Elemi Módszerek a Kombinatorikus Számelméletben

Gyarmati Katalin

katalin.gyarmati@ttk.elte.hu

Eötvös Loránd Tudományegyetem

Egyetemi Jegyzet

ELTE TTK, Matematikai Intézet

Tartalomjegyzék

Bevezetés

A kombinatorikus számelméletben gyakran használunk a kombinatorikából jól ismert módszereket, mint pl. leszámlálások, gráfok esetleg extremális halmazelmélet, és ezeket kombináljuk a szokásos számelméleti eszközeinkkel.

Illusztrációként tekintsünk egy egyszerű példát. A feladat a következő: bizonyítsuk be, hogy az $n+1 \mid \binom{2n}{n}$ oszthatóság mindig fennáll.

Ez akár egy nehéz feladatnak is tűnhet, ha elemi számelméleti módszerekkel szeretnénk megoldani, de ha észrevesszük, hogy a $\frac{1}{n+1}\binom{2n}{n}$ tört a jól ismert Catalan-szám a kombinatorikából, amely történetesen mindig egész szám (mivel bizonyos elrendezések számához kapcsolódik), akkor a bizonyítás jóval egyszerűbbé válik.

A kedvenc bizonyításaim a kombinatorikus számelméletből a gráf elméleti alkalmazásokhoz (mint például Ramsey elmélet vagy extremális gráfelmélet) kapcsolódnak. Olyan bizonyításokat próbáltam a jegyzetbe belevenni, amelyek a lehető legegyszerűbbek és elegendő megértésükhöz alapfokú kombinatorika és az elemi számelmélet ismerete (ilyen pl. a fenti tárgyakhoz kapcsolódó egyetemi matematika BSc kurzusok anyaga).

A jegyzet írása során széleskörű irodalmat használtam, amelyet a fejeztek végén a referenciajegyzékben ismertettem, annyira pontosan, amennyire tudtam. Ezek közül kiemelném, hogy pár fejezet megírása során Sárközy András egyetemi előadásaira is támaszkodtam (ahol ez releváns, ott ezt szintén az irodalomjegyzékben feltüntettem).

A jegyzetet a 2020/21-es online félévben kezdtem angolul tanuló matematikus MSc hallgatók számára, hogy alkalmazkodni tudjak a nehéz körülményekhez, és helyettesíteni tudjam a hagyományos táblát.

1. Fermat kongruencia

Az olvasó esetleg hallott már Hilbert problémáiról. Hilbert összesen 23-at vetett fel, ezek közül pedig tízet a II. Nemzetközi Matematikai Kongresszuson ismertetett.

Hilbert problémái jelentős előrelépéshez vezetnek a matematikában. A 10. probléma a következő volt:

Létezik-e univerzális (véges) algoritmus diofantikus egyenletek megoldására? (Egy egyenletet diofantikusnak hívunk, ha csak az egész megoldásokat keressük.)

Ebben a fejezetben a diofantikus egyenleteket kombinatorikus szempontból vizsgáljuk.

Mielőtt továbbhaladnánk vessünk egy pillantást a legismertebb diofantikus egyenletekre.

$ax + by = c$	Lineáris diofantikus egyenletek.
$x^n + y^n = z^n$ ha $n \geq 3$	nagy Fermat-tétel
$x^2 + y^2 = z^2$	Pitagoraszi számhármasok

$x^4 + y^4 + z^4 = w^4$	Euler [6] azt sejtette, hogy csak triviális megoldások vannak. Ezt Elkies [1] 1988-ban megcáfolta.

Tipikus kérdések diofantikus egyenletek kapcsán:

1. Létezik megoldás?
2. A könnyen megtalálható megoldásokon túl léteznek-e további megoldások?
3. Véges vagy végtelen sok megoldás létezik?
4. Le tudjuk-e írni az összes megoldást?
5. A gyakorlatban is megadható-e egy teljes listája az összes megoldásnak?

Az első kérdésre, bizonyos esetekben (ha szerencsések vagyunk), létezik egy egyszerű megoldás, annak bizonyítására, hogy a diofantikus egyenletnek egyáltalán nincs megoldása.

Példák:

1. Az $x^2 + y^2 = 3z^2$ egyenletnek nincs egész megoldása. Tekintsük az egyenletet modulo 3.
2. Végtelen sok $m \in \mathbb{Z}$ létezik, amelyre $x^3 + y^3 + z^3 = m$ egyenletnek nincs megoldása $\mathbb{Z}$-ben (kapcsolódik az ún. Waring problémához [7]). Legyen $m \equiv \pm 4 \pmod 9$ és tekintsük az egyenletet modulo 9.

Visszatérve Hilbert 10. problémájához::

Vajon létezik-e általános algoritmus, amellyel minden diofantikus egyenlet megoldható?

Ez a kérdés sokáig megoldatlan volt. Végül Martin Davis, Yuri Matiyasevich, Hilary Putnam és Julia Robinson bebizonyította, hogy nincs ilyen algoritmus (további részletekért ld. [8]).

Amint azt az 1. és 2. Példában láttuk, az egyenletet modulo m redukálva, időnként azt kapjuk, hogy az egyenletnek egyáltalán nincs megoldása.

Ezen túlmenően, vannak bizonyos történelmi feltételezések is, melyek szerint régebben úgy gondolták, hogy a moduláris vizsgálatok szinte minden diofantikus egyenlet esetében célhoz vezethetnek.

Vegyük például a híres Fermat sejtést, mely szerint az

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

egyenletnek csak triviális megoldási vannak, ha $n \geq 3$.

A triviális megoldások a következők: $x = 0$ vagy $y = 0$ vagy $z = 0$.

Fermat 1637-ben fogalmazta meg híres sejtését. A sejtést annak a könyv margójára írta, amit éppen olvasott, s mely írás szerint egy gyönyörű és rövid bizonyítást talált, csak sajnos, a margó túl szűk ahhoz, hogy leírja.

Nagyon sok matematikus próbálta megtalálni Fermat eredeti gyönyörű bizonyítását, de kudarcot vallottak.

Végül, Wiles [4], [5] bizonyította a sejtést 1994-ben, de a bizonyítása több mint 120 oldal hosszú volt.

Azonban a sejtés több mint 350 évig nyitott volt.

Úgy sejtem, hogy a múltban számos matematikus próbálta úgy megoldani a sejtést, hogy különböző m modulusokra modulo m vizsgálta az egyenletet.

Mit gondolnak, igaz-e a következő?

Bebizonyítható-e, hogy végtelen sok p prím létezik, amelyre az

$$x^n + y^n \equiv z^n \pmod{p}$$

kongruencia nem oldható meg?

Ez nem igaz, mert pl. az

$$x \equiv 0 \ (p) \qquad y \equiv z \ (p)$$

mindig megoldás. A következők a triviális megoldások:

$$x \equiv 0 \ (p) \quad \text{vagy} \quad y \equiv 0 \ (p) \quad \text{vagy} \quad z \equiv 0 \ (p)$$
$$\Updownarrow$$
$$xyz \equiv 0 \ (p).$$

De a feladat a következőre módosítható:

Vajon létezik-e végtelen sok p prím, hogy az

$$x^n + y^n \equiv z^n \pmod{p}.$$

kongruenciának csak triviális megoldásai vannak?

Úgy gondolom régebben nagyon sok matematikus próbált ilyen p prímeket találni...

Hogyan következne ebből a Fermat-sejtés?

Tegyük fel, hogy $p_1 < p_2 < p_3 < \dots$ prímeknek egy növekvő sorozata, úgy hogy a

$$x^n + y^n \equiv z^n \pmod{p_i},$$

kongruenciának csak triviális megoldásai vannak.. Ekkor $x \equiv 0 \ (p_i)$ vagy $y \equiv 0 \ (p_i)$ vagy $z \equiv 0 \ (p_i)$. Vagyis $p_i \mid xyz$.

De ez azt jelentené xyz-nek végtelen prímosztója van, amely nyilván ellentmondás.

Történetesen ez a módszer nem működik, Schur [3] 1916-os eredménye szerint. A következő tételben a $\lceil \cdot \rceil$ zárójel a felső egészrészt jelöli.

1.1 TÉTEL. (Schur) *Ha* $p \geq \lceil en! \rceil + 1$*, akkor az*

$$x^n + y^n \equiv z^n \pmod{p}$$

kongruenciának van nem triviális megoldása.

A bizonyítás kombinatorikus számelméletet használ.

A matematikai kutatóintézetek, egyetemek számos hibás bizonyítást kapnak olyan híres sejtések megoldására mint a Fermat vagy Goldbach sejtés...

Schur tétele a Fermat-sejtés sok hibás bizonyítását cáfolta meg azonnal, lényegesen megkönnyítve ezzel a lektorok dolgát.

A bizonyítás gráfelméletet, speciálisan Ramsey-elméletet használ. A szükséges eszközöket a következő alfejezetben tárgyaljuk.

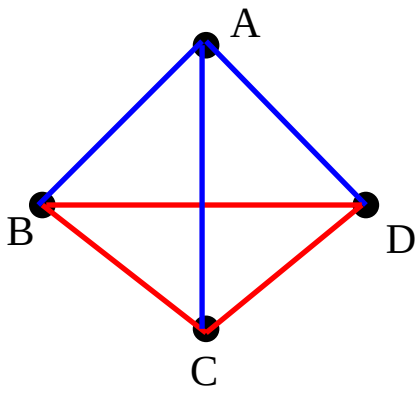
1.1. Ramsey-elmélet

Tegyük fel, hogy egy 6 tagú társaságban mindenki kölcsönösen ismeri vagy nem ismeri egymást, de a kapcsolat mindig szimmetrikus. Bizonyítsuk be, hogy létezik közöttük 3 ember, akik közül vagy mindenki ismer mindenkit, vagy senki nem ismer senkit.

Ez a feladat egy 6 szögpontú gráffal szemléltethető. Az embereket a szögpontok reprezentálják. Ha két ember ismeri egymást húzzunk közéjük egy kék élet, ha nem ismerik egymást, akkor pirosat.

Állítás: Ebben a gráfban létezik egyszínű háromszög.

Rögzítsünk egy A szögpontot. A skatulyaelv miatt létezik 3 másik szögpont, B, C és D, hogy az AB, AC, AD éleknek ugyanaz a színük, mondjuk kék.



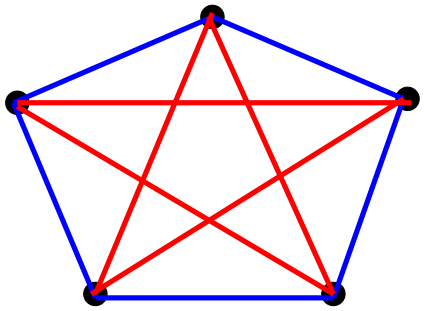
Amennyiben a BC él is kék, akkor ABC egy kék színű háromszög. Azaz a továbbiakban elegendő azt az esetet vizsgálni, amikor a BC él piros. Hasonlóan látható, hogy azt is feltehetjük, hogy a BD és CD élek pirosak. De ekkor mind BC, BD és CD élek pirosak, azaz BCD egy piros háromszög.

Jelölje $R_t(3)$ azt a legkisebb n természetes számot, amelyre igaz az, hogy egy n szögpontú teljes gráf éleit t darab színnel színezve, mindig létezik egyszínű háromszög.

Amennyiben egy 3 szögpontú teljes gráf éleit csak egy darab színnel színezzük, akkor abban nyilvánvalóan van egyszínű háromszög. Ezért:

$$R_1(3) = 3.$$

Az előző példában láttuk, hogy $R_2(3) \leq 6$. Másrészről $R_2(3) > 5$ mivel a következő ábrán megadtuk az 5 szögpontú teljes gráfnak egy olyan színezését, amely nem tartalmaz egyszínű háromszöget.



Így:

$$R_2(3) = 6.$$

Az előző ötletet általánosítva kapjuk, hogy

$$R_t(3) \leq t\,(R_{t-1}(3) - 1) + 2. \tag{1.1}$$

Lássuk a bizonyítás részleteit: Legyen $\mathcal{G}$ egy teljes gráf n szögponton.

Legyen $n \geq t\,(R_{t-1}(3) - 1) + 2$. Bebizonyítjuk, hogy ha egy n szögpontú G gráf éleit t darab színnel színezzük, akkor az mindig tartalmaz egyszínű háromszöget. Ebből (1.1) következik.

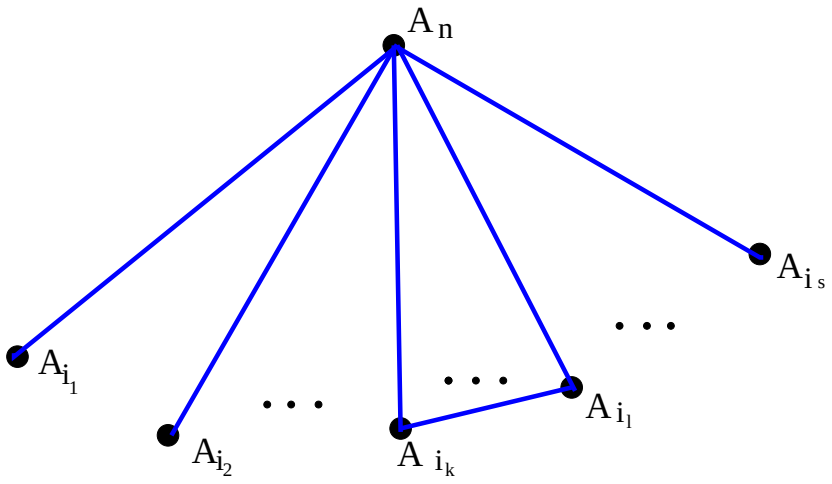
Jelölje a $\mathcal{G}$ gráf szögpontjait: $A_1, A_2, \ldots, A_n$. Rögzítsünk egy szögpontot, mondjuk A_n-et, és tekintsük az $A_1, A_2, \ldots, A_{n-1}$ szögpontokat. Ekkor

$$n - 1 \geq t\,(R_{t-1}(3) - 1) + 1,$$

így a skatulyaelv szerint létezik $s = R_{t-1}(3)$ darab szögpont, $A_{i_1}, A_{i_2}, \ldots, A_{i_s}$, melyekre az

$$A_nA_{i_1}, A_nA_{i_2}, \ldots, A_nA_{i_s}$$

élek azonos színűek. Legyen ez a szín mondjuk kék. Amennyiben $A_{i_1}, A_{i_2}, \ldots, A_{i_s}$ szögpontok között van kék él, mondjuk $A_{i_k}A_{i_\ell}$, akkor létezik kék színű háromszög: $A_nA_{i_k}A_{i_\ell}$:



Amennyiben pedig az $A_{i_1}, A_{i_2}, \ldots, A_{i_s}$ szögpontok között nincs kék él, akkor tekintsük azt a G_0 részgráfot, amelyek ezek a szögpontok kifeszítenek. A G_0 gráfnak nincs kék éle, azaz ebben a részgráfban az élek csak $t-1$ darab színnel vannak színezve. Jelölje a $\mathcal{G}_0$ gráf szögpontjainak számát $V(\mathcal{G}_0)$. Mivel

$$V(\mathcal{G}_0) = s = R_{t-1}(3),$$

az $R_{t-1}(3)$ szám definíciója alapján azt kapjuk, hogy $\mathcal{G}_0$ tartalmaz egyszínű háromszöget.

A továbbiakban t-re vonatkozó indukcióval belátjuk, hogy

$$R_t(3) \leq t!\left(1+\frac{1}{1!}+\frac{1}{2!}+\cdots+\frac{1}{t!}\right)+1. \tag{1.2}$$

Valóban, ha $t=1$ akkor

$$R_1(3) = 3 \leq 1!\left(1+\frac{1}{1!}\right)+1.$$

Amennyiben az állítás igaz $t = k - 1$, akkor igaz lesz $t = k$-ra is, ugyanis (1.1) alapján

$$\begin{aligned} R_k(3) &\leq k\left(R_{k-1}(3) - 1\right) + 2 \\ &\leq k \cdot (k-1)! \left(1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{(k-1)!}\right) + 2 \\ &= k! \left(1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{k!}\right) + 1. \end{aligned}$$

Ezzel beláttuk (1.2)-t. Mivel

$$t! \left(1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{t!}\right) \leq t! \left(1 + \frac{1}{1!} + \frac{1}{2!} + \ldots\right) = t!e,$$

azt kapjuk, hogy

1.2 TÉTEL. (Schur)

$$R_t(3) \leq \lceil t!e \rceil.$$

Az $R_t(3)$ Ramsey számokról további érdekességek találhatóak a következő oldalon: link.

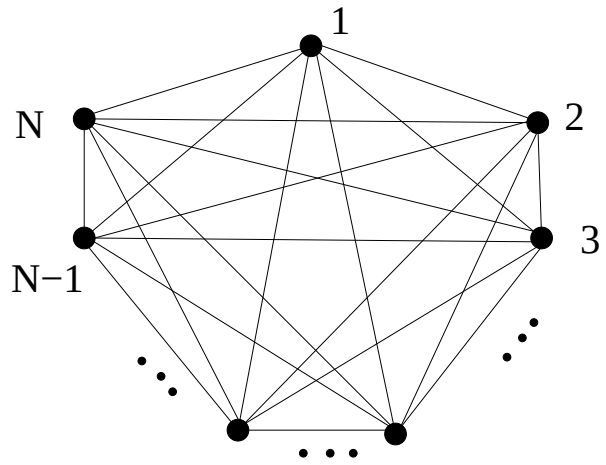
Az 1.2 Tételt használva kapjuk a következőt:

1.3 TÉTEL. (Schur) *Ha $N \geq \lceil t!e \rceil$ és az $\{1, 2, \ldots, N\}$ számokat t darab színnel színezzük, akkor az*

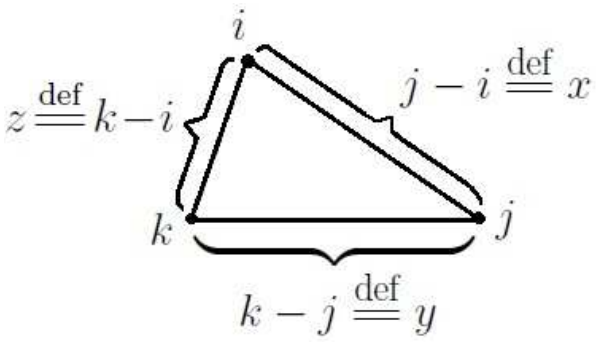
$$x + y = z.$$

egyenletnek létezik egyszínű, ún. monokromatikus megoldása (az-az x, y és z színe azonos).

Az 1.3 Tétel bizonyítása. Legyen $\mathcal{G}$ egy teljes gráf, amelynek szögpontjait az 1 és N közötti természetes számok reprezentálják.



A $\mathcal{G}$ gráf éleit t darab színnel színezzük a következő módon: Minden élhez hozzárendelünk egy értéket. Az i és j szögpontok között futó él értéke az $|i-j|$ természetes szám. Ekkor $|i-j| \in \{1,2,\ldots,N\}$, így ennek a természetes számnak van egy a tételben definiált színe. Ez a szín lesz az i és j szögpont között futó él színe. Mivel $R_t(3) \leq \lceil t!e \rceil \leq N$, a $\mathcal{G}$ gráf tartalmaz egyszínű háromszöget: $\{i,j,k\}$. Szimmetrikus okokból feltehetjük$i < j < k$. Ekkor:



A színezés definíciója miatt x, y és z azonos színű. Továbbá $x + y = z$ így $(j-i) + (k-j) = k-i$. Ezzel Schur tételét beláttuk.

Feladat. Hogyan következik Schur tételéből, hogy az $x^n + y^n \equiv z^n \pmod{p}$ Fermat kongruenciának mindig van nem triviális megoldása, ha p prím elég nagy?

Útmutató: Használjunk primitív gyököket!

Megoldás. Legyen p prímszám, amelyre $p \geq \lceil n!e \rceil + 1$. Legyen továbbá g egy primitív gyök $\mod p$. Ekkor

$$\{g^0, g^1, g^2, \ldots, g^{p-2}\}$$

egy redukált maradékrendszer $\mod p$. Vagyis $g^0, g^1, \ldots, g^{p-2}$ modulo p maradékosztályok megegyeznek az $1, 2, \ldots, p-2$ maradékosztályokkal (de nem ebben sorrendben). Azaz

$$\{g^0, g^1, g^2, \ldots, g^{p-2}\} \equiv \{1, 2, \ldots, p-1\} \pmod{p}.$$

Színezzük az $\{1, 2, 3, \ldots, p-1\}$ természetes számokat n darab különböző színnel.

Egy $s \in \{1, 2, \ldots, p-1\}$ természetes szám, akkor van színezve az r-edik színnel, ha létezik k egész szám, amelyre

$$s \equiv g^{kn+r} \pmod{p}.$$

Ez a következőképp illusztrálható:

$$\begin{aligned}
1.\text{ szín} &\equiv \{g, g^{n+1}, g^{2n+1}, \ldots\} \pmod{p} \\
2.\text{ szín} &\equiv \{g^2, g^{n+2}, g^{2n+2}, \ldots\} \pmod{p} \\
3.\text{ szín} &\equiv \{g^3, g^{n+3}, g^{2n+3}, \ldots\} \pmod{p} \\
&\vdots \\
n\text{-edik szín} &\equiv \{g^0, g^n, g^{2n}, \ldots\} \pmod{p}
\end{aligned}$$

A fenti színezésre fogjuk Schur tételét használni. Eszerint léteznek x, y és z egész számok, amelyekre

$$x + y = z$$

és x, y, z-nek azonos a színe. Jelöljük ezt a monokromatikus megoldást x_0, y_0, z_0-val. Ekkor

$$x_0 + y_0 = z_0.$$

Mivel x_0, y_0, z_0-nak azonos a színe, a színezés definíciója miatt létezik r, k, ℓ és m természetes számok, melyekre

$$\begin{aligned} x_0 &\equiv g^{kn+r} \pmod{p} \\ y_0 &\equiv g^{\ell n+r} \pmod{p} \\ z_0 &\equiv g^{mn+r} \pmod{p}. \end{aligned}$$

Ekkor

$$\begin{aligned} x_0 + y_0 &= z_0 \\ x_0 + y_0 &\equiv z_0 \pmod{p} \\ g^{kn+r} + g^{\ell n+r} &\equiv g^{mn+r} \pmod{p} \\ g^{kn} + g^{\ell n} &\equiv g^{mn} \pmod{p} \end{aligned}$$

Így, ha a, b és c-t $a \equiv g^k,\ b \equiv g^\ell,\ c \equiv g^m \pmod{p}$-val definiáljuk, akkor

$$a^n + b^n \equiv c^n \pmod{p},$$

amivel beláttuk a tétel állítását.

Hivatkozások

[1] N. Elkies, *On $A^4 + B^4 + C^4 = D^4$*, Mathematics of Computation. 51 (184) (1988), 825–835.

[2] P. Erdős, J. Surányi, *Válogatott Fejezetek a Számelméletből*, Polygon 2004, link.

[3] I. Schur, *Über die Kongruenz* $x^m + y^m \equiv z^m \mod p$, Jahresber. Deutsche Math.-Verein. 25, 114-116, 1916.

[4] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Annals of Mathematics. 141 (3) (1995), 443–551.

[5] R. Taylor, A. Wiles, *Ring theoretic properties of certain Hecke algebras*, Annals of Mathematics. 141 (3) (1995), 553–572.

[6] Wikipedia, Euler's sum of powers conjecture, link.

[7] Wikipedia, Waring's problem, link.

[8] Wikipedia, Hilbert's tenth problem, link.

[9] Kép, David Hilbert, Wikipedia, link.

[10] Kép of Léonard Cotte, Paris, link.

[11] Fejezetbeli ábrák, házi készítésűek.

2. További Ramsey-elméleti alkalmazások

Az első fejezetben a Ramsey-elmélet egy trükkös alkalmazását láttuk. Most két másik számelméleti alkalmazást mutatunk be. De mielőtt továbbmennénk, néhány szó az elmélet megalkotójáról: Ramseyt nemcsak a matematika nyűgözte le, de sok más területen is dolgozott, különösen a közgazdaságtanban. Többek között még érdekelte a pszichoanalízis is.

