\frac{1}{2}}. \tag{6.14}$$

Ebből következik, hogy

$$|A|^2 - |A| > 4p - |A| \geq 3p > p - 1,$$

vagyis az (5.1) feltétel teljesül, ezért az 5.1 tétel alkalmazható. Legyen $B + C$ az 5.1 tételben megkapott reducibilis halmaz ott megadott felbontása és legyen $A' = B + C$. Ekkor A' reducibilis és (5.2) miatt kapjuk, hogy

$$D(A, A') = |A \setminus (B + C)| = |A| - |B + C| \leq |A| - \tfrac{|A|^2 - |A|}{p-1} = -(\tfrac{|A|}{(p-1)^{\frac{1}{2}}} - \tfrac{(p-1)^{\frac{1}{2}}}{2})^2 + \tfrac{p-1}{4} + \tfrac{|A|}{p-1} \leq \tfrac{p-1}{4} + \tfrac{p}{p-1} = \tfrac{p}{4} + 1 + (\tfrac{1}{p-1} - \tfrac{1}{4}) < \tfrac{p}{4} + 1$$

és ez bizonyítja (6.13)-t.

2. eset: tegyük fel, hogy $|A| \leq 2p^{\frac{1}{2}}$. Vegyük a következő halmazt:

$$A' = \{0,1,2\} = \{0,1\} + \{0,1\}.$$

Ekkor A' reducibilis és $p > 100$ esetén a következőt kapjuk:

$$D(A,A') = |A \setminus A'| + |A' \setminus A| \leq |A| + |A'| \leq 2p^{\frac{1}{2}} + 3 < \tfrac{p}{5} + \tfrac{p}{30} < \tfrac{p}{4}$$

és ez bizonyítja a felső korlátot ebben az esetben is. Ezzel a (6.12) felső korlátját bizonyítottuk.
Az alsó korlát bizonyításához a következő, Alon, Granville és Ubis által bizonyított tételt fogjuk felhasználni:

F_p reducibilis részhalmazainak száma kevesebb, mint $1,9602^p$, ha p elég nagy.*

A (6.12) állítással ellentétben tegyük fel, hogy

$$M(p) \leq 0.0029p \tag{6.15}$$

és legyen

$$k = [0.0029p] + 1. \tag{6.16}$$

Ekkor $M(p)$ definíciója és (6.15) miatt nincsen k-primitív $A \subset F_p$ részhalmaz erre a k-ra. Jelöljük R_p-vel F_p reducibilis részhalmazainak halmazát. Minden $A \subset F_p$ részhalmazra létezik egy $R = R(A) \subset R_p$, hogy

$$D(A,R) \leq k. \tag{6.17}$$

Rögzített $R \subset F_p$ részhalmazra legyen $A(R)$ azon $A \subset F_p$ részhalmazok halmaza, melyre (6.17) teljesül. Ha R rögzített, akkor minden $A \subset A(R)$ megkapható R-ből pontosan i darab elem megváltoztatásával, ahol $i \leq k$. Ezt az i darab elemet $\binom{p}{i}$ féleképpen tudjuk kiválasztani. Ezért azt kapjuk, hogy

$$|A(R)| = \sum_{i=0}^{k} \binom{p}{i} \leq (k+1)\binom{p}{k}. \tag{6.18}$$

Mivel minden $A \subset F_p$ részhalmazhoz van $R \in F_p$, hogy $A \in A(R)$, így (6.18) és (*) miatt kapjuk, hogy

$$2^p = |\{A : A \subset F_p\}| = |\cup_{R \in R_p} \{A : A \in A(R)\}| \leq$$

$$\leq \sum_{R \in R_p} |A(R)| \leq \sum_{R \in R_p} (k+1)\binom{p}{k} = (k+1)\binom{p}{k}|R_p| < (k+1)\binom{p}{k}1,9602^p,$$

vagyis

$$(k+1)\ \binom{p}{k} > (\frac{2}{1,9602})^p. \tag{6.19}$$

A továbbiakhoz felhasználjuk a következő lemmát, amit a Stirling formulával lehet bizonyítani.

