Gyarmati Katalin

Hatvány-, hatványteli és hatványmentes számok összegsorozatokban és multiplikatív struktúrákban.

Témavezető: Dr. Sárközy András

Tartalomjegyzék

1. Bevezetés

Gyakran felmerülő kérdés a számelméletben természetes számokból álló sorozatok, halmazok sűrűségének becslése. A klasszikus számelmélet a speciális sorozatok (prímszámok, négyzetszámok stb) tulajdonságait vizsgálta, míg a XX. században megkezdődött az általános sorozatok, vagyis a sűrűségi feltételekkel karakterizált sorozatok vizsgálata. Hibrid problémán olyan problémát értünk, melyben mind speciális, mind általános sorozat szerepel.

Definiáljuk az $\mathcal{A}, \mathcal{B} \subseteq \mathbb{N}$ halmazok összegét az $\mathcal{A}+\mathcal{B} = \{a+b : \ a \in \mathcal{A}, \ b \in \mathcal{B}\}$ halmazzal, és legyen $\mathcal{A} \times \mathcal{B} + 1 = \{ab+1 : \ a \in \mathcal{A}, \ b \in \mathcal{B}\}$, $\mathcal{A} \cdot \mathcal{A} + 1 = \{aa'+1 : \ a, a' \in \mathcal{A}, \ a \neq a'\}$. Ekkor $\mathcal{A} \times \mathcal{A} + 1 \neq \mathcal{A} \cdot \mathcal{A} + 1$, mivel az egyik esetben az összes $a, a' \in \mathcal{A}$-ra, a másik esetben csak a különböző $a, a' \in \mathcal{A}$ $(a \neq a')$ esetén képeztük az $aa'+1$ számokat ahhoz, hogy a halmaz elemeit megkapjuk. Dolgozatomban azokat a speciális eseteket tekintem át, amikor $\mathcal{A}+\mathcal{B}$, $\mathcal{A} \times \mathcal{B} + 1$, $\mathcal{A} \cdot \mathcal{A} + 1$ halmazok valamelyike része egy előre megadott $\mathcal{P}$ halmaznak. Ekkor $\mathcal{P}$-től függően különböző becslések adódnak az $\mathcal{A}$ és a $\mathcal{B}$ halmaz méretére. Az egyik, első ilyen jellegű megállapítás Diofantosztól származik, aki megadott egy olyan 4 elemű $\mathcal{A}$ halmazt, amelyre $\mathcal{A} \cdot \mathcal{A} + 1$ minden eleme egy racionális szám négyzete.

A következő jelöléseket fogjuk használni: Legyen a p elemű test F_p. Tetszőleges n természetes szám pozitív osztóinak számát $d(n)$-nel, különböző prímosztóinak számát $\omega(n)$-nel, a Mangoldt szimbólumot $\Lambda(n)$-nel jelöljük. $\pi(x)$ az x-et meg nem haladó prímszámok száma, míg $P(x)$ az x legnagyobb prímosztója. Multiplikatív illetve additív karakterek esetén mindig χ_0 a főkarakter. Definició szerint $e(x) \stackrel{\text{def}}{=} e^{2\pi i x}$. Tetszőleges G egyszerű gráf szögpontjainak halmazát $V(G)$, éleinek halmazát $E(G)$ jelölje. Legyen végül $K_{r,r}$ az a teljes páros gráf, melyben a két osztály elemszáma r.

2. Előzmények

Ebben a fejezetben egy rövid áttekintést, vagy inkább szemléltetést szeretnék adni a témakörben eddig elért eredményekről, tételekről.

A III. században Diofantosz talált egy racionális számokból álló 4 elemű halmazt: $\{\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{4}\}$, mely azzal a tulajdonsággal rendelkezik, hogy bármely két különböző elem szorzatához 1-et adva egy racionális szám négyzetét kapjuk. Később Fermat az egész számok körében vizsgálta a problémát, és az $\{1, 3, 8, 120\}$ halmazt adta meg az előbb említett tulajdonsággal. (Könnyen látjuk, hogy ha a halmaz elemei egész számok, akkor bármely két különböző elem szorzatához 1-et adva, nemcsak egy racionális szám négyzetét, hanem mindíg négyzetszámot is kell kapnunk.) Felmerül a kérdés létezik-e ennél több elemű $\mathcal{A}$ halmaz, melyre $\mathcal{A} \cdot \mathcal{A} + 1$ minden eleme egy racionális szám négyzete. Az egész számok körében még nem találtak ilyen, 5 elemű $\mathcal{A}$ halmazt. Viszont a racionális számok körében már három 5 elemű halmaz is van, sőt nemrég Phil Gibbs [13] egy 6 elemű halmazt adott meg: $\left\{\frac{11}{192}, \frac{35}{192}, \frac{155}{27}, \frac{512}{27}, \frac{1235}{36}, \frac{180873}{16}\right\}$. A továbbiakban csak egész számokból álló halmazokat tekintünk.

Euler bebizonyította, hogy minden két elemű $\mathcal{A}$ halmaz, a fenti tulajdonsággal, 4 tagúvá bővíthető lásd [5]. Arkin, Hoggatt, Straus [1] pedig azt, hogy ez minden 3 elemű halmazra is igaz.

Felső becslést Dujella [4] adott: Ha $\mathcal{A} \subseteq \mathbb{N}$, és $\mathcal{A} \cdot \mathcal{A} + 1$ minden eleme négyzetszám, akkor $|\mathcal{A}| \leq 9$. Később általánosította eredményét az $\mathcal{A} \cdot \mathcal{A} + n$ esetre, ekkor $\mathcal{A}$ elemszámát n függvényében becsülte [6].

Erdős [7] és Moser [32] kérdezték a probléma additív analogonját: Mit mondhatunk akkor, ha az $\mathcal{A}$ halmaz bármely két különböző elemének az összege négyzetszám? J. Lagrange [23] és Nicolas [25] talált egy ilyen 6 elemű $\mathcal{A}$ halmazt. A. Sárközy, J. Rivat, C. L. Stewart [26] igazolta azt, hogy ha $\mathcal{A} \subseteq \{1, 2, \ldots, N\}$ és rendelkezik az előbb említett tulajdonsággal, akkor $|\mathcal{A}| \ll \log N$.

A hibrid problémák témakörében, az összegsorozatokra vonatkozó eredmények közül az egyik első, nagyon szép és elemien is igazolható Erdős Pál és Turán Pál [12] tétele.

2.1. Tétel. *Létezik c pozitív állandó, hogy ha $\mathcal{A} \subseteq \mathbb{N}$ véges sorozat, akkor*

$$\omega\left(\prod_{a,a' \in \mathcal{A}} (a + a')\right) > c \log |\mathcal{A}| .$$

A most következő bizonyítás Erdős Pál és Surányi János [11]: Válogatott fejezetek a számelméletből című könyvében található.

Az alábbi kissé erősebb állítást fogjuk igazolni: *Ha $\mathcal{A}$ minden eleme pozitív egész, és $|\mathcal{A}| = 2^k + 1$, akkor*

$$\omega\left(\prod_{a,a' \in \mathcal{A}} (a + a')\right) \geq k + 1.$$

Abban, hogy a kéttagú összegek prímosztói közt sok különbözőt találjunk, az egyik fő akadály az, hogy egy összeg egy prímszám magas hatványával lehet osztható akkor is, ha az egyes összeadandókra ez nem áll. Ezért úgy próbálunk egy-egy p prímszámhoz minél több számot kiválasztani, hogy közülük kettőnek az összege p-nek ne legyen magasabb hatványával osztható, mint az összeadandók. Így várható, hogy a kettős összegeknek sok más prímosztója is lesz. Ennek a célkitűzésnek a megvalósítására egy lemmát látunk be.

Legyen adva páratlan számú különböző pozitív egész szám:

$$n_1, n_2, \ldots, n_{2\ell+1}$$

és egy p páratlan prímszám. Írjuk a számokat

$$n_i = p^{\alpha_i} q_i \quad (i = 1, 2, \ldots, 2\ell + 1)$$

alakban, ahol q_i már nem osztható p-vel. Ekkor kettőnek, mondjuk n_i-nek és n_j-nek az összege, ha $\alpha_i \leq \alpha_j$,

$$n_i + n_j = p^{\alpha_i}(q_i + p^{\alpha_j - \alpha_i} q_j).$$

Ha $\alpha_i \neq \alpha_j$, akkor a zárójelben levő összeg nem lehet p-vel osztható, ha azonban $\alpha_i = \alpha_j$, akkor gondoskodnunk kell arról, hogy $q_i + q_j$ ne legyen p-vel osztható. Ez biztosan bekövetkezik, ha vagy mindkét összeadandó $p/2$-nél kisebb maradékot ad p-vel osztva, vagy mindkettő $p/2$-nél nagyobbat. Ilyen választással a maradékok összege 0 és p közé, illetőleg p és $2p$ közé esik, a határokat már nem engedve meg, s így az összeg nem lehet p-vel osztható. A

$$q_1, q_2, \ldots, q_{2\ell+1}$$

számok maradékai közt azonban, ha p-vel osztunk (legkisebb nemnegatív maradékot véve) vagy $p/2$ alá, vagy $p/2$ fölé legalább $\ell + 1$ esik. Ezzel a következőt láttuk be:

2.2. Lemma. *Ha p páratlan prímszám, akkor $2\ell+1$ különböző pozitív egész szám közül kiválasztható $\ell+1$ úgy, hogy kettőnek az összege ne legyen p-nek magasabb hatványával osztható, mint bármelyik összeadandó.*

Ez a lemma a kulcsa a tétel bizonyításának. Legyen adva 2^k+1 különböző pozitív egész szám (ahol k legalább 1). Az ezekből képezett kéttagú összegek prímszám osztói közt szerepel a 2, mivel legalább három számunk van. Az összegek páratlan prímosztói legyenek $p_1, p_2, \ldots, p_i$. Megmutatjuk indirekt okoskodással, hogy $i \geq k$.

Tegyük fel, hogy $i < k$ volna. Alkalmazzuk ismételten a segédtételt. E-szerint a 2^k+1 szám közül kiválasztható $2^{k-1}+1$ úgy, hogy ha valamelyik kettőnek az összege osztható $p_1^{\alpha_1}$-nal, akkor mindegyik összeadandó is osztható vele. Ezek közül kiválasztható $2^{k-2}+1$ szám úgy, hogy ezen kivül teljesüljön az is, hogy ha valamelyik kettőnek az összege osztható p_2^{β}-nal, akkor az összeadandók külön-külön is oszthatók vele.

Az eljárást ismételgetve, végül kapunk $2^{k-i}+1$, tehát az indirekt feltevés szerint legalább három számot, amelyekre már $p_1, p_2, \ldots, p_i$ mindegyikét illetően teljesül a p_1-re és p_2-re kimondott tulajdonság. Legyen a megmaradt számok közül három a_1, a_2, a_3. Mivel feltettük, hogy a kéttagú összegek összes páratlan prímszám osztóit felsoroltuk, így a kettős összegek ilyen alakúak:

$$a_1 + a_2 = 2^{u_0} p_1^{u_1} p_2^{u_2} \ldots p_i^{u_i}, \quad a_1 + a_3 = 2^{v_0} p_1^{v_1} p_2^{v_2} \ldots p_i^{v_i},$$

$$a_2 + a_3 = 2^{w_0} p_1^{w_1} p_2^{w_2} \ldots p_i^{w_i}.$$

Itt a_1 és a_2 is osztható kell, hogy legyen $p_1^{u_1} p_2^{u_2} \ldots p_i^{u_i}$-nel, tehát egyik sem lehet még 2^{u_0}-nal is osztható. Az összegük azonban csak úgy lehet 2-nek magasabb hatványával osztható, mint az összeadandók, ha a 2 mindkét szám kanonikus felbontásában ugyanazon a kitevőn szerepel. Ugyanez igaz a_1-re és a_3-ra is, tehát a három szám ilyen alakú:

$$a_i = 2^t b_i, \quad i = 1, 2, 3,$$

ahol b_1, b_2 és b_3 páratlan, továbbá kettőnek az összege

$$b_1 + b_2 = 2^{r_1} p_1^{u_1} p_2^{u_2} \dots p_i^{u_i}, \quad b_1 + b_3 = 2^{r_2} p_1^{v_1} p_2^{v_2} \dots p_i^{v_i},$$
$$b_2 + b_3 = 2^{r_3} p_1^{w_1} p_2^{w_2} \dots p_i^{w_i}.$$

alakú ($r_1 = u_0 - t,\ r_2 = v_0 - t,\ r_3 = w_0 - t$). A b-kre fennáll ezenkivül, hogy pl. b_1 és b_2 osztható $p_1^{u_1} p_2^{u_2} \dots p_i^{u_i}$-nel, tehát ennél egyik sem kisebb, sőt legalább az egyik ennél nagyobb, mert a számok különbözőek.

Eszerint kell, hogy r_1 legalább 2 legyen. Ugyanígy r_2, r_3 is lagalább 2. Ennélfogva

$$b_1 + b_2 = 4x, \quad b_1 + b_3 = 4y, \quad b_2 + b_3 = 4z,$$

valamilyen x, y, z egész számokkal. Ezeket összeadva és 2-vel osztva

$$b_1 + b_2 + b_3 = 2x + 2y + 2z.$$

Ez azonban nem lehetséges, mert a baloldalon három páratlan szám összege áll, míg a jobboldal páros. Nem lehet tehát $i < k$. Ezzel a 2.1. tételt bebizonyítottuk.

Sokáig sejtés volt, hogy a tétel általánosítható két különböző sorozat esetére is. Győry, Stewart és Tijdeman [20] 1986-ban igazolta ezt a sejtést. A következőt látták be:

2.3. Tétel. *Ha* $|\mathcal{A}| \geq |\mathcal{B}| \geq 2$, *akkor*

$$\omega\left(\prod_{a\in\mathcal{A}}\prod_{b\in\mathcal{B}}(a+b)\right) > c\log|\mathcal{A}|\,.$$

A tétel multiplikatív analogonját Győry, Sárközy, Stewart [19] bizonyította tíz évvel később.

2.4. Tétel. *Ha* $|\mathcal{A}| \geq |\mathcal{B}| \geq 2$, *akkor*

$$\omega\left(\prod_{a\in\mathcal{A}}\prod_{b\in\mathcal{B}}(ab+1)\right) > c\log|\mathcal{A}|\,.$$

Ezután a 2.3 tétel bizonyítását vázoljuk, a főlemma bizonyítása nélkül, mivel az, Evertsenek egy S-egység egyenletek megoldásszámára vonatkozó mély eredményre épül. (Megjegyzem, hogy e tételre máig nem ismeretes elemi bizonyítás.)

2.5. Lemma. *Legyen* λ, μ *és* ν *pozitív egész számok,* $p_1, p_2, \ldots, p_w$ *különböző prímszámok. Ekkor a*

$$\lambda x + \mu y = \nu z$$

egyenletnek legfeljebb $3 \times 7^{2w+3}$ *olyan megoldása van* x, y, z*-ben, ahol* x, y, z *páronként relatív prímek, és mindegyik prímtényezős felbontásában csak a* $p_1, p_2, \ldots, p_w$ *számok közül szerepelnek a prímszámok.*

Legyen $b_1, b_2 \in \mathcal{B}$. Jelölje $p_1, p_2, \ldots, p_w$ azokat a prímeket, melyek osztják a

$$\prod_{a\in\mathcal{A}}\prod_{b\in\mathcal{B}}(a+b)$$

számot. Az

$$x - y = (b_1 - b_2)z$$

egyenletnek $x = a + b_1,\ y = a + b_2,\ z = 1$ megoldása minden $a \in \mathcal{A}$-ra. Mivel $a + b_1$ és $a + b_2$ minden prímosztója $p_1, p_2, \ldots, p_w$ prímszámok között van, ezért a 2.5. lemma szerint az ilyen megoldások száma legfeljebb $3 \times 7^{2w+3}$. Tehát

$$|\mathcal{A}| \leq 3 \times 7^{2w+3}.$$

Ebből $w \gg \log |\mathcal{A}|$, és ez igazolja a 2.3. tételt.

Erdős, Stewart, Tijdeman [10]-ben foglalkozott a problémával, hogy mennyire pontos ez az eredmény.

2.6. Tétel. *Legyen $0 < \varepsilon < 1$ valós szám, $f : \mathbb{R}_{>1} \to \mathbb{R}$ függvény, melyre $f(x) \to \infty$ ha $x \to \infty$. Legyen továbbá k és $2 \leq \ell \leq \frac{\log k}{f(k)}$ pozitív egészek, ahol még $k > c(\varepsilon, f)$ is teljesül ($c(\varepsilon, f)$ csak ε-tól, f-től függő konstans). Ekkor léteznek $a_1, a_2, \ldots, a_k$ különböző pozitív egészek és $b_1, b_2, \ldots, b_l$ különböző természetes számok, hogy*

$$P\left(\prod_{i=1}^{k}\prod_{j=1}^{l}(a_i + b_j)\right) < \left((1+\varepsilon)\frac{\log k}{\ell}\log\left(\frac{\log k}{\ell}\right)\right)^{\ell}.$$

Itt ennél a tételnél egy kicsit kevesebbet igazolunk annyiban, hogy egy konkrét f függvényre mondjuk ki azt, de a bizonyítás alapötlete és menete megegyezik Erdős, Stewart, Tijdeman eredeti bizonyításával.