A Ramsey-elmélet jól ismert a matematikában az alkalmazkodóképességéről; nem csak a számelméletben, hanem a harmonikus elemzésben is alkalmazzák, ergodikus elmélet, geometria, információelmélet, logika stb.

A Ramsey-elmélet jól ismert a matematikában az alkalmazásairól is; nem csak a számelméletben, hanem a harmonikus analízisben is használják, továbbá ergodikus elméletben, geometriában, információelméletben, logikában stb.

A következő példa Sárközytől [4] származik.

2.1 TÉTEL. (Sárközy) *Legyen p egy $4k+1$ alakú prímszám. Ekkor létezik $\mathcal{A} \subseteq \mathbb{Z}_p$, amelyre*

$$|\mathcal{A}| \geq \left\lceil \frac{1}{4} \log p \right\rceil$$

és minden $a - a'$ különbség, ahol $a, a' \in \mathcal{A}$ kvadratikus maradék modulo p vagy nulla.

A 2.1 Tétel bizonyítása. A tétel bizonyításához gráfelmélet szükséges. Megint Ramsey-elméletet használunk.

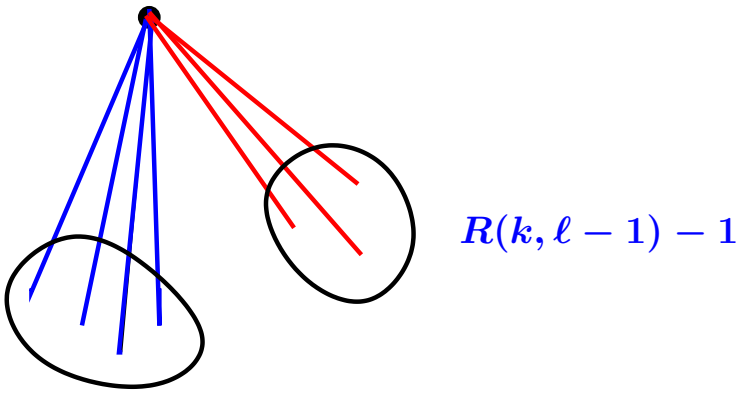
Általában, ha $\mathcal{G}$ egy gráf, akkor $V(\mathcal{G})$ jelöljük a gráf szögpontjainak halmazát, $E(\mathcal{G})$ pedig a gráf éleinek halmazát.

Jelölje K_n pedig az n szögpontú teljes gráfot.

Továbbá, jelölje $R(k, \ell)$ a legkisebb természetes számot, amelyre igaz, hogy minden olyan $\mathcal{G}$ gráf, amelyre $|V(\mathcal{G})| \geq R(k, \ell)$ rendelkezik a következő tulajdonsággal: Ha a $\mathcal{G}$ gráf éleit két színnel színezzük, mondjuk pirossal és kékkel, akkor mindig létezik kék színű monokromatikus K_k vagy piros színű monokromatikus K_ℓ. Ekkor

$$R(k, \ell) \leq R(k-1, \ell) + R(k, \ell-1). \tag{2.1}$$

A bizonyítás a következő ábrával szemléltethető:



Valóban, tegyük fel, hogy a $\mathcal{G}$ gráfra fennáll

$$|V(\mathcal{G})| \geq R(k-1, \ell) + R(k, \ell-1). \tag{2.2}$$

Bebizonyítjuk, hogy ekkor vagy G tartalmaz kék K_k-t, vagy G piros K_ℓ-t. Ezzel megkapjuk (2.1)-t.

Tehát tegyük fel, hogy $\mathcal{G}$ gráfra fennáll (2.2), de az állítással ellentétben, $\mathcal{G}$ nem tartalmaz sem kék K_k-t, sem piros K_ℓ-t. Rögzítsük a gráf egy A szögpontját. Ekkor $\mathcal{G}$ többi szögpontját két csoportra osztjuk: V_0 azon B szögpontokat tartalmazza, amelyre az AB él kék, V_1 azon C szögpontokat tartalmazza, amelyre az AC él piros.

Legyen $\mathcal{G}_0$ az a teljes gráf, amelyet V_1-beli szögpontok feszítenek ki, $\mathcal{G}_1$ pedig, amelyet a V_2-beli szögpontok.

Ha $\mathcal{G}_0$ tartalmaz kék K_{k-1}, akkor $\mathcal{G}$ tartalmaz kék K_k, mivel az A szögpontot hozzávéve a kék K_{k-1} egy teljes kék K_k-t nyerünk $\mathcal{G}$-ben. Azaz, ha $\mathcal{G}$ nem tartalmaz kék K_k-t és piros K_ℓ-t, akkor $\mathcal{G}_0$ nem tartalmaz kék K_{k-1}-t és piros K_ℓ-t. Így

$$|V(\mathcal{G}_0)| \leq R(k-1,\ell) - 1.$$

Hasonlóan,

$$|V(\mathcal{G}_1)| \leq R(k,\ell-1) - 1.$$

Azaz

$$\begin{aligned} |V(\mathcal{G})| &= |V(\mathcal{G}_0)| + |V(\mathcal{G}_1)| + 1 \\ &\leq (R(k-1,\ell) - 1) + (R(k,\ell-1) - 1) + 1 \\ &= R(k-1,\ell) + R(k,\ell-1) - 1, \end{aligned}$$

amely ellentmond (2.2)-nek. Így bebizonyítottuk (2.1)-t.

Teljes indukcióval könnyen belátható, hogy

2.2 TÉTEL.

$$R(k,\ell) \leq \binom{k+\ell-2}{\ell-1}.$$

A 2.2 Tétel bizonyítása. A tétel állítását teljes indukcióval bizonyítjuk. Először azt látjuk be, hogy $R(2,\ell) = \ell$ és $R(k,2) = k$.

Valóban, ha egy gráf ℓ szögpontból áll, akkor vagy tartalmaz kék élt, vagy minden éle piros, és ebben az esetben tartalmaz piros K_ℓ-t. Hasonlóan kapjuk, hogy $R(k,2)=k$.

Ezek után belátjuk, hogy ha a tétel fennáll minden olyan k-re és ℓ-re, amelyre $n=k+\ell$, akkor olyan k-ra és ℓ-re is fennáll, amelyre $n+1=k+\ell$.

Legyen $n+1=k+\ell$. Ekkor (2.1) és az indukciós feltevés alapján

$$\begin{aligned} R(k,\ell) &\le R(k-1,\ell)+R(k,\ell-1) \\ &\le \binom{k+\ell-3}{\ell-1}+\binom{k+\ell-3}{\ell-2} \\ &= \binom{k+\ell-2}{\ell-1}, \end{aligned}$$

ami a bizonyítandó állítás volt.

A binomiális tétel alapján a következőt kapjuk:

2.3 Következmény.

$$R(k,k) \le \binom{2k-2}{k-1} < (1+1)^{2k-2} < 4^k.$$

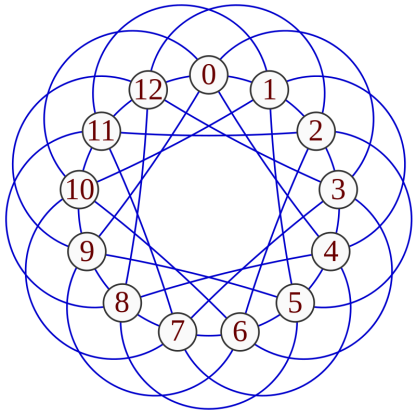
A 2.1 Tétel bizonyítása. Legyen a G teljes gráf szögpontjai most $\mathbb{Z}_p$ elemei. A gráfot a következőképp színezzük:

Minden $a \neq a'$ esetén az (a,a') él kék, ha $a-a'$ kvadratikus maradék. Továbbá az (a,a') él piros, ha $a-a'$ kvadratikus nemmaradék. Ekkor a gráf színezése jól definiált, hiszen

$$\left(\frac{a-a'}{p}\right) = \left(\frac{a'-a}{p}\right). \tag{2.3}$$

Valóban, amennyiben p egy $4k+1$ alakú prím, akkor $\left(\frac{-1}{p}\right) = 1$, s a Legendre szimbólum multiplikativitását használva, megkapjuk (2.3)-t.

Megjegyezzük, hogy a fenti módon definiált gráfot Paley gráfnak hívjuk, Raymond Payley után. A következő ábra a $p = 13$esetet illusztrálja:



Ezután visszatérünk a tétel bizonyításához. Legyen $k = \left[\frac{1}{4}\log p\right]$. Ekkor

$$R(k,k) \leq \binom{2k}{k} < 4^k < p.$$

Azaz a gráf (amely éleit pirossal és kékkel színeztük) tartalmaz monokromatikus K_k-t, ahol $k = \left[\frac{1}{4}\log p\right]$.

Ha ez a szín kék, akkor a kék színű K_k szögpontjait $a_1, a_2, \ldots, a_k$-val jelölve, azt kapjuk, hogy $a_i - a_j$ mindig kvadratikus maradék.

Ha ez a szín piros, rögzítsünk egy n kvadratikus nem maradékot. Akárcsak az előbb, jelölje a piros K_k szögpontjait $a_1, a_2 \ldots, a_k$. Ekkor minden $a_i - a_j$ különbség kvadratikus nem-maradék. Definiáljuk

az S_k halmazt

$$S_k \stackrel{\text{def}}{=} \{na_1, na_2, \ldots, na_k\}.$$

képlettel. Ekkor $na_i - na_j$ mindig kvadratikus maradék, mivel:

$$\left(\frac{na_i - na_j}{p}\right) = \left(\frac{n}{p}\right)\left(\frac{a_i - a_j}{p}\right) = (-1)(-1) = 1.$$

Így az S_k halmaz elemei eleget tesznek a tétel állításának, és ezzel a bizonyítást befejeztük.

Feladatok

1. Működik-e ez a bizonyítás $a + a'$ összegekkel az $a - a'$ különbségek helyett?
2. Létezik-e hasonló bizonyítás az $aa' + 1$ eltolt szorzatokra?
3. Tud adni felső becslést az $\mathcal{A}$ halmaz elemszámára, ha azt tudjuk, hogy $\mathcal{A} \subseteq \mathbb{Z}_p$ és $a \neq a'$ esetén $a - a'$ különbség mindig kvadratikus maradék modulo p?

A feladatok megoldása.

1.) A kérdésre az a válasz, hogy igen, és a bizonyítás nagyon hasonló az előzőhöz. A következőt bizonyítjuk:

2.4 TÉTEL. *Legyen p prímszám. Ekkor létezik $\mathcal{A} \subseteq \mathbb{Z}_p$ halmaz, amelyre*

$$|\mathcal{A}| \geq \left[\frac{1}{4}\log p\right]$$

és az $a + a'$ összegek $a \neq a'$, $a, a' \in \mathcal{A}$ esetén mindig kvadratikus maradékok modulo p vagy nullák.

A 2.4 Tétel bizonyítása. Jelölje $\mathcal{G}$ azt a teljes gráfot, amelynek szögpontjai $\mathbb{Z}_p$ elemei. A következő színezést fogjuk használni: Minden $a \neq a'$ esetén az (a, a') él kék, ha $a + a'$ kvadratikus maradék vagy 0. Az (a, a') él piros, ha $a + a'$ kvadratikus nem-maradék. Ez jó definíció, hiszen

$$\left(\frac{a + a'}{p}\right) = \left(\frac{a' + a}{p}\right).$$

Legyen $k = \left[\frac{1}{4} \log p\right]$. Akárcsak az előbb

$$R(k, k) \leq \binom{2k}{k} < 4^k < p.$$

Azaz a gráf tartalmaz monokromatikus K_k-t, ahol $k = \left[\frac{1}{4} \log p\right]$.

Ha ez a szín kék, jelölje a teljes K_k szögpontjait $a_1, a_2, \ldots, a_k$. A színezés definíciója miatt az $a_i + a_j$ összegek kvadratikus maradékok vagy nullák.

Ha ez a szín piros, rögzítsünk egy n kvadratikus nem-maradékot. Jelölje a piros K_k szögpontjait $a_1, a_2 \ldots, a_k$. Ekkor minden $a_i + a_j$ összeg kvadratikus nem-maradék. Az S_k halmazt definiáljuk a

$$S_k \stackrel{\text{def}}{=} \{na_1, na_2, \ldots, na_k\}.$$

képlettel. Ekkor $na_i + na_j$ mindig kvadratikus maradék, mivel:

$$\left(\frac{na_i + na_j}{p}\right) = \left(\frac{n}{p}\right)\left(\frac{a_i + a_j}{p}\right) = (-1)(-1) = 1,$$

és ezzel a tétel bizonyítását befejeztük.

2.) A következőt fogjuk bizonyítani:

2.5 TÉTEL. (Gyarmati [2]) *Létezik p_0, hogy ha p egy $4k+1$ alakú prím és $p > p_0$, akkor létezik $\mathcal{A} \subseteq \mathbb{Z}_p$, amelyre $|\mathcal{A}| \geq \frac{1}{6\log 3}\log p$ és $aa' + 1$ mindig kvadratikus maradék vagy $0 \mod p$ minden $a, a' \in \mathcal{A}$, $a \neq a'$ esetén.*

A 2.5 Tétel bizonyítása. Ez a tétel a következő Ramsey-elméletbeli tétel következménye:

2.6 LEMMA. *Ha s_1, s_2, s_3 természetes számok, akkor létezik egy r természetes szám, a következő tulajdonsággal: Ha G egy teljes gráf, $|G| \geq r$ és C a G gráf tetszőleges színezése 3 darab színnel, c_1, c_2, c_3-mal, akkor létezik $1 \leq i \leq 3$, hogy a G gráfnak van egy monokromatikus G' részgráfja, melyet ha a c_i színnel színeztük, akkor $|G'| \geq s_i$.*
Továbbá a legkisebb ilyen természetes r számot $R(s_1, s_2, s_3)$-mal jelölve kapjuk, hogy:

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

A 2.6 Lemma bizonyítása. Ha az s_1, s_2, s_3 számok valamelyike 0, akkor a lemma triviális mivel $R(s_1, s_2, s_3) = 0$. Tehát feltehetjük, hogy $s_1, s_2, s_3 > 0$. A következő egyenlőtlenség jól ismert, a bizonyítást megtalálhatjuk pl. [1, 75. o.]-ben (amely egy tipikus Ramsey-elméleti bizonyítás):

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

ha $s_1, s_2, s_3 > 0$. Indukcióval könnyen bebizonyítható, hogy:

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

Tekintsük azt a gráfot, amelynek szögpontjai a modulo p maradékosztályok. Mivel p egy $4k+1$ alakú prím, létezik i egész, amelyre $i^2 \equiv -1 \pmod{p}$.

Tegyük fel, hogy az e él az a és b maradékosztályokat köti össze. Az e élet c_1-gyel színezzük, ha $\left(\frac{ab+1}{p}\right) = 1$ vagy 0. Továbbá az e élet c_2-vel színezzük, ha $\left(\frac{-ab+1}{p}\right) = 1$ vagy 0, de $\left(\frac{ab+1}{p}\right) = -1$. Végül e-t c_3-mal színezzük, ha $\left(\frac{-a^2b^2+1}{p}\right) = 1$ vagy 0 és $\left(\frac{ab+1}{p}\right) = \left(\frac{-ab+1}{p}\right) = -1$ (most definíció szerint $\left(\frac{0}{p}\right) = 0$).

Minden élet megszíneztünk különben:

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

Így:

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

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

Legyen $c = \left[\frac{1}{3\log 3}\log p\right] + 1$. A lemmát alkalmazva kapjuk, hogy:

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

A Stirling formula szerint, ha $c \to \infty$, akkor

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

Így ha p prímszám elég nagy, akkor $R(c,c,c) \leq p$. Azaz a gráf tartalmaz egy monokromatikus X részgráfot, amely a c_j színnel van színezve ($1 \leq j \leq 3$) és $|X| \geq c$.

Legyen $\mathcal{A}$ az X részgráf szögpontjainak halmaza, ha X-et a c_1 színnel színeztük. Legyen $\mathcal{A}$ az $\{ix : x \in V(X)\}$ halmaz, ha X-et a c_2 színnel színeztük. Legyen $\mathcal{A}$ az $\{ix^2 : x \in V(X)\}$ halmaz, ha X-et a c_3 színnel színeztük.

Ekkor $|\mathcal{A}| \geq \frac{1}{2}|X|$ mindig fennáll. A színezés definícióját használva, világos, hogy két tetszőleges elemet összeszorozva és hozzáadva egyet mindig kvadratikus maradékot vagy 0-t kapunk $\mathbf{mod}\ p$.

3.) A következőt bizonyítjuk:

2.7 TÉTEL. (folklór) *Legyen p prímszám. Ha $\mathcal{A} \subset \mathbb{Z}_p$ olyan halmaz, hogy minden $a \neq a'$, $a, a' \in \mathcal{A}$ pár esetén az $a-a'$ különbség kvadratikus maradék modulo p, akkor*

$$|\mathcal{A}| \leq \sqrt{p}.$$

A 2.7 Tétel bizonyítása.

Tegyük fel, hogy az $A-A$ halmaz csak kvadratikus maradékokat tartalmaz és 0-t. Legyen $n \in \mathbb{Z}_p$ egy rögzített kvadratikus nem-maradék. Ekkor minden

$$a - na', \qquad a, a' \in A$$

típusú különbség különböző. Valóban, tegyük fel, hogy

$$a_0 - na_0{}' \equiv a_1 - na_1{}' \pmod{p}.$$

Ekkor

$$a_0 - a_1 \equiv n(a_0{}' - a_1{}') \pmod{p}.$$

Viszont a kongruencia baloldalán kvadratikus maradék áll, a jobboldalon kvadratikus nem-maradék, ami ellentmondás. (Az egyetlen

kivétel, ha $a_0 = a_1$, $a_0{}' = a_1{}'$.) Vagyis minden

$$a - na', \qquad a, a' \in A$$

típusú különbség különböző.

Az $a, a' \in A$ párok száma $|\mathcal{A}|^2$, így

$$|\mathcal{A}|^2 \leq p,$$
$$|\mathcal{A}| \leq \sqrt{p}.$$

A fenti tételnél a legjobb eredmény is csak konstansszorzót javít, és Hanson és Pertidis-től származik [3], akik az $|\mathcal{A}| \leq \sqrt{p/2} + 1$ egyenlőtlenséget bizonyították.

Hivatkozások

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

[2] K. Gyarmati, *On a problem of Diophantus*, Acta Arith. 97.1 (2001), 53-65.

[3] B. Hanson, G. Pertidis, *Refined estimates concerning sumsets contained in the roots of unity*, available at https://arxiv.org/abs/1905.09134

[4] A. Sárközy, *On difference sets of integers II*, Ann. Univ. Sci. Budapest. 21 (1978).

[5] Kép, Frank Plumpton Ramsey, Wikipedia, link.

[6] Ábra, Payley graph, Wikipedia, link.

[7] Ábra, Ramsey-elmélet, saját készítésű.

3. Gallagher nagyobb szitája

A fejezetben szereplő szita Patrik Ximenes Gallagher-től származik, és minden valószínűség szerint a legegyszerűbb a sziták között.

A bizonyítás pusztán a Cauchy-Schwarz egyenlőtlenséget, és elemi megfontolásokat használ.

A szita formulák mögött az a gondolat áll, hogy ha ismerjük a moduláris szerkezetét a természetes számok egy részhalmazának (pontosabban sok m esetén, a halmaz csak néhány maradékosztályt metsz $\mathbf{mod}\ m$), akkor erős felső becslést adhatunk a halmaz elemszámára.

Mielőtt ismertetnénk Gallagher nagyobb szitáját, egy alkalmazást mutatunk példaként:

3.1 TÉTEL. (Rivat, Stewart, Sárközy [7]) *Létezik egy x_0 egész szám, hogyha $x_0 < x \in \mathbb{N}$, $\mathcal{A} \subset \{1, 2, 3, \ldots, x\}$, és tudjuk, hogy $a, a' \in \mathcal{A}$ esetén $a + a'$ mindig négyzetszám, akkor*

$$|\mathcal{A}| < 37 \log x. \tag{3.1}$$

Nem tudjuk mennyire erős ez a tétel. De megjegyezzük, hogy J. Lagrange [5] és J.-L. Nicolas [6] talált 6 elemű halmazt a fenti tulajdonsággal, nevezetesen:

$$\mathcal{A} = \{-15863902, 17798783, 21126338, 49064546, 82221218, 447422978\}.$$

Az a sejtésünk van egy nem ismert 6-nál több elemű halmaz a fenti tulajdonsággal.

Rivat, Stewart és Sárközy eredménye helyett, egy kissé egyszerűbb állítást látunk be.

3.2 TÉTEL. (Gyarmati [4]) *Létezik egy x_0 egész szám, hogyha $x_0 < x \in \mathbb{N}$, $\mathcal{A} \subset \{1, 2, 3, \dots, x\}$, és tudjuk, hogy minden $a > a' \in \mathcal{A}$ esetén $a - a'$ négyzetszám, akkor*

$$|\mathcal{A}| < 2.01 \log x. \tag{3.2}$$

A bizonyítás ugyanaz mint az $a + a'$ esetben, az egyetlen különbség, hogy az itt használt lemma (ld. 2.7 Tétel a jegyzetben) bizonyítása elemi, és nem használ exponenciális összegeket.

A bizonyítás főeszköze Gallagher nagyobb szitája [7]. A jelen változatot Erdős, Stewart és Sárközy [2] mondta ki 1994-ben.

3.3 TÉTEL. (Gallagher nagyobb szitája) *Tegyük fel, hogy $m, n \in \mathbb{N}$, $\mathcal{A} \subset \{m+1, m+2, \dots, m+n\}$ és $\mathcal{B} \subset \mathbb{N}$ egy véges halmaz,*

amelynek elemei páronként relatív prímek. Minden $b \in \mathcal{B}$-re jelölje $\nu(b)$ azon $\mod b$ maradékosztályok számát, amelyek metszik $\mathcal{A}$-t. Ekkor

$$|\mathcal{A}| \leq \frac{\sum\limits_{b\in\mathcal{B}} \log b - \log n}{\sum\limits_{b\in\mathcal{B}} \frac{\log b}{\nu(b)} - \log n}, \tag{3.3}$$

feltéve, hogy a nevező pozitív.

Gallagher az állítást először $\mathcal{B} = \mathcal{P}$ esetben fogalmazta meg, ahol $\mathcal{P}$ csak prímeket tartalmazott.

Miért hívunk egy ilyen tételt szitának? Ebben az esetben az $\mathcal{A}$ halmaz elemszámát a $\nu(b)$ függvények segítségével becsüljük. Ha $\mathcal{A}$ sok $\mod b$ maradékosztályból nem tartalmaz elemet, akkor $\nu(b)$ kicsi, így (3.3) nevezőjében szereplő tört nagy, ami $|\mathcal{A}|$ elemszámára erős felső becslést ad.