Lemma: Legyen $0 \leq a < b$ és $\epsilon > 0$. Ekkor létezik egy pozitív szám $\delta = \delta(a, b, \epsilon)$ és egy pozitív egész $m_0(a, b, \epsilon)$, hogy ha $m \geq m_0(a, b, \epsilon)$, $|u - bm| < \delta m$ és $|v - am| < \delta m$, akkor

$$\binom{u}{v} < 2^{(bd(\frac{a}{b})+\epsilon)m}$$

teljesül, ahol $d(x) = -\frac{1}{log2}(x \log x + (1-x)\log(1-x))$, ha $0 < x < 1$ és $d(0) = d(1) = 0$.

Ekkor (6.16) miatt a lemmából ($m = u = p$, $v = k$, $a = 0,0029$, $b = 1$ választásokkal) következik, hogy $p \to \infty$ esetén

$$(k+1)\ \binom{p}{k} < 2^{(d(0,0029)+o(1))p} \tag{6.20}$$

teljesül. (6.19) és (6.20)-ból következik, hogy

$$\frac{2}{1,9062} \leq 2^{d(0,0029)},$$

vagyis

$$(\log 2)\ \mathrm{d}(0,0029) + \log 0,9801 \geq 0$$

$$\text{-}0,0029 \log 0,0029 \text{ - } 0,9971 \log 0,9971 + \log 0,9801 \geq 0. \tag{6.21}$$

Ugyanakkor egy kis számolással látható, hogy (6.21) bal oldala kisebb nullánál, ezért a (6.21) egyenlőtlenség nem állhat fenn. Ez az ellentmondás bizonyítja, hogy (6.15) sem áll fenn és ezzel kész az alsó korlát bizonyítása is. □

Emlékeztetünk, hogy egy $A \subset F_p$ halmazról akkor mondjuk, hogy k-reducibilis, ha létezik additív, vagy multiplikatív k-felbontása. Persze, ha egy halmaz k-reducibilis, akkor l-reducibilis is, minden $1 < l \leq k$ számra is. Az alábbi tételben ennek a fordítottját vizsgáljuk.

6.3 Tétel (K. Gyarmati, A. Sárközy): Legyen $p > 22$ prím és A olyan részhalmaza F_p-nek, amely

$$A = \{0, 1\} \cup A_0 \tag{6.22}$$

alakú, ahol

$$A_0 \subset [\tfrac{p}{4}, \tfrac{p}{2}), \tag{6.23}$$

$$A_0 = \cup_{j=1}^{r} \{a_j, a_j + 1, ..., a_j^{'}\}, \tag{6.24}$$

ahol $r \geq 1$, továbbá

$$a_j^{'} > a_j, \qquad j = 1, 2, ..., r \tag{6.25}$$

és

$$a_{j+1} \geq a_j^{'} + 2, \qquad j = 1, 2, ..., r - 1. \tag{6.26}$$

Ekkor A 2-reducibilis, de nem 3-reducibilis. Jelöljük G-vel azon halmazok halmazát, melyek a fent leírt alakúak. Ekkor $|G| > 2^{\frac{p}{8}-2}$

Bizonyítás: Legyen $B = \{0\} \cup (\cup_{j=1}^{r} \{a_j, a_{j+1}, ..., a_j^{'} - 1\})$. Ekkor $A = \{0, 1\} + B$ egy nem triviális felbontása A-nak. Tegyük fel, hogy A 3-reducibilis, vagyis

$$A = B + C + D \tag{6.27}$$

teljesül, ahol $|B|, |C|, |D| \geq 2$ és $B, C, D \subset F_p$. $0 \in A$ és (6.27) miatt létezik $b \in B$ és $c \in C$ és $d \in D$, hogy $0 = b + c + d$. Ekkor $B' = B - \{b\}$, $C' = C - \{c\}$, $D' = D - \{d\}$ halmazokra teljesül, hogy

$$A = B' + C' + D' \tag{6.28}$$

A-nak egy nem triviális 3-felbontása és

$$0 \in B', C', D' \tag{6.29}$$

Mivel (6.28) A-nak egy nem triviális 3-felbontása, ezért léteznek nem nulla $b' \in B'$, $c' \in C'$ és $d' \in D'$ elemek. Ekkor (6.28) és a b', c', d' nem nulla elemekre azt kapjuk, hogy

$$\{b', c', d', b'+c', b'+d', c'+d', b'+c'+d'\} \subset \{0, b'\} + \{0, c'\} + \{0, d'\} \subset B' + C' + D' = A. \tag{6.30}$$

Három esetet különböztetünk meg.