2.7. Tétel. *Létezik $c > 0$ konstans, hogy minden $k \geq \ell$ pozitív egészekre létezik $\mathcal{A}, \mathcal{B} \subseteq \mathbb{N}$, melyre $|\mathcal{A}| \geq k$, $|\mathcal{B}| = \ell$ és*

$$P\left(\prod_{a \in \mathcal{A}}\prod_{b \in \mathcal{B}}(a + b)\right) \leq (c \log |\mathcal{A}| \log\log |\mathcal{A}|)^{\ell}$$

A tételből azonnal következik, hogy a fenti $\mathcal{A}$ és $\mathcal{B}$ halmazokra

$$\omega\left(\prod_{a\in\mathcal{A}}\prod_{b\in\mathcal{B}}(a+b)\right) \le (c^*\log|\mathcal{A}|)^{\ell}(\log\log|\mathcal{A}|)^{\ell-1}$$

is fenn áll valamilyen $c^* > 0$ konstansra. A 2.7. tétel a 2.10. lemmából következik, amit a 2.8. és 2.9. lemmából vezetünk le.

2.8. Lemma. *Legyen N pozitív egész, $\mathcal{W} \subseteq \{1, 2, \dots N\}$ nem üres halmaz, ℓ egész szám, $1 \le \ell \le |\mathcal{W}|$. Ekkor létezik $\mathcal{A}, \mathcal{B}$ halmazpár, hogy $0 \in \mathcal{B}$, $|\mathcal{B}| = \ell$, és*

$$\mathcal{A}+\mathcal{B} \subseteq \mathcal{W}, \quad |\mathcal{A}| \ge \frac{\binom{|\mathcal{W}|}{\ell}}{\binom{N-1}{\ell-1}}$$

$\mathcal{W}$-nek minden ℓ elemű részhalmaza felírható $\{w_1, w_2, \dots, w_\ell\}$ alakban, ahol $w_1 < w_2 < \dots < w_\ell$. Ekkor minden ilyen $\{w_1, w_2, \dots, w_\ell\}$ halmazhoz rendeljük hozzá a $\{w_2-w_1, \dots, w_\ell-w_1\} \subseteq \{1, 2, \dots, N\}$, $\ell-1$ elemű halmazt. A skatulyaelv szerint létezik az $\{1, 2, \dots, N\}$ halmaznak olyan $\ell - 1$ elemű $\{b_1, \dots, b_{\ell-1}\}$ részhalmaza, melyet $\mathcal{W}$-nek k darab ℓ elemű részhalmazához rendeltük hozzá, ahol

$$k \ge \frac{\binom{|\mathcal{W}|}{\ell}}{\binom{N-1}{\ell-1}}.$$

Jelölje $a_1, a_2, \dots, a_k$ e k darab részhalmaz legkisebb elemeit. Könnyen ellenőrizhető, hogy $\mathcal{A} = \{a_1, \dots, a_k\}$, $\mathcal{B} = \{0, b_1, \dots, b_{\ell-1}\}$ eleget tesz a lemma feltételeinek.

Jelölje $\psi(x, y)$ azon pozitív egészek számát, amelyek x-et nem haladják meg, és nincsen y-nál nagyobb prímosztójuk. Canfield, Erdős, Pomarence, [2, 3.1.tétel] igazolta a következő lemmát.

2.9. Lemma. *Létezik c konstans, hogy ha x pozitív egész, $u \geq 3$ valós szám, akkor*

$$\psi(x, x^{1/u}) \geq x \exp\left(-u\left(\log u + \log\log u - 1 + c\left(\frac{\log\log u}{\log u}\right)\right)\right).$$

Ez utóbbi két lemma segítségével igazoljuk az alábbit.

2.10. Lemma. *Legyen ℓ, N pozitív egész, és*

$$m = \left\lceil \exp\left(\frac{\log N}{2\log\log N}\right)\right\rceil,$$

$$t = \left[(\log N)^{\ell}\right].$$

Ekkor van olyan $c(\ell)$, csak ℓ-től függő konstans, hogy ha $N > c(\ell)$ teljesül, akkor létezik $\mathcal{A}, \mathcal{B} \subseteq \mathbb{N}$ halmazpár, melyre $|\mathcal{A}| = m$, $|\mathcal{B}| = \ell$ valamint

$$P\left(\prod_{a\in\mathcal{A}}\prod_{b\in\mathcal{B}}(a+b)\right) \leq t.$$

Legyen $\mathcal{W} = \{n \leq N : \ P(n) \leq t\}$. Ekkor $|\mathcal{W}| = \psi(N,t)$. Ha N elég nagy

$$\psi(N,t) \geq t \geq \ell^3 \geq \ell.$$

Tehát alkalmazhatjuk a 2.8. lemmát. Eszerint létezik $\mathcal{A}, \mathcal{B}$ halmazpár, melyre $0 \in \mathcal{B}$, $|\mathcal{B}| = \ell$, és $P(a+b) \leq t$ minden $a \in \mathcal{A}$, $b \in \mathcal{B}$ esetén. Így a lemma igazságához elegendő belátni, hogy $|\mathcal{A}| \geq m$. A 2.8. lemma szerint még

$$|\mathcal{A}| \geq \frac{\binom{\psi(N,t)}{\ell}}{\binom{N-1}{\ell-1}} \geq \frac{(\psi(N,t)-\ell)^{\ell}}{\ell N^{\ell-1}} \geq (1+o(1))\,\frac{(\psi(N,t))^{\ell}}{\ell N^{\ell-1}} \tag{2.1}$$

is teljesül az $\mathcal{A}$ halmazra. Ezután $\psi(N,t)$-re adunk alsó becslést. Ehhez Legyen $u = \frac{\log N}{\log t} = \frac{\log N}{\ell \log\log N + o(1)}$, így u definiciója miatt $t = N^{1/u}$. A 2.9. lemma alapján:

$$\psi(N,t) = \psi(N, N^{1/u}) \geq N \exp\left(-u\left(\log u + \log\log u - 1 + o(1)\right)\right).$$

Mivel

$$\begin{aligned} \log u &= \log\log N - \log \ell - \log\log\log N + o(1), \\ \log\log u &= \log\log\log N + o(1), \\ \log u + \log\log u - 1 &\leq \log\log N - 1 + o(1), \end{aligned}$$

ezért

$$\begin{aligned} \psi(N,t) &\geq N \exp\left(-\frac{\log N}{\ell \log\log N + o(1)}\left(\log\log N - 1 + o(1)\right)\right) \\ &= N \exp\left(-\frac{\log N}{\ell} + (1+o(1))\frac{\ell \log N}{\log\log N}\right). \end{aligned}$$

Ezt (2.1)-be írva kapjuk:

$$|\mathcal{A}| \geq \frac{(1+o(1))}{\ell} \exp\left((1+o(1))\frac{\log N}{\log\log N}\right) \geq \exp\left(\frac{\log N}{2\log\log N}\right),$$

ha N elég nagy. Ezzel a lemmát igazoltuk.

A 2.10. lemmából már könnyen bizonyítható a 2.7. tétel. Legyen $N = [\exp(4\log k \log\log k)]$. Ha k, ℓ függvényében, elég nagy, akkor alkalmazható a 2.10. lemma. A lemmabeli t-re teljesül, hogy

$$t = \left[(\log N)^{\ell}\right] \leq (4 \log k \log\log k)^{\ell}.$$

Tehát már csak azt kell belátnunk, hogy

$$k \leq m = \left\lceil \exp\left(\frac{\log N}{2\log\log N}\right)\right\rceil.$$

Valóban

$$\log N = 4 \log k \log\log k + o(1),$$

$$\log\log N = (1 + o(1)) \log\log k,$$

$$\left\lceil \exp\left(\frac{\log N}{2 \log\log N}\right)\right\rceil > k.$$

A multiplikatív esetben Győry, Sárközy, Stewart [20] a következőt igazolta:

2.11. Tétel. *Minden $\varepsilon > 0$ valós számra, $k \geq \ell$ pozitív egészekre létezik $\mathcal{A}, \mathcal{B} \subseteq \mathbb{N}$, melyre $|\mathcal{A}| \geq k$, $|\mathcal{B}| = \ell$ és*

$$P\left(\prod_{a\in\mathcal{A}}\prod_{b\in\mathcal{B}}(ab+1)\right) \leq (\log|\mathcal{A}|)^{\ell+1+\varepsilon}.$$

Érdemes még megemlíteni a következő, karakterekre vonatkozó tételt, annál is inkább, mivel a dolgozatban később felhasználjuk. A tétel és bizonyítása Erdőstől és Shapirotól [9] származik.

2.12. Tétel. *Legyen $\mathcal{A}$, $\mathcal{B} \subseteq \{1, 2, \ldots, p\}$ és $\chi \neq \chi_0$ multiplikatív karakter mod p. Ekkor:*

$$\left|\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\chi(a+b)\right| \leq \sqrt{p\,|\mathcal{A}|\,|\mathcal{B}|}.$$

A 2.12. tétel bizonyításának céljából Gauss-összegeket használunk:

$$\tau(\chi) \stackrel{\text{def}}{=} \sum_{i=1}^{n} \chi(m) e\left(\frac{m}{q}\right),$$

ahol χ primitív karakter mod p. Ekkor $|\tau(\chi)| = \sqrt{p}$ (lásd például [3, 66.o.]). A Gauss-összegekre vonatkozik a következő két lemma.

2.13. Lemma. *Ha χ primitív karakter mod p, akkor minden n-re:*

$$\chi(n) = \frac{1}{\tau(\overline{\chi})} \sum_{h=1}^{p} \overline{\chi}(h) e\left(\frac{hn}{p}\right).$$

A bizonyítás megtalálható [3, 68.o.]-ban. Egyszerű és jól ismert az alábbi Parseval típusú azomosság.

2.14. Lemma. $T(\alpha) = \sum_{n=1}^{p} c_n e(n\alpha)$ *esetén*

$$\sum_{h=1}^{p} \left| T\left(\frac{h}{p}\right) \right|^2 = p \sum_{n=1}^{p} |c_n|^2 .$$

A bizonyítást az olvasóra hagyjuk.

A 2.13. lemma, a háromszögegyenlőtlenség és $|\tau(\overline{\chi})| = \sqrt{p}$ miatt:

$$\begin{aligned} S &\stackrel{def}{=} \left| \sum_{a\in\mathcal{A}} \sum_{b\in\mathcal{B}} \chi(a+b) \right| = \left| \frac{1}{\tau(\overline{\chi})} \sum_{a\in\mathcal{A}} \sum_{b\in\mathcal{B}} \sum_{h=1}^{p} \overline{\chi}(h) e\left(\frac{(a+b)h}{p}\right) \right| \\ &\le \frac{1}{\sqrt{p}} \sum_{h=1}^{p} \left| \sum_{a\in\mathcal{A}} e\left(\frac{ah}{p}\right) \right| \left| \sum_{b\in\mathcal{B}} e\left(\frac{bh}{p}\right) \right| . \end{aligned}$$

A Cauchy-Schwarz egyenlőtlenség szerint:

$$S \le \frac{1}{\sqrt{p}} \sqrt{ \sum_{h=1}^{p} \left| \sum_{a\in\mathcal{A}} e\left(\frac{ah}{p}\right) \right|^2 \sum_{h=1}^{p} \left| \sum_{b\in\mathcal{B}} e\left(\frac{bh}{p}\right) \right|^2 } . \tag{2.2}$$

Alkalmazzuk a 2.14 lemmát a következő helyetesítéssel:

$$c_n = \begin{cases} 0 & \text{ha } n \notin \mathcal{A}, \\ 1 & \text{ha } n \in \mathcal{A}. \end{cases}$$

Ebből azt kapjuk, hogy:

$$\sum_{h=1}^{p} \left| \sum_{a\in\mathcal{A}} e\left(\frac{ah}{p}\right) \right|^2 = p\,|\mathcal{A}| .$$

Hasonlóan

$$\sum_{h=1}^{p}\left|\sum_{a\in\mathcal{A}} e\left(\frac{bh}{p}\right)\right|^2 = p\,|\mathcal{B}|\,.$$

Az utóbbi két egyenletet (2.2)-be írva azonnal adódik a tétel állítása.

Ezeken kívül számos más tulajdonságát is vizsgálták hibrid sorozatoknak. Erdős Pál és Sárközy András [8] adott becslést az $\mathcal{A}$ halmaz méretére, ha $\mathcal{A}+\mathcal{A}$ minden eleme négyzetmentes szám. A problémát Sárközy Gábor [29] terjesztette ki két különböző halmaz és k-adik hatványok esetére. Bebizonyította, hogy ha $k,\ N > N_0(k)$ pozitív egészek, $\mathcal{A},\mathcal{B} \subseteq \{1,2,\dots,N\}$, és $|\mathcal{A}|\,|\mathcal{B}| > c(k)N^{2-1/k}$, akkor létezik p prím, $a\in\mathcal{A},\ b\in\mathcal{B}$, hogy $p^k|a+b$. Alsó becslésként pedig megadott egy olyan $\mathcal{A},\mathcal{B} \subseteq \{1,2,\dots,N\}$ halmazpárt, melyre nem létezik p prím, hogy $p^k|a+b$ teljesül valamilyen $a\in\mathcal{A},\ b\in\mathcal{B}$-re, és

$$|\mathcal{A}|\,|\mathcal{B}| > \frac{(k-1)N(\log N)^{k-1}}{65e^4(3k)^{k-1}}.$$

Dolgozatom további részeiben saját, illetve társszerzőkkel közösen írt cikkeink tartalmát ismertetem a [15], [16], [17] és [18] alapján, azonban az ottani bizonyításokat kissé átdolgozva, helyenként egyszerűsítve.

3. Diofantosz problémájának kiterjesztése

Ebben a fejezetben Diofantosz problémájának két különböző sorozatra való általánosítását vizsgáljuk. A most következő tétel érdekessége, hogy $k \geq 3$ esetén sokkal jobb becslést ad k-adik hatványokra mint négyzetszámokra.

3.1. Tétel. *Ha $\mathcal{A}, \mathcal{B} \subseteq \{1, 2, 3, \ldots, N\}$ és $\mathcal{A} \times \mathcal{B} + 1$ minden eleme k-adik hatvány, akkor:*

a)

$$\min\left(|\mathcal{A}|, |\mathcal{B}|\right) \leq \frac{1}{\log 2} \log N \quad \textit{ha } k = 2,$$

b)

$$\min\left(|\mathcal{A}|, |\mathcal{B}|\right) \leq \frac{1}{\log(k-1)} \log\log N + 1 \quad \textit{ha } k \geq 3.$$

Legyen $\mathcal{A}$ és $\mathcal{B}$ a tételnek megfelelő halmazok. A bizonyítás a következő lemmán alapul:

3.2. Lemma. *Legyen $k \geq 2$ és $x < y$, $c < d$ pozitív egész számok. Ha $xc+1, xd+1, yc+1, yd+1$ számok mindegyike k-adik hatvány, akkor*

$$yd > k^k (xc)^{k-1}.$$

Valóban, ha $x < y$ és $c < d$, akkor

$$(y-x)(d-c) > 0.$$

Ez utóbbi ekvivalens az

$$(xc+1)(yd+1) > (xd+1)(yc+1)$$

egyenlőtlenséggel. Mivel $(xc+1)(yd+1)$ k-adik hatvány és $\sqrt[k]{(xd+1)(yc+1)}$ egész szám, ezért:

$$xycd + xc + yd + 1 \geq \left(\sqrt[k]{(xd+1)(yc+1)} + 1\right)^k.$$

A binomiális tétel szerint becsülve a jobboldalt, kapjuk:

$$xycd + xc + yd + 1 \geq xycd + xd + yc + 1 + k(xycd)^{\frac{k-1}{k}}.$$

Rendezve:

$$yd \geq xd + yc - xc + k(xycd)^{\frac{k-1}{k}}.$$

$d > c$ miatt $xd + yc - xc > 0$, tehát

$$yd > k^k(xc)^{k-1}.$$

Ezzel a 3.2. lemmát igazoltuk. Most már rátérhetünk a 3.1. tétel bizonyítására.

Legyen $\mathcal{A} = \{a_1, a_2, \ldots, a_m\}$, $\mathcal{B} = \{b_1, b_2, \ldots, b_n\}$ ahol $a_1 < a_2 < \cdots < a_m$ és $b_1 < b_2 < \cdots < b_n$. Az általánosság megsértése nélkül feltehetjük, hogy $m \leq n$.

$k = 2$ esetén $a_1b_1 \geq 4$ vagy $a_2b_2 \geq 16$, mivel $a_ib_j + 1$ négyzetszám minden $1 \leq i \leq j \leq 2$ esetén. Így a 2.1. tétel alapján kapjuk:

$$N^2 \geq a_mb_m > 4a_{m-1}b_{m-1} > \cdots > 4^m.$$

Tehát: $m \leq \frac{1}{\log 2} \log N$.