A 3.3 Tétel bizonyítása. Legyen

$$n_k \overset{\text{def}}{=} \left|\{a : a \in \mathcal{A},\ a \equiv k \pmod b\}\right|.$$

Ekkor Cauchy-Schwarz egyenlőtlenséget használva $\mu(b)$ darab nem nulla tagra kapjuk, hogy:

$$\sum_{k=1}^{b} n_k^2 \geq \frac{\left(\sum_{k=1}^{b} n_k\right)^2}{\nu(b)} = \frac{|\mathcal{A}|^2}{\nu(b)}.$$

Másrészről:

$$\sum_{k=1}^{b} n_k^2 = \sum_{k=1}^{b} \sum_{\substack{a,a'\in\mathcal{A} \\ a\equiv a'\equiv k \pmod b}} 1$$

$$= \sum_{\substack{a,a' \in \mathcal{A} \\ a \equiv a' \pmod{b}}} 1$$

$$= |\mathcal{A}| + \sum_{\substack{a,a' \in \mathcal{A},\ a \neq a' \\ b \mid a - a'}} 1.$$

Így:

$$\frac{|\mathcal{A}|^2}{\nu(b)} \leq |\mathcal{A}| + \sum_{\substack{a,a' \in \mathcal{A},\ a \neq a' \\ b \mid a - a'}} 1.$$

Ezután $\log b$-vel szorozva:

$$|\mathcal{A}|^2 \frac{\log b}{\nu(b)} \leq |\mathcal{A}| \log b + \sum_{\substack{a,a' \in \mathcal{A},\ a \neq a' \\ b \mid a - a'}} \log b.$$

Összegezve az összes $b \in \mathcal{B}$-re:

$$|\mathcal{A}|^2 \sum_{b \in \mathcal{B}} \frac{\log b}{\nu(b)} \leq |\mathcal{A}| \sum_{b \in \mathcal{B}} \log b + \sum_{\substack{a,a' \in \mathcal{A} \\ a \neq a'}} \sum_{\substack{b \mid a - a' \\ b \in \mathcal{B}}} \log b.$$

Az utolsó szummában:

$$\sum_{\substack{b \mid a - a' \\ b \in \mathcal{B}}} \log b = \log \prod_{\substack{b \mid a - a' \\ b \in \mathcal{B}}} b \leq \log n.$$

Így:

$$|\mathcal{A}|^2 \sum_{b \in \mathcal{B}} \frac{\log b}{\nu(b)} \leq |\mathcal{A}| \sum_{b \in \mathcal{B}} \log b + \sum_{\substack{a,a' \in \mathcal{A} \\ a \neq a'}} \log n$$

$$|\mathcal{A}| \sum_{b \in \mathcal{B}} \frac{\log b}{\nu(b)} \leq \sum_{b \in \mathcal{B}} \log b + (|\mathcal{A}| - 1) \log n$$

$$|\mathcal{A}| \left(\sum_{b \in \mathcal{B}} \frac{\log b}{\nu(b)} - \log n \right) \leq \sum_{b \in \mathcal{B}} \log b - \log n.$$

Itt, ha az $|\mathcal{A}|$ követő szorzó pozitív, akkor leoszthatunk vele.

A 3.2 Tétel bizonyítása. Tudjuk, hogy $a, a' \in \mathcal{A},\ a > a'$ esetén az $a - a'$ különbség mindig négyzetszám. Vagyis $a, a' \in \mathcal{A},\ a > a'$ esetén $a - a'$ mindig kvadratikus maradék $\mod p$ vagy 0 minden p prímszámra.

Ha -1 kvadratikus maradék $\mod p$, akkor $a' - a$ is kvadratikus maradék $\mod p$ vagy 0, nemcsak $a - a'$.

Tudjuk, hogy -1 akkor és csak akkor kvadratikus maradék $\mod p$, ha $p \equiv 1 \pmod 4$.

Vagyis $p \equiv 1 \pmod 4$ esetén tetszőleges $a, a' \in \mathcal{A}$-ra $a - a'$ kvadratikus maradék $\mod p$ (azaz a továbbiakban az $a > a'$ feltétel nem szükséges).

A 2.7 Tételt lemmaként fogjuk használni.

3.4 Lemma. *Legyen p prímszám. Ha a $\mathcal{C} \subset \mathbb{Z}_p$ halmazra teljesül, hogy $a \neq a'$, $a, a' \in \mathcal{C}$ esetén $a - a'$ kvadratikus maradék modulo p, akkor*

$$|\mathcal{C}| \leq \sqrt{p}.$$

Jelölje $\mathcal{C}$ azon $\mod p$ maradékosztályok halmazát, amelyek tartalmaznak $\mathcal{A}$-ból elemet. Ekkor $|\mathcal{C}| \leq \sqrt{p}$.

Vagyis a 3.3 Tétel jelöléseit használva, az előző lemmából az következik, hogy $\nu(p) \leq \sqrt{p}$.

Ezután Gallagher nagyobb szitáját alkalmazzuk. Ehhez legyen

$$\mathcal{B} = \{p : \ p \text{ prím}, \ p \equiv 1 \pmod 4, \ 2 \le p \le c(\log x)^2\},$$

ahol az alkalmazott c konstans értékét később rögzítjük. Egyelőre elegendő feltenni, hogy $c > 1$.

Gallagher nagyobb szitája szerint:

$$|\mathcal{A}| \le \frac{\sum\limits_{p\equiv 1 \pmod 4,\ p\le c(\log x)^2} \log p - \log x}{\sum\limits_{p\equiv 1 \pmod 4,\ p\le c(\log x)^2} \frac{\log p}{\sqrt{p}} - \log x}. \tag{3.4}$$

Azaz a felső becslés bizonyításához az egyenlőtlenség jobboldalán álló kifejezést kell becsülnünk. Ehhez bevezetjük a következő jelöléseket:

$$\pi(y,4,1) \stackrel{\text{def}}{=} \sum_{p\equiv 1 \pmod 4,\ p\le y} 1$$

$$\theta(y,4,1) \stackrel{\text{def}}{=} \sum_{p\equiv 1 \pmod 4,\ p\le y} \log p$$

$p_n(4,1)$ az n-edik legkisebb pozitív prím, amely $\equiv 1 \pmod 4$.

Szerencsékre, a fenti függvényekre egyre pontosabb becsléseket adtak a matematikusok. Pl., Bennet, Martin, O'Bryan és Rechnitzer eredménye [1] szerint:

$\pi(y,4,1) = (1+o(1))\dfrac{y}{2\log y}$ ld. „Theorem 1.4" [1]-ben,

$\theta(y,4,1) = (1+o(1))\dfrac{y}{2}$ ld. „Corollary 1.7" [1]-ben,

$$p_n(4,1) \quad = (1+o(1))2n\log n \quad \text{ld. „Theorem 1.5” [1]-ben.}$$

A $\theta(y,4,1)$-re vonatkozó eredményből következik az alábbi:

$$\sum_{p\equiv 1 \pmod 4,\ p\le c(\log x)^2} \log p - \log x$$

$$= \theta(c(\log x)^2,4,1) - \log x$$

$$= (1+o(1))\frac{c}{2}(\log x)^2 - \log x$$

$$= (1+o(1))\frac{c}{2}(\log x)^2. \tag{3.5}$$

A (3.4)-beli tört nevezőjének becslése már bonyolultabb:

$$\sum_{p\equiv 1 \pmod 4,\ p\le c(\log x)^2} \frac{\log p}{\sqrt{p}} - \log x$$

$$= \sum_{n=1}^{\pi(c(\log x)^2,4,1)} \frac{\log p_n(4,1)}{\sqrt{p_n(4,1)}} - \log x$$

$$= (1+o(1)) \sum_{n=1}^{\pi(c(\log x)^2,4,1)} \frac{\log(2n\log n)}{\sqrt{2n\log n}} - \log x$$

$$= (1+o(1))\frac{1}{\sqrt{2}} \sum_{n=1}^{\pi(c(\log x)^2,4,1)} \frac{\log n}{\sqrt{n \log n}} - \log x$$

$$= (1+o(1))\frac{1}{\sqrt{2}} \sum_{n=1}^{\pi(c(\log x)^2,4,1)} \frac{\sqrt{\log n}}{\sqrt{n}} - \log x$$

$$= (1+o(1))\frac{1}{\sqrt{2}} \int_{n=1}^{\pi(c(\log x)^2,4,1)} \frac{\sqrt{\log n}}{\sqrt{n}} dn - \log x$$

$$= (1+o(1))\sqrt{2}\ \sqrt{n \log n}\Big]_1^{\pi(c(\log x)^2,4,1)} - \log x$$

$$= (1+o(1))\sqrt{2}\sqrt{\pi(c(\log x)^2,4,1) \log\left(\pi(c(\log x)^2,4,1)\right)} - \log x$$

$$= (1+o(1))\sqrt{2}\sqrt{\frac{c(\log x)^2}{2\log\left(c(\log x)^2\right)} \log\left(\frac{c(\log x)^2}{2\log\left(c(\log x)^2\right)}\right)} - \log x$$

$$= (1+o(1))\sqrt{2}\sqrt{\frac{c(\log x)^2}{4\log\log x} 2\log\log x} - \log x$$

$$= (1+o(1))\sqrt{c}\log x - \log x$$

$$= (1+o(1))(\sqrt{c}-1)\log x.$$

Ezt az eredményt és (3.5)-t beírva (3.4)-be kapjuk, hogy:

$$|\mathcal{A}| \leq (1+o(1))\frac{c}{2\left(\sqrt{c}-1\right)}\log x,$$

ha $c > 1$. Most már rögzíthetjük c értékét, legyen pl. $c = 4$. Ekkor

$$|\mathcal{A}| \leq 2.01 \log x,$$

ha $x > x_0$, és ezzel a tételt igazoltuk.

Hivatkozások

[1] M. A. Bennet, G. Martin, K. O'Bryant, A. Rechnitzer, *Explicit bounds for primes in arithmetic progressions*, Illinois J. Math. 62 (2018), no. 1-4, 427–532.

[2] P. Erdős, A. Sárközy, C.L. Stewart, *On prime factors of subset sums*, Journal of the London Math. Soc. 49 (2) (1994), 209-218.

[3] P. X. Gallagher, *A larger sieve*, Acta Arithmetica 18 (1971), 77-81.

[4] K. Gyarmati, *On Diophantine square tuples*, Int. J. Number Theory, közlésre leadva.

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

[6] J.-L. Nicolas, *Six nombres dont les sommes deux à deux sont des carrés*, Calculateuren Math. (1975, Limoges), Bulletin de la Société Mathématique de France, mémoire 49-50, (1977), pp. 141–143.

[7] J. Rivat, A. Sárközy és C.L. Stewart, *Congruence properties of the Omega-function on sumsets*, Illinois J. Math., 43 (1999), 1-18.

[8] Kép, Archeologist clip art, link.

4. Diophantosz egy problémája

Alexandriai Diophantosz, görög matematikus észrevette, hogy az $\frac{1}{16}$, $\frac{33}{16}$, $\frac{17}{4}$, és $\frac{105}{16}$ racionális számok rendelkeznek a következő tulajdonsággal: bármely kettő szorzatához egyet adva mindig négyzetszámot kapunk.

Később Fermat talált 4 pozitív egész számot, a fenti tulajdonsággal: {1,3,8,120}.

Phil Gibbs észrevette, hogy a következő 6 racionális szám is rendelkezik ugyanezzel a tuulajdonsággal: $\left\{\frac{11}{192}, \frac{32}{192}, \frac{155}{27}, \frac{512}{27}, \frac{1235}{48}, \frac{180873}{16}\right\}$ (ld. [4]).

2004-ben Andrej Dujella [3] bebizonyította a következőt:

4.1 TÉTEL. (Dujella) *Nem létezik 6 egész szám úgy, hogy bármely kettő szorzatához egyet adva mindig négyzetszámot kapjunk.*

Azonban ez az eredmény túl mély ahhoz, hogy a jegyzet keretein belül bizonyítsuk. Az érdeklődők Dujella honlapján utánanézhetnek: link.

Dujella eredményét egy több mint 40 oldalas cikkben javította meg He, Togbé és Ziegler [6]. A következőt bizonyították:

4.2 TÉTEL. (He-Togbé-Ziegler) *Nem létezik* 5 *egész szám úgy, hogy bármely kettő szorzatához egyet adva mindig négyzetszámot kapjunk.*

De ezt az eredményt használva könnyen igazolható az alábbi:

4.3 TÉTEL. (Bugeaud, Gyarmati [2]) *Legyen* $\mathcal{A}$ *pozitív egészek halmaza, melyre* $|\mathcal{A}| \geq 5$*. Ekkor az*

$$\{(a, a') : \ a, a' \in \mathcal{A},\ a > a',\ aa' + 1 \ \textit{négyzetszám}\}$$

halmaznak legfeljebb $\frac{3}{8}\,|\mathcal{A}|^2$ *darab eleme van.*

Valójában 4.2-nél egy kicsit gyengébbet bizonyítottunk [2]-ben (mivel akkor még He-Togbé-Ziegler nem bizonyították a 4.2 Tételt).

A 4.3 Tétel bizonyítása. A bizonyítás Turán [8] jól ismert tételére épül:

4.4 LEMMA. (Turán) *Legyen* G *egy* n *szögpontú gráf, melynek legalább*

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

darab éle van, ahol $r \geq 3$*. Ekkor* G *tartalmaz teljes* r *szögpontú részgráfot.*

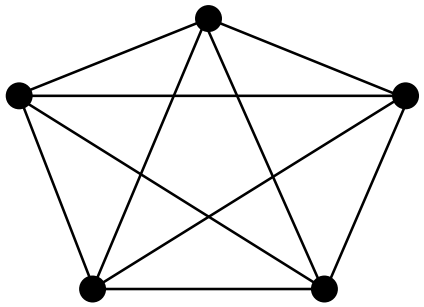
A 4.4 Lemma bizonyítása. Turán Pál eredeti bizonyítása [8]-ban található magyar nyelven. Azóta a tételnek számtalan bizonyítását fedezték fel, pl. [1] öt különböző bizonyítást ismertet.

Térjünk vissza a 4.3 Tétel bizonyításához.

Jelölje $a_1, a_2, \ldots, a_n$ az $\mathcal{A}$ halmaz elemeit.

Jelölje a G gráf szögpontjait $a_1, a_2, \ldots, a_n$ és két szögpont között, a_i és a_j között pontosan akkor fut él, ha $a_i a_j + 1$ négyzetszám.

A 4.2 Tétel szerint, G nem tartalmaz K_5-öt részgráfként.



A 4.4 Lemmából adódóan G-nek legfeljebb $\frac{3}{8}n^2 = \frac{3}{8}|\mathcal{A}|^2$ éle van. Ezzel a 4.3 Tételt igazoltuk.

Egy kicsit többet is igazolhatunk, ha feltesszük, hogy az $\mathcal{A}$ halmaz elemei nem egy túl hosszú intervallumban fekszenek. Nevezetesen:

4.5 TÉTEL. (Gyarmati) *Legyen $\mathcal{A} \subset \{N, N+1, N+2, \ldots, M\}$ pozitív egészek egy halmaza, melyre $N < M < \sqrt{3}N$. Ekkor az*

$$\{(a, a') : a, a' \in \mathcal{A},\ a > a',\ aa' + 1 \text{ négyzetszám}\}$$

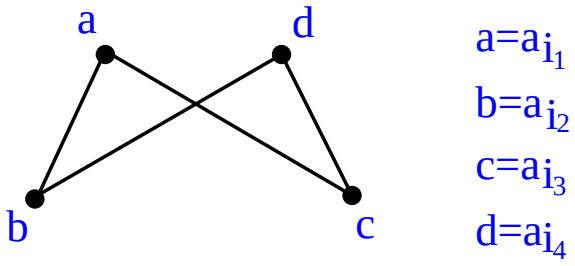
halmaznak legfeljebb $\frac{1}{2}|\mathcal{A}|^{3/2} + \frac{1}{4}|\mathcal{A}|$ eleme van.

A 4.5 Tétel bizonyítása. A $\mathcal{G}$ gráfot ugyanúgy definiáljuk mint a 4.3 Tétel bizonyításánál.

A következőt bizonyítjuk:

4.6 LEMMA. *A $\mathcal{G}$ gráf nem tartalmaz 4 hosszú kört.*

A 4.6 Lemma bizonyítása Tegyük fel, hogy a gráf tartalmaz egy 4 hosszú kört. Jelölje ennek a 4 hosszú körnek a legkisebb elemét $a = a_{i_1}$. A körben a-nak két szomszédja van, a kisebbet jelöljük $b = a_{i_2}$-vel, a nagyobbat $c = a_{i_3}$-mal. A kör utolsó eleme $d = a_{i_4}$.



Tudjuk $a < d$ (mivel a volt a legkisebb elem) és $b < c$ (mivel b volt a kisebb a szomszédai közül). Ekkor:

$$(ac+1)(bd+1) < (ab+1)(cd+1), \tag{4.1}$$

hiszen a zárójeleket felbontva azt kapjuk, hogy

$$abcd + ac + bd + 1 < abcd + ab + cd + 1.$$

Ekvivalens átalakításokat végezve:

$$\begin{aligned} ac + bd &< ab + cd \\ 0 &< ab + cd - ac - bd \\ 0 &< (d-a)(c-b), \end{aligned}$$

ahol az utolsó állítás azért igaz, mert $a < d$ és $b < c$. Azaz (4.1) alapján:

$$\sqrt{(ac+1)(bd+1)} < \sqrt{(ab+1)(cd+1)},$$

de $\sqrt{ac+1}, \sqrt{bd+1}, \sqrt{ab+1}$ és $\sqrt{cd+1}$ egész számok, hiszen a gráf a_i és a_j szögpontja között pontosan akkor fut él, ha $a_i a_j + 1$ négyzetszám.

Vagyis $\sqrt{(ac+1)(bd+1)}$ és $\sqrt{(ab+1)(cd+1)}$ olyan egész számok, ahol az első kisebb mint a második, így

$$\sqrt{(ac+1)(bd+1)}+1 \leq \sqrt{(ab+1)(cd+1)}.$$

Négyzetreemlve:

$$(ac+1)(bd+1)+2\sqrt{(ac+1)(bd+1)}+1 \leq (ab+1)(cd+1)$$
$$abcd+ac+bd+1+2\sqrt{(ac+1)(bd+1)}+1 \leq abcd+ab+cd+1$$
$$ac+bd+1+2\sqrt{abcd} < ab+cd.$$

A számtani-mértani közép közötti egyenlőtlenség szerint $ac+bd \geq 2\sqrt{abcd} \geq 2ab$. Így

$$2ab+2\sqrt{abcd} < ab+cd$$
$$4ab < ab+cd$$
$$3ab < cd.$$

Mivel az $\mathcal{A}$ halmaz elemeire fennáll, hogy $\mathcal{A} \subset \{N, N+1, \ldots, M\}$, vagyis $N \leq a, b$ és $c, d \leq M < \sqrt{3}N$. Ekkor

$$3N^2 \leq 3ab < cd < 3N^2,$$

ami ellentmondás. Ezzel a lemmát igazoltuk.

A fenti bizonyítás [5]-ban is megtalálható, ahol picit általánosabban mondtuk ki, négyzetszámok helyett k-adik hatványokra.

Ezután a következő lemmát használjuk:

4.7 LEMMA. (Reiman [7]) *Ha $G = (V, E)$ egy olyan gráf n szögponton, amely nem tartalmaz 4 hosszú kört, akkor*

$$|E| \leq \frac{n}{4}\left(1+\sqrt{4n-3}\right).$$

Mivel a $\mathcal{G}$ gráf nem tartalmaz C_4-et, ezért a 4.6 Lemma szerint, nincs több éle van mint mint

$$\frac{|\mathcal{A}|}{4}\left(1+\sqrt{4\,|\mathcal{A}|-3}\right) < \frac{|\mathcal{A}|^{3/2}}{2}+\frac{|\mathcal{A}|}{4}.$$

Ezzel a 4.5 Tétel bizonyítását befejeztük.

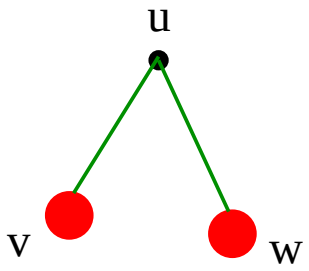
A teljesség kedvéért ismertetjük a 4.7 Lemma bizonyítását is.

A 4.7 Lemma bizonyítása. Legyen $G=(V,E)$ egy C_4-mentes gráf, ahol a szögpontok halmazát $V=v_1,\ldots,v_n$ jelöli, és a szögpontokhoz tartozó fokszámok pedig rendre $d_1,d_2,\ldots,d_n$.

Jelölje S az összes olyan $(u,\{v,w\})$ számhármast, ahol u,v,w a G szögpontjai, $v\neq w$ és u pedig szomszédos mind v-vel és w-vel G-ben.

Az S halmaz elemszámát kétféle módon is meghatározzuk.

Azaz kétféle módon is meghatározzuk a „cseresznyék” számát G-ben.



Minden u-ra, összesen $\binom{d}{2}$ féleképpen választhatunk ki egy kételemű részhalmazt a szomszédai közül, ha u-nak d darab szomszédja van. Azaz, ha az összes u-ra szummázunk, azt kapjuk, hogy

$$S=\sum_{i=1}^{n}\binom{d_i}{2}.$$

Mivel G nem tartalmaz C_4-et, tudjuk, hogy minden v, w szögpont párnak legfeljebb egy közös szomszédja lehet. Azaz, ha minden párra szummázunk, a következőt kapjuk:

$$|S| \leq \binom{n}{2}.$$

Vagyis

$$\sum_{i=1}^{n} \binom{d_i}{2} \leq \binom{n}{2},$$

amivel ekvivalens

$$\sum_{i=1}^{n} d_i^2 - \sum_{i=1}^{n} d_i \leq n(n-1).$$

Itt $\sum_{i=1}^{n} d_i = 2\,|E|$, így

$$\sum_{i=1}^{n} d_i^2 - 2\,|E| \leq n(n-1). \tag{4.2}$$

A számtani-négyzetes közép közötti egyenlőtlenség szerint:

$$\sum_{i=1}^{n} d_i^2 \geq n \left(\frac{\sum_{i=1}^{n} d_i}{n} \right)^2 = \frac{4\,|E|^2}{n}.$$

Ezt (4.2)-be írva kapjuk, hogy

$$\frac{4\,|E|^2}{n} - 2\,|E| \leq n(n-1)$$

$$|E|^2 - \frac{n}{2}\,|E| - \frac{n^2(n-1)}{2} \leq 0.$$

A másodfokú egyenlőtlenséget megoldva, adódik E-re a kívánt becslés.

Hivatkozások

[1] M. Aigner, G. M. Ziegler, *Proofs from THE BOOK* (6th ed.) (2018), Springer-Verlag, pp. 285–289,

[2] Y. Bugeaud, K. Gyarmati, *On generalizations of a problem of Diophantus*, Illinois J. Math. 48 (2004), 1105-1115.

[3] A. Dujella, *There are only finitely many Diophantine quintuples*, J. Reine Angew. Math. 566 (2004), 183–214.

[4] P. Gibbs, *Some Rational Diophantine Sixtuples*, arXiv:math/9902081.

[5] K. Gyarmati, *On a problem of Diophantus*, Acta Arith. 97.1 (2001), 53-65.

[6] B. He, A. Togbé, V. Ziegler, *There is no Diophantine quintuple*, Trans. Amer. Math. Soc. 371 (2019), 6665-6709.

[7] I. Reiman, *Über ein Problem von K. Zarankiewicz*, Acta Math. Acad. Sci. Hungar. 9 (1958), 269-273.

[8] P. Turán, *On an extremal problem in graph theory*, Matematikai és Fizikai Lapok 48 (1941), 436–452.

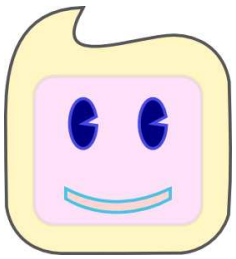
[9] Kép, Diophantus of Alexandria, Wikipedia, link.

5. Négyzetszám-mentes különbség halmazok

Eddig olyan A halmazokat tanulmányoztunk, amelyekre az $A - A$ vagy az $A + A$, esetleg az $A \cdot A + 1$ halmaz kizárólag, csak négyzetszámokat tartalmazott. Itt $A - A$, $A + A$ és $A \cdot A + 1$ a következő halmazokat jelölte:

$$A - A = \{a - a' : \ a > a', \ a, a' \in \mathcal{A}\},$$
$$A + A = \{a + a' : \ a > a', \ a, a' \in \mathcal{A}\},$$
$$A \cdot A + 1 = \{aa' + 1 : \ a > a', \ a, a' \in \mathcal{A}\}.$$

Érdekes kérdéskört kapunk, ha megfordítjuk a gondolatmenetünket, és azt kérdezzük mi mondható akkor az A halmaz méretére, ha pl. $A - A$ sosem tartalmaz négyzetszámot.