1. eset: Tegyük fel, hogy b', c' és d' közül egyik sem 1. Mivel egyik sem nulla, ezért

$$b', c', d' \in A \setminus \{0, 1\}.$$

(6.22) és (6.23) miatt

$$\tfrac{p}{4} \leq b', c', d' < \tfrac{p}{2},$$

vagyis

$$\tfrac{p}{2} \leq b'+c', b'+d', c'+d' < p. \tag{6.31}$$

(6.30) és (6.31)-ből kapjuk, hogy $b'+c', b'+d', c'+d' \in A \cap [\frac{p}{2}, p)$, de (6.22) és (6.23) miatt $A \cap [\frac{p}{2}, p)$ üres, tehát ellentmondásra jutottunk.

2. eset: Tegyük fel, hogy $b' = 1$, de c' és d' nem 1. (a többire ugyanígy megy) Ekkor a c'-re és d'-re tett feltétel miatt miatt

$$c', d' \notin \{0, 1\},$$

ezért (6.22), (6.23) és (6.30) miatt

$$c', d' \in A \setminus \{0, 1\} = A_0 \subset [\tfrac{p}{4}, \tfrac{p}{2}),$$

vagyis

$$\tfrac{p}{4} \leq c', d' < \tfrac{p}{2},$$

$$\tfrac{p}{2} \leq c'+d' < p. \tag{6.32}$$

Így (6.30) és (6.32) miatt újra kapjuk, hogy $c'+d' \in A \cap [\frac{p}{2}, p)$, ami megint ellentmondás.

3. eset: Tegyük fel, hogy b', c' és d' közül legalább két darab egyes szerepel, feltehetjük, hogy $b' = c' = 1$. Ekkor (6.30) miatt

$$b'+c' = 2 \in A.$$

Mivel $p > 9$, így

$$2 \in A \cap (1, \tfrac{p}{4}),$$

de (6.22) és (6.23) miatt $A \cap (1, \frac{p}{4})$ üres, vagyis ellentmondásra jutottunk. Mindhárom esetben ellentmondásra jutottunk, így (6.27) nem állhat fenn, vagyis A nem 3-reducibilis.

$|G| > 2^{\frac{p}{8}-2}$ igazolásához nézzük az összes nem üres

$$E_0 \subset [\tfrac{p}{4}, \tfrac{3p}{8}) \subset F_p \tag{6.33}$$

halmazt és egy ilyen E_0 halmazt írjunk fel a következőképpen:

$$E_0 = \cup_{j=1}^{r} \{e_j, e_j + 1, ..., e_j^{'}\}, \tag{6.34}$$

ahol

$$e_j' \geq e_j, \quad j = 1, 2, ...r \tag{6.35}$$

és

$$e_{j+1} \geq e_j' + 2, \quad j = 1, 2, ...r - 1. \tag{6.36}$$

Jelölje H ezen részhalmazok halmazát. Minden $E_0 \in H$ halmazhoz konstruálunk egy $A_0 = A_0(E_0)$ halmazt a következő módon. Először az a_j és a_j' elemeket definiáljuk $j = 1, 2, ...r$ esetén:

$$a_j = e_j + (j-1) \quad \text{és} \quad a_j' = e_j' + j, \quad j = 1, 2, ..., r. \tag{6.37}$$

Legyen $A_0 = A_0(E_0)$, mint (6.24)-ben és $A = A(E_0)$, mint (6.22)-ben. Ekkor (6.33), (6.34), (6.35), (6.36) és (6.37) miatt (6.24), (6.25) és (6.26) teljesül. $a \in A_0$-ra kapjuk, hogy

$$a \geq e_1 \geq \tfrac{p}{4}. \tag{6.38}$$

Sőt (6.33)-(6.37)-ből következik, hogy

$$\frac{3p}{8} > e_r' = \sum_{j=1}^{r}(e_j' - e_j) + \sum_{j=1}^{r-1}(e_{j+1} - e_j') + e_1 \geq \sum_{j=1}^{r} 0 + \sum_{j=1}^{r-1} 2 + \left[\frac{p}{4}\right] = 2(r-1) + \left[\frac{p}{4}\right]$$

vagyis $p > 22$ miatt

$$r < \frac{1}{2}(\frac{3p}{8} - \left[\frac{p}{4}\right]) + 1 \leq \frac{1}{2}(\frac{3p}{8} - \frac{p-3}{4}) + 1 < \frac{p}{8},$$