Hasonló állítások állnak fenn $k > 2$ esetén is. Ekkor: $a_{t+1}b_{t+1} > (a_tb_t)^{k-1}$, ha $1 \leq t \leq m$. Mivel most $a_1b_1 > 2^{k-1}$, ezért:

$$N^2 \geq a_mb_m > k^{k-1}(a_{m-1}b_{m-1})^{k-1} > \cdots > k^{(k-1)^{m-1}}2^{(k-1)^m} = (2\sqrt[k-1]{k})^{(k-1)^m}.$$

Tehát:

$$m \leq \frac{1}{\log(k-1)} \log\log N + 1.$$

Ezzel a bizonyítást befejeztük.

Az előző tétel a két halmaz közül csak a kisebbik méretére adott felső becslést. Valószínűleg $k = 2$ esetén bármelyik halmaz elemszáma kisebb mint $\log N$-nek egy konstansszorosa, ezt azonban csak egy további feltétel mellett tudtam igazolni.

3.3. Tétel. *Legyen $\mathcal{A}, \mathcal{B} \subseteq \{1, 2, 3, \ldots, N\}$, és $\mathcal{A} \times \mathcal{B} + 1$ minden eleme négyzetszám. Tegyük fel, hogy létezik $a_1, a_2 \in \mathcal{A}$, amelyre $a_1 \leq a_2 \leq 2a_1$. Ekkor:*

$$|\mathcal{B}| \leq \frac{1}{\log 2} \log N.$$

Legyen $\mathcal{B} = \{b_1, b_2, \ldots, b_n\}$ továbbra is. A 2.2. lemma szerint $a_2 b_{t+1} > 4a_1 b_t$ ha $1 \leq t \leq n-1$. A $2a_1 > a_2$ feltétel miatt ebből azt kapjuk, hogy $b_{t+1} > 2b_t$. Innen már azonnal adódik az állítás.

Pell-egyenletek segítségével könnyen látható, hogy a 3.3. tételben a $\mathcal{B}$ halmaz méretére adott felső becslés konstans szorzótól eltekintve éles:

3.4. Tétel. *Az $\mathcal{A} = \{1, 2\}$ halmazhoz létezik $\mathcal{B} \subseteq \{1, 2, 3, \ldots, N\}$, melyre*

$$|\mathcal{B}| \geq \left[\frac{1}{\log 36} \log N\right]$$

és $\mathcal{A} \times \mathcal{B} + 1$ minden eleme négyzetszám.

Definiáljuk az $\{x_n\}$ sorozatot a következőképpen: $x_0 = 1$, $x_1 = 5$ és $n \geq 2$ esetén $x_n = 6x_{n-1} - x_{n-2}$. Ekkor $x_n \leq 6x_{n-1}$. Ezt többszörösen alkalmazva adódik, hogy $x_n < 6^n$. Legyen $\mathcal{B} = \{{x_i}^2 - 1 : x_i < \sqrt{N},\ i \geq 1\}$. Ezek után már csak két dolgot kell igazolnunk. Egyrészt, hogy $|\mathcal{B}| \geq \left[\frac{1}{\log 36} \log N\right]$, másrészt $a \in \mathcal{A}, b \in \mathcal{B}$ esetén $ab + 1$ négyzetszám.

Ha $6^i \leq \sqrt{N}$ és $i \geq 1$, akkor ${x_i}^2 - 1 \in \mathcal{B}$ tehát $|\mathcal{B}| \geq \left[\frac{1}{\log 36} \log N\right]$. Legyen

$$y_n = \frac{1}{2} x_{n+1} - \frac{3}{2} x_n.$$

minden n-re. Ebből $x_{n+1} = 2y_n + 3x_n$, valamint:

$$y_{n+1} = \frac{1}{2}(6x_{n+1} - x_n) - \frac{3}{2}x_{n+1} = 4x_n + 3\left(\frac{1}{2}x_{n+1} - \frac{3}{2}x_n\right) = 4x_n + 3y_n.$$

Összefoglalva:

$$\begin{aligned} y_{n+1} &= 3y_n + 4x_n, \\ x_{n+1} &= 2y_n + 3x_n. \end{aligned}$$

Mivel a 3, 2 számpár az $y^2 - 2x^2 = 1$ Pell-egyenlet legkisebb megoldása, és $x_0 = y_0 = 1$ esetén $y_0^2 - 2x_0^2 = -1$, ezért az y_n, x_n számpár az $y^2 - 2x^2 = -1$ Pell-egyenlet megoldása. Vagyis $2\left(x_i{}^2 - 1\right) + 1 = y_i{}^2$. Azaz minden $a \in \mathcal{A}$, $b \in \mathcal{B}$ esetén $ab + 1$ teljes négyzet. Ezzel a tételt igazoltuk.

Érdemes megvizsgálni a probléma moduláris változatát, mivel itt Diofantosz problémájával ellentétben, akármilyen nagy halmaz megadható a megfelelő tulajdonsággal.

3.5. Tétel. *Létezik olyan p_0 konstans, hogy ha p $4k + 1$ alakú prím, és $p > p_0$, akkor létezik $\mathcal{A} \subseteq \mathbb{Z}_p$ halmaz, amelyre*

$$|\mathcal{A}| \geq \frac{1}{6\log 3}\log p,$$

valamint $\mathcal{A} \cdot \mathcal{A} + 1$ minden eleme kvadratikus maradék vagy 0 mod p.

A bizonyítás érdekessége, hogy gráfelméleten alapul. Nevezetesen, ismeretes a Ramsey tételnek a következő általánosítása:

3.6. Lemma. *Minden s_1, s_2, s_3 nem negatív számokra létezik egy r egész szám az alábbi tuljdonsággal:*

Ha G olyan teljes gráf, amelyre $V(G) \geq r$, és C tetszőleges három színezése G gráfnak a c_1, c_2, c_3 színekkel, akkor létezik $1 \leq i \leq 3$, hogy G-nek van egyszínű G' részgráfja, ahol $|V(G')| \geq s_i$. Jelöljük az ilyen r számok közül a legkisebbet $R(a, b, c)$-vel. Ekkor:

$$R(s_1, s_2, s_3) \leq \frac{(s_1 + s_2 + s_3)!}{s_1! s_2! s_3!}.$$

Ha az s_1, s_2, s_3 számok valamelyike 0, akkor az állítás triviális, mert $R(s_1, s_2, s_3) = 0$. $s_1, s_2, s_3 > 0$ esetén igaz és jól ismert az alábbi egyenlőtlenség (lásd [14]):

$$R(s_1, s_2, s_3) \leq R(s_1 - 1, s_2, s_3) + R(s_1, s_2 - 1, s_3) + R(s_1, s_2, s_3 - 1)$$

Ebből $s_1 + s_2 + s_3$-ra vonatkozó indukcióval kapjuk: $R(s_1, s_2, s_3) \leq \frac{(s_1+s_2+s_3)!}{s_1!s_2!s_3!}$.

Nézzük most azt a gráfot, amelynek pontjai a mod p maradékosztályok. Mivel p $4k + 1$ alakú prím, ezért létezik i maradékosztály, hogy $i^2 \equiv -1$ mod p. Az élek színét a Legendre szimbólum segítségével határozzuk meg $\left(\frac{0}{p}\right)$ értékét vegyük 0-nak.

Az a és b maradékosztályokat összekötő élt színezzük
c_1 színnel, ha $\left(\frac{ab+1}{p}\right) = 1$ vagy 0,
c_2 színnel, ha $\left(\frac{-ab+1}{p}\right) = 1$ vagy 0, és $\left(\frac{ab+1}{p}\right) = -1$.
c_3 színnel, ha $\left(\frac{-a^2b^2+1}{p}\right) = 1$ vagy 0, és $\left(\frac{ab+1}{p}\right) = \left(\frac{-ab+1}{p}\right) = -1$.
Ekkor minden élt megszíneztünk, ellenkező esetben ugyanis:

$$\left(\frac{ab+1}{p}\right) = \left(\frac{-ab+1}{p}\right) = \left(\frac{-a^2b^2+1}{p}\right) = -1.$$

Tehát:

$$-1 = \left(\frac{(ab+1)(-ab+1)(-a^2b^2+1)}{p}\right) = \left(\frac{(a^2b^2-1)^2}{p}\right).$$

De ez ellentmond a nyilvánvaló ténynek, hogy $\left(\frac{\left(a^2b^2-1\right)^2}{p}\right) = 1$ vagy 0.

Legyen $c = \left[\frac{1}{3\log 3}\log p\right] + 1$. A 3.6. lemma szerint:

$$R(c,c,c) \leq \frac{(3c)!}{c!c!c!}.$$

Az egyenlőtlenség jobboldalát Stirling formulával becsüljük. Elég nagy c esetén:

$$\frac{(3c)!}{c!c!c!} \leq (1+o(1))\frac{\left(\frac{3c}{e}\right)^{3c}\sqrt{2\pi 3c}}{\left(\left(\frac{c}{e}\right)^{c}\sqrt{2\pi c}\right)^3} \leq 3^{3c-3} \leq p.$$

Azaz, ha p elég nagy, akkor $R(c,c,c) \leq p$. Tehát van a gráfban egy c darab szögpontból álló egyszínű G' részgráf.

Legyen

$$\mathcal{A} = \begin{cases} V(G') & \text{ha a } G' \text{ éleit } c_1 \text{ színnel színeztük,} \\ \{ig : g \in V(G')\} & \text{ha a } G' \text{ éleit } c_2 \text{ színnel színeztük,} \\ \{ig^2 : g \in V(G')\} & \text{ha a } G' \text{ éleit } c_3 \text{ színnel színeztük.} \end{cases}$$

Ekkor $|\mathcal{A}| \geq \frac{1}{2}|V(G')|$. A színezés definiciója miatt $\mathcal{A}$ halmaz bármely két elemének szorzatához 1-et adva mindig kvadratikus maradékot vagy 0-t kapunk mod p.

Hasonló konstrukciót adott Erdős és Sárközy [28] a probléma additív analogonja esetén. Ahhoz, hogy felső becslést tudjunk adni a moduláris esetben, szükségünk van Vinogradov [34] következő tételére.

3.7. Tétel. *Legyen* $\mathcal{A},\mathcal{B} \subseteq \mathbb{Z}_p$ *és* $S = \sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\left(\frac{ab+1}{p}\right)$, *akkor* $|\mathcal{S}| \leq \sqrt{2p|\mathcal{A}||\mathcal{B}|}$.

Ebből már könnyen levezethető az alábbi tétel.

3.8. TÉTEL. *Legyen p prím, $\mathcal{A}, \mathcal{B} \subseteq \{1, 2, \ldots, p-1\}$, és $\mathcal{A} \times \mathcal{B} + 1$ minden eleme kvadratikus maradék vagy 0 mod p. Ekkor $|\mathcal{A}|\,|\mathcal{B}| \leq \left(\sqrt{2p}+1\right)^2$.*

A bizonyítás során feltehetjük, hogy $|\mathcal{A}| \leq |\mathcal{B}|$. A tétel feltétele szerint minden $a \in \mathcal{A}, b \in \mathcal{B}$ esetén $\left(\frac{ab+1}{p}\right) = 1$ vagy 0. A 3.7. tételből következik, hogy

$$|\mathcal{A}|\,|\mathcal{B}| - \sqrt{|\mathcal{A}|\,|\mathcal{B}|} \leq |\mathcal{A}|\,(|\mathcal{B}|-1) \leq \sum_{a \in \mathcal{A}} \sum_{b \in \mathcal{B}} \left(\frac{ab+1}{p}\right) \leq \sqrt{2p\,|\mathcal{A}|\,|\mathcal{B}|}.$$

De ez ekvivalens az állítással.

Ahhoz, hogy Diofantosz problémáját, illetve annak, additív változatát a moduláris esetben 2-nél magasabb hatványokra is vizsgálni tudjuk, multiplikatív karakterekre van szükségünk. A következő tétel a) része Vinogradov eredményét általánosítja, míg b) részét Erdős és Shapiro [9] bizonyította, és a 2. fejezetben tárgyaltuk.

3.9. TÉTEL. *Legyen $\mathcal{A}$, $\mathcal{B} \subseteq \{1, 2, \ldots, p\}$ és $\chi \neq \chi_0$ multiplikatív karakter mod p. Ekkor:*

a)

$$\left|\sum_{a \in \mathcal{A}} \sum_{b \in \mathcal{B}} \chi(ab+1)\right| \leq \sqrt{p\,|\mathcal{A}|\,|\mathcal{B}|},$$

b)

$$\left|\sum_{a \in \mathcal{A}} \sum_{b \in \mathcal{B}} \chi(a+b)\right| \leq \sqrt{p\,|\mathcal{A}|\,|\mathcal{B}|}.$$

A 3.9.a tétel bizonyításában Gauss-összegeket használunk:

$$\tau(\chi) \overset{\mathrm{def}}{=} \sum_{i=1}^{n} \chi(m) e\left(\frac{m}{q}\right),$$

ahol χ primitív karakter mod p. Ekkor $|\tau(\chi)| = \sqrt{p}$ (lásd például [3, 66.o.]).

A 2.13. lemma szerint:

$$S \stackrel{\text{def}}{=} \left| \sum_{a\in\mathcal{A}} \sum_{b\in\mathcal{B}} \chi(ab+1) \right| = \left| \frac{1}{\tau(\overline{\chi})} \sum_{a\in\mathcal{A}} \sum_{b\in\mathcal{B}} \sum_{h=1}^{p} \overline{\chi}(h) e\left(\frac{(ab+1)h}{p}\right) \right|.$$

$h = \ell b^{-1}$ helyettesítve, és $|\tau(\overline{\chi})| = \sqrt{p}$-t használva kapjuk:

$$S = \frac{1}{\sqrt{p}} \left| \sum_{a\in\mathcal{A}} \sum_{b\in\mathcal{B}} \sum_{\ell=1}^{p} \overline{\chi}(\ell b^{-1}) e\left(\frac{(a\ell + \ell b^{-1})}{p}\right) \right|.$$

Legyen $\mathcal{B}' = \{b^{-1} : b \in \mathcal{B}\}$. Nyilván $|\mathcal{B}'| = |\mathcal{B}|$. Továbbá:

$$\begin{aligned} S &= \frac{1}{\sqrt{p}} \left| \sum_{\ell=1}^{p} \overline{\chi}(\ell) \sum_{a\in\mathcal{A}} e\left(\frac{a\ell}{p}\right) \sum_{b\in\mathcal{B}'} \overline{\chi}(b) e\left(\frac{b\ell}{p}\right) \right| \leq \\ &\leq \frac{1}{\sqrt{p}} \sum_{\ell=1}^{p} \left| \sum_{a\in\mathcal{A}} e\left(\frac{a\ell}{p}\right) \right| \left| \sum_{b\in\mathcal{B}'} \overline{\chi}(b) e\left(\frac{b\ell}{p}\right) \right|. \end{aligned}$$

A Cauchy-Schwarz egyenlőtlenség szerint:

$$S \leq \frac{1}{\sqrt{p}} \sqrt{ \sum_{\ell=1}^{p} \left| \sum_{a\in\mathcal{A}} e\left(\frac{a\ell}{p}\right) \right|^2 \sum_{\ell=1}^{p} \left| \sum_{b\in\mathcal{B}'} \overline{\chi}(b) e\left(\frac{b\ell}{p}\right) \right|^2 }. \tag{3.1}$$

A 2. fejezetben már beláttuk, hogy

$$\sum_{\ell=1}^{p} \left| \sum_{a\in\mathcal{A}} e\left(\frac{a\ell}{p}\right) \right|^2 = p\,|\mathcal{A}|. \tag{3.2}$$

Alkalmazzuk a 2.13 lemmát a következő helyetesítéssel:

$$c_n = \begin{cases} 0 & \text{ha } n \notin \mathcal{B}, \\ \overline{\chi}(n) & \text{ha } n \in \mathcal{B}. \end{cases}$$

Ebből azt kapjuk, hogy:

$$\sum_{\ell=1}^{p} \left| \sum_{b\in\mathcal{B}'} \overline{\chi}(b) e\left(\frac{b\ell}{p}\right) \right|^2 = p\,|\mathcal{B}|. \tag{3.3}$$

(3.2)-t és (3.3)-t beírva a (3.1) egyenlőtlenségbe, kapjuk:

$$S \leq \sqrt{p}\sqrt{|\mathcal{A}|\,|\mathcal{B}|}.$$

Ezzel a 3.9. tételt igazoltuk.

A fenti, karakterekre vonatkozó tétel lehetővé teszi, hogy a moduláris esetben a triviálisnál jobb felső becslést adjunk a halmazok méretére.