Ilyenkor azt várnánk, hogy nagyon nagy A halmazok is léteznek a kívánt tulajdonsággal, de ez nincs így.

Másrészről, Ruzsa Imre [3] megadott egy ügyes konstrukciót a fenti tulajdonsággal, viszonylag sok elemmel, megcáfolva pár sejtést. A következőkben az ő eredményét ismertetjük, de csak a négyzetszámok esetében (Ruzsa általában k-adik hatványok esetében vizsgálta a kérdést.)

De nézzük először is, hogy mi történt a területen időrendben:

Lovász felvetette és Sárközy [4] bebizonyította, ha S a természetes számoknak egy pozitív aszimptotikus sűrűségű sorozata, akkor szükségszerűen $S - S$ tartalmaz négyzetszámot.

Jelölje $D(x)$ azon halmazok maximális elemszámát, amelyek az $[1, x]$-ből választhatóak ki úgy, hogy egy különbség sem négyzetszám. Sárközy bebizonyította, hogy

$$D(x) = O(x(\log x)^{-1/3}).$$

Itt nem ismertetjük a bizonyítást, mivel az Hardy-Littlewood körmódszert használ, amely nem tartozik a jegyzet témái közé.

A következőkben egy nagyon egyszerű konstrukciót adunk meg olyan S halmazra, amelyre $S - S$ nem tartalmaz négyzetszámot. Rögzítsünk egy p prímszámot, amelyre $\frac{\sqrt{x}}{2} \leq p \leq \sqrt{x}$. Legyen

$$S = \{p, 2p, 3p, \ldots, p^2\}.$$

Ekkor

$$S - S = \{p, 2p, 3p, \ldots, p^2 - p\}.$$

Vagyis $p \mid m$, de $p^2 \nmid m$ minden $m \in S - S$, így m nem lehet négyzetszám.

A fenti konstrukció mutatja, hogy $D(x) \geq \frac{\sqrt{x}}{2}$.

Erdős a következő sejtést vetette fel:

$$D(x) = O(x^{1/2}(\log x)^k)$$

fennáll alkalmas k konstanssal.

Sárközy [5] megcáfolta a sejtést, de még mindig azt gondolta, hogy

$$D(x) = O(x^{1/2+\varepsilon}).$$

Ezt a sejtést Ruzsa cáfolta meg, bebizonyítva a következőt:

5.1 TÉTEL. *$D(x) > \frac{1}{65}x^{\gamma}$, ahol*

$$\gamma = \frac{1}{2}\left(1 + \frac{\log 7}{\log 65}\right) = 0.733077\ldots .$$

Valójában, Ruzsa kicsit többet igazolt. Nevezetesen, ha $r(m)$ jelöli azon $\bmod m$ maradékosztályok maximális számát, melyek közül nem választható ki kettő, amely különbsége négyzetszám $\bmod m$, akkor:

5.2 TÉTEL. *Minden négyzetmentes m-re fennáll*

$$D(x) \geq \frac{1}{m}x^{\gamma(m)},$$

ahol

$$\gamma(m) = \frac{1}{2} + \frac{\log r(m)}{2\log m}.$$

Először az 5.2 Tételt igazoljuk.

5.2 Tétel bizonyítása. Legyen $R \subseteq [1, m]$ egy olyan halmaz, amelynek nincs két eleme, melyek különbsége négyzetszám modulo m.

Legyen S azon természetes számok halmaza, melyek felírhatóak

$$s = \sum_{j=0}^{n-1} r_j m^j + 1$$

alakban, ahol $r_j \in R$ ha j páros és $0 \leq r_j < m$ tetszőleges ha j páratlan. Nyilván

$$\begin{aligned} S(m^n) &\stackrel{\text{def}}{=} |S \cap \{1, 2, 3, \ldots, m^n\}| \\ &= r(m)^{1+[(n-1)/2]} m^{(n-1)-[(n-1)/2]}. \end{aligned}$$

Legyen $m^n \leq x < m^{n+1}$. Egyszerű számítások mutatják:

$$S(x) \geq S(m^n)$$

$$
\begin{aligned}
&= r(m)^{1+[(n-1)/2]} m^{(n-1)-[(n-1)/2]} \\
&= m^{(1+[(n-1)/2])\frac{\log r(m)}{\log m}+n-1-[(n-1)/2]} \\
&= m^{\frac{\log r(m)}{\log m}+n-1+[(n-1)/2]\left(\frac{\log r(m)}{\log m}-1\right)} \\
&\geq m^{\frac{\log r(m)}{\log m}+n-1+\frac{n-1}{2}\left(\frac{\log r(m)}{\log m}-1\right)} \\
&= m^{\frac{\log r(m)}{\log m}+\frac{n-1}{2}+\frac{n-1}{2}\frac{\log r(m)}{\log m}} \\
&= \frac{1}{m} m^{\frac{n+1}{2}+\frac{n+1}{2}\frac{\log r(m)}{\log m}} \\
&\geq \frac{1}{m} x^{\frac{1}{2}+\frac{\log r(m)}{2\log m}} \\
&= \frac{1}{m} x^{\gamma(m)}.
\end{aligned}
$$

Bebizonyítjuk, hogy $S - S$ nem tartalmaz négyzetszámot. Tegyük fel, hogy $s - s' = t^2$, ahol $s, s' \in S$. Legyen

$$
s = \sum_{j=0}^{n-1} r_j m^j + 1, \quad s' = \sum_{j=0}^{n-1} r'_j m^j + 1.
$$

Jelölje k azt a legkisebb k indexet, amelyre $r_k \neq r'_k$. Ekkor:

$$
t^2 = s - s' = (r_k - r'_k) m^k + z m^{k+1}.
$$

Ha k páratlan, akkor $m^k \mid t^2$, de $m^{k+1} \nmid t^2$, amely lehetetlen négyzetmentes m-re. Ha k páros, legyen $k = 2\ell$, és ekkor

$$
\left(t/m^\ell\right)^2 \equiv r_k - r'_k \pmod{m}, \quad \text{ahol } r_k,\ r'_k \in R,
$$

ami ellentmondásban van R definíciójával. Ezzel a tételt igazoltuk.

Az 5.1 Tétel könnyen levezethető az 5.2 Tételből.

Az 5.1 Tétel bizonyítása. Az 5.1 Tétel bizonyításához csak annyi szükséges, hogy

$$
r(65) \geq 7.
$$

Tekintsük a

$$(0,0),\ (0,2),\ (1,8),\ (2,1),\ (2,3),\ (3,9),\ (4,7)$$

párokat, ahol a számpárok első tagja a modulo 5 maradékot jelöli, míg a második a modulo 13-t. Könnyű látni, hogy ebben a halmazban két eleme különbsége mindig vagy kvadratikus nem-maradék $\mathbf{mod}\ 5$ vagy kvadratikus nem-maradék $\mathbf{mod}\ 13$. Ezzel az állítást igazoltuk.

A következőkben mutatunk néhány javítást az eddigi eredményeken.

Pintz, Steiger és Szemerédi [6] finomított Sárközy érvelésén, belátva, hogy $D(x) \leq \frac{x}{(\log x)^{c \log\log\log\log x}}$.

Bloom és Maynard [1] tovább javította a becslést, nevezetesen

$$D(x) \leq \frac{x}{(\log x)^{c \log\log\log x}}.$$

Lewko [2] pedig Ruzsa alsó becslését javította:

$$D(x) \gg x^{\delta},$$

ahol $\delta = \frac{1}{2} + \frac{\log 12}{\log 205} = 0.733412\cdots$.

Hivatkozások

[1] T. F. Bloom, J. Maynard, *A new upper bound for sets with no square differences*, Compos. Math. 158 (2022), no. 8, 1777–1798.

[2] M. Lewko, *An improved lower bound related to the Furstenberg-SárkÖzy theorem*, Electron. J. Combin. 22 (2015), no. 1, Paper 1.32, 6 pp.

[3] I. Ruzsa, *Difference sets without squares*, Periodica Mathematica Hungarica 15 (1984), 205–209.

[4] A. Sárközy, *On difference sets of sequences of integers, I*, Acta Math. Acad. Sci. Hungar. 31 (1978), 125-149.

[5] A. Sárközy, *On difference sets of sequences of integers, II*, Ann. Univ. Sci. Budapest. Eötvös Sect. Math. 21 (1978), 45-53.

[6] J. Pintz, W. L. Steiger, E. Szemerédi, *On sets of natural numbers whose difference set contains no squares*, J. Lond. Math. Soc. (2)37(1988), 219–231.

[7] Kép, Smiley square face, link.

6. Sidon sorozatok

Még hallgatóként, Sidon Simon, 1932-ben egy kérdést tett fel Erdősnek. A kérdés Simon és Erdős témavezetőjének, Fejérnek (aki maga is rendkívül kreatív volt) egy végtelen sorozatok összegezésbeli vizsgálataihoz kapcsolódott.

Sidon bizonyos Fourier sorok L_p-beli normájának vizsgálatakor fogalmazta meg kérdését elemzésekor fogalmazta meg kérdését. A probléma modern megfogalmazása a következő:

A számelméletben Sidon sorozat (vagy Sidon halmaz) egy természetes számokból álló sorozat $\mathcal{A} = \{a_0, a_1, a_2, ...\}$ sorozat, ha az összes $a_i + a_j$ összeg különböző, ahol $i \leq j$.

Feladat. Mutassunk példákat Sidon sorozatokra

Például a kettőhatványok.

6.1 Definíció. *Jelölje $S(N)$ azon Sidon halmazok maximális elemszámát, melynek elemei az $\{1, 2, 3, \ldots, N\}$ halmazból valóak:*

$$S(N) = \max_{\substack{\mathcal{A} \subseteq \{1,2,\ldots,N\} \\ \mathcal{A} \text{ Sidon}}} |\mathcal{A}| \tag{6.1}$$

Erdős azonnal észrevette, hogy a mohó algoritmussal bebizonyítható, hogy $S(N) > (2N)^{1/3}$. Ezt az eredményt röviden bebizonyítjuk, de előbb lássunk néhány felső becslést.

A legegyszerűbb felső becslés a következő:

6.2 Tétel.

$$S(N) \leq 2\sqrt{N}.$$

A 6.2 Tétel bizonyítása. Tekintsünk egy

$$\mathcal{A} = \{a_1, a_2, \ldots, a_S\} \subseteq \{1, 2, \ldots, N\}.$$

Sidon sorozatot. Bebizonyítjuk, hogy

$$S = |\mathcal{A}| \leq 2\sqrt{N}.$$

Ehhez tekintsük a számegyenest, és rajta az $1, 2, \ldots, 2N$ számokat.

Tegyünk egy X-et azon egész számokra, amelyek felírhatóak $a + a'$ alakban, ahol $a, a' \in \mathcal{A}$. Ekkor az X-ek száma:

$$\begin{array}{c} \binom{S}{2} + S \longleftarrow a_i = a_j, \\ \uparrow \\ (a_i, a_j) \quad a_i \neq a_j. \end{array}$$

Tudjuk, hogy minden összeg különböző és

$$2 \leq a + a' \leq 2N.$$

Így

$$\begin{aligned} \binom{S}{2} + S &\leq 2N, \\ \frac{S(S+1)}{2} &\leq 2N, \\ S^2 < S(S+1) &\leq 4N, \\ S &< 2\sqrt{N}, \end{aligned}$$

ami bizonyítja a tételt.

Ez az eredmény kicsit javítható, ha összeg helyett különbségeket veszünk.

$$a_0 + {a_0}' = a_1 + {a_1}'$$
$$\Updownarrow$$
$$a_0 - a_1 = {a_1}' - {a_0}'$$

Így az $\mathcal{A}$ halmaz akkor Sidon halmaz, ha minden $a - a'$ különbség (ahol $a, a' \in \mathcal{A}$, $a \neq a'$) különböző.

Tekintsük megint a számegyenest, és ezúttal rajta az $1, 2, \ldots, N-1$ egész számokat.

Tegyünk egy X-et azon egész számokra, amelyek felírhatóak $a - a'$ alakban, ahol $a, a' \in \mathcal{A}$ és $a - a'$ pozitív.

Ekkor az X-ek száma $\binom{S}{2}$.

Minden $a - a'$ különbség különböző és

$$1 \leq a - a' \leq N - 1,$$

így

$$\begin{aligned}
\binom{S}{2} &\leq N - 1, \\
S(S-1) &\leq 2N - 2, \\
S^2 - S + \frac{1}{4} &\leq 2N - \frac{7}{4}, \\
\left(S - \frac{1}{2}\right)^2 &\leq 2N - \frac{7}{4}, \\
S - \frac{1}{2} &\leq \sqrt{2N - \frac{7}{4}} < \sqrt{2}\sqrt{N},
\end{aligned}$$

$$S < \sqrt{2} \cdot \sqrt{N} + \frac{1}{2}.$$

Még cselesebb ötletekkel a tételben szereplő $\sqrt{2}$ szorzótól is megszabadulhatunk. A következő trükkös bizonyítás Erdőstől és Turántól [5] származik.

6.3 TÉTEL.

$$S(N) < \sqrt{N} + \sqrt[4]{N} + 1.$$

A következő bizonyítás Erdős és Surányi könyvéből, Válogatott Fejezetek a Számelméletből [4] való.

A 6.3 Tétel bizonyítása.

A t természetes szám értékét később rögzítjük.

A $[0, N]$ intervallumot részintervallumokra osztjuk. Tekintsük a következő $N + t$ darab intervallumot:

$$[-t + 1, 0], [-t + 2, 1], \ldots, [N, N + t - 1].$$

Legyen $\mathcal{A} \subseteq \{1, 2, \ldots, N\}$ egy Sidon halmaz. Az $\mathcal{A}$ halmaz elemei közül rendre

$$A_1, \quad A_2, \quad \ldots \quad A_{N+t}$$

darab esik a fenti intervallumokba.

Az intervallumok között átfedés is van, és könnyű látni, hogy $\mathcal{A}$ minden eleme t darab egymást követő intervallumban szerepel. Így

$$\sum_{i=1}^{N+t} A_i = ts.$$

A következőkben azt számoljuk ki, hogy egy (a_i, a_j) pár ($i > j$ esetén) összesen hány darab intervallumba esik bele.

Legyen ezek összesített száma D.

Egyrészről világos hogy

$$D = \sum_{i=1}^{n+t} \binom{A_i}{2} = \frac{1}{2}\sum_{i=1}^{n+t} A_i^2 - \frac{1}{2}\sum_{i=1}^{n+t} A_i.$$

Másrészt, ha egy számpár különbsége d, akkor az pont $t-d$ darab intervallumba esik bele.

Mivel minden különbség legfeljebb egyszer szerepel, minden d differenciához maximum egy számpár tartozik, amelyek különbsége d. Ez a számpár összesen $t-d$ intervallumba esik bele, így

$$D \leq \sum_{d=1}^{t-1}(t-d) = \frac{t(t-1)}{2}.$$

A D-re vonatkozó két becslést összevetve adódik, hogy

$$\sum_{i=1}^{n+t} A_i^2 - \sum_{i=1}^{n+t} A_i \leq t(t-1).$$

Láttuk, hogy a második szumma összege éppen ts.

A számtani-négyzetes közép közti egyenlőtlenséget alkalmazva kapjuk, hogy:

$$\sum_{i=1}^{n+t} A_i^2 \geq \frac{\left(\sum_{i=1}^{n+t} A_i\right)^2}{n+t} = \frac{t^2 s^2}{n+t}.$$

Ezeket a becsléseket az egyenlőtlenségbe írva, majd rendezve, és végül $(n+t)/t^2$-tel szorozva kapjuk, hogy

$$s^2 - s\left(\frac{n}{t}+1\right) - \left(\frac{n}{t}+1\right)(t-1) \leq 0.$$

A másodfokú egyenlőtlenséget s-re megoldva adódik, hogy

$$s \le \frac{n}{2t} + \frac{1}{2} + \sqrt{n + t + \frac{n^2}{4t^2} - \frac{n}{2t} - \frac{3}{4}}$$
$$= \frac{n}{2t} + \frac{1}{2} + \sqrt{n + t + \left(\frac{n}{2t} - \frac{1}{2}\right)^2 - 1}.$$

Ezután (hogy minél élesebb becslést kapjunk) rögzítsük $t = \left[\sqrt[4]{n^3}\right] + 1$-nek. Ekkor a becslésben az első tag nem nagyobb mint $\frac{1}{2}\sqrt[4]{n}$, míg az utolsó tag kisebb mint $\sqrt{n} + \frac{1}{2}\sqrt[4]{n} + \frac{1}{2}$.

Ezzel a kívánt egyenlőtlenséget bebizonyítottuk.

Balogh, Füredi és Roy [2] kicsit javított az eredményen, de csak 0.2%-kal:

$$S(N) \le \sqrt{N} + 0.998N^{1/4}.$$

A következőkben alsó becsléseket adunk $S(N)$-re.

Először Erdős alsó becslését igazoljuk, mely a mohó algoritmusra épült.

6.4 Tétel. *Minden N-re létezik egy $\mathcal{A} \subseteq \{1, 2, \dots, N\}$ Sidon halmaz, melyre $|\mathcal{A}| \ge [(2N)^{1/3}]$.*

A 6.4 Tétel bizonyítása. Elegendő a következőt megmutatni: ha

$$\{a_1, a_2, \dots, a_t\} \subseteq \{1, 2, \dots, N\}$$

egy Sidon halmaz, melynek elemszáma t, ahol $t \le (2N)^{1/3} - 1$, akkor létezik egy b egész szám, amelyre

$$1 \le b \le N \quad \text{és} \quad b \notin \{a_1, a_2, \dots, a_t\}, \tag{6.2}$$

továbbá

$$\{a_1, a_2, \dots, a_t\} \cup \{b\}$$

Sidon halmaz. Egy b számot „rossznak” hívunk, ha $\{a_1, a_2, \dots, a_t\} \cup \{b\}$ nem Sidon halmaz, és „jónak” hívunk, ha $\{a_1, a_2, \dots, a_t\} \cup \{b\}$ Sidon halmaz.

A bizonyítás befejezéséhez elegendő annyit belátni, hogy ha $t \leq (2N)^{1/3} - 1$ fennáll, akkor létezik jó b elem, s amelyre (6.2) is teljesül.

Először számoljuk össze a rossz b-k darabszámát. Mivel $\{a_1, a_2, \dots, a_t\}$ Sidon halmaz, ha b rossz (azaz $\{a_1, a_2, \dots, a_t\} \cup \{b\}$ nem Sidon halmaz), akkor létezik a_i, a_j, a_k elemek, melyekre

$$a_i + a_j = a_k + b \tag{6.3}$$

vagy létezik a_u, a_v, melyekre

$$a_u + a_v = b + b. \tag{6.4}$$

Így azon rossz b-k száma, amelyekre (6.3) fennáll

$$\leq \left(\binom{t}{2} + t\right)(t-1) = \frac{t(t^2-1)}{2}.$$

Míg azon rossz b-k száma, amelyekre (6.4) fennáll

$$\leq \binom{t}{2} = \frac{t(t-1)}{2}.$$

Így a rossz b-k összesített száma $\leq \frac{t(t^2-1)}{2} + \frac{t(t-1)}{2} = \frac{t(t-1)(t+3)}{2}$. Végül azon b-k száma, melyre $b \in \{a_1, a_2, \dots, a_t\}$ teljesül t. Ha

$$\frac{t(t-1)(t+3)}{2} + t < N,$$

akkor létezik jó b, melyre (6.2) fennáll. Amennyiben $t \leq (2N)^{1/3} - 1$ ez nyilvánvalóan teljesül:

$$\frac{t(t-1)(t+3)}{2} + t < \frac{(t+1)^3}{2} \leq N,$$

amivel az állítást igazoltuk.

A következőkben mutatunk néhány trükkös konstrukciót Sidon sorozatokra.

Először Erdősnek és Turán [5] egy konstrukciójának kissé módosított változatát ismertetjük.

6.5 Tétel. *Létezik* $\mathcal{A} \subseteq \{1, 2, \ldots, N\}$ *Sidon halmaz, melyre*

$$|\mathcal{A}| \geq \frac{\sqrt{N}}{4}.$$

A 6.5 Tétel bizonyítása. Tegyük fel, hogy $N \geq 16$.

Csebisev tétele szerint minden $n \geq 2$ esetén létezik prímszám n és $2n$ között. (Erről a tételről bővebben olvashatunk a kapcsolódó Wikipédia oldalon: link. A tételre Erdős Pál is adott egy elemi bizonyítást, ld. pl. itt link.)

Csebisev tételét alkalmazva megkapjuk, hogy létezik p prímszám, amelyre

$$\frac{\sqrt{N}}{2} < p < \sqrt{N}.$$

Mivel $N \geq 16$, ez a prímszám páratlan. Jelölje $r_p(x)$ az x egész szám legkisebb nemnegatív maradékát modulo p. Azaz

$$x \equiv r_p(x) \pmod{p} \quad \text{és } 0 \leq r_p(x) \leq p-1.$$

Definiáljuk az $\mathcal{A}$ halmazt az

$$\mathcal{A} \stackrel{\text{def}}{=} \{a : \ a = x + p r_p(x^2),\ 0 \leq x \leq \frac{p-1}{2}\}$$

képlettel. Bebizonyítjuk, hogy ez a halmaz Sidon halmaz.

Világos, hogy $\mathcal{A}$ tartalmaz $\frac{p+1}{2}$ darab különböző elemet, mivel különböző x-ekre az $x + pr_p(x^2)$-nek más-más maradéka van modulo p.

Ezután bebizonyítjuk, hogy $\mathcal{A}$ Sidon halmaz. Tegyük fel, hogy

$$a_1 + a_2 = b_1 + b_2, \tag{6.5}$$

ahol $a_1, a_2, b_1, b_2 \in \mathcal{A}$. Ekkor létezik $0 \leq x_1, x_2, y_1, y_2 \leq \frac{p-1}{2}$ melyekre

$$\begin{aligned} a_1 &= x_1 + pr_p(x_1^2) \\ a_2 &= x_2 + pr_p(x_2^2) \\ b_1 &= y_1 + pr_p(y_1^2) \\ b_2 &= y_2 + pr_p(y_2^2). \end{aligned}$$

Ekkor (6.5) alapján

$$x_1 + x_2 + p\left(r_p(x_1^2) + r_p(x_2^2)\right) = y_1 + y_2 + p\left(r_p(y_1^2) + r_p(y_2^2)\right). \tag{6.6}$$

Így

$$x_1 + x_2 \equiv y_1 + y_2 \pmod{p}.$$

Mivel $0 \leq x_1 + x_2, y_1 + y_2 \leq p - 1$, tudjuk, hogy

$$x_1 + x_2 = y_1 + y_2. \tag{6.7}$$

Ekkor (6.6) és (6.7) miatt

$$\begin{aligned} r_p(x_1^2) + r_p(x_2^2) &= r_p(y_1^2) + r_p(y_2^2) \\ x_1^2 + x_2^2 &\equiv y_1^2 + y_2^2 \pmod{p}. \end{aligned} \tag{6.8}$$

Ekkor (6.7)-t Négyzetreemlve, és abból (6.8)-t kivonva kapjuk, hogy

$$2x_1x_2 \equiv 2y_1y_2 \pmod{p}$$

$$x_1 x_2 \equiv y_1 y_2 \pmod{p} \tag{6.9}$$

A gyökök és együtthatók közötti összefüggés alapján, (6.7)-ből és (6.9)-ből adódóan kapjuk, hogy x_1, x_2 és y_1, y_2 ugyanannak a másodfokú egyenletnek a gyökei.

A fokszám tétel miatt minden másodfokú kongruenciának legfeljebb két gyöke van, így

$$\{x_1, x_2\} = \{y_1, y_2\},$$

azaz

$$\{a_1, a_2\} = \{b_1, b_2\}.$$

Tehát $\mathcal{A}$ olyan Sidon halmaz, melyre $|\mathcal{A}| \geq \frac{\sqrt{N}}{4}$, és ezzel a bizonyítást befejeztük.