így minden $a \in A_0$-ra kapjuk, hogy

$$a \leq a'_r = e'_r + r < \frac{3p}{8} + \frac{p}{8} = \frac{p}{2}. \tag{6.39}$$

Ezért (6.23) következik (6.38) és (6.39)-ből. Tehát minden $A = A(E_0)$ halmaz eleget tesz (6.22)-(6.26)-nak, így ők elemei G-nek. Ha E_0 és E'_0 különböző elemei H-nak akkor $A(E_0) \neq A(E'_0)$, ezért $|H| = |G|$.

$$|H| = 2^{|\{n:n\in N, \frac{p}{4}\leq n<\frac{3p}{8}\}|} - 1 \geq 2^{\frac{p}{8}-1} - 1 > 2^{\frac{p}{8}-2}.$$

Vagyis $|G| > 2^{\frac{p}{8}-2}$ Ezzel kész a 6.3 tétel bizonyítása. □

A következő tételben a legnagyobb olyan k számot becsüljük, melyre F_p egy adott részhalmazának létezik k-reducibilis részhalmaza.

Definíció: Ha G egy additív csoport, $d \in N$ és y,$x_1, x_2, ...x_d$ G-nek elemei, akkor a

$$H = \{y + \sum_{i=1}^{d} \epsilon_i x_i : \ \ \epsilon_i \in \{0,1\}, \ \ i = 1,2,...d\} \tag{6.40}$$

halmazt d-dimenziós Hilbert kockának nevezzük.

6.4 Lemma: Ha $N > N_0$, $E \subset \{1,2,...,N\}$ olyan, hogy

$$|E| \geq N^{\frac{4}{5}} \tag{6.41}$$

és

$$d = [\frac{11}{10} log \frac{log(3N)}{log(3N/|E|)}], \tag{6.42}$$

akkor létezik d-dimenziós H Hilbert kocka, melyre $x_i \neq x_j$, $1 \leq i < j \leq d$ és $H \subset E$ teljesül.

6.5 Tétel (K. Gyarmati, A. Sárközy): Ha $p > p_0$ prím, $A \subset F_p$, olyan, hogy

$$|A| \geq p^{\frac{4}{5}} \tag{6.43}$$

és

$$k = [\frac{11}{10} log \frac{log(3p)}{log(3p/|A|)}], \tag{6.44}$$

akkor A-nak van k-reducibilis B részhalmaza.

Bizonyítás: Az állítás bizonyításához A minden elemét reprezentáljuk a legkisebb pozitív egésszel modulo F_p. Az így keletkezett halmazt jelöljük A'-vel. (6.43) és (6.44) miatt alkalmazhatjuk a 6.4 lemmát a $p = N$, $A' = E$ és $k = d$ szereposztással. Kapjuk, hogy létezik egy d-dimenziós Hilbert kocka H', melyre $H' \subset A'$ teljesül. Ha a maradékosztályokat y,$x_1, x_2, ...x_k$ jelöli akkor

$$H = \{y + \sum_{i=1}^{k} \epsilon_i x_i : \ \ \epsilon_i \in \{0,1\}, \ \ i = 1,2,...k\} \subset A.$$

Ha $B_1 = \{y, y + x_1\}$ és $B_i = \{0, x_i\}$, $i = 2, ..., k$, akkor $H = B_1$+B_2+...+$B_k \subset A$, tehát H egy k-reducibilis részhalmaza A-nak.□

A továbbiakban egy $B + C = R \subset A \subset F_p$ felbontásban a B és C méretét becsüljük. Ehhez először egy lemmát mondunk ki.

6.6 Lemma: Ha $D_1, D_2, ...D_t$ részhalmazai F_p-nek és $|D_1| = |D_2| = ... = |D_t| = 2$, akkor

$$|D_1 + D_2 + ... + D_t| \geq min\{t + 1, p\}$$

Bizonyítás: A Cauchy-Davenport tételből (4.1 tétel) indukcióval következik. □

6.7 Következmény: Ha $A \subset F_p$, p és k a (6.43) és (6.44) feltételeknek eleget tesznek, akkor A-nak létezik egy R reducibilis részhalmaza, hogy

$$R = B + C \tag{6.45}$$

esetén

$$\min\{|B|, |C|\} \geq [\tfrac{k}{2}] + 1 \tag{6.46}$$

Bizonyítás: (6.46) a B_i halmazok definíciójából következik. □

A következőkben a célunk, hogy a $min\{|B|, |C|\}$ számra adjunk pontosabb alsó korlátot.