3.10. Tétel. *Legyen k pozitív egész. Ha p prímszám, $(p-1,k) \neq 1$, $\mathcal{A},\mathcal{B} \subseteq \{1,2,\ldots,p-1\}$ és*

a) minden $a \in \mathcal{A}$, $b \in \mathcal{B}$ estén létezik egy x egész, hogy $ab+1 \equiv x^k \pmod{p}$,

vagy

b) minden $a \in \mathcal{A}$, $b \in \mathcal{B}$ esetén létezik egy x egész, hogy $a+b \equiv x^k \pmod{p}$,

akkor $|\mathcal{A}|\,|\mathcal{B}| \leq (\sqrt{p}+2)^2$.

A $(p-1,k) \neq 1$ feltétel mindenképpen szükséges a tételben, mivel $(p-1,k) = 1$ esetén az $x^k \equiv a \pmod{p}$ egyenletnek rögzített a-ra pontosan 1 megoldása van x-ben. Így ekkor tetszőleges $\mathcal{A},\mathcal{B} \subseteq \{1,2,\ldots,p-1\}$ halmazpár eleget tenne a tétel feltételeinek.

Legyen $f(a,b)$ $ab+1$ az a) esetben és $a+b$ a b) esetben. Elegendő azt belátni, hogy a tétel igaz akkor, ha k prím. Megadható ugyanis k helyett egy olyan k_0, ami már prím és eleget tesz a tétel feltételeinek. Valóban, az általános esetben, ha $(k,\ p-1) \neq 1$, akkor k-nak létezik egy olyan k_0 prímosztója, amelyre $k_0|p-1$. Ekkor minden $a \in \mathcal{A}$, $b \in \mathcal{B}$-re, $f(a,b)$ nemcsak k-adik, hanem k_0-adik hatvány is mod p, és $(k_0,\ p-1) \neq 1$.

Tehát az általánosság megsértése nélkül feltehetjük, hogy k prím, és szimmetrikus okokból azt is, hogy $|\mathcal{A}| \leq |\mathcal{B}|$. Ekkor $k|p-1$. Ismeretes a következő egyszerű állítás: Ha $(x,p)=1$, úgy:

$$\sum_{\chi:\chi^k=\chi_0} \chi(x) = \begin{cases} k & \text{ha } x \text{ } k\text{-adik hatvány mod } p \text{ és } x \not\equiv 0 \text{ mod } p, \\ 0 & \text{ha } x \text{ nem } k\text{-adik hatvány mod } p \text{ vagy } x \equiv 0 \text{ mod } p. \end{cases}$$

Ezt, a 3.9. tételt, és $|\mathcal{A}| \leq |\mathcal{B}|$ használva kapjuk:

$$\begin{aligned} k\left(|\mathcal{A}|\,|\mathcal{B}| - \sqrt{|\mathcal{A}|\,|\mathcal{B}|}\right) &\leq k\,|\mathcal{A}|\,(|\mathcal{B}|-1) \leq \sum_{a\in\mathcal{A}} \sum_{\substack{b\in\mathcal{B} \\ f(a,b)\neq 0}} \sum_{\chi:\chi^k=\chi_0} \chi\left(f(a,b)\right) \leq \\ &\leq |\mathcal{A}|\,|\mathcal{B}| + \sum_{\substack{\chi:\chi^k=\chi_0 \\ \chi\neq\chi_0}} \sum_{a\in\mathcal{A}} \sum_{b\in\mathcal{B}} \chi\left(f(a,b)\right) \leq \\ &\leq |\mathcal{A}|\,|\mathcal{B}| + (k-1)\sqrt{p}\sqrt{|\mathcal{A}|\,|\mathcal{B}|}. \end{aligned}$$

Ebből:

$$|\mathcal{A}|\,|\mathcal{B}| \leq \left(\sqrt{p} + \frac{k}{k-1}\right)^2.$$

Ezután már bebizonyíthajuk a következő összegsorozatokra vonatkozó tételt, a 3.1. tétel additív megfelelőjét.

3.11. Tétel. *Minden $k>1$ egész esetén létezik N_0, hogy ha $N \geq N_0$, $\mathcal{A},\mathcal{B} \subseteq \{1,2,\dots,N\}$ és $\mathcal{A}+\mathcal{B}$ minden eleme k-adik hatvány, akkor*

$$\min\left(|\mathcal{A}|, |\mathcal{B}|\right) \leq 4k\log N.$$

A bizonyítás Gallagher nagyobb szitáján alapul.

3.12. Lemma. *(Gallagher) Legyen $X \subseteq \{M+1, M+2, \dots, M+N\}$ egész számokból álló halmaz. Minden p prímre jelölje $\nu_X(p)$ azon mod p maradék osztályok számát, amelyek tartalmaznak X-ből elemet. Ha $\mathcal{P}$ prímszámok* *egy véges halmaza, akkor*

$$|X| \leq \frac{\sum\limits_{p\in\mathcal{P}} \log p - \log N}{\sum\limits_{p\in\mathcal{P}} \frac{\log p}{\nu_X(p)} - \log N}$$

feltéve, hogy a nevező pozitív.

A lemma bizonyítása megtalálható például [26]-ben

Legyen p prím és $p \equiv 1 \mod k$. Ezután hagyjuk el egy pillanatra az $\mathcal{A}$ és a $\mathcal{B}$ halmazokból a p-vel osztható elemeket. A 3.12. tétel szerint az alábbi egyenlőtlenséget kapjuk:

$$\left(\nu_{\mathcal{A}}\left(p\right)-1\right)\left(\nu_{\mathcal{B}}\left(p\right)-1\right) \leq \left(\sqrt{p}+2\right).$$

Ebből:

$$\min\{\nu_{\mathcal{A}}\left(p\right), \nu_{\mathcal{B}}\left(p\right)\} \leq \sqrt{p}+3.$$

Legyen $P = \{p: \ p \text{ prím}, p \equiv 1 \mod k, \ p \leq 4\left(\phi(k)\log N)^2\right)\}$. Osszuk a P halmazt két diszjunkt részre:

$$P_A = \{p \in P: \ \min\{\nu_{\mathcal{A}}\left(p\right), \nu_{\mathcal{B}}\left(p\right)\} = \nu_{\mathcal{A}}\left(p\right)\},$$

$$P_B = \{p \in P: \ \min\{\nu_{\mathcal{A}}\left(p\right), \nu_{\mathcal{B}}\left(p\right)\} \neq \nu_{\mathcal{A}}\left(p\right)\}.$$

3.14. lemma szerint az alábbi egyenlőtlenségek közül az áll fenn, amelyikre teljesül, hogy a jobboldalon álló tört nevezője pozitív.

$$|\mathcal{A}| \leq \frac{\sum\limits_{p\in\mathcal{P}_{\mathcal{A}}} \log p - \log N}{\sum\limits_{p\in\mathcal{P}_{\mathcal{A}}} \frac{\log p}{\nu_{\mathcal{A}}(p)} - \log N},$$

$$|\mathcal{B}| \leq \frac{\sum\limits_{p\in\mathcal{P}_\mathcal{B}} \log p - \log N}{\sum\limits_{p\in\mathcal{P}_\mathcal{B}} \frac{\log p}{\nu_\mathcal{B}(p)} - \log N}.$$

Szimmetrikus okokból feltehetjük, hogy

$$\sum_{p\in\mathcal{P}_\mathcal{A}} \frac{\log p}{\nu_\mathcal{A}(p)} - \log N \geq \sum_{p\in\mathcal{P}_\mathcal{B}} \frac{\log p}{\nu_\mathcal{B}(p)} - \log N.$$

A Mertens tétel és a kis modulusú számtani sorozatokra vonatkozó prímszámtétel szerint:

$$2\left(\sum_{p\in\mathcal{P}_\mathcal{A}} \frac{\log p}{\nu_\mathcal{A}(p)} - \log N\right) \geq \sum_{p\in\mathcal{P}_\mathcal{A}} \frac{\log p}{\nu_\mathcal{A}(p)} - \log N + \sum_{p\in\mathcal{P}_\mathcal{B}} \frac{\log p}{\nu_\mathcal{B}(p)} - \log N =$$

$$\sum_{p\in\mathcal{P}} \frac{\log p}{\min(\nu_\mathcal{A}(p), \nu_\mathcal{B}(p))} - 2\log N \geq \sum_{p\in P} \frac{\log p}{\sqrt{p}+3} - 2\log N = (2+o(1))\log N$$

Ahonnan:

$$|\mathcal{A}| \leq \frac{\sum\limits_{p\in\mathcal{P}} \log p - \log N}{(1+o(1))\log N} \leq 4k\log N.$$

Tehát igaz a 3.13. tétel állítása.

Végül általánosítjuk a 3.12. tétel eredményét x^k helyébe más $h(x)$ polinomt írva.

3.13. Tétel. *Legyen p prím és $h(x) \in F_p[x]$ n-edfokú polinom, ahol $2 \leq n < p$. Legyen $\mathcal{A}$, $\mathcal{B} \subseteq \{1, 2, \ldots, p-1\}$ és $|\mathcal{A}|\,|\mathcal{B}| \geq p\left(\frac{p-1}{p-n}\right)^2 (n-1)^2$, ekkor:*
a) Ha $p-1$-nek nincs olyan $d > 1$ osztója, amelyre $h(x)$ egy polinom d-edik hatványának a konstansszorosa, akkor létezik $a \in \mathcal{A}$, $b \in \mathcal{B}$, melyre $ab \equiv h(x) \pmod p$ kongurencia megoldható. Sőt, e kongruencia megoldásszámát (a, b, x)-ben N-nel jelölve,

$$|N - |\mathcal{A}|\,|\mathcal{B}|| < \frac{n}{p-1}|\mathcal{A}|\,|\mathcal{B}| + (n-1)\sqrt{p\,|\mathcal{A}|\,|\mathcal{B}|}$$

is fenn áll.

b) Létezik $a \in \mathcal{A}$, $b \in \mathcal{B}$, hogy az $a + b \equiv h(x) \mod p$ kongruencia megoldható, továbbá a kongruencia megoldásszámát (a, b, x)-ben M-mel jelölve, kapjuk:

$$|M - |\mathcal{A}|\,|\mathcal{B}|| < (n-1)\sqrt{p\,|\mathcal{A}|\,|\mathcal{B}|}.$$

A tétel a) részében a $h(x)$-re vonatkozó feltétel szükséges, hiszen ha $d|p-1$ és $h(x) = c\,(h'[x])^d$, úgy létezik $m \in F_p$, amely nem d-edik hatvány a p elemű testben. Legyen $\mathcal{A} = \{x^d : x \in F_p,\ x \neq 0\}$, $\mathcal{B} = \{cmx^d : x \in F_p,\ x \neq 0\}$. Ekkor az $ab \equiv h(x) \equiv c\,(h'(x))^d \mod p$ kongurenciának nincs megoldása $a \in \mathcal{A}$, $b \in \mathcal{B}$-ben, mert $\mathcal{A}$ és $\mathcal{B}$ halmaz definiciója miatt, ekkor $ab = cmy^d$ teljesül valamiyen $y \in F_p$-re, ami ellentmond m választásának. Viszont $|\mathcal{A}|\,|\mathcal{B}| = \left(\frac{p-1}{d}\right)^2$.

Először a tétel a) részét bizonyítjuk. Könnyen igazolható és jól ismert az alábbi lemma.

3.14. Lemma.

$$\sum_{\chi} \left| \sum_{n=1}^{p-1} c_n \chi(n) \right|^2 = (p-1) \sum_{n=1}^{p-1} c_n^2.$$

A következő lemma A. Weiltől származik. A bizonyítás megtalálható [31, 43.o]-ban.

3.15. Lemma. *Legyen χ mod p multiplikatív karakter rendeje $d > 1$. Tegyük fel, hogy $f(x) \in F_p[x]$ polinomnak m különböző gyöke van F_p algebrai lezártja felett, és nincs olyan polinom, amely d-edik hatványának kons-*

tansszorosa $f(x)$. Ekkor:

$$\left|\sum_{x\in F_p} \chi\left(f(x)\right)\right| \le (m-1)\sqrt{p}.$$

Tetszőleges karakterre igaz az alábbi összefüggés:

$$\sum_{\chi} \chi\left(a^{-1}b^{-1}h(x)\right) = \begin{cases} p-1 & \text{ha } ab \equiv h(x) \mod p, \\ 0 & \text{különben.} \end{cases}$$

Ez alapján az $ab \equiv h(x) \mod p$ kongruencia akkor és csak akkor oldható meg $a \in \mathcal{A}$, $b \in \mathcal{B}$, $x \in F_p$-ben, ha

$$0 < (p-1)N = \sum_{a\in\mathcal{A}} \sum_{b\in\mathcal{B}} \sum_{x=0}^{p-1} \sum_{\chi} \chi\left(a^{-1}b^{-1}h(x)\right).$$

Jelölje H a $h(x)$ polimom különböző gyökeinek számát. Így:

$$\left|(p-H)\left|\mathcal{A}\right|\left|\mathcal{B}\right| - (p-1)N\right| = \left|\sum_{a\in\mathcal{A}} \sum_{b\in\mathcal{B}} \sum_{x=0}^{p-1} \sum_{\chi\ne\chi_0} \chi\left(a^{-1}b^{-1}h(x)\right)\right|.$$

A Cauchy-Schwarz egyenlőtlenséget, a 3.14. és 3.15. lemmát használva kapjuk:

$$\left|\sum_{a\in\mathcal{A}} \sum_{b\in\mathcal{B}} \sum_{x=0}^{p-1} \sum_{\chi\ne\chi_0} \chi\left(a^{-1}b^{-1}h(x)\right)\right| \le$$

$$\le \sum_{\chi\ne\chi_0} \left|\sum_{a\in\mathcal{A}} \chi(a^{-1}) \sum_{b\in\mathcal{B}} \chi(b^{-1})\right| \left|\sum_{x=0}^{p-1} \chi\left(h(x)\right)\right| \le$$

$$\le \sqrt{\sum_{\chi\ne\chi_0} \left|\sum_{a\in\mathcal{A}} \chi(a^{-1})\right|^2} \sqrt{\sum_{\chi\ne\chi_0} \left|\sum_{b\in\mathcal{B}} \chi(b^{-1})\right|^2} (H-1)\sqrt{p} \le$$

$$\le (H-1)(p-1)\sqrt{p\left|\mathcal{A}\right|\left|\mathcal{B}\right|}.$$

Tehát ha $|\mathcal{A}|\,|\mathcal{B}| \geq p\left(\frac{p-1}{p-n}\right)^2 (n-1)^2$, akkor $\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\sum_{x=0}^{p-1}\sum_{\chi}\chi\left(a^{-1}b^{-1}h(x)\right) > 0$.

Továbbá:

$$(H-1)\sqrt{p\,|\mathcal{A}|\,|\mathcal{B}|} > \left|N - \frac{p-H}{p-1}\,|\mathcal{A}|\,|\mathcal{B}|\right| \geq \left|N - |\mathcal{A}|\,|\mathcal{B}|\right| - \frac{H}{p-1}\,|\mathcal{A}|\,|\mathcal{B}|\,.$$

Ezzel a tétel a) részét igazoltuk.

A b) rész igazolásához Weil tételének egy másik alakját használjuk.

3.16. Lemma. *Legyen p prím és $g(x) = a_n x^n + \cdots + a_0$ olyan egész együtthatós polynom, ahol $0 < n < p$ és $p \not| a_n$. Ekkor:*

$$\left|\sum_{x=0}^{p-1} e\left(\frac{g(x)}{p}\right)\right| \leq (n-1)\sqrt{p}.$$

A bizonyítás megtalálható [31, 45.o.]-ben. Tekintsük a következő egyszerű összefüggést:

$$\sum_{k=0}^{p-1} e\left(\frac{k\left(h(x)-a-b\right)}{p}\right) = \begin{cases} p & \text{ha } a+b \equiv h(x) \mod p, \\ 0 & \text{különben.} \end{cases}$$

Ez alapján az $a+b \equiv h(x) \mod p$ kongruencia akkor és csak akkor oldható meg $a \in \mathcal{A}$, $b \in \mathcal{B}$, $x \in F_p$-ben, ha

$$0 < pN = \sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\sum_{x=0}^{p-1}\sum_{k=0}^{p-1} e\left(\frac{k\left(h(x)-a-b\right)}{p}\right).$$

Ebből:

$$\left|p\,|\mathcal{A}|\,|\mathcal{B}| - pN\right| = \left|\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\sum_{x=0}^{p-1}\sum_{k=1}^{p-1} e\left(\frac{k\left(h(x)-a-b\right)}{p}\right)\right|.$$

A Cauchy-Schwarz egyenlőtlenséget, a 2.14. és 3.16. lemmát használva kapjuk:

$$\left|\sum_{a\in\mathcal{A}}\sum_{b\in\mathcal{B}}\sum_{x=0}^{p-1}\sum_{k=1}^{p-1} e\left(\frac{k\left(h(x)-a-b\right)}{p}\right)\right| =$$

$$= \sum_{k=1}^{p-1} \left| \sum_{a \in \mathcal{A}} e\left(-\frac{ka}{p}\right) \sum_{b \in \mathcal{B}} e\left(-\frac{kb}{p}\right) \right| \left| \sum_{x=0}^{p-1} e\left(\frac{kh(x)}{p}\right) \right| \leq$$

$$\leq \sqrt{\sum_{k=1}^{p-1} \left| \sum_{a \in \mathcal{A}} e\left(-\frac{ka}{p}\right) \right|^2} \sqrt{\sum_{k=1}^{p-1} \left| \sum_{b \in \mathcal{B}} e\left(-\frac{kb}{p}\right) \right|^2} (n-1)\sqrt{p} \leq$$

$$\leq (n-1)p\sqrt{p\,|\mathcal{A}|\,|\mathcal{B}|}.$$

Tehát ha $|\mathcal{A}|\,|\mathcal{B}| > p(n-1)^2$, akkor $\sum_{a \in \mathcal{A}} \sum_{b \in \mathcal{B}} \sum_{x=0}^{p-1} \sum_{k=1}^{p-1} e\left(\frac{k(h(x)-a-b)}{p}\right) > 0$. Ezzel a 3.13. tételt bizonyítását befejeztük.