A következő trükkös bizonyítás Ruzsától származik [3], aki eltüntette az $\frac{1}{4}$-es szorzót az előző tételben. Először a következőt igazoljuk:

6.6 Tétel. *Legyen p egy páratlan prímszám. Ekkor létezik $p-1$ darab a_i egész szám, amelyre az $a_i - a_j$ különbségek (ahol $i \neq j$) inkongruensek modulo $p^2 - p$.*

A 6.6 Tétel bizonyítása. Legyen g egy primitív gyök modulo p, és legyenek a_i-k a modulo $p^2 - p$ egyértelműen meghatározott megoldásai a

$$\begin{aligned} x &\equiv i \pmod{p-1}, \\ x &\equiv g^i \pmod{p}. \end{aligned}$$

szimultán kongruencia-rendszernek (a kínai maradéktétel miatt tudjuk, hogy ilyen megoldás létezik és egyértelmű). Azt kell megmutatnunk, hogy az

$$a_i - a_j \equiv a_r - a_s \pmod{p^2 - p},$$

kongruenciának, vagy evvel ekvivalensen az

$$a_i + a_s \equiv a_r + a_j \pmod{p^2 - p},$$

kongruenciának csak triviális megoldásai vannak. Más szóval minden c-re legfeljebb egy olyan i, j pár létezik, hogy

$$c \equiv a_i + a_j \pmod{p^2 - p}.$$

Az a_i-k definíciója alapján, ez ekvivalens a

$$\begin{aligned} c &\equiv i + j \pmod{p-1}, \\ c &\equiv g^i + g^j \pmod{p}. \end{aligned}$$

szimultán kongruencia-rendszerrel Az első kongruencia ekvivalens a következővel:

$$g^c \equiv g^i g^j \pmod{p}.$$

Ekkor a gyökök és együtthatók közötti összefüggés szerint a g^i és g^j modulo p maradékosztályok egyértelműen meghatározottak, mivel mindketten megoldásai az

$$x^2 - cx + g^c \equiv 0 \pmod{p}.$$

másodfokú kongruenciának. A fokszám tétel miatt a másodfokú kongruenciának legfeljebb 2 gyöke van, így a gyökök valóban egyértelműen meghatározottak. Azaz i és j is egyértelműen meghatározott.

A fenti módon megkonstruált a_i-k valóban Sidon halmazt alkotnak $\mathbb{Z}_{p^2-p}$-ben. Ezzel a tétel állítását beláttuk.

Nyilvánvaló, hogy ha egy mod p^2-p Sidon halmaz elemeihez hozzárendeljük a vele kongruens legkisebb pozitív egészet, akkor Sidon halmazt kapunk $\{1,2,\ldots,p^2-p\}$-ben.

Így ha történetesen N egy p^2-p alakú szám (ahol p prím), akkor

$$S(N) \geq p-1 = \frac{1}{2}(\sqrt{4N+1}+1)-1 > \sqrt{N}-1.$$

Tetszőleges N-re olyan p prímet választunk, amelyre p^2-p közel van N-hez.

Van egy híres sejtés, miszerint minden pozitív δ-ra n és $n+n^\delta$ közé esik prím, feltéve, hogy n elegendően nagy. A sejtés bizonyítása reménytelennek tűnik.

De ha az összes pozitív δ-ra nem is, de pár kicsi konkrét δ-ra azért sikerült igazolni a sejtést.

Azon δ-k értéke melyre igazolt a sejtés, egyre jobbak, egyre kisebbek. Jelenleg a legélesebb eredmény Bakertől, Harmantól és Pintztől [1] származik, nevezetesen $\delta = 0.525$.

Így tudunk p prímet választani $\sqrt{N}-N^{0.2625}$ és $\sqrt{N}$ között, és ekkor

$$S(N) \geq S(p^2-p) \geq p-1 \geq \sqrt{N}-O(N^{0.2625}).$$

Sidon sorozatokról Erdős számtalan sejtést fogalmazott meg, ezekről bővebben pl. itt olvashatunk: link. Sajnos, ma már (leg-

jobb tudomásom szerint) nem jár pénzjutalom a problémák megfejtésért...

Hivatkozások

[1] R. C. Baker, G. Harman, J. Pintz, *The difference between consecutive primes, II*, Proceedings of the London Mathematical Society. 83 (3) (2001), 532–562.

[2] J. Balogh, Z. Füredi, S. Roy, *An Upper Bound on the Size of Sidon Sets*, The American Mathematical Monthly, DOI: 10.1080/00029890.2023.2176667.

[3] I. Z. Ruzsa, *Solving a linear equation in a set of integers. I*, Acta Arith.65 (1993), 259–282.

[4] P. Erdős, J. Surányi, *Válogatott Fejezetek a Számelméletből*, Polygon 2004, link.

[5] P. Erdős és P. Turán, *On a problem of Sidon in additive number theory and related problems*, Journ. London Math. Soc.16 (1941), 212—215.

7. Cauchy-Davenport tétel

A csoportelmélet egyik alapvető kérdése, hogy milyen alsó becsléseket adhatunk részhalmazok összegére, $|\mathcal{A}+\mathcal{B}|$-re $|\mathcal{A}|$ és $|\mathcal{B}|$ függvényében. Véges csoportok esetén ilyen jellegű egyszerű tétel a következő:

7.1 Tétel. *Ha $\mathcal{G}$ egy véges Ábel csoport, $\mathcal{A},\mathcal{B}$ nem üres részhalmazai $\mathcal{G}$-nek, ahol*

$$|\mathcal{A}|+|\mathcal{B}|>|\mathcal{G}|,$$

akkor

$$\mathcal{A}+\mathcal{B}=\mathcal{G}.$$

A 7.1 Tétel bizonyítása. Legyen $g\in\mathcal{G}$ tetszőleges. Bebizonyítjuk, hogy g felírható $g=a+b$ alakban, ahol $a\in\mathcal{A}$, $b\in\mathcal{B}$. A bizonyításhoz tekintsük a

$$g-\mathcal{B}=\{g-b : b\in\mathcal{B}\}$$

halmazt. Mivel $|g-\mathcal{B}|=|\mathcal{B}|$, így

$$|\mathcal{A}|+|g-\mathcal{B}|>|\mathcal{G}|,$$

amelyből adódóan $\mathcal{A}\cap(g-\mathcal{B})\neq\emptyset$. Azaz ekkor létezik $a\in\mathcal{A}$ és $b\in\mathcal{B}$ melyekre $a=g-b\Longrightarrow g=a+b$.

Az első ismert eredmény az additív csoportelméletből a híres Cauchy-Davenport tétel, mely a fejeztünk témája lesz.

A tételt Cauchy [1] fedezte fel 1813-ban, majd Davenport [3] (nem ismerve Cauchy eredményét) újra felfedezte 1935-ben. (ld. még pl. [4]).

A tétel alsó becslést ad $|\mathcal{A}+\mathcal{B}|$-re $|\mathcal{A}|$ és $|\mathcal{B}|$ függvényében, ha $\mathcal{A}$ és $\mathcal{B}$ a $\mathbb{Z}_p$ halmaznak nem üres részhalmazai, ahol p prím.

7.2 Tétel. (Cauchy–Davenport) *Legyen p prím és $\mathcal{A},\mathcal{B}\subseteq\mathbb{Z}_p$ nem üres részhalmazok. Ekkor*

$$|\mathcal{A}+\mathcal{B}|\geq\min\{p,|\mathcal{A}|+|\mathcal{B}|-1\}.$$

A 7.2 Tétel bizonyítása. A következő lemmát használjuk:

7.3 Lemma. *Legyen $\mathcal{A}\subseteq\mathbb{Z}_p$, $d\in\mathbb{Z}_p$, $d\neq 0$. Ha*

$$\mathcal{A}+d\subseteq\mathcal{A},$$

akkor

$$\mathcal{A}=\mathbb{Z}_p.$$

A 7.3 Lemma bizonyítása. Ha $\mathcal{A}+d\subseteq\mathcal{A}$, akkor $a\in\mathcal{A}\Longrightarrow a+d\in\mathcal{A}$. Ezt az állítást többször alkalmazva kapjuk

$$a,a+d,a+2d,\ldots,a+(p-1)d\in\mathcal{A}. \tag{7.1}$$

De $a,a+d,a+2d,\ldots,a+(p-1)d$ egy teljes maradékrendszert alkot modulo p, mivel a fenti halmaznak p darab eleme van, és bármely két elem inkongruens modulo p. Valóban, ha

$$a+id\equiv a+jd\pmod p$$

egy $0 \leq i, j \leq p-1$ párra, akkor

$$\begin{aligned} id &\equiv jd \pmod{p} \quad / : d \\ i &\equiv j \pmod{p} \\ i &= j. \end{aligned}$$

Így (7.1) alapján

$$\mathbb{Z}_p \subseteq \mathcal{A}.$$

Mivel $\mathcal{A} \subseteq \mathbb{Z}_p$ szintén fennáll:

$$\mathcal{A} = \mathbb{Z}_p.$$

7.4 Lemma. *Legyen $\mathcal{A} \subseteq \mathbb{Z}_p$, $x, y \in \mathbb{Z}_p$, $x \neq y$. Ekkor ha*

$$\mathcal{A} + x \subseteq \mathcal{A} + y,$$

akkor

$$\mathcal{A} = \mathbb{Z}_p.$$

A 7.4 Lemma bizonyítása. Ha $\mathcal{A} + x \subseteq \mathcal{A} + y$, akkor

$$\mathcal{A} + (x - y) \subseteq \mathcal{A}.$$

Legyen $x - y = d$, ekkor

$$\mathcal{A} + d \subseteq \mathcal{A}.$$

A 7.3 Lemma alapján $\mathcal{A} = \mathbb{Z}_p$.

Feladat

Bizonyítsuk be a Cauchy–Davenport tételt ha $|\mathcal{B}| = 1$ vagy $|\mathcal{B}| = 2$.

Megoldás

Legyen

$$\mathcal{A} = \{\alpha_1, \alpha_2, \ldots, \alpha_m\},$$
$$\mathcal{B} = \{\beta_1, \beta_2, \ldots, \beta_n\}$$

Ha $n = 1$, akkor

$$|\mathcal{A} + \mathcal{B}| = |\mathcal{A} + \beta_1| = |\mathcal{A}| = m$$
$$= m + 1 - 1 = m + n - 1.$$

Így $n = 1$ esetén beláttuk a tétel állítását.

Következőleg azt az esetet tanulmányozzuk, amikor $n = 2$. Legyen $\mathcal{B} = \{\beta_1, \beta_2\}$ jelölje d a két elem különbségét, azaz $d = \beta_2 - \beta_1$.

$$\beta_1 \not\equiv \beta_2 \pmod{p} \implies (d, p) = 1.$$

Két esetet különböztetünk meg.

I. Eset: $\mathcal{A} + d \subseteq \mathcal{A}$.

Ekkor 7.3 Lemma alapján $\mathcal{A} = \mathbb{Z}_p$, így $\mathcal{A} + \mathcal{B} = \mathbb{Z}_p$, azaz

$$|\mathcal{A} + \mathcal{B}| = |Z_p| = p \geq \min\{p, |\mathcal{A}| + |\mathcal{B}| - 1\},$$

vagyis az I. Esetben fennáll a tétel állítása.

II. Eset: $\mathcal{A} + d \not\subseteq \mathcal{A}$.

Ekkor $\exists\ \alpha \in \mathcal{A}$, amelyre $\alpha + d \notin \mathcal{A}$.
Feltehetjük, hogy $\alpha = \alpha_1$. Így

$$\alpha_1 + d \notin \mathcal{A},$$

$$\alpha_1 + \beta_2 - \beta_1 \notin \mathcal{A},$$
$$\alpha_1 + \beta_2 - \beta_1 \neq \alpha_i \text{ ahol } 1 \leq i \leq m,$$
$$\alpha_1 + \beta_2 \neq \alpha_i + \beta_1 \text{ ahol } 1 \leq i \leq m,$$

Ekkor:

$$\{\alpha_1 + \beta_2\} \cap \{\alpha_i + \beta_1,\ 1 \leq i \leq m\} = \emptyset,$$
$$|\mathcal{A} + \mathcal{B}| \geq 1 + m = m + 2 - 1 = m + n - 1.$$

Ezzel bebizonyítottuk a Cauchy-Davenport tételt $n = 1$-re és $n = 2$-re.

Amikor $|\mathcal{A}| = p$ vagy $|\mathcal{B}| = p$ (azaz $\mathcal{A} = \mathbb{Z}_p$ vagy $\mathcal{B} = \mathbb{Z}_p$) akkor a tétel triviális.

Ezután bebizonyítjuk a Cauchy-Davenport tételt teljes általánosságában n-re vonatkozó teljes indukcióval.

Az $n = 1$ és $n = 2$ esetben már láttuk a bizonyítást.

Az indukciós feltevés szerint, feltehetjük, hogy a tételt már bizonyítottuk minden olyan $\mathcal{A}'$ és $\mathcal{B}'$ halmazpárra, ahol

$$1 \leq |\mathcal{B}'| < n,$$

és ebből következőleg beszeretnék látni egy olyan $\mathcal{A}, \mathcal{B} \subseteq \mathbb{Z}_p$ halmazpárra, ahol $|\mathcal{B}| = n < p$ és $|\mathcal{A}| < p$. (Ez az indukciós lépés.)

Először tekintsük a következő speciális esetet:

I. Eset: Amikor $\mathcal{A} \cap \mathcal{B}$ nem üres, valódi részhalmaza $\mathcal{B}$-nek.

Legyen

$$\mathcal{A}' \overset{\text{def}}{=} \mathcal{A} \cup \mathcal{B},$$

$$\mathcal{B}' \stackrel{\text{def}}{=} \mathcal{A} \cap \mathcal{B}.$$

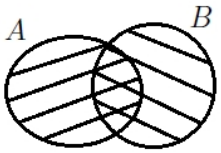
Ekkor $\mathcal{B}'$ valódi nem üres részhalmaza $\mathcal{B}$-nek, így

$$1 \leq |\mathcal{B}'| < |\mathcal{B}| = n.$$

Az indukciós feltevés szerint:

$$|\mathcal{A}' + \mathcal{B}'| \geq \min\{p, |\mathcal{A}'| + |\mathcal{B}'| - 1\}, \tag{7.2}$$

A következőt tetszőleges $\mathcal{A}$ és $\mathcal{B}$ halmazokra tudjuk:



$$\begin{aligned} |\mathcal{A}| + |\mathcal{B}| &= |\mathcal{A} \cup \mathcal{B}| + |\mathcal{A} \cap \mathcal{B}| \\ &= |\mathcal{A}'| + |\mathcal{B}'|. \end{aligned}$$

Másrészt, be fogjuk látni, hogy

$$\mathcal{A}' + \mathcal{B}' \subseteq \mathcal{A} + \mathcal{B}. \tag{7.3}$$

Valóban, tegyük fel, hogy $x \in \mathcal{A}' = \mathcal{A} \cup \mathcal{B}$ és $y \in \mathcal{B}' = \mathcal{A} \cap \mathcal{B}$. Bebizonyítjuk, hogy $x + y \in \mathcal{A} + \mathcal{B}$.

Ha $x \in \mathcal{A}$ akkor $y \in \mathcal{B}$ miatt $x + y \in \mathcal{A} + \mathcal{B}$. Ha $x \in \mathcal{B}$ akkor $y \in \mathcal{A}$ miatt $x + y \in \mathcal{A} + \mathcal{B}$. Így beláttuk (7.3)-t.

Ekkor (7.2) és (7.3) alapján kapjuk, hogy

$$\begin{aligned} |\mathcal{A} + \mathcal{B}| &\geq |\mathcal{A}' + \mathcal{B}'| \geq \min\{p, |\mathcal{A}'| + |\mathcal{B}'| - 1\} \\ &= \min\{p, |\mathcal{A}| + |\mathcal{B}| - 1\}. \end{aligned}$$

Ezzel az I. Esetben beláttuk a Cauchy–Davenport tétel állítását.

Az általános esetet (vagyis, ha $\mathcal{A} \cap \mathcal{B}$ nem szükségszerűen üres, valódi részhalmaza $\mathcal{B}$-nek) a következőkben fogjuk tanulmányozni. Ekkor a következőt állítjuk:

7.5 LEMMA. *Amennyiben $|\mathcal{A}| < p$, létezik egy $c \in \mathbb{Z}_p$ elem, amelyre $\mathcal{B} \cap (\mathcal{A} + c)$ nem üres valódi részhalmaza $\mathcal{B}$-nek.*

A 7.5 Lemma bizonyítása. Legyen

$$\mathcal{A} = \{\alpha_1, \alpha_2, \ldots, \alpha_m\},$$
$$\mathcal{B} = \{\beta_1, \beta_2, \ldots, \beta_n\}.$$

Ha c-t $\beta_i - \alpha_j$ alakban keressük, akkor $\mathcal{B} \cap (\mathcal{A} + c) = \mathcal{B} \cap (\mathcal{A} + \beta_i - \alpha_j)$ nem üres halmaz, mivel

$$\beta_i \in \mathcal{B} \quad \text{és} \quad \beta_i = \alpha_j + \beta_i - \alpha_j \in \mathcal{A} + (\beta_i - \alpha_j).$$

Először két elemet rögzítünk $\mathcal{B}$-ben: β_k-t és β_i-t, ahol $\beta_k \neq \beta_i$. Feltehetjük, hogy

$$\mathcal{A} + (\beta_k - \beta_i) \not\subseteq \mathcal{A},$$

mivel különben a 7.3 Lemma miatt $\mathcal{A} = \mathbb{Z}_p$, és akkor a tétel triviális.

Legyen α_j olyan, hogy $\alpha_j + (\beta_k - \beta_i) \notin \mathcal{A}$. Ekkor

$$\beta_k \notin \mathcal{A} + \beta_i - \alpha_j,$$
$$\beta_k \notin \mathcal{B} \cap (\mathcal{A} + \beta_i - \alpha_j).$$

Azaz $\mathcal{B} \cap (\mathcal{A} + \beta_i - \alpha_j) \neq \mathcal{B}$ és nem üres halmaz (mivel $\beta_i \in \mathcal{B} \cap (\mathcal{A} + \beta_i - \alpha_j)$), így valódi részhalmaza $\mathcal{B}$-nek. Ezzel a lemma állítását igazoltuk.

Ezután visszatérünk a Cauchy-Davenport tétel bizonyításához. Rögzítünk egy $c \in \mathbb{Z}_p$ elemet, melyre a 7.5 Lemma fennáll. A már igazolt I. Eset miatt az $\mathcal{A} + c$ és $\mathcal{B}$ halmazokra alkalmazhatjuk a Cauchy-Davenport tételt. Ekkor:

$$|\mathcal{A} + \mathcal{B}| = |(\mathcal{A} + c) + \mathcal{B}|$$

$$\geq \min\{p, |\mathcal{A}+c| + |\mathcal{B}| - 1\}$$
$$= \min\{p, |\mathcal{A}| + |\mathcal{B}| - 1\}.$$

A következőkben a Cauchy-Davenport tétel néhány általánosítását mutatjuk meg, immár bizonyítás nélkül.

Az első tétel Chowla-tól [2] származik (ld. még [6], [7]) és a Cauchy-Davenport tételt általánosítja összetett modulusra.

7.6 Tétel. (Chowla) *Legyen $\mathcal{A}, \mathcal{B} \subseteq \mathbb{Z}_n$ nem üres halmazok. Ha $0 \in \mathcal{B}$ és $(b, n) = 1$ minden $b \in \mathcal{B} \setminus \{0\}$-re, akkor*

$$|\mathcal{A} + \mathcal{B}| \geq \min\{n, |\mathcal{A}| + |\mathcal{B}| - 1\}.$$

Pillai [8] az összetett modulusok esetén további általánosítást talált:

7.7 Tétel. (Pillai) *Legyen $\mathcal{A}, \mathcal{B} \subseteq \mathbb{Z}_n$ nem üres halmazok. Írjuk $\mathcal{B} = \{\beta_1, \ldots, \beta_m\}$ alakba, és legyen*

$$d = \max_{i \neq j}(n, \beta_i - \beta_j).$$

Ekkor

$$|\mathcal{A} + \mathcal{B}| \geq \min\left\{\frac{n}{d},\ |\mathcal{A}| + |\mathcal{B}| - 1\right\}.$$

Kneser tétele [5], mely a Cauchy-Davenport tételt végtelen csoportokra általánosítja, ma már klasszikus. Itt szükségünk van egy új fogalomra, a stabilizátorra, melyet $\mathcal{C} \subseteq G$ esetén (ahol G egy Ábel csoport, $\mathcal{C}$ pedig G tetszőleges részhalmaza) a

$$\mathrm{stab}(\mathcal{C}) = \{g \in \mathcal{G},\ g + \mathcal{C} = \mathcal{C}\}.$$

képlettel adunk meg.

7.8 TÉTEL. (Kneser) *Legyen G egy Ábel csoport (általában végtelen), $\mathcal{A}, \mathcal{B} \subseteq \mathcal{G}$ véges nem üres részhalmazok. Ekkor, ha*

$$H = \text{stab}(\mathcal{A} + \mathcal{B}) = \{g \in \mathcal{G},\ g + (\mathcal{A} + \mathcal{B}) = \mathcal{A} + \mathcal{B}\},$$

úgy

$$|\mathcal{A} + \mathcal{B}| \geq |\mathcal{A} + H| + |\mathcal{B} + H| - |H|.$$

Hivatkozások

[1] A. L. Cauchy, *Recherches sur les nombres*, J. École Polytech. 9 (1813), 99–123.

[2] I. Chowla, *A theorem on the addition of residue classes: application to the number $\Gamma(k)$ in Waring's problem*, Proc. Indian Acad. Sci.,2 (1935), 242–243.

[3] H. Davenport, *On the addition of residue classes*, J. London Math. Soc.,10 (1935), 30–32.

[4] H. Davenport, *A historical note*, J. London Math. Soc. 22 (1947), 100–101.

[5] M. Kneser, *Abschätzung der asymptotischen Dichte von Summenmengen*, Math. Z., 58 (1953), 459–484.

[6] H. B. Mann, *Addition Theorems in Group Theory and Number Theory*, R. E. Krieger Publishing Company, Huntington, New York, 1976.

[7] M. B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Springer, 1996.

[8] S. S. Pillai, *Generalization of a theorem of Davenport on the addition of residue classes*, Proc. Indian Acad. Sci. A, 6 (1937), 179–180.

[9] Kép, Augustin Louis Cauchy, Wikipedia, link.

[10] Kép, Harold Davenport, Wikimedia Commons, link.

8. A Kombinatorikus Nullstellensatz

Ez a fejezet Alontól [1] származó Kombinatorikus Nullstellensatzt tárgyalja, illetve annak egy ügyes alkalmazását, mely kissé általánosítja a Cauchy-Davenport tételt.

8.1 TÉTEL. (Kombinatorikus Nullstellensatz) *Legyen F egy tetszőleges test és $P(x_1, \ldots, x_n)$ egy többváltozós polinom $F[x_1, \ldots, x_n]$-ben. Tegyük fel, hogy P fokszáma $\deg P = \sum_{i=1}^{n} k_i$, ahol k_i nemnegatív egész számok, és az $x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$ tag együtthatója P-ben nem nulla. Ekkor F tetszőleges $A_1, \ldots, A_n$ részhalmazaira, ahol $|A_i| \geq k_i + 1$ minden $i = 1, 2, \ldots, n$, létezik $a_1 \in A_1, \ldots, a_n \in A_n$, melyekre $P(a_1, \ldots, a_n) \neq 0$.*

A következő rövid bizonyítás Michalek [6] cikkére alapozódik.

A 8.1 Tétel bizonyítása. A bizonyítás P fokszáma szerinti teljes indukcióval történik. Ha $\deg P = 1$, a tétel triviális.

Ezután feltesszük, hogy $\deg P = n > 1$, és a tételt már bebizonyítottuk minden n-nél kisebb fokú polinom esetében. Be akarjuk bizonyítani az állítást P-re is. Innen indirekten folytatjuk a bizonyítást.