Definíció: Ha a H Hilbert kocka olyan, hogy a $\sum_{i=1}^{d} \epsilon_i x_i$ ($\epsilon_i \in \{0,1\}$, $i = 1, 2, ...d$) összegek páronként különböznek, vagyis

$$|H| = |\{y + \sum_{i=1}^{d} \epsilon_i x_i : \ \ \epsilon_i \in \{0,1\} \ \ i = 1,2,...,d\}| = 2^d,$$

akkor H-t egy nem-degenerált d-dimenziós Hilbert kockának nevezzük.

6.8 Lemma: Ha $N > N_0$, $E \subset \{1, 2, ...N\}$ és (6.41) teljesül és d-t (6.42) definiálja, akkor létezik egy nem-degenerált d-dimenziós Hilbert kocka E-ben.

Bizonyítás: Megtalálható Gyarmati Katalin és Sárközy András: On reducible and primitiv subsets of F_p, II című cikkében.

6.9 Tétel (K. Gyarmati, A. Sárközy): Ha $A \subset F_p$, p és k a (6.43) és (6.44) feltételeknek eleget tesznek, akkor A-nak létezik egy R reducibilis részhalmaza, hogy

$$R = B + C \tag{6.47}$$

esetén

$$\min\{|B|, |C|\} \geq 2^{[\frac{k}{2}]} \tag{6.48}$$

Bizonyítás: A 6.8 lemma szerint A tartalmaz egy nem-degenerált d-dimenziós Hilbert kockát

$$H = \{y + \sum_{i=1}^{d} \epsilon_i x_i : \ \epsilon_i \in \{0, 1\} \ i = 1, 2, ..., d\} \subset A \tag{6.49}$$

Ekkor $B_1 = \{y, y + x_\}$, $B_i = \{0, x_i\}$ és $R = H$ halmazokra véve a $B = B_1 + B_2 + ... + B_{[\frac{k}{2}]}$ és $C = B_{[\frac{k}{2}]+1} + ... + B_{k-1} + B_k$ halmazokat kapjuk, hogy (6.47) következik H definíciójából, illetve B és C nem-degenerált Hilbert kockák $[\frac{k}{2}]$ és $k - [\frac{k}{2}] \geq [\frac{k}{2}]$ dimenziókkal, ezért elemszámuk eleget tesz a (6.48) feltételnek. □

7. Kvadratikus maradékok additív felbontása

Először bevezetünk néhány jelölést: ha G véges Abel-csoport és f, g egy G-ből C-be képező függvény, akkor $(f*g)(x) = \sum_{y\in G} f(y)g(x-y)$, jelölje χ az F_p Legendre-szimbólumát, $\langle f, g\rangle$ jelöli két komplex függvény skaláris szorzatát, $\langle f, 1\rangle = \langle f\rangle$, $\| g \|_2^2$ pedig az l_2 norma négyzete.

7.1 Tétel (A. Sárközy, Shkredov): Legyen p prím és $R \subset F_p$ kvadratikus maradékok halmaza.

$$\text{Ha } A + A = R, \text{ akkor } p = 3$$

$$\text{Ha } A \dot{+} A = R, \text{ akkor } p = 3, 7, 13,$$

ahol $A \dot{+} A = \{a + a' : \ a, a' \in A, \ a \neq a'\}$

Bizonyítás: Megtalálható Shkredov: Sumsets in quadratic residues című cikkében, itt a terjedelemre való tekintettel nem bizonyítjuk.

A következő tételhez kimondunk két lemmát, melyek a bizonyítása megtalálható Shkredov: Sumsets in quadratic residues című cikkében.

7.2 Lemma: Legyenek $g, h : F_p \longrightarrow C$ komplex függvények. Ekkor

$$|\sum_{x,y} g(x)h(y)\chi(x+y)| \leq \| g \|_2 \ (p \ \| h \|_2^2 - |\langle h\rangle|^2)^{\frac{1}{2}} \leq \| g \|_2 \ \| h \|_2 \ p^{\frac{1}{2}}$$

és

$$((g\circ\chi)\circ(h\circ\chi))(x) = p(h\circ g) - \langle g\rangle \ \langle h\rangle.$$