A 3.13. tételnek egyszerű következménye az általánosított Fermat kongruencia megoldhatóságára vonatkozó állítás.

3.17. Következmény. *Legyen $f(x), g(x), h(x) \in F_p[x]$ polinomok fokszáma közül a legnagyobb n, p prím és $p > n^4$.*

a) Tegyük fel, hogy az $f(x), g(x), h(x)$ polinomok között van egy, amely $p-1$-nek semelyik $d > 1$ osztójára nem áll elő $c\,(q(x))^d$ alakban, ahol $c \in F_p$ és $q(x) \in F_p[x]$. Ekkor az $f(x)g(y) \equiv h(z) \mod p$ kongruencia megoldható.

b) Az $f(x) + g(y) \equiv h(z) \mod p$ kongruencia megoldható.

Ez az állítás nem új (lásd [21, 97-98.o.]); csak a nézőpont, amellyel megközelítettük a problémát, hiszen ezt az eredményt speciális eseteként kaptuk meg egy hibrid sorozatokra vonatkozó általános tételnek.

A tétel a) részének igazolásakor csak azt az esetet nézzük, amikor $d|p-1$, $d > 1$ esetén $h(x)$ nem egy polinom d-edik hatványának konstansszorosa. A többi eset ugyanúgy bizonyítható mint ez. Legyen $\mathcal{A} = \{f(x) : x \in F_p\}$, $\mathcal{B} = \{g(y) : y \in F_p\}$. Ekkor $|\mathcal{A}|, |\mathcal{B}| \geq \frac{p-1}{n}$ mivel az $f(x) \equiv a \mod p$, $g(y) \equiv a$

mod p kongurenciák bármelyikének legfeljebb n megoldása van. Így $|\mathcal{A}|\,|\mathcal{B}| > p\left(\frac{p-1}{p-n}\right)^2(n-1)^2$. Ezután a 3.13. tételt alkalmazva a 3.18. következmény állítását kapjuk.

4. ab+1 alakú számoknak egy oszthatósági tulajdonsága

Diofantosz problémájának egy lehetséges megfordítása az, ha olyan $\mathcal{A}, \mathcal{B}$ halmazok méretét becsüljük, ahol $\mathcal{A} \times \mathcal{B} + 1$ minden eleme négyzetmentes szám. Először felső becslést adunk.

4.1. Tétel. *Ha $\mathcal{A}, \mathcal{B} \subseteq \{1, 2, \ldots, N\}$ és $\mathcal{A} \times \mathcal{B} + 1$ minden eleme négyzetmentes szám, akkor*

$$|\mathcal{A}|\,|\mathcal{B}| \ll N^{\frac{3}{2}}(\log N)^2.$$

A bizonyításhoz a következő jelöléseket használjuk: Minden m-re, legyen $f(m)$ azon mod m maradékosztályok száma, amelyek metszik $\mathcal{A}$-t. Hasonlóan $g(m)$ azon mod m maradékosztályok száma, amelyek metszik $\mathcal{B}$-t. Legyen végül $\rho(m)$ azon mod m maradékosztályok száma, amelyek diszjunktak $\mathcal{A}$-tól. A következő lemma a kínai maradéktételre épül.

4.2. Lemma. *Legfeljebb egy p prím létezik, hogy $\sqrt[4]{\frac{N}{2}} \leq p \leq \sqrt[4]{N}$ és $\rho(p^2) < p^c$, ahol $c = 2\frac{\log|\mathcal{A}| - \log 2}{\log N}$.*

Tegyük fel ugyanis, hogy két különböző prím is eleget tesz a lemma feltételeinek: p_1 és p_2. A kínai maradéktétel szerint legfeljebb $\rho(p_1^2)\rho(p_2^2)$ darab olyan mod $p_1^2p_2^2$ maradékosztály van, amely metszi $\mathcal{A}$-t. Felhasználva ezt, és azt, hogy $\sqrt[4]{\frac{N}{2}} \le p_1, p_2 \le \sqrt[4]{N}$, kapjuk:

$$|\mathcal{A}| \le \rho(p_1^2)\rho(p_2^2)\left\lceil \frac{N}{p_1^2p_2^2} \right\rceil \le 2\rho(p_1^2)\rho(p_2^2) < 2(p_1p_2)^c \le 2N^{\frac{c}{2}} = |\mathcal{A}|\,.$$

Ezzel ellentmondásra jutottunk.

A 4.1. tétel bizonyítása során feltehetjük, hogy $|\mathcal{A}| \ge 2\sqrt{N}(\log N)^2$ és $|\mathcal{B}| \ge 2\sqrt{N}(\log N)^2$, különben a tétel triviális. Ha $N \ge e^4$ és $\sqrt[4]{\frac{N}{2}} \le p \le \sqrt[4]{N}$, úgy

$$2\frac{\log|\mathcal{A}| - \log 2}{\log N} \ge 2\frac{\log\left(\sqrt{N}(\log N)^2\right)}{\log N} = 1 + \frac{4\log\log N}{\log N} \ge$$

$$\ge 1 + \frac{8\log 2}{\log N} \ge 1 + \frac{\log 2}{\log\sqrt[4]{\frac{N}{2}}} \ge \frac{\log(2p)}{\log p}.$$

Ez alapján, a 4.2. lemmát alkalmazva kapjuk, hogy legfeljebb egy olyan $p_{\mathcal{A}}$ prím létezik, melyre $\sqrt[4]{\frac{N}{2}} \le p_{\mathcal{A}} \le \sqrt[4]{N}$ és $\rho(p_{\mathcal{A}}^2) < 2p_{\mathcal{A}}$. Ezért, ha $\sqrt[4]{\frac{N}{2}} \le p \le \sqrt[4]{N}$ prím és $p \ne p_{\mathcal{A}}$, akkor $f(p^2) \le p^2 - 2p$. Hasonlóan bizonyíthatjuk, hogy legfeljebb egy $p_{\mathcal{B}}$ prím kivételével, minden $\sqrt[4]{\frac{N}{2}} \le p \le \sqrt[4]{N}$ prímre teljesül az, hogy $g(p^2) \le p^2 - 2p$.

Legyen x egy tetszőleges mod p^2 maradékosztály, amely metszi $\mathcal{A}$-t és $(x, p^2) = 1$. Ekkor egyértelműen létezik egy x^* maradékosztály, melyre

$$xx^* \equiv -1 \mod p^2.$$

Nyilvánvaló, hogy ez az x^* maradékosztály diszjunkt $\mathcal{B}$-től. Ezért $\rho(p^2) - p \le g(p^2)$, és így $p^2 - f(p^2) - p \le g(p^2)$. Tehát:

$$f(p^2) + g(p^2) \ge p^2 - p.$$

A nagy szita következő alakját Sárközy Gábor [29, 274.o.] bizonyította: Ha $\mathcal{A}, \mathcal{B} \subseteq \{1, 2, \ldots, N\}$, $\mathcal{M} \subseteq \{1, 2, \ldots, [\sqrt{N}]\}$, és $\mathcal{M}$ elemei páronként relatív prímek, akkor

$$|\mathcal{A}| \leq \frac{2N}{\sum\limits_{m \in \mathcal{M}} \frac{f(m)}{m-f(m)}}, \ |\mathcal{B}| \leq \frac{2N}{\sum\limits_{m \in \mathcal{M}} \frac{g(m)}{m-g(m)}}.$$

Összeszorozva e két egyenlőtlenséget:

$$|\mathcal{A}|\,|\mathcal{B}| \leq \frac{4N^2}{\sum\limits_{m \in \mathcal{M}} \frac{f(m)}{m-f(m)} \sum\limits_{m \in \mathcal{M}} \frac{g(m)}{m-g(m)}}. \tag{4.1}$$

Legyen $\mathcal{M} = \{p^2 : \sqrt[4]{\frac{N}{2}} \leq p \leq \sqrt[4]{N},\ p \text{ prím},\ p \neq p_{\mathcal{A}} \text{ és } p \neq p_{\mathcal{B}}\}$. A (4.1) jobboldalán álló tört nevezőjét alulról becsüljük a Cauchy-Schwarz egyenlőtlenség segítségével.

$$\sum_{p^2 \in \mathcal{M}} \frac{f(p^2)}{p^2 - f(p^2)} \sum_{p^2 \in \mathcal{M}} \frac{g(p^2)}{p^2 - g(p^2)} \geq$$

$$\geq \left(\sum_{p^2 \in \mathcal{M}} \sqrt{\frac{f(p^2)g(p^2)}{p^4 - (f(p^2) + g(p^2))p^2 + f(p^2)g(p^2)}} \right)^2.$$

Mivel $f(p^2) + g(p^2) \geq p^2 - p$ és $f(p^2), g(p^2) \leq p^2 - 2p$, ha $p^2 \in \mathcal{M}$, ezért ekkor

$$f(p^2)g(p^2) \geq (p^2 - 2p)(f(p^2) + g(p^2) - (p^2 - 2p)) \geq (p^2 - 2p)p \geq \frac{p^3}{3}.$$

Így:

$$\left(\sum_{p^2 \in \mathcal{M}} \sqrt{\frac{f(p^2)g(p^2)}{p^4 - (f(p^2) + g(p^2))p^2 + f(p^2)g(p^2)}} \right)^2 \geq$$

$$\geq \left(\sum_{p^2 \in \mathcal{M}} \sqrt{\frac{f(p^2)g(p^2)}{p^3 + f(p^2)g(p^2)}} \right)^2 = \left(\sum_{p^2 \in \mathcal{M}} \sqrt{1 - \frac{p^3}{p^3 + f(p^2)g(p^2)}} \right)^2 \geq$$

$$\geq \left(\sum_{p^2 \in \mathcal{M}} \sqrt{1 - \frac{p^3}{p^3 + p^3/3}} \right)^2 = \left(\sum_{p^2 \in \mathcal{M}} \frac{1}{2} \right)^2 \gg \frac{\sqrt{N}}{(\log N)^2}.$$

Ezt a (4.1) egyenlőtlenségbe írva, kapjuk:

$$|\mathcal{A}|\,|\mathcal{B}| \ll N^{\frac{3}{2}} (\log N)^2.$$

Ezzel a 4.1. tételt igazoltuk.

Ezután egy alsó becslést adunk $|\mathcal{A}| = |\mathcal{B}|$ esetén.

4.3. Tétel. *a) Léteznek $\mathcal{A}, \mathcal{B} \subseteq \{1, 2, \ldots, N\}$ halmazok, melyekre*

$$|\mathcal{A}| = |\mathcal{B}| \gg (\log N)^2,$$

és $\mathcal{A} + \mathcal{B}$ minden eleme négyzetmentes szám.

b) Léteznek $\mathcal{A}, \mathcal{B} \subseteq \{1, 2, \ldots, N\}$ halmazok, melyekre

$$|\mathcal{A}| = |\mathcal{B}| \gg (\log N)^2$$

és $\mathcal{A} \times \mathcal{B} + 1$ minden eleme négyzetmentes szám.

Az alsó és a felső becslés elég messze van egymástól. Valószínűnek tartom, hogy a két becslés közül, az alsó van közelebb az igazsághoz. A fenti tétel gráfelméleten alapul.

Jelölje p_i az i-edik prímszámot, és legyen N elég nagy pozitív egész szám. Definiáljuk K-t a következő módon:

$$\prod_{i=1}^{K-1} p_i < N^{\frac{1}{6}} \leq \prod_{i=1}^{K} p_i. \tag{4.2}$$

Legyen $P \overset{\text{def}}{=} \prod_{i=1}^{K} p_i$. Ekkor, a prímszám tétel szerint

$$\log P = \sum_{i=1}^{K} \log p_i \sim \sum_{n \leq p_K} \Lambda(n) \sim p_K. \tag{4.3}$$

Így nagy N-ekre:

$$N^{\frac{1}{6}} \leq P < N^{\frac{1}{5}}. \tag{4.4}$$

Tekintsük a következő gráfelméleti lemmát.

4.4. Lemma. *Tegyük fel, hogy a G egyszerű gráfnak n szögpontja és m éle van. Ha G nem tartalmaz $K_{r,r}$-t, akkor*

$$2m < \sqrt[r]{r-1} \cdot n^{2-\frac{1}{r}} + (r-1)n.$$

A bizonyítás megtalálható [24]-ben. Ebből a lemmából vezetjük le a következőt.

4.5. Lemma. *Létezik n_0 pozitív szám, hogy ha $n \geq n_0$, és G egyszerű gráfnak n szögpontja, m éle van, továbbá*

$$r \leq \min\left\{\frac{2m}{n}, \frac{\binom{n}{2}-m}{n}, \frac{n^2 \log n}{7\left(\binom{n}{2}-m\right)} - \frac{3\log n}{7}\right\},$$

akkor G tartalmaz $K_{r,r}$-t.

Tegyük fel, hogy a lemma állítás nem igaz. Ekkor a 4.4. lemma szerint:

$$2m < \sqrt[r]{r-1} \cdot n^{2-\frac{1}{r}} + (r-1)n.$$

$r \leq \frac{2m}{n}$, tehát:

$$(2m-(r-1)n)^r < (r-1)n^{2r-1}.$$

Ebből, és az $r-1 \leq \sqrt{\frac{\binom{n}{2}-m}{n}\frac{n^2\log n}{7\left(\binom{n}{2}-m\right)}} \leq n^{\frac{4}{7}}$, $rn \leq \binom{n}{2}-m$, $1+x < e^x$ egyenlőtlenségekből kapjuk:

$$n^{\frac{3}{7}} \leq \frac{n}{r-1} < \left(\frac{n^2}{2m-(r-1)n}\right)^r = \left(1+\frac{2\left(\binom{n}{2}-m\right)+rn}{n^2-2\left(\binom{n}{2}-m\right)-rn}\right)^r <$$

$$< \left(1 + \frac{3\left(\binom{n}{2} - m\right)}{n^2 - 3\left(\binom{n}{2} - m\right)}\right)^r < e^{r\frac{3\left(\binom{n}{2}-m\right)}{n^2-3\left(\binom{n}{2}-m\right)}}.$$

Ezt r-re rendezve:

$$\frac{n^2 \log n}{7\left(\binom{n}{2} - m\right)} - \frac{3 \log n}{7} < r,$$

ami ellentmondás.

Legyen $f(a,b)$ értéke $a+b$ az a) esetben és $ab+1$ a b) esetben. A 4.3. tétel bizonyítása céljából nézzük azt a gráfot, amelynek szögpontjai $1, 2P+1, 4P+1, \ldots, \left[\frac{N-1}{2P}\right] 2P+1$. Az x, y szögpontokat pontosan akkor köti össze él G-ben, ha $f(x,y)$ négyzetmentes szám. Ha $x, y \in \{1, 2P+1, 4P+1, \ldots, \left[\frac{N-1}{2P}\right] 2P+1\}$, akkor (x,y) pár értéke legyen $f(x,y)$.

P definiciója miatt nincs olyan (x,y) pár, amelynek értéke osztható egy olyan q^2-tel, ahol $q \le p_K$ és q prím. Azon pároknak a száma, melyeknek értéke osztható egy olyan q^2-tel, ahol $q \ge p_K$ és q prím:

$$\sum_{k=0}^{\left[\frac{N-1}{2P}\right]} \sum_{\substack{\ell=0 \\ q^2 | f(2Pk+1, 2P\ell+1)}}^{\left[\frac{N-1}{2P}\right]} 1 \le \sum_{k=0}^{\left[\frac{N-1}{2P}\right]} \left(\frac{\left[\frac{N-1}{2P}\right]}{q^2} + 1\right) =$$

$$= \frac{\left[\frac{N-1}{2P}\right]^2 + \left[\frac{N-1}{2P}\right]}{q^2} + \left[\frac{N-1}{2P}\right] + 1. \tag{4.5}$$

Mivel $x + y \le 2N$ így az a) esetben nincs olyan (x,y) pár, amelynek az értéke osztható egy $\frac{N^2}{P^2}$-nél nagyobb számmal.