Tegyük fel, hogy $\deg P > 1$ és P eleget tesz a tétel feltételeinek, de a tétel állítása hamis, azaz, $P(x) = 0$ minden $x \in A_1 \times \cdots \times A_n$.

Az általánosság elvesztése nélkül feltehetjük, hogy $k_1 > 0$. Rögzítsünk egy $a \in A_1$-t és legyen

$$P = (x_1 - a)Q + R, \tag{8.1}$$

ahol a polinomokra vonatkozó maradékos osztással elosztottuk P-t $x_1 - a$-val.

A (8.1) egyenlet egy formális azonosság a polinomok gyűrűjében, ahol a változó x_1 az együtthatók pedig $F[x_2, \ldots, x_n]$ gyűrűből valóak.

Mivel az R polinom fokszáma az x_1 változóban szigorúan kisebb mint $\deg(x_1 - a)$, az R polinom egyáltalán nem tartalmaz x_1-et.

A tétel feltétele szerint P polinomnak van egy olyan $x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$ tagja, amely maximális fokszámú és nem nulla együtthatós. Ebből adódóan Q polinomban is van egy maximális fokszámú és nem nulla együtthatós $x_1^{k_1-1} x_2^{k_2} \cdots x_n^{k_n}$ tag, ahol $\deg Q = \sum_{i=1}^{n} k_i - 1 = \deg P - 1$.

Tekintsünk egy tetszőleges $x \in \{a\} \times A_2 \times \cdots \times A_n$ elemet és helyettesítsük be (8.1)-be.

Mivel $P(x) = 0$ tudjuk, hogy $R(x) = 0$.

De R nem tartalmaz x_1 tagot, ezért azt kapjuk, hogy R eltűnik az $(A_1 \setminus \{a\}) \times A_2 \times \cdots \times A_n$ halmazon.

Ezután írjunk $x \in (A_1 \setminus \{a\}) \times A_2 \times \cdots \times A_n$ elemet (8.1)-be. Mivel $x_1 - a$ nem nulla, ezért $Q(x) = 0$.

Vagyis Q eltűnik a $(A_1 \setminus \{a\}) \times A_2 \times \cdots \times A_n$, halmazon, amely ellentmond az indukciós feltevésnek.

Erdős és Heilbronn [4] a következőt sejtette 1964-ben.

8.2 SEJTÉS. (Erdős-Heilbronn) *Ha p prímszám, és $\mathcal{A}$ nem üres részhalmaz $\mathbb{Z}_p$-nek, akkor*

$$|\{a + a' : \ a, a' \in \mathcal{A}, \ a \neq a'\}| \geq \min\{p, \ 2|\mathcal{A}| - 3\}.$$

Dias Da Silva és Hamidoune [3] lineáris algebrát és szimmetrikus csoportokra vonatkozó reprezentáció elméleti eszközöket használva igazolta a tételt.

Alon, Nathanson és Ruzsa [2] leegyszerűsítette a bizonyítást a Kombinatorikus Nullstellensatz-t használva.

Az eredményük két darab halmazra megfogalmazva a következő volt:

8.3 TÉTEL. *Legyen p prímszám, $\mathcal{A}$ és $\mathcal{B}$ nem üres részhalmazai $\mathbb{Z}_p$-nek. Ekkor ha $|\mathcal{A}| \neq |\mathcal{B}|$, akkor*

$$|\{a+b:\ a\in\mathcal{A},\ b\in\mathcal{B},\ a\neq b\}| \geq \min\{p,\ |\mathcal{A}|+|\mathcal{B}|-2\}.$$

Amennyiben nem tesszük fel az $|A| \neq |B|$ feltételt, az előző tételnek azonnali következménye az alábbi:

8.4 TÉTEL. *Legyen p prímszám, $\mathcal{A}$ és $\mathcal{B}$ nem üres részhalmazai $\mathbb{Z}_p$-nek. Ekkor*

$$|\{a+b:\ a\in\mathcal{A},\ b\in\mathcal{B},\ a\neq b\}| \geq \min\{p,\ |\mathcal{A}|+|\mathcal{B}|-3\}.$$

Ez az eredmény kicsit (de csak nagyon kicsit) gyengébb mint az előző tétel. Károlyi Gyula [5] pontosan meg tudta határozni azokat a halmazokat, melyekre csak a fenti gyengébb becslés áll fenn.

8.5 TÉTEL. *Legyen p prímszám, $\mathcal{A}$ és $\mathcal{B}$ két nem-üres részhalmaza $\mathbb{Z}_p$-nek. Ekkor*

$$|\{a+b:\ a\in\mathcal{A},\ b\in\mathcal{B},\ a\neq b\}| \geq \min\{p, |\mathcal{A}|+|\mathcal{B}|-2\},$$

kivéve, ha $\mathcal{A}=\mathcal{B}$ és a következő feltételek közül egy fennáll:

(i) $|\mathcal{A}| = 2$ *vagy* $|\mathcal{A}| = 3$*;*

(ii) $|\mathcal{A}| = 4$ *és* $\mathcal{A} = \{a, a+d, c, c+d\}$*;*

(iii) $|\mathcal{A}| \geq 5$ *és* $\mathcal{A}$ *egy számtani sorozat.*

Michalek [6] cikke alapján, mi csak a 8.4 Tételt igazoljuk itt.

A 8.4 Tétel bizonyítása. Legyen

$$\mathcal{C} = \{a + b : \ a \in \mathcal{A},\ b \in \mathcal{B},\ a \neq b\}.$$

Azt szeretnénk bizonyítani, hogy

$$|\mathcal{C}| \geq \min\{p, |\mathcal{A}| + |\mathcal{B}| - 3\}.$$

Ha $p = 2$ a tétel triviális. Tegyük fel, hogy $p > 2$.

Ha $\min\{p,\ |\mathcal{A}| + |\mathcal{B}| - 3\} = p$, akkor az $\mathcal{A}$ és $g - \mathcal{B}$ halmazoknak legalább két különböző közös eleme van tetszőleges $g \in \mathbb{Z}_p$ esetén.

Így, ha a különbözik $\frac{g}{2}$-től, akkor $g = a + b$ valamilyen $b \in \mathcal{B}$-re, ahol b különbözik a-tól.

Ezzel beláttuk $g \in \mathcal{C}$, és így $\mathcal{C} = \mathbb{Z}_p$.

Tegyük fel, hogy $|\mathcal{A}| + |\mathcal{B}| - 3 < p$ és a tétel állítása nem igaz.

Ebben az esetben létezik egy $\mathcal{D}$ halmaz, melyre $C \subseteq D$ és $|\mathcal{D}| = |\mathcal{A}| + |\mathcal{B}| - 4$.

Definiálunk két különböző polinomot:

$$P(x, y) = \prod_{d \in \mathcal{D}} (x + y - d) \quad \text{és} \quad Q(x, y) = P(x, y)(x - y).$$

Világos, hogy $P(a,b) = 0$ minden $a \in \mathcal{A}$, $b \in \mathcal{B}, a \neq b$ esetén, így $Q(a,b) = 0$ minden $a \in \mathcal{A}$, $b \in \mathcal{B}$ esetén.

Ha $i + j = |\mathcal{D}|$, akkor $x^i y^j$ tag együtthatója $P(x,y)$-ben $\binom{|\mathcal{D}|}{i}$.

Ebből következőleg, ha $i+j = |\mathcal{D}|+1$, akkor az $x^i y^j$ tag együtthatója $Q(x,y)$-ban $\binom{|\mathcal{D}|}{i-1} - \binom{|\mathcal{D}|}{i} = \frac{|\mathcal{D}|!}{i!(|\mathcal{D}|-i+1)!}(i - (|\mathcal{D}| - i + 1))$.

Ez az együttható akkor és csak akkor 0 ($\mathbb{Z}_p$-ben), ha $i = \frac{|\mathcal{D}|+1}{2}$.

Mivel $|\mathcal{D}|+1 = |\mathcal{A}|+|\mathcal{B}|-3$, így az $x^{|\mathcal{A}|-1}y^{|\mathcal{B}|-2}$ és $x^{|\mathcal{A}|-2}y^{|\mathcal{B}|-1}$ tagok közül valamelyik együtthatója nem nulla.

A 8.1 Tételt és a $\deg Q = |\mathcal{A}| + |\mathcal{B}| - 3$ összefüggést használva ellentmondásra jutunk.

Hivatkozások

[1] N. Alon, *Combinatorial Nullstellensatz*, Combin. Prob.Comput. 8 (1999), 7-29.

[2] N. Alon, M. B. Nathanson, I. Ruzsa, *The Polynomial Method and Restricted Sums of Congruence Classes*, Journal of Number Theory 56 (2), (1996), 404-417.

[3] J. A. Dias da Silva, Y. O. Hamidoune, *Cyclic spaces for Grassmann derivatives and additive theory,* Bull. London Math. Soc. 26 (1994), 140-146.

[4] P. Erdős és R. L. Graham, *Old and New Problems and Results in Combinatorial Number Theory,*, L'Enseignement Mathématique, Geneva, 1980.

[5] Gy. Károlyi, *Restricted set addition: The exceptional case of the Erdős–Heilbronn conjecture*, Journal of Combinatorial Theory, Series A 116 (3), (2009), 741-746.

[6] M. Michalek, *A Short Proof of Combinatorial Nullstellensatz*, The American Mathematical Monthly 117 (9), (2010), 821-823.

9. Erdős-Ginzburg-Ziv Tétel

Az Erdős-Ginzburg-Ziv tétel jól szemlélteti a Cauchy-Davenport-tétel alkalmazhatóságát, amelyet szerzői (Erdős, Ginzburg és Ziv) 1961-ben dolgoztak ki [1]. A következőkben [1] és a kapcsólódó Wikipédia oldal [2] alapján ismertetjük a tétel bizonyítását.

9.1 TÉTEL. (Erdős–Ginzburg–Ziv) *Tetszőlegesen megadott $2m-1$ darab egész szám közül mindig kiválasztható m darab, amelyek összege osztható m-mel.*

A 9.1 Tétel bizonyítása. Először a tételt csak prímekre igazoljuk.

Legyen p prímszám, és jelöljük az adott egészeket $a_1, a_2, \ldots, a_{2p-1}$-gyel. Feltehetjük, hogy

$$0 \leq a_1 \leq a_2 \leq \ldots \leq a_{2p-1} < p.$$

Ha $a_i = a_{i+p-1}$ valamilyen $1 \leq i \leq p-1$-re, ekkor

$$a_i + a_{i+1} + \ldots + a_{i+p-1} = pa_i = 0 \quad (\mathbb{Z}_p\text{-ben}),$$

amiből a kívánt eredmény következik. Különben meg, definiáljuk az A_i kételemű halmazokat

$$A_i = \{a_i, a_{i+p-1}\}$$

képlettel. A Cauchy-Davenport tétel ismételt alkalmazásával

$$\{A_1+A_2+\ldots+A_{p-1}\} \geq \min\{p, |A_1|+\ldots+|A_{p-1}|-(p-2)\} = p.$$

Azaz azt kaptuk, hogy minden $\bmod p$ maradékosztály felírható $p-1$ darab elem összegeként, ahol az elemek a $a_1, a_2, \ldots, a_{2p-2}$

halmazból valóak. Speciálisan $-a_{2p-1}$ is felírható, amely egyenletet rendezve, megkapjuk a tétel állítását.

A jövőben az Erdős-Ginzburg-Ziv tételt EGZT-nek rövidítjük.

9.2 LEMMA. *Az EGZT prímekre igaz.*

Ezt az állítást most láttuk be.

9.3 LEMMA. *Ha az EGZT igaz az m és n természetes számokra, akkor mn-re is igaz.*

A 9.3 Lemma bizonyítása. Először k-ra vonatkozó teljes indukcióval belátjuk, hogy $k \cdot m + m - 1$ darab egész közül mindig kiválasztható $a_1, a_2, \ldots, a_{km}$ egészek, melyekre $0 \leq i \leq k-1$ esetén

$$a_{im+1} + a_{im+2} + \ldots + a_{(i+1)m} \tag{9.1}$$

osztható m-mel.

Így $k = 1$ esetén az állítás egyszerűen az EGZT az m modulusra, amelynek igazsága a 9.3 Lemma feltételei között szerepel.

Ezután tegyük fel, hogy az állítást igazoltuk $k \cdot m + (m-1)$ darab egészre és beszeretnénk bizonyítani $k \cdot m + (2m-1) = (k+1)m + m - 1$ darab egészre.

Az indukciós feltevés szerint léteznek $a_1, a_2, \ldots, a_{km}$ egészek, melyekre

$$a_{im+1} + a_{im+2} + \ldots + a_{(i+1)m}$$

osztható m-mel, ha $0 \leq i \leq k-1$.

Egy rövid időre töröljük ki a halmazunkból az $a_1, a_2, \ldots, a_{km}$ egészeket.

Ekkor csak $2m-1$ darab egész marad, amelyek közül kiválaszthatunk m darabot, úgy hogy az összegük osztható m-mel. Jelöljük ezeket a számokat

$$a_{km+1}, a_{km+2}, \ldots, a_{km+m}\text{-mel.}$$

(Ez az EGZT az m modulusra.) Így beláttuk (9.1)-t.

Ezután (9.1)-t használjuk $k = 2n-1$-re, és azt kapjuk, hogy

$$(2n-1)m + m - 1 = 2nm - 1$$

darab egész között létezik $(2n-1)m$ darab, nevezetesen $a_1, a_2, \ldots, a_{(2n-1)m}$, melyekre

$$b_i \overset{\text{def}}{=\!=} \frac{a_{im+1} + a_{im+2} + \ldots + a_{(i+1)m}}{m} \tag{9.2}$$

mindig egész szám, ha $0 \leq i \leq 2n-2$.

Ha az EGZT használjuk az n modulusra és a $b_0, b_1, \ldots, b_{2n-2}$ egész számokra, azt kapjuk, hogy a b_i egész számok között van n darab, melyek összege osztható n-nel.

Tekintsük most azokat az a_j-ket, melyek összege meghatározta a fenti n darab kiválasztott b_i-t (9.2)-ben. Ezekből az a_i-kből összesen nm darab van, és az összegük osztható nm-mel. Ezzel a tétel állítását beláttuk.

Hivatkozások

[1] P. Erdős, A. Ginzburg és A. Ziv, *Theorem in the additive number theory*. Bull. Res. Council Israel. 10F (1961), 41–43.

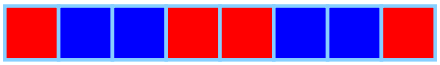
[2] Wikipedia, Erdős-Ginzburg-Ziv tétel, link.

10. Színezéses és sűrűségi tételek alkalmazásokkal

Van der Waerden [12] mindössze 24 éves volt, amikor bebizonyította nevezetes tételét (mely eredetileg Baudet egy sejtése volt), megalkotva ezáltal a kombinatorika és a számelmélet egy közös területét.

10.1 TÉTEL. (van der Waerden) *Minden pozitív egész r és k számra létezik egy N pozitív egész, hogy ha az $1, 2, \ldots, N$ számokat r darab színnel színezzük, akkor mindig lesz egyszínű (monokromatikus) k-tagú számtani sorozat. A legkisebb ilyen N-et ezentúl van der Waerden számnak nevezzük, és $W(r, k)$-val jelöljük.*

Például, ha $r = 2$, akkor két színünk van, mondjuk piros és kék. Ekkor $W(2, 3)$ nagyobb mint 8, mert 1 és 8 között színezhetőek a számok az alábbi módon, úgy hogy nincs benne monokromatikus 3-tagú számtani sorozat:



Ha minden esetet külön-külön megvizsgálunk (összesen $2^9 = 512$ darab eset), könnyen látható, hogy bárhogy színezzük két szín-

nel az $1, 2, 3, \ldots, 9$ számokat, azok mindig tartalmaznak egyszínű 3 tagú számtani sorozatot.

Azaz $W(2, 3) = 9$.

Sajnálatos módon nem ismerjük az összes van der Waerden szám pontos értékét. Az ismert értékekről egy ügyes összefoglaló található az alábbi Wikipedia oldalon: link.

Gowers [11] bizonyította a legélesebb általános felső becslést a van der Waerden számokra:

$$W(r, k) \leq 2^{2^{r^{2^{2^{k+9}}}}}.$$

Berlekamp [3] a következő ügyes alsó becslést adta két szín esetében és p prímekre:

$$W(2, p + 1) \geq p \cdot 2^p.$$

Általában, a van der Waerden számokra adott felső becslések rendkívül komplikáltak (akárcsak a később szóba kerülő Szemerédi tétel esetében), így ezek részletezésére nem térünk ki a jegyzetben.

Viszont egy nagyon ügyes alsó becslés adható, egyszerű, elemi valószínűségszámítási módszerekkel. Az alább található bizonyítás [7]-ből származik.

10.2 Tétel. $W(2, k) \geq \sqrt{\frac{k}{3}} \cdot 2^{(k-1)/2}$.

A 10.2 Tétel bizonyítása. Először azt állítjuk, hogy a k-tagú számtani sorozatok száma az $\{1, 2, 3, \ldots, N\}$ halmazban kevesebb mint $\frac{N^2}{k}$.

Ha a k tagú számtani sorozat első eleme a, akkor $a+(k-1)d \leq N$, amiből $d \leq \frac{N-a}{k-1}$.

Így az összes k-tagú számtani sorozat száma $\{1, 2, 3, \ldots, N\}$-ben

$$\sum_{a=1}^{N-1} \frac{N-a}{k-1} = \frac{N(N-1)}{2(k-1)} < \frac{N^2}{k}.$$

Legyen $N = \sqrt{\frac{k}{3}} \cdot 2^{(k-1)/2}$.

Ezután pénzfeldobással színezzük 1 és N között a számokat. Minden $1 \leq x \leq N$ szám esetén feldobunk egy pénzérmét, ha fej x-et kék színnel színezzük, ha írás x-et piros színnel színezzük.

Legyen p annak a valószínűsége, hogy az így kapott színezésben van egyszínű k-tagú számtani sorozat.

Megmutatjuk, hogy $p < 1$ és így a pénzfeldobás eredményeképpen kaphatunk olyan színezést is, amiben nincs monokromatikus k-tagú számtani sorozat

Tudjuk, hogy $\frac{N^2}{k}$ egy felső becslés a k-tagú számtani sorozatok számára.

A véletlen színezés definíciója alapján minden k-tagú számtani sorozat pontosan $\frac{1}{2^{k-1}}$ valószínűséggel lesz egyszínű, így ezen valószínűségek összege felső becslést ad arra a valószínűségre, hogy a színezésben létezik egyszínű k-tagú számtani sorozat:

$$p \leq \frac{N^2}{k} \cdot \frac{1}{2^{k-1}} = \frac{1}{3}$$

Azaz annak a valószínűsége, hogy létezik jó színezése (azaz k-tagú számtani sorozat mentes) az $1, 2, 3, \ldots, N$ számoknak $\geq 2/3$. Ezzel a bizonyítást befejeztük.

Nem is gondolnánk erre, de a van der Waerden tételnek van egy meglepő következménye: végtelen sok prím létezik.

Bár erre a tényre, Eukleidesz óta számtalan bizonyítás létezik, engem nagyon meglepett, hogy a van der Waerden tételből is következik.

A következő bizonyítás Levent Alpoge [1] cikkéből származik.

10.3 TÉTEL. *Végtelen sok prím létezik.*

A 10.3 Tétel bizonyítása. Jelölje $\nu_p(n)$ azt a legnagyobb kitevőt egy p prím, és n egész esetén, amelyre $p^{\nu_p(n)} \mid n$. Világos, hogy

$$n = \prod_p p^{\nu_p(n)}.$$

Azt is tudjuk, hogy $\mu_p(ab) = \nu_p(a) + \nu_p(b)$ és

$$\nu_p(a+b) \geq \min(\nu_p(a), \nu_p(b)), \tag{10.1}$$

ahol $\nu_p(a) \neq \nu_p(b)$ esetén egyenlőség áll fenn.

Tegyük fel, hogy véges sok prím létezik. Színezzük a pozitív egészeket aszerint, hogy mely prímek osztják őket és a kitevőknek milyen a paritása.

Vagyis, ha P egy véges halmaza prímeknek, akkor definiáljuk $f: \mathbb{Z}^+ \to (\{0,1\} \times \{0,1\})^P$-et az

$$f(n) = \left(\begin{cases} 1 & p \mid n \\ 0 & p \nmid n \end{cases}, \ \nu_p(n) \pmod 2 \right)_P, \quad \text{ha } n = \prod_p p^{\nu_p(n)}.$$

képlettel.

Ez a színezés véges sok színt használ. Így van der Waerden tétele alapján tudjuk, hogy van benne tetszőlegesen hosszú egyszínű számtani sorozat.

Vegyünk egy monokromatikus számtani sorozatot, $a, a+d, \ldots, a+dr$-t, melyre r nagyobb mint bármelyik prím négyzete (most feltettük, hogy véges sok prím létezik).

Tegyük fel, hogy p osztja a-t. Mivel a számtani sorozatban minden számot ugyanazok a prímek osztanak, ezért p osztja $a+d$-t, és így $d = (a+d) - a$-t is.

Azt állítjuk, hogy $\nu_p(a) < \nu_p(d)$.

Valóban, tegyük fel, hogy $\nu_p(a) > \nu_p(d)$. Ekkor (10.1) alapján

$$\nu_p(a+d) = \nu_p(d). \tag{10.2}$$

Világos, hogy $\nu_p(pd) = \nu_p(d) + 1$. Így ha $\nu_p(a) > \nu_p(pd) = \nu_p(d) + 1$, akkor

$$\nu_p(a+pd) = \nu_p(pd) = \nu_p(d) + 1 = \nu_p(a+d) + 1,$$

amely ellentmond $\nu_p(a+pd) \equiv \nu_p(a+d) \pmod 2$-nek (ld. a színezés definícióját).

Ha $\nu_p(a) = \nu_p(d)+1$, akkor $\nu_p(a) = \nu_p(a+d)+1$ (ld. (10.2)), amely ellentmond $\nu_p(a) \equiv \mu_p(a+d) \pmod 2$-nek.

Ha $\nu_p(a) = \nu_p(d)$, akkor

$$\nu_p(a+kd) = \nu_p(a)+1 \not\equiv \nu_p(a) \pmod 2,$$

alkalmasan választott $k < p^2$-re (itt az $A + kD \equiv p \pmod{p^2}$ kongruenciát kell megoldanunk, ahol A és D azon részei a-nak és d-nek, melyek relatív prímek p-hez).

Tehát bebizonyítottuk, hogy a-nak minden p prímosztójára $\nu_p(a) < \nu_p(d)$. Ekkor (10.1) alapján

$$\nu_p(a+d) = \nu_p(a).$$

Vagyis a színezés definíciója alapján, a-nak és $a+d$-nek ugyanazok a prímosztóik, sőt, a kitevőik is azonosak, és ez ellentmond az egyértelmű prímtényezős felbontásnak, ha $d \geq 1$.

A van der Waerden tételnek volt egy rendkívül fontos következménye a matematikában. Turán és Erdős [6] 1936-ban megfogalmazta a következő sejtést.

Minden pozitív egész számokból álló $\mathcal{A}$ halmaz, melynek pozitív a sűrűsége tartalmaz k-tagú számtani sorozatot tetszőleges k-ra.

Szemerédi Endre [10] 1975-ben igazolta a sejtést, és 2012-ben Abel díjat kapott érte.

10.4 TÉTEL. (Szemerédi) *Minden* $\varepsilon \in \mathbb{R}^+$ *és* $k \in \mathbb{N}$ *esetén létezik* $N_0 = N_0(\varepsilon, k)$ *küszöbindex, melyre ha* $N > N_0$, $A \subseteq \{1, 2, 3, \ldots, N\}$ *és* $|\mathcal{A}| > \varepsilon N$, *akkor* $\mathcal{A}$ *tartalmaz* k*-tagú számtani sorozatot.*

A Szemerédi-tételnek többféle bizonyítása létezik, beleértve a kombinatorikusokat is (amelyek a híres Szemerédi-regularitási lemmát használják), ergodikus elméleti, Fourier-analitikus, és egy a hipergráf eltávolításos lemmán alapuló.