7.3 Lemma: Legyen c egy egész szám és $\alpha : G \longrightarrow Z$ egy függvény. Ekkor

$$\| \alpha \|_2^2 \ \geq \ \ c|\sum_x \alpha(x)| - (c-1) \ |\sum_{x:0<\alpha(x)|<c} \alpha(x)|$$

és

$$\| \alpha \|_2^2 \ = \ \ c\sum_x \alpha(x) + \sum_k |\{x : \alpha(x) = k\}|(k^2 - ck)$$

7.4 Tétel (C. Bachoc, M. Matolcsi, I. Z. Ruzsa): Legyen p prím, $R \subset F_p$ kvadratikus maradékok halmaza, $A \subset F_p$. Ha $|A - A| \subset R \cup \{0\}$ teljesül akkor:

$$p \geq |A|^2 + |A| - 1, \text{ ha } |A| \text{ páros}$$

illetve

$$p \geq |A|^2 + 2|A| - 2, \text{ ha } |A| \text{ páratlan}$$

Bizonyítás: Legyen $|A| = a$ és legyen $\epsilon(x)$ olyan függvény, melyre

$$(A * \chi)(x) = (a-1)A(x) + \epsilon(x), \tag{7.1}$$

ahol $\epsilon(x) = 0$, ha $x \in A$. A 7.2 lemma szerint

$$\| \epsilon \|_2^2 = pa - a^2 - a(a-1)^2, \quad \text{és} \quad \langle \epsilon \rangle = -a(a-1).$$

Sőt

$$\epsilon(x) = 2|R \cap (x - A)| - a \tag{7.2}$$

minden $x \notin A$ elemre. Először legyen a egy páros szám. Ekkor (7.2) szerint $\epsilon(x)$ értéke minden x-re páros ($\epsilon(x) = 0$, ha $x \in A$). A 7.3 lemmát alkalmazva $c = 2$-vel kapjuk, hogy

$$\| \epsilon \|_2^2 = pa - a^2 - a(a-1)^2 \geq 2a(a-1)$$

vagyis

$$p \geq a^2 + a - 1$$

amint állítottuk.
Tegyük fel, hogy a páratlan 1-nél nagyobb szám. $\epsilon(x) = 0$ az A halmazon, de a (7.2) formula szerint minden más x-re $\epsilon(x)$ páratlan. Először belátjuk, hogy létezik olyan $x \notin A$, melyre $\epsilon(x) \neq 1$ teljesül. Ha nem így lenne, akkor (7.1) miatt

$$\langle A, \chi \rangle = \langle \epsilon, \chi \rangle = pA(0) - a - (a-1)\langle A, \chi \rangle \tag{7.3}$$

Eltolással elérhetjük, hogy $0 \in A$ teljesüljön és így $\langle A, \chi \rangle = a - 1$. Behelyettesítve (7.3)-ba kapjuk, hogy $p = a^2$, ami ellentmondás. Legyen $p_k = |\{x \in F_p : \epsilon(x) = k\}|$, $k \in Z$. Ekkor $p_0 = a$ és $p_{2l} = 0$ minden l nem nulla egészre. A 7.3 lemma feltételét $c = -2$-re alkalmazva és felhasználva, hogy p_{-1} kisebb $\frac{p-1}{2}$-nél a következőhöz jutunk:

$$\| \epsilon \|_2^2 = pa - a^2 - a(a-1)^2 = -2\langle \epsilon \rangle + \sum_k (k^2 + 2k)p_k \geq 2a(a-1) - p_{-1} + 3 \sum_{k \neq -1,0} p_k =$$

$$= 2a(a-1) + 3p - 4p_{-1} - 3a \geq 2a(a-1) + p + 2 - 3a$$

más szóval

$$p \geq a^2 + a - 4 + \tfrac{p+2}{a}.$$

Kis számolás után kapjuk, hogy $p \geq a^2 + 2a - 2$ teljesül, feltéve, hogy $a > 1$. Ezzel kész a bizonyítás. □

Irodalomjegyzék

-Gyarmati Edit, Freud Róbert: Számelmélet

-Gyarmati Katalin, Sárközy András: On reducible and primitiv subsets of F_p, I

-Gyarmati Katalin, Sárközy András: On reducible and primitiv subsets of F_p, II

-Elekes György: Sums versus products

-Noga Alon, Andrew Granville, Adrián Ubis: The number of sumsets in a finite field

-Ruzsa Imre: Sumsets and structure

-Shkredov: Sumsets in quadratic residues