A b) esetben pedig legfeljebb $\left(\pi(N) - \pi\left(\frac{N}{P}\right)\right) P^2 < P^2 N$ olyan $xy+1$ szám van, melynek létezik egy q^2 alakú osztója, ahol $q^2 > \frac{N^2}{P^2}$, és q prím. Wigert's tétele [35] szerint, ha N elég nagy, és $xy+1$ értéke adott, úgy x legfeljebb $d(xy) \le \max\limits_{m \le N^2} d(m) \le N^{\frac{2}{\log\log N}}$ értéket vehet fel. Összefoglalva, a b) esetben legfeljebb $P^2 N^{1+\frac{2}{\log\log N}}$ olyan (x,y) pár van, amelynek értéke osztható egy olyan q^2 számmal, ahol $q^2 > \frac{N^2}{P^2}$ és q prím. (4.4) alapján $P^2 N^{1+\frac{2}{\log\log N}} < \frac{N^2}{P^2 \log N}$.

(4.3), (4.4) és (4.5) szerint, azoknak az (x,y) pároknak a száma, amelyeknek az értéke nem négyzetmentes, kevesebb mint

$$\frac{N^2}{P^2\log N} + \sum_{\substack{p_{K+1}\le q\le \frac{N}{P}\\ q\ prime}} \left(\frac{\left[\frac{N-1}{2P}\right]^2}{q^2} + 3\left[\frac{N-1}{2P}\right]\right) \le \frac{N^2}{P^2\log N} + \sum_{p_{K+1}\le q} \frac{\left[\frac{N-1}{2P}\right]^2}{q(q-1)}$$

$$+3\left[\frac{N-1}{2P}\right]\pi\left(\frac{N}{P}\right) \ll \frac{N^2}{P^2\log N} + \frac{\left[\frac{N-1}{2P}\right]^2}{p_{K+1}-1} \ll \frac{\left[\frac{N-1}{2P}\right]^2}{\log\left[\frac{N-1}{2P}\right]}.$$

Kiszámoltuk tehát, hogy a G gráfnak $n = \left[\frac{N-1}{2P}\right] + 1$ szögpontja és $m > \binom{n}{2} - c\frac{n^2}{\log n}$ éle van, ahol c konstans. Hagyjunk el G-ből éleket addíg, amig a G-nek pontosan $\left[\binom{n}{2} - c\frac{n^2}{\log n}\right] + 1$ darab éle nem lesz. A 4.5. lemmát alkalmazva, azonnal adódik, hogy G tartalmaz $K_{r,r}$-t, ahol $r = \left[\frac{(\log n)^2}{8c}\right]$. Könnyen látszik, hogy ha $\mathcal{A}$ és $\mathcal{B}$ halmazoknak $K_{r,r}$ két osztályát választjuk, úgy azok eleget tesznek a 4.3. tétel feltételeinek.

Felmerül a kérdés, hogy egy halmaz esetén, hogyan módosul ez az alsó becslés.

4.6. Tétel. *a) Létezik $\mathcal{A} \subseteq \{1,2,\dots,N\}$ halmaz, melyre $|\mathcal{A}| \gg \log N$ és $\mathcal{A}+\mathcal{A}$ minden eleme négyzetmentes szám.*
b) Létezik $\mathcal{A} \subseteq \{1,2,\dots,N\}$ halmaz, melyre $|\mathcal{A}| \gg \log N$ és $\mathcal{A}\times\mathcal{A}+1$ minden eleme négyzetmentes szám.

A tétel a) része Erdős Páltól és Sárközy Andrástól [8] származik. Most egy új bizonyítást adunk erre a tényre, együtt kezelve az additív és a multiplikatív esetet.

Legyen $f(a,b)$ értéke továbbra is $a+b$ az a) esetben és $ab+1$ a b) esetben. Kicsit módosítjuk az előző bizonyításban szereplő G gráf definicióját.

$$V(G) \stackrel{\text{def}}{=} \left\{2\ell P+1 : f(2\ell P+1, 2\ell P+1) \text{ négyzetmentes, } 1 \le \ell \le \left[\tfrac{N-1}{2P}\right]\right\}.$$

Erre azért van szükség, mert különben előfordulhatna, hogy $a \in \mathcal{A}$ esetén $a+a$ (illetve a b) esetben $aa+1$) nem négyzetmetes szám. Az éleket ugyanúgy definiáljuk, ahogy a 4.3. tétel bizonyításában.

Érdemes G gráfban minél nagyobb teljes gráfot keresni, és annak csúcsait választani az $\mathcal{A}$ halmaznak. Ehhez először G gráf n szögpontszámát és m élszámát becsüljük.

Az a) esetben triviális, hogy $n \gg \left[\frac{N-1}{2P}\right]$. Belátjuk, hogy ugyanez fennáll a b) esetben is. Ehhez azon ℓ-ek számát kell becsülni, ahol $(2\ell P+1)^2+1$ nem négyzetmentes szám. Két esetet különböztetünk meg aszerint, hogy $(2\ell P+1)^2+1$-nek létezik-e olyan q^2 osztója, ahol $q > \left(\frac{N}{12P}\right)$ és q prím.

Legyen q prím. Ha $q < p_K$ úgy $q^2 \nmid (2\ell P+1)^2+1$. Ha $p_K < q$ akkor legfeljebb $\frac{N-1}{p^2P}+2$ olyan $1 \le \ell \le \left[\frac{N-1}{2P}\right]$ szám van, amelyre $q^2 \mid (2\ell P+1)^2+1$. Tehát legfeljebb

$$\frac{N}{6P} + \frac{N-1}{p_K^2 P} + \frac{N-1}{p_{K+1}^2 P} + \frac{N-1}{p_{K+2}^2 P} \cdots < \frac{N}{6P} + \frac{2N}{P\log P} < \frac{N}{5P}$$

olyan $1 \le \ell \le \left[\frac{N-1}{2P}\right]$ szám van, amelyre $(2\ell P+1)^2+1$-nek van egy q^2 osztója, ahol $q \le \frac{N}{12P}$ és q prím. A másik esetben, mikor $(2\ell P+1)^2+1$-nek olyan q^2 osztója van, ahol $q > \frac{N}{12P}$ és q prím, felírhatjuk a következő Pell-egyenletet:

$$(2\ell P+1)^2+1 = q^2 D.$$

Ekkor $D \le \frac{(2\ell P+1)^2+1}{\left(\frac{N}{12P}\right)^2} \le \frac{N^2+1}{\left(\frac{N}{12P}\right)^2} < 150P^2$. Fix D-re az $a^2-p^2D=-1$ Pell-egyenlet megoldásszáma $a \in \{1,2,\ldots,N\}$, $q \in \mathbb{N}$-re nem haladja meg $\frac{\log N}{\log 2}$-t.

Ezért a

$$(2\ell P+1)^2 - p^2 D = -1$$

egyenlet megoldásszáma $2\ell P+1 \in \{1,\dots,N\}$, $q \in \mathbb{N}$, $D \in \{1,\dots 150P^2\}$-re kevesebb mint $150P^2 \frac{\log N}{\log 2} < 500P^2 \log N$. Összesen, tehát legfeljebb

$$\frac{N}{5P} + 500P^2 \log N < \frac{1}{2}\left[\frac{N-1}{2P}\right]$$

olyan $1 \le \ell \le \left[\frac{N-1}{2P}\right]$ szám van, amelyre $(2\ell P+1)^2+1$ nem négyzetmentes szám. Ezzel a b) esetben is beláttuk, hogy $V(G) = n \gg \left[\frac{N-1}{2P}\right]$.

A 4.3. tétel bizonyítása szerint $E(G) = m > \binom{n}{2} - c' \frac{n^2}{\log n}$, ahol c' konstans. A Turán tételt [33] alkalmazva adódik a 4.6. tétel állítása.

5. Hatvány, hatványteli számok összegsorozatokban

A. Sárközy, J. Rivat, C.L.Stewart [26] foglalkozott azzal a problémával, amikor $a, a' \in \mathcal{A}$, $a \ne a'$ esetén $a+a'$ négyzetszám. Ennek egy további lehetséges általánosítása az, ha $a, a' \in \mathcal{A}$, $a \ne a'$ esetén $a+a'$ mindig hatványszám. Később ennek az eredménynek egy részhalmaz összegekre vonatkozó analogonját vizsgáljuk.

Legyen V a hatványszámok halmaza:

$$V = \left\{x^k : x \in \mathbb{N},\ k \in \mathbb{N},\ k \ge 2\right\},$$

és minden K egész számra

$$V_K = \left\{x^k : x \in \mathbb{N},\ k \in \mathbb{N},\ 2 \le k \le K\right\}.$$

Egy n számot pontosan akkor nevezünk hatványtelinek, ha $p \mid n$, p prím esetén $p^2 \mid n$ is teljesül. A hatványteli számok halmaza legyen W:

$$W = \left\{ n : n \in \mathbb{N},\ p \mid n\ p \text{ prím esetén } p^2 \mid n \right\}.$$

Végül az $\mathcal{A}$ halmaz minden véges részhalmazára vegyük a benne lévő elemek összegét:

$$\mathcal{P}(\mathcal{A}) = \left\{ \sum_{a \in \mathcal{A}} \varepsilon_a a : a \in \mathcal{A}\ \varepsilon_a = 0 \text{ vagy } 1,\ 0 < \sum_{a \in \mathcal{A}} \varepsilon_a < \infty \right\}.$$

5.1. Tétel. *Létezik $c_1 > 0$ konstans, hogy ha $N, K > 1$ egész számok, $\mathcal{A} \subseteq \{1, 2, \ldots, N\}$ és $a, a' \in \mathcal{A}$, $a \neq a'$ esetén $a + a' \in V_K$, akkor*

$$|\mathcal{A}| < c_1 e^{46K} \log N.$$

Az 5.1. tétel bizonyításhoz szükségünk van néhany lemmára. Az 5.2. lemmában és bizonyításában $q, q_1, q_2, \ldots$ prímeket jelöl.

5.2. Lemma. *Legyen $K \geq 2$ egész szám és $Q_K = \prod_{q \leq K} q$. Tegyük fel, hogy p prímre*

$$p \equiv 1 \pmod{Q_K}. \tag{5.1}$$

Legyen $\mathcal{B} \subseteq \mathbb{Z}_p$ halmaz, melyre $b, b' \in \mathcal{B}$ $b \neq b'$ esetén létezik egy k és x egész, hogy $2 \leq k \leq K$, továbbá

$$b + b' \equiv x^k \mod p. \tag{5.2}$$

Ekkor létezik egy abszolút $c_2 > 0$ konstans, melyre

$$|\mathcal{B}| < c_2 (\log K) 2^{\pi(K)} p^{\frac{1}{2}}. \tag{5.3}$$

Ha rögzített b, b' és k esetén megoldható a (5.2) kongruencia, úgy nyilvánvaló, hogy

$$b + b' \equiv y^q \pmod p$$

kongruencia is megoldható, ha q prím és $q \mid k$. Minden q prímre és n egészre $f_q(n)$-t a következőképpen definiáljuk:

$$f_q(n) = \begin{cases} 1 & \text{ha } n \equiv y^q \pmod p \text{ kongruencia megoldható,} \\ 0 & \text{különben.} \end{cases}$$

Az előző megjegyzésből következik, hogy az $F_K(n) \stackrel{\text{def}}{=} 1 - \prod_{2 \le q \le K}(1 - f_q(n))$ függvényre teljesül az alábbi:

$$F_K(n) = \begin{cases} 1 & \text{ha } n \equiv y^k \pmod p \text{ kongruencia megoldható} \\ & \text{valamilyen } 2 \le k \le K \text{ egész számra,} \\ 0 & \text{különben.} \end{cases}$$

A lemma $\mathcal{B}$-re vonatkozó feltétele miatt:

$$\sum_{b \in \mathcal{B}} \sum_{b' \in \mathcal{B}} F_K(b + b') \ge \sum_{\substack{b, b' \in \mathcal{B} \\ b \ne b'}} 1 = |\mathcal{B}|^2 - |\mathcal{B}|.$$

Legyen g primitív gyök modulo p. Ha $q \le K$ prím, akkor jelölje χ_q azt az egyértelműen meghatározott modulo p karaktert, amelyre

$$\chi_q(g) = e\left(\frac{1}{q}\right);$$

megjegyezzük, hogy $q \le K$ és (5.1) miatt $p \mid q - 1$, tehát valóban létezik ilyen karakter. Mivel ez a karakter q-ad rendű:

$$f_q(n) = \frac{1}{q} \sum_{j=0}^{q-1} \chi_q^j(n) \qquad \text{ha } (n, p) = 1. \tag{5.4}$$

$F_K(n)$ definiciójából és (5.4)-ből következik, hogy ha $(n,p)=1$, akkor:

$$\begin{aligned}
F_K(n) &= \sum_{\ell=1}^{\pi(K)} (-1)^{\ell+1} \sum_{q_1<\dots<q_\ell\le K} \prod_{i=1}^{\ell} f_{q_i}(n) \\
&= \sum_{\ell=1}^{\pi(K)} (-1)^{\ell+1} \sum_{q_1<\dots<q_\ell\le K} \frac{1}{q_1\cdots q_\ell} \sum_{j_1=0}^{q_1-1} \cdots \sum_{j_\ell=0}^{q_\ell-1} \chi_{q_1}^{j_1}\cdots\chi_{q_\ell}^{j_\ell}(n).
\end{aligned} \tag{5.5}$$

Érdemes külön vizsgálni azt a két esetet, amikor $\chi_{q_1}^{j_1}\dots\chi_{q_\ell}^{j_\ell}$ főkarakter illetve azt, amikor nem az. $\chi_{q_1}^{j_1}\dots\chi_{q_\ell}^{j_\ell}$ pontosan akkor főkarakter, ha $(\chi_{q_1}(g))^{j_1}\dots(\chi_{q_\ell}(g))^{j_\ell} = e\left(\frac{j_1}{q_1}+\dots+\frac{j_\ell}{q_\ell}\right)=1$, azaz $\frac{j_1}{q_1}+\dots+\frac{j_\ell}{q_\ell}$ egész, ami $0\le j_1<q_1,\dots,0\le j_\ell<q_\ell$ esetén ekvivalens azzal, hogy $j_1=\dots=j_\ell=0$. Így (5.5) alapján:

$$\begin{aligned}
\sum_{\substack{b,b'\in\mathcal{B}\\(b+b',p)=1}} F_K(b+b') &= \sum_{\ell=1}^{\pi(K)} (-1)^{\ell+1} \sum_{q_1<\dots<q_\ell\le K} \frac{1}{q_1\cdots q_\ell} \sum_{\substack{b,b'\in\mathcal{B}\\(b+b',p)=1}} 1 \\
&+ \sum_{\ell=1}^{\pi(K)} (-1)^{\ell+1} \sum_{q_1<\dots<q_\ell\le K} \frac{1}{q_1\cdots q_\ell} \sum_{\substack{0\le j_1<q_1,\dots,0\le j_\ell<q_\ell\\(j_1,\dots,j_\ell)\ne(0,\dots,0)}} \\
&\sum_{\substack{b,b'\in\mathcal{B}\\(b+b',p)=1}} \chi_{q_1}^{j_1}\cdots\chi_{q_\ell}^{j_\ell}(b+b') = \sum\nolimits_1 + \sum\nolimits_2 .
\end{aligned}$$

Ezután $\sum_1, \sum_2$ értékét becsüljük. $\sum_1$ szorzattá alkítható, majd a Mertens Tétel alapján felülről becsülhető:

$$\begin{aligned}
\left|\sum\nolimits_1\right| &= \left(1-\prod_{q\le K}\left(1-\frac{1}{q}\right)\right) \sum_{\substack{b,b'\in\mathcal{B}\\(b+b',p)=1}} 1 \le \left(1-\prod_{q\le K}\left(1-\frac{1}{q}\right)\right)|\mathcal{B}|^2 < \\
&< |\mathcal{B}|^2 - \frac{2\,|\mathcal{B}|^2}{c_2\log K}.
\end{aligned}$$

Mivel $\sum_2$-ben a $\chi_{q_1}^{j_1} \dots \chi_{q_\ell}^{j_\ell}$ karakter nem főkarater, ezért a 2.12. tételt használva a következőt kapjuk:

$$\begin{aligned}\left|\sum\nolimits_2\right| &\le \sum_{\ell=1}^{\pi(K)} \sum_{q_1<\dots<q_\ell\le K} \frac{1}{q_1\cdots q_\ell} \sum_{\substack{0\le j_1<q_1,\dots,0\le j_\ell<q_\ell \\ (j_1,\dots,j_\ell)\ne(0,\dots,0)}} \left| \sum_{\substack{b,b'\in\mathcal{B} \\ (b+b',p)=1}} \chi_{q_1}^{j_1}\cdots\chi_{q_\ell}^{j_\ell}(b+b')\right| \\ &\le \sum_{\ell=1}^{\pi(K)} \sum_{q_1<\dots<q_\ell\le K} \frac{1}{q_1\cdots q_\ell} \sum_{\substack{0\le j_1<q_1,\dots,0\le j_\ell<q_\ell \\ (j_1,\dots,j_\ell)\ne(0,\dots,0)}} p^{\frac{1}{2}}|\mathcal{B}| \\ &\le p^{\frac{1}{2}}|\mathcal{B}| \sum_{\ell=1}^{\pi(K)} \sum_{q_1<\dots<q_\ell\le K} 1 < p^{\frac{1}{2}}|\mathcal{B}|2^{\pi(K)}.\end{aligned}$$

Összefoglalva:

$$\begin{aligned}|\mathcal{B}|^2 - |\mathcal{B}| \le \sum_{b\in\mathcal{B}}\sum_{b'\in\mathcal{B}} F_K(b+b') \le \sum_{\substack{b,b'\in\mathcal{B} \\ (b+b',p)=1}} F_K(b+b') + |\mathcal{B}| = \sum\nolimits_1 + \sum\nolimits_2 + \\ + |\mathcal{B}| < |\mathcal{B}|^2 - \frac{2\,|\mathcal{B}|^2}{c_2 \log K} + p^{1/2}|\mathcal{B}|2^{\pi(K)} + |\mathcal{B}|.\end{aligned}$$

Ebből pedig már a lemma állítása már triviálisan következik.