Sőt, Szemerédi tételének kvantitatív változatai is léteznek. Ezek leginkább a $r_k(N)$ függvényt használják, amely az $\{1, 2, \ldots, N\}$ legnagyobb olyan részhalmazának a mérete, mely nem tartalmaz k-tagú számtani sorozatot.

A legjobb általános becslések:

$$CN \exp\left(-n2^{(n-1)/2}(\log N)^{1/n} + \tfrac{1}{2n}\log\log N\right) \leq r_k(N) \leq \frac{N}{(\log\log N)^{2^{-2^{k+9}}}},$$

ahol $n = \lceil \log k \rceil$.

A legjobb alsó becslést O'Bryant [8] adta, (eredménye számos az övét megelőző ötletre épült, pl. Behrend [2] tételére). A legjobb felső becslés Gowerstől [11] származik.

Hasonlóan a van der Waerden számokhoz, itt sem bizonyítunk felső becslést, mivel az túlmegy jelen jegyzet keretein. De egy alsó becslést azért adni fogunk.

De előtte tekintsük a következő Szemerédi tételt, melyet szintén Szemerédi [9] talált ki.

Fermat óta tudjuk, hogy négy négyzetszám sosem alkot számtani sorozatot.

Vagyis, ha adott egy N-hosszú számtani sorozat $a, a+d, a+2d, \ldots, a+(N-1)d$, és mi aszerint színezünk pirosra egy t számot, hogy ebben a számtani sorozatban $a+td$ négyzetszám-e, akkor a $0, 1, 2, 3, ..., N-1$ számoknak egy olyan színezését kapjuk, mely nem tartalmaz 4-hosszú számtani sorozatot.

Így minden $\varepsilon > 0$-ra tudjuk, hogy ha $N > N_0(\varepsilon)$, akkor legfeljebb εN darab piros elemet tartalmaz a $\{0, 1, 2, \ldots, N-1\}$ halmaz Szemerédi tétele alapján. Összefoglalva eredményeinket a következőt kapjuk [9]:

10.5 Tétel. (Szemerédi) *Minden $\varepsilon \in \mathbb{R}^+$-ra létezik egy $N_0 = N_0(\varepsilon)$, hogy $N > N_0$ esetén, egy N-tagú számtani sorozat legfeljebb εN négyzetszámot tartalmaz.*

Ezt az eredményt azóta folyamatosan javítgatták, pl. 1992-ben Bombieri, Granwille és Pintz [4] a következőt igazolta.

10.6 Tétel. *Legfeljebb $c_1 N^{2/3} (\log N)^{c_2}$ darab négyzetszám van egy N-tagú számtani sorozatban, ahol c_1 és c_2 abszolút és hatékonyan kiszámolható konstansok.*

Bombieri és Zannier [5] a $2/3$ kitevőt $3/5$-re javította.

A következő fejezetben egy ügyes alsó becslést adunk $r_3(n)$-re, nevezetesen bebizonyítjuk Behrend tételét [2], mely egy geometriai észrevételen alapul.

Hivatkozások

[1] L. Alpoge, *van der Waerden and the primes*, The American Mathematical Monthly 122 (8) (2015), 784-785.

[2] F. A. Behrend, *On the sets of integers which contain no three terms in arithmetic progression*, Proceedings of the National Academy of Sciences. 32 (12) (1946) 331–332.

[3] E. Berlekamp, *A construction for partitions which avoid long arithmetic progressions*, Canadian Mathematical Bulletin. 11 (3) (1968), 409–414.

[4] E. Bombieri, A. Granville, J. Pintz, *Squares in arithmetic progressions*, Duke Mathematical Journal 66 (1992), 369–385.

[5] E. Bombieri, U. Zannier, *A Note on squares in arithmetic progressions, II*, Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti Lincei. Matematica e Applicazioni 13 (2) (2002), 69-75.

[6] P. Erdős, P. Turán, *On some sequences of integers*, Journal of the London Mathematical Society. 11 (4) (1936) 261–264.

[7] W. Gasarch, B. Haeupler, *Lower Bounds on van der Waerden Numbers: Randomized- and Deterministic-Constructive*, Electronic Journal of Combinatorics Vol 18, 2011.

[8] K. O'Bryant, *Sets of integers that do not contain long arithmetic progressions*. Electronic Journal of Combinatorics. 18 (1) (2011).

[9] 3E. Szemerédi, *The number of squares in arithmetic progressions*, Stud. Sci. Math. Hungar., 9 (1975) p.417.

[10] E. Szemerédi, *On sets of integers containing no k elements in arithmetic progression*, Acta Arithmetica 27 (1975), 199–245.

[11] G. Timothy, *A new proof of Szemerédi's theorem*, Geometric and Functional Analysis. 11 (3) (2001), 465–588.

[12] B. L. van der Waerden, *Beweis einer baudetschen vermutung*, Nieuw Arch. Wisk. 15 (1927), 212–216.

[13] Kép, Cartoon Businessman Flipping A Coin, link.

[14] Kép, Van der Waerden, Wikipedia, link.

11. Behrend konstrukciója

Ebben a fejezetben megadunk egy viszonylag nagy részhalmazát $\{1, 2, 3, \ldots, N\}$-nek, mely nem tartalmaz 3-tagú számtani sorozatot.

A következő tétel Behrend [1] konstrukciója lesz, amelynek alapja egy szórakoztató geometriai konstrukció. Az ismertetés során a [4] cikk terminológiáját használjuk.

11.1 Tétel. (Behrend, 1946.) *Létezik egy pozitív konstans c, hogy minden N-re meg tudunk adni egy*

$$\mathcal{A} \subset \{1, 2, 3, \ldots, N\}$$

halmazt, melyre

$$|\mathcal{A}| \geq N \exp(-c\sqrt{\log N})$$

és $\mathcal{A}$ nem tartalmaz 3-tagú számtani sorozatot.

A 11.1 Tétel bizonyítása. Behrend konstrukciója azon az észrevételen alapul, hogy egy egyenes egy gömböt legfeljebb 2 pontban metsz.

Ha $\mathrm{x}, \mathrm{y}, \mathrm{z}$ egy 3-tagú számtani sorozat, akkor $\mathrm{y} = \frac{\mathrm{x}+\mathrm{z}}{2}$.

Először megadunk egy n dimenziós konstrukciót, egy gömbhéjat, mely gömbhéj semely két pontjának nem tartalmazza az átlagát, mivel egy egyenes maximum két pontban metsz egy gömbhéjat.

Ezután a gömbhéj egész pontjaihoz hozzárendelünk egy $\mathcal{A} \subseteq \{1, 2, 3, \ldots, N\}$ halmazt.

Az n és M pozitív egészek értékét később rögzítjük.

Tekintsük az $\mathbf{x} = (x_1, x_2, ..., x_n) \in [1, M]^n$ halmazt. A fenti M^n darab pont mindegyikéhez hozzárendeljük az origótól vett távolság négyzetét, azaz az $r^2 = x_1^2 + ... + x_n^2$ egész számot.

Ezek a hozzárendelt értékek az $[n, nM^2]$ intervallumból valóak. Vagyis létezik egy r sugár, amelyre $S_n(r)$ gömbhéj legalább

$$|S_n(r)| \geq \frac{M^n}{nM^2 - n + 1} \geq \frac{M^n}{nM^2} \geq \frac{M^{n-2}}{n}$$

darab egész pontot tartalmaz.

Ezek után az $S_n(r)$ egész pontjaihoz egy egész számot rendelünk a következő $P : \mathbb{Z}^n \to \mathbb{Z}$ függvénnyel:

$$P(\mathbf{x}) \stackrel{\text{def}}{=} \frac{1}{2M} \sum_{i=1}^{n} x_i (2M)^i.$$

A P függvény alap tulajdonságai a következők:

1. P egész értékű.
2. $1 \leq P(\mathbf{x}) \leq (2M)^n$ minden $\mathbf{x} \in [1, M]^n$-re.
3. P lineáris.
4. P injektív $[1, M]^n$-en.

5. $P(z) - P(y) = P(y) - P(x) \Rightarrow z - y = y - x$ minden $x, y, z \in [1, M]^n$ esetén.

Az 1. tulajdonság nyilvánvaló, hiszen a szummában minden tag osztható $2M$-mel.

A 2. tulajdonság is igaz, hiszen $P(x)$ pozitív és a függvény a maximumát akkor éri el, ha minden x_i maximális, azaz pont M. Ekkor

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

A 3. tulajdonság szintén nyilvánvaló, legyen ugyanis $x, y \in \mathbb{Z}^n$ és $a, b \in \mathbb{Z}$. Ekkor P definíciójából könnyen látható, hogy

$$P(ax + by) = aP(x) + bP(y).$$

A 4. és 5. tulajdonságok igazolásához a következő lemmára van szükségünk:

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

A 11.2 Lemma bizonyítása. Ha $x = 0$, akkor $P(x) = 0$.

Megfordítva, tegyük fel, hogy létezik egy $x \neq 0$, amelyre $P(x) = 0$. Ekkor vegyük az $x = (x_1, x_2, \ldots, x_n)$ vektor koordinátái közül a legkisebb indexűt, amely nem 0, legyen ez x_j. Ekkor

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

Rendezve, azt kapjuk, hogy

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

ahol a jobboldal osztható $2M$-mel, míg a baloldalon $1 \leq x_j < 2M$, ami ellentmondás. Ezzel a lemma bizonyítását befejeztük.

A lemmát használva, bebizonyítjuk a 4. és 5. tulajdonságot.

A 4. tulajdonsághoz tegyük fel, hogy $P(\mathbf{x}) = P(\mathbf{y})$ fennáll egy $\mathbf{x}, \mathbf{y} \in [1, M]^n$ párra.

A linearitás alapján $0 = P(\mathbf{x}) - P(\mathbf{y}) = P(\mathbf{x} - \mathbf{y})$, de $\mathbf{x} - \mathbf{y} \in (-M, M)^n \subset (-2M, 2M)^n$, így a lemma alapján $\mathbf{x} - \mathbf{y} = \mathbf{0}$, azaz $\mathbf{x} = \mathbf{y}$. Eredményképpen megkaptuk, hogy P injektív.

Utoljára már csak az 5. tulajdonságot kell igazolnunk.

Tegyük fel, hogy $P(\mathbf{z}) - P(\mathbf{y}) = P(\mathbf{y}) - P(\mathbf{x})$ eleget tesz egy $\mathbf{x}, \mathbf{y}, \mathbf{z} \in [1, M]^n$ számhármasra. Ekkor $P(\mathbf{z}) - 2P(\mathbf{y}) + P(\mathbf{x}) = P(\mathbf{z} - 2\mathbf{y} + \mathbf{x}) = \mathbf{0}$. Azonban most $\mathbf{z} - 2\mathbf{y} + \mathbf{x} \in (-2M, 2M)^n$, így alkalmazhatjuk megint a lemmát, mely szerint $\mathbf{z} - 2\mathbf{y} + \mathbf{x} = \mathbf{0}$, azaz $\mathbf{z} - \mathbf{y} = \mathbf{y} - \mathbf{x}$. Ezzel a lemma állítását igazoltuk.

Ezután rögzítjük n és M értékét. Legyen $n = \lceil \sqrt{\log N} \rceil$, $M = [N^{1/n}/2]$.

Ekkor $\mathcal{A} \subset [1, (2M)^n] \subset [1, N]$.

A P függvény 5. tulajdonsága miatt tudjuk, hogy $\mathcal{A}$ nem tartalmaz 3-tagú számtani sorozatot.

Most már csak $\mathcal{A}$ elemszámát kell becsülnünk.

$$|\mathcal{A}| \geq \frac{M^{n-2}}{n} = \frac{[N^{1/n}/2]^{n-2}}{n} \geq \frac{\left(N^{1/n}/e\right)^{n-2}}{n} = e^{2-n}N^{1-2/n} \cdot \frac{1}{n}$$
$$= Ne^{2-\lceil\sqrt{\log N}\rceil} \cdot N^{-2/\lceil\sqrt{\log N}\rceil} \cdot \frac{1}{\lceil\sqrt{\log N}\rceil}$$
$$\geq Ne^{2-\left(\sqrt{\log N}+1\right)} \cdot N^{-2/\sqrt{\log N}} \cdot \frac{1}{\sqrt{\log N}+1}$$
$$\geq Ne^{1-\left(\sqrt{\log N}\right)} \cdot e^{-2\log N/\sqrt{\log N}} \cdot e^{-\sqrt{\log N}}$$
$$> Ne^{-4\sqrt{\log N}}.$$

Így az előző fejezetben definiált $r_3(N)$ értékre azt kapjuk, hogy,

$$r_3(N) > Ne^{-4\sqrt{\log N}}.$$

A másik oldalról, Roth [6] 1953-ban azt bizonyította, hogy ha $A \subseteq \{1, 2, 3, \ldots, N\}$ nem tartalmaz 3-tagú számtani sorozatot, akkor $|\mathcal{A}| \ll \frac{N}{\log\log N}$. Azóta ezt az eredményt folyamatosan javítgatták. A legjobb mostani eredmény Bloom és Sisasktól [2] származik, akik bebizonyították, hogy létezik olyan $c > 0$ konstans, amelyre $|\mathcal{A}| \ll \frac{N}{(\log N)^{1+c}}$.

A legjobb alsó becslés is Bloom és Sisasktól [3] származik (akik valójában Kelley és Meka [5] eredményét egyszerűsítették). Eszerint létezik olyan 3-tagú számtani sorozat mentes halmaz, amelynek elemszáma $\geq \exp(-c(\log N)^{1/11})N$.

Hivatkozások

[1] F. A. Behrend, *On the sets of integers which contain no three in arithmetic progression*, Proceedings of the National Academy of Sciences 23 (1946), 331-332.

[2] T. F. Bloom, O. Sisask, *Breaking the logarithmic barrier in Roth's theorem on arithmetic progressions*, link.

[3] T. F. Bloom, O. Sisask, *The Kelley–Meka bounds for sets free of three-term arithmetic progressions*, link.

[4] B. Gillespie, *Behrend's Construction*, link.

[5] Z. Kelley, R. Meka, *Strong Bounds for 3-Progressions*, link.

[6] K. Roth, *On certain sets of integers*. Journal of the London Mathematical Society. 28 (1) (1953), 104–109.

[7] Kép, Basketball Clip Art, link.

12. Összegszorzatok prímosztóinak száma

A következő eredményt Erdős és Turán alkotta, még egyetemista korukban.

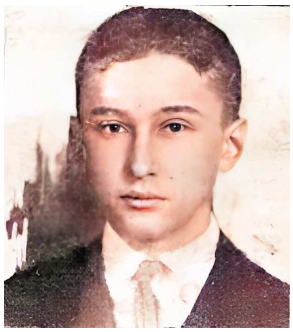
Jelölje $\omega(n)$ az n különböző prímosztóinak a számát.

12.1 Tétel. (Erdős–Turán, [3]) *Legyen $\mathcal{A} \subseteq \mathbb{N}^+$ pozitív egészek halmaza, melyre $|A| \geq 2^k + 1$. Ekkor*

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

12.2 Megjegyzés. *A tételből adódóan*

$$\omega\Big(\prod_{a,a' \in A} (a + a')\Big) \geq \log_2 |A|.$$



A bizonyítást Erdős-Surányi könyve [2] alapján ismertetjük.

A 12.1 Tétel bizonyítása. A bizonyítás kulcsa, hogy az $a+a'$ összegeknek sok prímosztóját találjunk, azon összefüggés alapján, hogy bizonyos esetekben igaz az, hogy

$$p^k \mid a + a' \implies p^k \mid a \text{ és } p^k \mid a'.$$

E célból először a következő lemmát igazoljuk:

12.3 Lemma. *Ha p páratlan prím, akkor $2\ell+1$ különböző páratlan szám között mindig található $\ell+1$ darab, hogy a belőlük képezett $a+a'$ összegekre fennáll*

$$p^k \mid a+a' \implies p^k \mid a \text{ és } p^k \mid a'.$$

A 12.3 Lemma bizonyítása. Legyen ez a $2\ell+1$ egész szám

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

Írjuk mindegyiket

$$n_i = p^{\alpha_i} q_i \quad \text{alakban, ahol} \quad p \nmid q_i.$$

Ekkor kettőnek az összegére, mondjuk n_i és n_j-re, (ahol szimmetrikus okokból feltehetjük, hogy $\alpha_i \le \alpha_j$), tudjuk, hogy

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

Ha $\alpha_i \neq \alpha_j$, akkor

$$p^{\alpha_i} \mid n_i + n_j \quad \text{és} \quad p^{\alpha_i} \mid n_i,\ p^{\alpha_i} \mid n_j,\ p^{\alpha_i+1} \nmid n_i + n_j.$$

Másrészt, ha $\alpha_i = \alpha_j$, akkor azt szeretnénk biztosítani, hogy $q_i + q_j$ nem osztható p-vel.

Ezt úgy tudjuk pl. garantálni, ha mind $q_i \pmod p$ és $q_j \pmod p$ kisebb mint $p/2$, vagy mindkettő nagyobb mint $p/2$ (mivel p páratlan, egyik sem lehet $p/2$).

Ugyanis a fenti esetekben az összeg szigorúan 0 és p, illetőleg szigorúan p és $2p$ közé esik.

A skatulyaelv szerint a

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

vagy tartalmaz $\ell+1$ darabot, amelyeknek modulo p maradéka szigorúan 0 és $p/2$ közé esik, vagy tartalmaz $\ell+1$ darabot, amelyeknek modulo p maradéka szigorúan $p/2$ és p közé esik. Ezzel a lemma állítását beláttuk.

A következőkben az Erdős-Turán tétel bizonyításával folytatjuk.

Legyen

$$|A| \geq 2^k + 1 \quad \text{ahol} \quad k \geq 1.$$

Mivel $|A| \geq 3$ az $\mathcal{A}$ elemei között létezik kettő, amelyek paritása azonos. Azaz $\prod_{a,a' \in A} (a + a')$ páros.

Jelöljük az $a + a'$ összegek páratlan prímosztóit

$$p_1, p_2, \ldots, p_i\text{-vel.}$$

Indirekten bebizonyítjuk, hogy $i \geq k$.

Tegyük fel, hogy $i < k$.

A 12.3 Lemma szerint a , $2^k + 1$ szám közül kiválaszthatunk $2^{k-1} + 1$ darabot, hogy ha

$$p_1^{\alpha_1} \mid a + a', \quad \text{akkor} \quad p_1^{\alpha_1} \mid a \quad \text{és} \quad p_1^{\alpha_1} \mid a'.$$

Ebből a $2^{k-1} + 1$ egész szám közül kiválasztható $2^{k-2} + 1$ darab, amelyre ha

$$p_2^{\alpha_2} \mid a + a', \quad \text{akkor} \quad p_2^{\alpha_2} \mid a \quad \text{és} \quad p_2^{\alpha_2} \mid a'.$$

Az eljárást folytatva kapunk $2^{k-i} + 1 \geq 3$ darab egész számot, hogy a fenti összefüggés a $p_1, p_2, \ldots, p_i$ mindegyikére igaz.

Legyen a_1, a_2, a_3 három darab rögzített szám a $2^{k-i}+1 \geq 3$ darab közül, melyeket a fenti eljárás végén maradt.

Ekkor (mivel $p_1.p_2, \ldots, p_i$ az összes páratlan prímosztója az összegeknek) azt kapjuk, hogy:

$$\begin{aligned} a_1 + a_2 &= 2^{u_0} p_1^{u_1} p_2^{u_2} \ldots p_i^{u_i}, \\ a_1 + a_3 &= 2^{v_0} p_1^{v_1} p_2^{v_2} \ldots p_i^{v_i}, \\ a_2 + a_3 &= 2^{w_0} p_1^{w_1} p_2^{w_2} \ldots p_i^{w_i}. \end{aligned}$$

Ekkor $p_1^{u_1} p_2^{u_2} \ldots p_i^{u_i} \mid a_1$ és a_2.

Így $2^{u_0} \mid a_1$ nem lehetséges, hiszen akkor az $a_1 + a_2$ túl nagy. Hasonlóan: $2^{u_0} \nmid a_2$.

Azt írjuk, hogy $2^\gamma \parallel x$ ha $2^\gamma \mid x$ de $2^{\gamma+1} \nmid x$. Amennyiben a 2 kitevője a_1-ben és a_2-ben különböző, akkor

$$\begin{gathered} 2^\gamma \parallel a_1 \quad 2^\delta \parallel a_2 \quad \gamma < \delta \\ 2^\gamma \parallel a_1 + a_2 \Longrightarrow \gamma = u_0 \Longrightarrow 2^{u_0} \parallel a_1, \end{gathered}$$

amely ellentmond $2^{u_0} \nmid a_1$-nek.

A $\gamma > \delta$ hasonlóan kezelhető. Így $\gamma = \delta$.

Azaz ha $2^\gamma \parallel a_1$, akkor $2^\gamma \parallel a_2$, $2^\gamma \parallel a_3$.

Legyen $a_i = 2^\gamma b_i$ ahol b_i páratlan. Ekkor

$$\begin{aligned} b_1 + b_2 &= 2^{r_1} p_1^{u_1} \ldots p_i^{u_i}, \\ b_1 + b_3 &= 2^{r_2} p_1^{v_1} \ldots p_i^{v_i}, \end{aligned}$$

$$b_2 + b_3 = 2^{r_3} p_1^{w_1} \dots p_i^{w_i}.$$

Mivel $p^\alpha \mid a_i + a_j$ esetén $p^\alpha \mid a_i$ és $p^\alpha \mid a_j$ ez szintén igaz b_i és b_j-re. Vagyis

$$p_1^{u_1} \dots p_i^{u_i} \mid b_1, b_2, \;\; b_1 \neq b_2.$$

Tehát $b_1 + b_2 \geq 3p_1^{u_1} \dots p_i^{u_i} \implies r_1 \geq 2$. Hasonlóan $r_2, r_3 \geq 2$, vagyis $b_1 + b_2 + b_3$ páros, amely ellentmond annak, hogy minden b_i páratlan.

Két különböző halmaz esetén Győry, Stewart és Tijdeman [4] a következőt igazolta:

12.4 Tétel. *Legyen $\mathcal{A}, \mathcal{B} \subseteq \mathbb{N}^+$ pozitív egészekből álló halmazok. Tegyük fel, hogy $|\mathcal{A}| > |\mathcal{B}|$. Ekkor*

$$\omega\left(\prod_{a \in \mathcal{A}, b \in \mathcal{B}} (a+b) \right) \geq c_1 \log |\mathcal{A}|.$$

Erdős, Stewart és Tijdeman [1] megmutatta, hogy a $c_1 \log |\mathcal{A}|$ alsó becslés nem javítható $\left(\frac{1}{8} + \varepsilon\right) (\log |\mathcal{A}|)^2 \log\log |\mathcal{A}|$-ra.

Győry, Sárközy és Tijdeman [5] hasonló alsó becslést igazolt $ab + 1$ alakú számok szorzata esetében.

Hivatkozások

[1] P. Erdős, C. L. Stewart, R. Tijdeman, *Some diophantine equations with many solutions*, Compositio Math. 66 (1988), 37-56.

[2] P. Erdős, J. Surányi, *Válogatott Fejezetek a Számelméletből*, Polygon 2004, link.

[3] P. Erdős, P. Turán, *On a Problem in the Elementary Theory of Numbers*, American Math. Monthly 40 (1934), 608-611.

[4] K. Győry, C. L. Stewart, R. Tijdeman, *On prime factors of sums of integers I*, Compositio Math. 59 (1) (1986), 81-88.

[5] K. Győry, C. L. Stewart, R. Tijdeman, *On the number of prime factors of integers of the form* $ab + 1$, Acta Arith. 74 (4) (1996), 365-385.

[6] Kép, Pál Erdős, KöMaL arcképcsarnok, link.

[7] Kép, Pál Turán, KöMaL arcképcsarnok, link.

13. A négyzetszámok additív bázist alkotnak

Az additív számelméletben központi kérdés, hogy vajon egy adott halmaz véges rendű additív bázis-e?