A Linnik konstans segítségével igazolható az alábbi lemma.

5.3. Lemma. *Léteznek q_0, c_3 konstansok, hogy ha $q \ge q_0$, $a \in \mathbb{Z}$, $(a,q) = 1$ és*

$$x \ge q^{80}, \tag{5.6}$$

akkor

$$\sum_{\substack{\frac{x}{q^8}<p<x \\ p\equiv a \pmod q}} \frac{\log p}{p} > c_3 \frac{\log q}{\varphi(q)}. \tag{5.7}$$

Mivel a bizonyítás kissé hosszadalmas, ezért elhagyjuk.

Most már rátérhetünk az 5.1. tétel bizonyítására. Tegyük fel, hogy $\mathcal{A}$ és K eleget tesz a tétel feltételeinek. Legyen $Q_K = \prod_{\substack{q \leq K, \\ q \text{ prím}}} q$, és $p \equiv 1 \mod Q_K$. $\mathcal{B}_p$ definiciója az alábbi:

$$\mathcal{B}_p = \{b : b \in \{0, 1, \dots, p-1\},\ \exists\ a \in \mathcal{A} \text{ melyre } a \equiv b \pmod{p}\}.$$

Mivel $\mathcal{B}_p$ halmaz teljesíti az 5.1. lemma feltételeit, ezért

$$|\mathcal{B}_p| < c_2 \log K 2^{\pi(K)} p^{1/2}.$$

A 3.12. lemma jelöléseit használva, ebből

$$\nu_{\mathcal{A}}(p) < c_2 \log K 2^{\pi(K)} p^{1/2}.$$

Legyen $\mathcal{P} = \left\{p : p \text{ prím},\ p \leq C Q_K^{80} (\log N)^2 \;\; p \equiv 1 \mod Q_K\right\}$, ahol C konstans elegendően nagy. A 3.12. és az 5.3. lemmát valamint a Brun-Titchmarsh egyenlőtlenséget alkalmazva, kapjuk:

$$|\mathcal{A}| \leq c_1 e^{46} \log N.$$

Ezzel az 5.1. tételt igazoltuk.

Az 5.1. tételben V_K-t V-vel helyettesítve lényegesen gyengébb felső becslést tudunk adni.

5.4. Tétel. *Létezik N_0 konstans, hogy ha $N > N_0$ positív egész, és $\mathcal{A} \subseteq \{1, 2, \dots, N\}$ halmazra teljesül, hogy $a, a' \in \mathcal{A},\ a \neq a'$ esetén $a + a' \in V$, akkor*

$$|\mathcal{A}| < \exp\left(22(\log N)^{1/2}\right).$$

A tételt indirekten bizonyítjuk. Tegyük fel, hogy

$$|\mathcal{A}| \geq \exp\left(22(\log N)^{1/2}\right).$$

Legyen $K = \frac{1}{5}(\log N)^{1/2}$, és $a \in \mathcal{A}$-ra jelölje $S(a)$ a következő halmazt:

$$S(a) = \{a' : \ a + a' = x^k, \text{ ahol } x \in \mathbb{N}, k \in \mathbb{N}, \ k > K\}.$$

Mivel $a + a' \leq 2N$ minden $a, a' \in \mathcal{A}$-ra, ezért

$$\begin{aligned} |S(a)| &\leq \left|\left\{x^k : \ x \in \mathbb{N}, \ k \in \mathbb{N}, \ k > K, \ x^k \leq 2N\right\}\right| \\ &\leq \sum_{K < k \leq \frac{\log 2N}{\log 2}} (2N)^{\frac{1}{K}} < \exp\left(11(\log N)^{\frac{1}{2}}\right) \end{aligned} \tag{5.8}$$

minden $a \in \mathcal{A}$ esetén. Legyen $L = \exp\left(11(\log N)^{\frac{1}{2}}\right)$ és $r = \left[\frac{|\mathcal{A}|}{2L}\right]$. $\mathcal{A}_0, \mathcal{A}_1, \ldots, \mathcal{A}_r$ halmazokat és $b_1, b_2, \ldots, b_r$ egész számokat a következő módon definiáljuk: $\mathcal{A}_0 = \mathcal{A}$, és ha $1 \leq i \leq r$, akkor legyen $b_i \in \mathcal{A}_{i-1}$, $b_i \notin \{b_1, \ldots, b_{i-1}\}$ tetszőleges egész, és $\mathcal{A}_i = \mathcal{A}_{i-1} \backslash S(b_i)$. (5.8)-ből következik, hogy $|\mathcal{A}_i| > |\mathcal{A}_{i-1}| - L$, így $|\mathcal{A}_i| > |\mathcal{A}| - iL$. Tehát

$$|\mathcal{A}_r| \geq |\mathcal{A}| - rL = |\mathcal{A}| - \left[\frac{|\mathcal{A}|}{2L}\right] L \geq \frac{|\mathcal{A}|}{2},$$

ezért az előző rekurzív definició valóban működik.

Legyen $\mathcal{B} = \{b_1, b_2, \ldots, b_r\}$. Ekkor

$$|\mathcal{B}| = r = \left[\frac{|\mathcal{A}|}{2L}\right] > \exp\left(10(\log N)^{\frac{1}{2}}\right).$$

Másrészt $b_1, \ldots, b_r$ számok és $\mathcal{A}_0, \mathcal{A}_1, \ldots, \mathcal{A}_r$ halmazok definiciója miatt $b_i + b_j \in V_K$, $1 \leq i < j \leq r$ esetén. Az 5.1.tétel szerint:

$$|\mathcal{B}| < c_1 e^{46K} \log N < \exp\left(10(\log N)^{\frac{1}{2}}\right),$$

ha N elég nagy. Ez azonban ellentmond $\mathcal{B}$ méretére vonatkozó előző eredményünknek.

A következő tétel végtelen sok elemből álló $\mathcal{A}$ halmazok sűrűségét vizsgálja. Ehhez legyen $A(x) = |\{a: \ a \in \mathcal{A}, \ a \leq x\}|$.

5.5. Tétel. *Ha $\mathcal{A} \subseteq \mathbb{N}$ halmazra teljesül, hogy $a, a' \in \mathcal{A}, \ a \neq a'$ esetén $a + a' \in V$, akkor*

$$\liminf_{x \to +\infty} \frac{A(x)}{\log x} \leq 4.$$

Megint indirekten bizonyítunk. Tegyük fel, hogy

$$\liminf_{x \to +\infty} \frac{A(x)}{\log x} > 4. \tag{5.9}$$

Ekkor $\mathcal{A}$ végtelen sok elemből áll. Tehát létezik tetszőlegesen nagy x, amelyre $\mathcal{A} \cap (x/2, \ x] \neq \emptyset$. Vagyis van egy $\overline{a} \in \mathcal{A}$, amelyre $\frac{x}{2} < \overline{a} \leq x$. Ha x elég nagy, akkor (5.9) szerint

$$A(x^{1/2}) > 4 \log x^{1/2} = 2 \log x.$$

Minden $a \in \mathcal{A}$ esetén létezik $y \in \mathbb{N}, \ \ell = \ell(a) \in \mathbb{N}, \ \ell \geq 2$ melyre $a + \overline{a} = y^{\ell}$. Ekkor:

$$2^{\ell} \leq y^{\ell} = a + \overline{a} \leq 2x$$

ahonnan, nagy x-re:

$$\ell \leq \frac{\log x}{\log 2} + 1 < 2 \log x.$$

A skatulya elv szerint létezik $a_1, a_2 \in \mathcal{A}$, $a_1 < a_2 \leq x^{1/2}$, melyre $\ell(a_1) = \ell(a_2) = \ell$. Vagyis létezik u és v egész, hogy

$$a_1 + \overline{a} = u^\ell,$$

$$a_2 + \overline{a} = v^\ell.$$

Ekkor

$$v^\ell - u^\ell = a_2 - a_1 < a_2 \leq x^{1/2}. \tag{5.10}$$

Másrészt

$$v^\ell - u^\ell \geq (u+1)^\ell - u^\ell \geq \ell u^{\ell-1} \geq \ell (u^\ell)^{1/2} > \ell \overline{a}^{1/2} > \ell \left(\frac{x}{2}\right)^{1/2} > x^{1/2}.$$

Ez ellentmond (5.10)-nek. Tehát a tétel állítás igaz. Alsó becslésként a következőt igazoljuk:

5.6. Tétel. *$N \geq 3$ esetén létezik olyan $\mathcal{A} \subseteq \{1, 2, \dots, N\}$ halmaz, melyre $\mathcal{A} + \mathcal{A} \subseteq V$ és*

$$|\mathcal{A}| \geq \left[\frac{\log \log N}{12 \log \log \log N}\right].$$

Legyen $\mathcal{A} = \{x, 2x, 3x, \dots, nx\}$, ahol $n = \left[\frac{\log \log N}{12 \log \log \log N}\right]$. x értékét később adjuk meg. Ekkor $\mathcal{A} + \mathcal{A} = \{2x, 3x, \dots, 2nx\}$. Jelölje az i-edik prímszámot p_i, és legyen ℓ az a lehető legnagyobb egész szám, amelyre

$$p_\ell \leq 2n.$$

$1 \leq t \leq 2n - 1$ esetén $t + 1$ prímtényezős felbontása legyen a következő:

$$t + 1 = p_1^{\beta_{1,t}} p_2^{\beta_{2,t}} \dots p_\ell^{\beta_{\ell,t}}.$$

A továbbiakban x értékét is $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_\ell^{\alpha_\ell}$ alakban keressük. Ekkor $(t+1)x$ akkor és csak akkor p_t-edik hatvány minden $1 \le t \le 2n-1$-re, ha

$$\alpha_i + \beta_{i,t} \equiv 0 \mod p_t \qquad 1 \le i \le \ell,\ 1 \le t \le 2n-1 \text{ esetén.} \tag{5.11}$$

A kínai maradéktétel szerint (5.11)-nek létezik megoldása $(\alpha_1, \alpha_2, \dots, \alpha_\ell)$-ben, sőt ez a megoldás egyértelmű modulo $p_1 p_2 \dots p_{2n-1}$. Ezért feltehetjük $\alpha_1, \alpha_2, \dots, \alpha_\ell$ eleget tesz (5.11)-nek, és

$$0 \le \alpha_i \le p_1 p_2 \dots p_{2n-1} \qquad \text{ha } 1 \le i \le \ell.$$

Vagyis ekkor $\mathcal{A} + \mathcal{A}$ minden eleme hatványszám. Továbbá:

$$\begin{aligned} 0 &\le \alpha_i \le p_1 p_2 \dots p_{2n-1} \le 4^{p_{2n-1}} < e^{11n \log n}, \\ nx &= n p_1^{\alpha_1} p_2^{\alpha_2} \dots p_\ell^{\alpha_\ell} < n(p_1 p_2 \dots p_\ell)^{e^{11n \log n}} < \\ &< n 4^{p_\ell e^{11n \log n}} < n 4^{2n e^{11n \log n}} < e^{e^{12n \log n}} < N. \end{aligned}$$

Így $\mathcal{A} = \{x, 2x, \dots, nx\} \subseteq \{1, 2, \dots, N\}$ is teljesül, ezzel a tétel állítását beláttuk.

Ezután rátérünk a hatványteli számok esetére. Ekkor is megadható akármilyen nagy halmaz a kivánt tulajdonsággal.

5.7. Tétel. *Létezik N_1 konstans, hogy $N > N_1$ esetén van olyan $\mathcal{A} \subseteq \{1, 2, \dots, N\}$ halmaz, melyre $\mathcal{A} + \mathcal{A} \subseteq W$ és*

$$|\mathcal{A}| > \frac{1}{5} \log N.$$

Legyen $P_x = \prod\limits_{\substack{p \le x \\ p \text{ prím}}} p$. Jelölje x azt a legnagyobb pozitív egészet, amelyre $\frac{1}{2} x P_x^2 \le N$. Könnyen ellenőrizhető, hogy az

$$\mathcal{A} = \{ i P_x^2 :\ 1 \le i \le \frac{x}{2},\ i \in \mathbb{N} \}$$

halmaz eleget tesz a tétel feltételeinek.

$\mathcal{A} + \mathcal{A} \subseteq W$ esetén csak triviális felső becsléseket tudunk adni az $\mathcal{A}$ halmaz méretére. Ezért inkább a kérdés részhalmaz összegekre vonatkozó analogonját vizsgáljuk. Jelölje $F(N)$ az olyan $\mathcal{A}$ halmazok elemszámának maximumát, amelyre $\mathcal{A} \subseteq \{1, 2, \dots, N\}$, $P(\mathcal{A}) \subseteq W$.

5.8. Tétel. *Létezik $c_4, c_5 > 0$ konstansok, hogy ha $N \geq 4$ egész, akkor*

$$c_4(\log N)^{1/2} < F(N) < c_5(\log N)^3(\log\log N)^{-1/2}.$$

Az alsó becslés bizonyítása hasonló mint az előző tételé. P_x-t ugyanúgy definiáljuk, ahogyan ott. Jelölje ezúttal azonban x azt a legnagyobb egészet, amelyre $x^{1/2}P_x^2 \leq N$. Ekkor az $\mathcal{A} = \{iP_x^2 :\ 1 \leq i \leq x^{1/2},\ i \in \mathbb{N}\}$ halmaz elemszáma nagyobb mint $c_4\,(\log N)^{1/2}$, és $\mathcal{P}(\mathcal{A}) \subseteq W$.

A következő lemmát Sárközy András bizonyította [30]-ben. (Megjegyzem, hogy [30]-ben c_6, c_7, c_8, c_9 konstansok értéke számszerűen volt megadva, nekünk azonban a pontos értékekre nincs szükségünk.)

5.9. Lemma. *Ha N pozitív egész, $\mathcal{A} \subset \{1, 2, \dots, N\}$ és*

$$|\mathcal{A}| > c_6(N\log N)^{1/2}, \tag{5.12}$$

akkor léteznek $d,\ y,\ z$ pozitív egészek, melyekre

$$d < c_7N|\mathcal{A}|^{-1},\ z > c_8|\mathcal{A}|^2,\ y < c_9Nz|\mathcal{A}|^{-2},$$

továbbá

$$\{yd,\ (y+1)d, \dots, zd\} \subset \mathcal{P}(\mathcal{A}).$$

Az 5.9. lemmából levezetjük a következőt:

5.10. Lemma. *Létezik $c_{10} > 0$ konstans, hogy ha p elegendően nagy prím, $\mathcal{B} \subset \{1, \dots, p^2 - 1\}$, $|\mathcal{B}| > c_{10} p (\log p)^{\frac{1}{2}}$, akkor van egy $s = \sum_{b \in \mathcal{B}} \varepsilon_b b \in \mathcal{P}(\mathcal{B})$, melyre $p \mid s$, $p^2 \nmid s$.*

Ha c_{10} konstans elég nagy, akkor $N = p^2$, $\mathcal{A} = \mathcal{B}$ helyettesítéssel alkalmazható az 5.9. lemma. Eszerint létezik d, z, y, melyre

$$\begin{aligned} & d < c_7 p^2 |\mathcal{B}|^{-1} < c_{11} p (\log p)^{-\frac{1}{2}}, \\ & z > c_8 |\mathcal{B}|^2 > c_{12} p^2 \log p, \\ & y < c_9 p^2 z |\mathcal{B}|^{-2} < c_{13} z (\log p)^{-1}, \end{aligned} \tag{5.13}$$

és

$$\{yd, (y+1)d \dots, zd\} \subset \mathcal{P}(\mathcal{B}). \tag{5.14}$$

Ha p prím nagy, akkor (5.13) miatt $(d, p) = 1$. Tekintsük az yd, $(y+1)d$, $(y+2)d, \dots$ számtani sorozatban az első két p-vel osztható elemet. $(d, p) = 1$, tehát ezek közül valamelyikre, mondjuk ud-re teljesül

$$p \mid ud, \quad p^2 \nmid ud.$$

Nyilvánvaló, hogy $y \le u \le u + 2p$. (5.13)-ből következik:

$$z - y > z - c_{13} z (\log p)^{-1} > \frac{z}{2} > c_{14} p^2 \log p.$$

Összefoglalva

$$y \le u \le y + 2p < y + c_{14} p^2 \log p < z.$$

Így $ud \in \mathcal{P}(\mathcal{A})$, és ezzel a lemmát beláttuk.

Az 5.10. lemma segítségével befejezhetjük az 5.8. tétel bizonyítását. Tegyük fel, hogy $\mathcal{A} \subseteq \{1, 2, \ldots, N\}$ és $\mathcal{P}(\mathcal{A})$ minden eleme hatványteli szám. $P_x = \prod_{p \le x,\ p \text{ prím}} p$ továbbra is, de most x azt a legkisebb pozitív egészet jelöli, amelyre $P_x^2 > N$. A prímszámtétel miatt

$$x = \left(\frac{1}{2} + o(1)\right) \log N. \tag{5.15}$$

Minden $p \le x$ prímre, legyen

$$\mathcal{A}_p = \{a : \ a \in \mathcal{A},\ p^2 \nmid a\}. \tag{5.16}$$

$A = \bigcup_{p \le x,\ p \text{ prím}} \mathcal{A}_p$, hiszen az ellenkező esetben, létezik $a \in \mathcal{A}$, hogy $a \notin \mathcal{A}_p$ minden $p \le x$ prímre. Ekkor $\mathcal{A}_p$ definiciója miatt $p^2 \mid a$ is teljesül minden $p \le x$ prímre. Tehát $P_x^2 \mid a$, ahonnan $N < P_x^2 \le a$, ami ellentmond $a \in \mathcal{A} \subseteq \{1, 2, \ldots, N\}$-nek.

Ezután $\mathcal{A}_p$ méretét becsüljük. Fix $p \le x$ prímre, $r(n)$ jelölje n-nek a legkisebb nem negatív maradékát modulo p^2.

$$r(n) \equiv n \mod p^2, \quad 0 \le r(n) < p^2.$$

Legyen

$$\mathcal{B} = \{b : \exists\ a \in \mathcal{A}_p,\ \text{melyre}\ \ r(a) = b\}.$$

(5.10) miatt $0 \notin \mathcal{B}$.

Tegyük fel, hogy van egy $s = b_1 + \cdots + b_t \in \mathcal{P}(\mathcal{B})$ (ahol $b_1, \ldots, b_t \in \mathcal{B}$, $b_1 < b_2 < \cdots < b_t$), amelyre $p \mid s$, $p^2 \nmid s$. $\mathcal{B}$ deiniciója miatt létezik $a_1, \ldots, a_t \in \mathcal{A}$, ahol

$$r(a_1) = b_1, \ldots, r(a_t) = b_t.$$

Innen $a_1 + \dots + a_t \equiv b_1 + \dots + b_t \equiv s \mod p^2$, és ezért

$$p \mid a_1 + \dots + a_t, \quad p^2 \nmid a_1 + \dots + a_t.$$

Tehát $a_1 + \dots + a_t$ nem lehet hatványteli szám. Ezzel ellentmondásra jutottunk, vagyis $s \in \mathcal{P}(\mathcal{B})$ esetén, ha p prím és $p \mid s$, akkor $p^2 \mid s$.

Az 5.10. lemma miatt

$$|\mathcal{B}| \le c_{10} p (\log p)^{1/2}. \tag{5.17}$$

Másrészt bebizonyítjuk, hogy minden $b \in \mathcal{B}$ esetén

$$\left|\{a : \ a \in \mathcal{A}_p, \ a \equiv b \pmod{p^2}\}\right| < p. \tag{5.18}$$

Valóban, az ellenkező esetben létezik:

$$a_1 \equiv \dots \equiv a_p \equiv b \mod p^2,$$

ahol $a_1, \dots, a_p \in \mathcal{A}$, $a_1 < \dots < a_p$. Ekkor $a_1 + \dots + a_p \equiv pb \mod p^2$. Így:

$$p \mid a_1 + \dots + a_p \quad \text{de} \quad p^2 \nmid a_1 + \dots + a_p.$$

Tehát $a_1 + \dots + a_p$ nem hatványteli szám, ami ellenmond $\mathcal{P}(\mathcal{A}) \subseteq W$-nek.

(5.17) és (5.18) szerint:

$$\begin{aligned} |\mathcal{A}_p| &= \sum_{b \in \mathcal{B}} \left|\{a : a \in \mathcal{A}_p, \ a \equiv b \pmod{p^2}\}\right| \\ &< \sum_{b \in \mathcal{B}} p = |\mathcal{B}| p \le c_{10} p^2 (\log p)^{1/2}. \end{aligned}$$

Mivel, $\mathcal{A} = \bigcup_{p \le x, \ p \text{ prím}} \mathcal{A}_p$, ezért (5.15) alapján:

$$\begin{aligned} |\mathcal{A}| &\le \sum_{p \le x} |\mathcal{A}_p| \le c_{10} \sum_{p \le x} p^2 (\log p)^{1/2} \\ &< c_{11} (\log N)^3 (\log \log N)^{-1/2}. \end{aligned}$$

Ezzel beláttuk az 5.8. tételt.

6. Hatványszámok multiplikatív struktúrákban

Az előző fejezetben, akkor becsültük az $\mathcal{A}$ halmaz méretét, ha $a, a' \in \mathcal{A}$, $a \neq a'$ esetén $a + a'$ hatványszám. Most ennek a multiplikatív analogonját vizsgáljuk, azt az esetet, amikor $\mathcal{A} \cdot \mathcal{A} + 1$ halmaz minden eleme hatványszám. Ehhez V_K és V halmazokat ugyanúgy definiáljuk, ahogyan az 5. fejezetben.

6.1. Tétel. *Létezik N_0 konstans, hogy ha $N > N_0$, $K \geq 2$ egész, $\mathcal{A} \subseteq \{1, \dots, N\}$ és $\mathcal{A} \cdot \mathcal{A} + 1 \subseteq V_K$, akkor*

$$|A| < 160 \frac{K^2}{(\log K)^2} \log \log N.$$

A tétel bizonyítása két gráfelméleti lemmán alapul. A Turán tétel [33] egyszerű következménye az alábbi.

6.2. Lemma. *Tegyük fel, hogy $r \geq 2$ egész, és G egyszerű gráfnak n szögpontja és m éle van. Ha*

$$m > \frac{r-2}{2(r-1)} n^2,$$

akkor G tartalmaz r szögpontú teljes gráfot.

P. Kővári, V. Sós, P. Turán [22]-tól származik az következő lemma.

6.3. Lemma. *Tegyük fel, hogy a G egyszerű gráfnak n szögpontja és m éle van. Ha*

$$m > \frac{1}{2} \left(n^{\frac{3}{2}} + n - n^{\frac{1}{2}} \right),$$

akkor G tartalmaz $K_{r,r}$-t.

A tétel bizonyításához, az állítással ellentétben, tegyük fel, hogy

$$|A| \geq 160 \frac{K^2}{(\log K)^2} \log \log N.$$

Mivel $M = 1 + \frac{1}{\log 2} \log(\log N / \log 2)$ esetén $N < 2^{2^{M+1}}$, ezért ha N elég nagy, létezik $1 \leq m \leq 1 + \frac{1}{\log 2} \log(\log N / \log 2) = M$ egész, amelyre

$$\left| \mathcal{A} \cap \{2^{2^m}, 2^{2^m} + 1, \ldots, 2^{2^{m+1}} - 1\} \right| > 110 \frac{K^2}{(\log K)^2}.$$

Legyen a fenti $\mathcal{A} \cap \{2^{2^m}, 2^{2^m} + 1, \ldots, 2^{2^{m+1}} - 1\}$ halmaz $\mathcal{A}_m$, és G teljes gráfnak a szögpontjai $\mathcal{A}_m$ elemei. Ekkor $n = V(G) > 110 \frac{K^2}{(\log K)^2}$. Ezután G gráf minden élét megszínezzük a $c_2, c_3, \ldots, c_K$ színek valamelyikével a következő módon: az $a, a' \in V(G)$ között futó él színe c_ℓ, ahol ℓ az a legkisebb pozitív egész, amelyre $aa' + 1$ ℓ-edik hatvány. Ekkor persze ℓ prím. Jelölje $2 \leq i \leq K$ esetén b_i a c_i színű élek számát G-ben.

Ha $b_2 > \frac{7}{16} n^2$, akkor a 6.2. lemma szerint G gráfban van 9 szögpont, hogy közöttük minden él színe c_2, azaz létezik 9 szám, hogy bármely kettő szorzatához 1-et adva mindig négyzetszámot kapunk. Dujella [4]-ben bebizonyította, hogy nem létezik 9 szám a fenti tulajdonsággal. Tehát $b_2 \leq \frac{7}{16} n^2$. Ebből

$$b_3 + \cdots + b_K \geq \binom{n}{2} - \frac{7}{16} n^2 = \frac{n^2}{16} - \frac{n}{2}.$$

Rosser és Schoenfeld [27] bebizonyította, hogy $\pi(K) \leq \frac{5K}{4 \log K}$. Vagyis a skatulya elv miatt van $3 \leq p \leq K$ prím, hogy

$$b_p \geq \frac{4 \log k}{5k} \left(\frac{n^2}{16} - \frac{n}{2} \right).$$

Legyen G_p szögpontjai G-nek szögpontjai, és G_p élei G-nek c_p színű élei. Mivel $n > 110\frac{K^2}{(\log K)^2}$, ezért

$$\frac{4\log K}{5k}\left(\frac{n^2}{16}-\frac{n}{2}\right) = n^{\frac{3}{2}}\frac{\log K}{K}\,\frac{n^{\frac{1}{2}}}{20}\left(1-\frac{8}{n}\right) >$$
$$> n^{\frac{3}{2}}\frac{\sqrt{110}}{20}\left(1-\frac{8}{110}\left(\frac{\log 3}{3}\right)^2\right) > 0.519n^{\frac{3}{2}}.$$

Viszont

$$\frac{1}{2}\left(n^{\frac{3}{2}}+n-n^{\frac{1}{2}}\right) < \frac{1}{2}n^{\frac{3}{2}}\left(1+\frac{1}{\sqrt{n}}\right) < \frac{1}{2}n^{\frac{3}{2}}\left(1+\frac{1}{\sqrt{110}}\,\frac{\log 3}{3}\right) < 0.518n^{\frac{3}{2}}.$$

Tehát:

$$b_p > \frac{4\log K}{5K}\left(\frac{n^2}{16}-\frac{n}{2}\right).$$

Vagyis 6.3. lemma szerint G_p-ben van $K_{2,2}$. Azaz létezik $x < y, c < d$, melyre $x, y, c, d \in V(G_p)$, és $xc+1, xd+1, yc+1, yd+1$ számok mindegyike p-edik hatvány. Az 1.2. lemma szerint

$$yd > (xc)^{p-1} \geq (xc)^2 .$$

De $x, y, c, d \in \{2^{2^m}, 2^{2^m}+1, \dots, 2^{2^{m+1}}-1\}$, ahonnan

$$yd < \left(2^{2^{m+1}}-1\right)^2 < 2^{2^{m+2}} \leq (xc)^2.$$

Ezzel ellentmondásra juttotunk. Tehát a tétel állítása igaz.

V_K helyett V-t írva a 6.1. tételben, a következőt tudjuk igazolni.

6.4. Tétel. *Létezik N_0 konstans, hogy ha $N > N_0$, pozitív egész, $\mathcal{A} \subseteq \{1, \dots, N\}$ és $\mathcal{A}\cdot\mathcal{A}+1 \subseteq V_K$, akkor*

$$|A| < 1340\frac{(\log N)^2}{\log\log N}.$$

Valóban, legyen K_0 a lehető legkisebb pozitív egész, amelyre $N^2+1 \leq 2^{K_0}$. Ekkor $2^{K_0-1} < N^2+1$, tehát $K_0 < 1 + \frac{1}{\log 2}\log(N^2+1)$. Mivel $a, a' \in \mathcal{A}$, $a \neq a'$ esetén $aa'+1 \leq N^2+1$, ezért $aa'+1$ legfeljebb K_0-adik hatvány. A 6.1. tételt alkalmazva megkapjuk a tétel állítását.

Szeretném megköszönni Sárközy András Tanár Úrnak a szép témát és a dolgozat megírásához nyújtott segítségét.

Hivatkozások

[1] J. Arkin, V. E. Hogatt, E. G. Straus,*On Euler's solution of a problem of Diophantus*, Fibonacci Quart 17 (1979), 333-339.

[2] E. R. Canfield, P. Erdős, C. Pomarence, *On a problem of Oppenheim concerning "Factorisatio Numerorum"*, J. Number Theory 17 (1983), 1-28.

[3] H. Davenport, *Multiplicative Number Theory*, Markham Publishing Co., Chicago, first ed., 1967.

[4] A. Dujella, *An absolute bound for the size of Diophantine m-tuples*, J. Number Theory, publikálás alatt.

[5] A. Dujella, *On Diophantine quintuples*, Acta Arithmetica 81 (1997), 69-79.

[6] A. Dujella, *On the size of Diophantine m-tuples*, Math. Proc. Cambridge Philos. Soc., publikálás alatt.

[7] P. Erdős, *Quelques problems de la theorie des nombres*, Monographie de l'enseignement mathematique, Geneve, (1963), 81-135.

[8] P. Erdős, A. Sárközy, *On divisibility properties of integers of the form a+a'*, Acta Math. Hung. 50 (1987), 117-122

[9] P. Erdős, N. H. Shapiro, *On the least primitive root of a prime*, Pacific J. Math. 7 (1957), 861-865.

[10] P. Erdős, C. L. Stewart, R. Tijdeman, *Some diophantine equations with many solutions*, Composito Mathematica 66 (1988), 37-48.

[11] P. Erdős, J. Surányi, *Válogatott fejezetek a számelméletből*, Polygon, Szeged, 1996, 215-217.

[12] P. Erdős, P. Turán, *On a problem in the elementary theory of numbers*, Amer. Math. Monthly 41 (1934), 608-611.

[13] P. Gibbs, *Some rational Diophantine sixtuples*, publikálás alatt.

[14] R.L. Graham, B.L. Rothschild, J.H. Spencer, *Ramsey Theory*, Wiley 1980, 75.

[15] K. Gyarmati, *On a problem of Diophantus*, Acta Arithmetica 97 (2001), 53-65.

[16] K. Gyarmati, *On divisibility properties of integers of the form ab+1*, Period. Math. Hungar. 43 (2001), 71-79.

[17] K. Gyarmati, A. Sárközy, C. L. Stewart, *On sums which are powers*, Acta Math. Hungar., publikálás alatt

[18] K. Gyarmati, A. Sárközy, C. L. Stewart, *On shifted products which are powers*, Mathematika, publikálás alatt.

[19] K. Győry, C. L. Stewart, R. Tijdeman, *On prime factors of sums of integers, I.*, Composito Math. 59 (1986), 81-88.

[20] K. Győry, A. Sárközy, C. L. Stewart, *On the number of prime factors of integers of form ab+1*, Acta Arithmetica 74 (1996), 365-385.

[21] K. Ireland, M. Rosen *A Classical Introduction to Modern Number Theory*, Springer-Verlag, 1980.

[22] P. Kővári, V. Sós and P. Turán, On a problem of K. Zarankiewicz, *Colloq.Math.* **3** (1954), 50-57.

[23] J. Lagrange, *Six entiers dont les sommes deux à deux sont des carrés*, Acta Arithmetica 40 (1981), 91-96.

[24] L. Lovász *Combinatorical Problems and Exercises*, Akadémiai Kiadó Budapest, 1979, 10. fejezet, 37. feladat.

[25] J.-L. Nicolas, *Six nombres dont les sommes deux à deux sont des carrés*, Calculeteur en Math (1975), Limoges, Bull. Soc. Math. France 49-50 (1977), 141-143.

[26] J. Rivat, A. Sárközy, C.L.Stewart, *Two problems on sum sets*, Illinois J. Math., publikálás alatt.

[27] J. B. Rosser, L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, *Illinois J. Math.* (1962), 64-94.

[28] A. Sárközy, *On difference sets of sequences of integers II.*, Annales Univ. Budapest Eötvös 21 (1978), 41-53.

[29] G. N. Sárközy, *On a problem of Erdős*, Acta Math. Hung. 60 (1992), 271-282.

[30] A. Sárközy, *Finite addition theorems, II.*, J. Number Theory **48** (1994), 197-218.

[31] W.M. Schmidt, *Equations over Finite Fields an Elementary Approach*, Lecture Notes in Mathematics, Vol. 536., Sringer-Verlag, 1976.

[32] W. Sierpienski, *A Solution of Problems in the Theory of Numbers*, Pergamon Press. Warszawa, first ed., 1964.

[33] P. Turán, *On the theory of graphs*, Coll. Math. 3 (1953) 19-30.

[34] I.M. Vinogradov, *A számelmélet alapjai*, Tankönyvkiadó, Budapest, 1952, 5. fejezet, 8. feladat.

[35] S. Wigert, *Sur l'ordre de grandeur du nombre de diviseurs d'un entier*, Arkiv für Mathematik 3 (1906/1907), 1-9.