Más szóval, mely $\mathcal{B}$ halmazokra létezik k pozitív egész, hogy minden természetes szám felírható k darab $\mathcal{B}$-beli elem összegeként?

Lagrange négy-négyzetszám tétele valószínűleg az első, az ilyen jellegű tételek közül. A tétel a következőt állítja:

13.1 TÉTEL. (Lagrange négy-négyzetszám tétel) *Minden természetes szám felírható 4 darab négyzetszám összegeként.*

Először csak azt vizsgáljuk meg mely számok írhatóak fel két négyzetszám összegeként.

A probléma eredete Albert Girard-ig nyúlik vissza, aki észrevette, hogy minden $4k + 1$ alakú szám felírható két négyzetszám összegeként. Eredményét 1625-ben publikálta [1].

A probléma egy variánsát Fermat is megírta levélben Mersennenek. Továbbá, Fermat az is megadta, hogy egy p^α prímhatvány hányféleképpen írható fel két négyzetszám összegeként.

Természetes számokra, a két-négyzetszám tétel kapcsolódik a prímtényezős felbontáshoz. Nevezetesen:

13.2 Tétel. *Egy $n \geq 2$ természetes szám pontosan akkor írható fel két négyzetszám összegeként, ha prímtényezős felbontása nem tartalmaz olyan p^k prímhatvány szorzót, ahol $p \equiv 3 \pmod 4$ és k páratlan.*

Ha $n = x^2$ négyzetszám, az állítás triviális, ugyanis $n = x^2 = 0^2 + x^2$. (Megjegyezendő, hogy néhány négyzetszámnak van nem triviális felbontása is, pl. $25 = 4^2 + 3^2$ vagy $100 = 8^2 + 6^2$. Ezeket a hármasok pitagoraszi számhármasok néven ismertek.)

Példák

A 2450 prímtényezős felbontása $2450 = 2 \cdot 5^2 \cdot 7^2$. A felbontásban szereplő prímek között (melyek 2, 5 és 7), csak a 7 kongruens 3-mal modulo 4. A 7 kitevője a prímtényezős felbontásban 2, amely páros. Így a tétel azt állítja 2450 felírható két négyzetszám összegeként. Valóban: $2450 = 7^2 + 49^2$.

A 3430 prímtényezős felbontása $2 \cdot 5 \cdot 7^3$. Ezúttal a 7 kitevője a 3, ami páratlan szám. Így 3430 nem írható fel két négyzetszám összegeként.

Ahhoz, hogy a tételt belássuk, először a következőt igazoljuk:

13.3 Lemma. *Ha a és b felírható két négyzetszám összegeként, akkor a szorzatuk ab is felírható.*

A 13.3 Lemma bizonyítása. Legyen $a = x^2 + y^2$ és $b = u^2 + v^2$. Ekkor

$$ab = (x^2 + y^2)(u^2 + v^2) = (xu - yv)^2 + (xv + yu)^2.$$

Ahhoz, hogy a lemmát alkalmazni tudjuk, először azt kell tudnunk eldönteni, hogy mely p prímek írhatóak fel két négyzetszám összegeként.

A fenti tételt Girard tételének is szokták hívni, de úgyis ismert, hogy Fermat két-négyzetszám tétele.

13.4 TÉTEL. *Legyen p prímszám. Ekkor az*

$$x^2 + y^2 = p$$

egyenlet akkor és csak akkor oldható meg az egészek között, ha $p = 2$ vagy p egy $4k + 1$ alakú prím.

Először bebizonyítjuk a 13.4 Tételt, majd rátérünk a 13.2 Tétel bizonyítására, melyet a 13.4 Tételből vezetünk le.

A 13.4 Tétel bizonyítása. Először csak annyit igazolunk, hogy ha p egy $4k + 3$ alakú prímszám, akkor p nem írható fel két négyzetszám összegeként. Tegyük fel ugyanis, hogy nem igaz az állítás, és p mégiscsak felírható két négyzetszám összegeként. Vagyis létezik x és y egész szám, melyre

$$x^2 + y^2 = p.$$

Ekkor

$$x^2 + y^2 \equiv p \pmod 4.$$

De mivel p egy $4k+3$ alakú prím, ezért

$$x^2 + y^2 \equiv 3 \pmod 4.$$

Egy négyzetszám négyes maradéka csak 0 vagy 1 lehet. Azaz $x^2 + y^2$ négyes maradéka $0, 1$ vagy 2 lehet, de sohasem 3. Ezzel ellentmondásra jutottunk, és az állítást igazoltuk.

Ezután bebizonyítjuk, hogy a 2 és a $4k+1$ alakú prímek valóban felírhatóak két négyzetszám összegeként. Az állítás $p = 2$ esetén triviális:

$$2 = 1^2 + 1^2.$$

A következőkben p legyen egy $4k+1$ alakú prím. Ekkor -1 kvadratikus maradék modulo p. Azaz az

$$x^2 \equiv -1 \pmod p \tag{13.1}$$

kongruencia megoldható. Jelöljön s a (13.1)-beli kongruencia egy megoldását. Ekkor

$$s^2 \equiv -1 \pmod p$$
$$p \mid s^2 + 1$$

Tekintsük az összes $a + bs$ alakú számot, ahol $a, b \in \mathbb{N}$ és

$$0 \leq a < \sqrt{p},\ 0 \leq b < \sqrt{p}.$$

Az ilyen számok száma $\left([\sqrt{p} + 1]\right)^2 > p$, vagyis a skatulyaelv szerint létezik közöttük kettő, amelyek kongruensek modulo p:

$$a_1 + b_1 s \equiv a_2 + b_2 s \pmod p$$

Legyen $a = a_1 - a_2$ és $b = b_1 - b_2$. Ekkor:

$$a + bs \equiv 0 \pmod p$$

$$a \equiv -bs \pmod{p}$$
$$a^2 \equiv b^2 s^2 \pmod{p}$$
$$a^2 \equiv -b^2 \pmod{p}$$
$$p \mid a^2 + b^2.$$

Mivel $0 \leq a_1, a_2 < \sqrt{p}$ és $0 \leq b_1, b_2 < \sqrt{p}$ tudjuk, hogy $-\sqrt{p} < a < \sqrt{p}$ és $-\sqrt{p} < b < \sqrt{p}$. Vagyis

$$0 < a^2 + b^2 < 2p.$$

Mivel $p \mid a^2 + b^2$, ez csak úgy lehet, ha $a^2 + b^2 = p$.

Ezután bebizonyítjuk a 13.2 Tételt.

A 13.2 Tétel bizonyítása. Először is megjegyezzük, hogy a 13.1 Tétel ekvivalens a következő állítással:

Ha n prímtényezős felbontása

$$n = 2^{\alpha} p_1^{\alpha_1} \cdots p_r^{\alpha_r} q_1^{\beta_1} \cdots q_s^{\beta_s} \tag{13.2}$$

alakú, ahol a p_i prímek a $4k+1$ alakú prímek és q_i prímek a $4k+3$ alakú prímek, akkor n akkor és csak akkor írható fel két négyzetszám összegeként, ha minden β_i páros.

Először is megjegyezzük, hogy azok az n-ek, amelyek (13.2) felírásában a β_i-k párosak valóban előállnak két négyzetszám összegeként. Ugyanis a 13.4 Tétel alapján a 2 és a p_i prímek előállnak két négyzetszám összegeként. Az is világos, hogy $q_i^{\beta_i}$ is előáll két négyzetszám összegeként, ha β_i páros, hiszen

$$q_i^{\beta_i} = 0^2 + \left(q_i^{\beta_i/2}\right)^2.$$

A 13.3 Lemma ismételt alkalmazásával megkapjuk az állítást.

Következőleg azt bizonyítjuk, hogy ha

$$n = q^\beta m \tag{13.3}$$

alakú, ahol $q \nmid m$, q egy $4k+3$ alakú prím és β páratlan, akkor n nem írható fel két négyzetszám összegeként. Ebből a 13.4 Tétel állítása már következik.

Indirekten okoskodunk. Tegyük fel, hogy az állítás nem igaz, azaz n (13.3) alakú és n mégis két négyzetszám összege. Ezen n-ek közül vegyünk egy olyat, amire β minimális. (Itt β páratlan, tehát $\beta \geq 1$.) Ekkor

$$\begin{aligned} x^2 + y^2 &= q^\beta m \\ x^2 + y^2 &\equiv 0 \pmod{q} \\ x^2 &\equiv -y^2 \pmod{q}. \end{aligned} \tag{13.4}$$

Ha $q \nmid x$ és $q \nmid y$, akkor a $(q-1)/2$-dik hatványát véve (13.4)-nek, kapjuk, hogy

$$x^{q-1} \equiv (-1)^{(q-1)/2} y^{q-1} \pmod{q}.$$

Mivel q egy $4k+3$ alakú prím, ezért $(q-1)/2$ páratlan, tehát

$$x^{q-1} \equiv -y^{q-1} \pmod{q}.$$

A kis Fermat-tétel szerint $x^{q-1} \equiv 1 \pmod{q}$ és $y^{q-1} \equiv 1 \pmod{q}$, így

$$1 \equiv -1 \pmod{q},$$

ami ellentmondás. Tehát $q \nmid x$ és $q \nmid y$ nem lehetséges. Vagyis $q \mid x$ vagy $\mid y$. Ekkor (13.4) alapján azonban egyszerre áll fenn a két oszthatóság, tehát

$$q \mid x \text{ és } q \mid y.$$

Vagyis

$$x = qx_0 \text{ és } y = qy_0,$$

ahol x_0 és y_0 egész számok. A fenti jelöléseket használva

$$\begin{aligned} x^2 + y^2 &= q^\beta m = n \\ (qx_0)^2 + (qy_0)^2 &= q^\beta m \\ x_0^2 + y_0^2 &= q^{\beta-2} m. \end{aligned}$$

Ez azonban ellentmond n választásának, hiszen úgy választottuk, hogy β minimális, és most kaptunk egy az eredeti β-nál kisebb β-val való példát. Ezzel igazoltuk a 13.4 Tételt.

Most már rátérhetünk Lagrange négy négyzetszám tételének bizonyítására. Ez a tétel azt állítja, hogy a négyzetszámok additív bázist alkotnak.

Illusztrációképpen írjuk fel a 3, 31 és 310 számokat négy négyzetszám összegeként:

$$3 = 1^2 + 1^2 + 1^2 + 0^2$$

$$31 = 5^2 + 2^2 + 1^2 + 1^2$$

$$310 = 17^2 + 4^2 + 2^2 + 1^2.$$

Diofantosz könyvében is szerepeltek már példák a fenti tételre, amelyek világosan mutatják, hogy már Diofantosz is ismerte az állítást. Azonban azt csak Lagrange igazolta 1770-ben.

Később Carl Gustav Jakob Jacobi talált egy egyszerű formulát a lehetséges reprezentációk számáról 1834-ben.

A 13.1 Tétel bizonyítása. Először is megjegyezzük, hogy a tételt elegendő páratlan prímekre bizonyítani. Mivel a tétel azonnal következik az Euler négy négyzetszám formulából (az, hogy az 1 és a 2 előáll négy négyzetszám összegeként triviális).

13.5 LEMMA. (Euler négy négyzetszám formula) *Ha a és b felírható négy négyzetszám összegeként, akkor a szorzatuk ab is felírható.*

Az azonosság azonnal következik az alábbiból:

$$\begin{aligned}(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2) = \\ (x_1y_1+x_2y_2+x_3y_3+x_4y_4)^2 \\ +(x_1y_2-x_2y_1+x_3y_4-x_4y_3)^2 \\ +(x_1y_3-x_2y_4-x_3y_1+x_4y_2)^2 \\ +(x_1y_4+x_2y_3-x_3y_2-x_4y_1)^2. \quad (13.5)\end{aligned}$$

De hogyan lehet ezt kitalálni? Tekintsük az

$$\begin{aligned}\alpha &= x_1+x_2i+x_3j+x_4k \\ \beta &= y_1-y_2i-y_3j-y_4k\end{aligned}$$

kvaterniókat. A konjugáltjukra

$$\begin{aligned}\overline{\alpha} &= x_1-x_2i-x_3j-x_4k \\ \overline{\beta} &= y_1+y_2i+y_3j+y_4k\end{aligned}$$

Egy α kvaternió normáját a $N(\alpha)=\alpha\cdot\overline{\alpha}$ képlettel definiáljuk. Ekkor

$$\begin{aligned}N(\alpha) &= x_1^2+x_2^2+x_3^2+x_4^2 \\ N(\beta) &= y_1^2+y_2^2+y_3^2+y_4^2. \quad (13.6)\end{aligned}$$

Legyen $\gamma=\alpha\beta$. Ekkor

$$\gamma = (x_1y_1+x_2y_2+x_3y_3+x_4y_4)$$

$$+ (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)i$$
$$+ (x_1y_3 - x_2y_4 - x_3y_1 + x_4y_2)j$$
$$+ (x_1y_4 + x_2y_3 - x_3y_2 - x_4y_1)k.$$

Így

$$\begin{aligned} N(\gamma) = &(x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 \\ &+ (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 \\ &+ (x_1y_3 - x_2y_4 - x_3y_1 + x_4y_2)^2 \\ &+ (x_1y_4 + x_2y_3 - x_3y_2 - x_4y_1)^2. \end{aligned}$$

Másrészt

$$\begin{aligned} N(\gamma) &= N(\alpha\beta) = \alpha\beta\overline{\alpha\beta} \\ &= \alpha\beta\overline{\beta}\overline{\alpha} = \alpha N(\beta)\overline{\alpha} = \alpha\overline{\alpha}N(\beta) \\ &= N(\alpha)N(\beta). \end{aligned}$$

A fenti összefüggést és (13.6)-t használva megkapjuk (13.5)-t, ami a bizonyítandó állítás volt.

Ezután bebizonyítjuk Lagrange tételét. Mint már említettük elég a tételt p páratlan prímekre igazolni.

Először azt igazoljuk, hogy p-nek van olyan np többszöröse, amely előáll négy négyzetszám összegeként és $1 \leq n < p$.

Tudjuk, hogy az a^2 modulo p maradékosztályok mind különbözőek, amint a a $[0, (p-1)/2]$ intervallumon fut, mivel ha

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

akkor

$$p \mid x^2 - y^2$$

$$p \mid (x-y)(x+y)$$
$$p \mid x-y \quad \text{vagy} \quad p \mid x+y.$$

Mivel most $1 \leq x, y \leq p-1$ így az utóbbi ekvivalens a következővel

$$x = y \quad \text{vagy} \quad x = p-y.$$

Hasonlóan, amint b a $[0,(p-1)/2]$ intervallumon fut, a $-b^2-1$ számok különböző maradékot adnak modulo p. A skatulyaelv szerint létezik a és b egész számok a fenti intervallumon, melyekre a^2 és $-b^2-1$ kongruensek modulo p, azaz

$$a^2 \equiv -b^2 - 1 \pmod{p}$$
$$a^2 + b^2 + 1 \equiv 0 \pmod{p}$$
$$a^2 + b^2 + 1^2 + 0^2 = np \qquad \text{egy adott egész } n\text{-re.}$$

Mivel $0 \leq a, b \leq (p-1)/2$ azt kapjuk, hogy

$$np \leq 2\left(\frac{p-1}{2}\right)^2 + 1 < p^2,$$

azaz $n < p$. Ez igazolja állításunkat.

Legyen most m a legkisebb pozitív egész, amelyre mp négy négyzetszám összege, azaz $mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$. (Épp az előbb bizonyítottuk be, hogy ekkor $m < p$.)

Indirekten bebizonyítjuk, hogy $m = 1$. Feltesszük ugyanis, hogy $m > 1$, és ekkor bebizonyítjuk egy olyan r pozitív egész létezését, amelyre rp négy négyzetszám összege, de $r < m$. Ez ellentmond r minimális voltának. (A fenti bizonyítás Fermat végtelen leszállás módszerével történik.)

Először bebizonyítjuk, hogy m páratlan. Tegyük fel, hogy m is páros. Ekkor

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

$$\frac{m}{2}p = \frac{1}{2}\left(x_1^2 + x_2^2 + x_3^2 + x_4^2\right)$$
$$\frac{m}{2}p = \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2,$$

azaz állításunk fennáll $r = m/2$-lel. Következőleg feltesszük m páratlan.

Mindegyik x_i-re tekintsük azt az y_i-t, amely kongruens x_i-vel modulo m, valamint $-(m-1)/2$ és $(m-1)/2$ közé esik. Ekkor

$$0 \equiv mp = x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv y_1^2 + y_2^2 + y_3^2 + y_4^2 \pmod{m}.$$

Így $y_1^2 + y_2^2 + y_3^2 + y_4^2 = mr$, valamilyen adott nemnegatív egész r-re.

Először azt látjuk be, hogy r pozitív és kisebb mint m. Valóban, ha $r = 0$, akkor $y_1^2+y_2^2+y_3^2+y_4^2 = 0$, így $y_1 = y_2 = y_2 = y_4 = 0$. Azaz $m \mid x_1, x_2, x_2, x_4$. De ekkor $m^2 \mid x_1^2 + x_2^2 + x_3^2 + x_4^2 = mp$. Tehát $m \mid p$ amiből az adódik, hogy $m = 1$ ugyanis $0 < m < p$. De most azt is feltettük, hogy $m > 1$, amivel ellentmondásra jutottunk. Másrészt

$$mr = y_1^2 + y_2^2 + y_3^2 + y_4^2 \leq 4\left(\frac{m-1}{2}\right)^2 < m^2,$$

így $r < m$.

Végül, Euler négy négyzetszám azonossága alapján $mpmr = z_1^2 + z_2^2 + z_3^2 + z_4^2$. De mivel mindegyik x_i kongruens y_i-vel modulo m, azt kapjuk, hogy mindegyik z_i osztható m-mel. Valóban:

$$\begin{aligned} z_1 &= x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \\ &\equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 = mp \equiv 0 \pmod{m}, \end{aligned}$$

$$
\begin{aligned}
z_2 &= x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3 \\
&\equiv x_1x_2 - x_2x_1 + x_3x_4 - x_4x_3 = 0 \pmod{m}, \\
z_3 &= x_1y_3 - x_2y_4 - x_3y_1 + x_4y_2 \\
&\equiv x_1x_3 - x_2x_4 - x_3x_1 + x_4x_2 = 0 \pmod{m}, \\
z_4 &= x_1y_4 + x_2y_3 - x_3y_2 - x_4y_1 \\
&\equiv x_1x_4 + x_2x_3 - x_3x_2 - x_4x_1 = 0 \pmod{m}.
\end{aligned}
$$

Azaz azt kaptuk, hogy $w_i = z_i/m$-ekre $w_1^2+w_2^2+w_3^2+w_4^2 = rp$, ahol $r < m$, de ez ellentmond m minimális voltának.

Végül, néhány szó Legendre három-négyzetszám tételéről.

13.6 Tétel. (Legendre három négyzetszám tétel) *Egy adott n természetes szám, akkor és csak akkor írható fel három négyzetszám összegeként, azaz*

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

ha n nem $n = 4^k(8m+7)$ alakú, ahol k és m természetes számok.

Legendre eredeti bizonyítása hiányos volt.

Gauss később általánosította a tételt, pontosan megadva a lehetséges reprezentációk számát is.

Az akkor és csak akkor típusú állításunk, egyik része, nevezetesen, ha n három négyzetszám összege, akkor nem $n = 4^k(8m+7)$ alakú majdnem triviális.

Először csak annyit igazolunk, hogy ha n egy $8m+7$ alakú egész szám, akkor n nem írható fel három négyzetszám összegeként.

Valóban, minden négyzetszám kongruens $0, 1$ vagy 4 modulo 8, így három négyzetszám összege kongruens lehet a $0+0+0$, $0+0+1$, $0+1+1$, $1+1+1$, $4+0+0$, $4+0+1$, $4+1+1$, $4+4+0$, $4+4+1$ vagy $4+4+4$ összegek valamelyikével modulo 8. De ezen összegek között a 7 nem szerepel, azaz három négyzetszám összege nem lehet $8m+7$ alakú.

Ezután tegyük fel, hogy n egy

$$n = 4^k(8m+7) \tag{13.7}$$

alakú szám, ahol k pozitív egész, $m \in \mathbb{N}$, és n három négyzetszám összege.

Feltehetjük, hogy (13.7)-ben n-et úgy választottuk, hogy a k pozitív egész értéke minimális. Ekkor n osztható 4-gyel.

Minden négyzetszám kongruens 0-val vagy 1-gyel modulo 4. Könnyen látható, hogy a 0 maradékosztály modulo 4, csak úgy állítható elő három darab elem összegeként a $\{0, 1\}$ halmazból, ha mindegyik 0. Más szóval, ha

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

akkor mindegyik négyzetszám osztható 4-gyel. Legyen $x = 2x_0$, $y = 2y_0$ és $z = 2z_0$, ahol x_0, y_0 és z_0 egész számok. Ekkor

$$\frac{n}{4} = x_0^2 + y_0^2 + z_0^2,$$

így $\frac{n}{4} = 4^{k-1}(8m + 7)$ szintén felírható három négyzetszám összegeként, amely ellentmond annak, hogy (13.7)-ben n-et úgy választottuk, hogy k minimális. A fentiek Legendre tételének egyik irányát igazolják, a másik irány jóval bonyolultabb, itt nem bizonyítjuk.

Hivatkozások

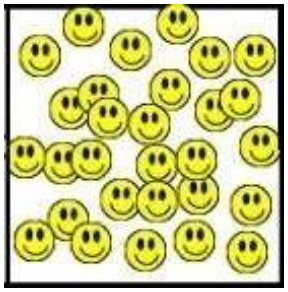
[1] S. Stevin, *l'Arithmétique de Simon Stevin de Bruges, annotated by Albert Girard*, Leyde 1625, p. 622.

[2] Kép, Giuseppe Luigi Lagrangia, link.

[3] Kép, Adrien-Marie Legendre, link.

14. Schnirelmann sűrűség

A számelméletben jó néhány sűrűség fogalom van, első ránézésre biztos nem a legtermészetesebb, de az a sűrűség, amit úgy hívunk, hogy Schnirelmann sűrűség sok praktikus alkalmazással rendelkezik.



A következő definíció Lev Schnirelmann-tól, orosz matematikustól származik [1], [2] 1930-ban.

14.1 DEFINÍCIÓ. *Legyen* $\mathcal{A} \subseteq \mathbb{N} \cup \{0\}$. *Ekkor az* $\mathcal{A}$ *halmaz Schnirelmann sűrűsége*

$$\sigma(\mathcal{A}) = \inf_{n \in \mathbb{N}} \frac{\mathcal{A}(n)}{n},$$

ahol $\mathcal{A}(n) \overset{\text{def}}{=} |\mathcal{A} \cap \{1, 2, \ldots, n\}|$.

Világos, hogy $\sigma(\mathcal{A})$ mindig egy nemnegatív egész szám. Először két propozíciót állítunk.

14.2 Propozíció.

$$\sigma(\mathcal{A}) > 0 \iff 1 \in \mathcal{A} \text{ és } \exists\, c > 0\ \forall n\ \mathcal{A}(n) > cn.$$

14.3 Propozíció.

$$\sigma(\mathcal{A}) = 1 \iff \mathcal{A} = \mathbb{N}^+ \text{ vagy } \mathcal{A} = \mathbb{N} \cup \{0\}.$$

A 14.2 Propozíció bizonyítása. Először azt bizonyítjuk, hogy ha $\sigma(\mathcal{A}) > 0$ akkor $1 \in \mathcal{A}$ és $\exists\, c > 0$, amelyre $\mathcal{A}(n) \geq cn$ minden pozitív egész n-re. Valóban, ekkor

$$\sigma(\mathcal{A}) = \inf_{n \in \mathbb{N}^+} \frac{\mathcal{A}(n)}{n} \leq \frac{\mathcal{A}(1)}{1} = \mathcal{A}(1). \tag{14.1}$$

Ha $1 \notin \mathcal{A}$, akkor $\mathcal{A}(1) = 0$, azaz (14.1) alapján azt kapjuk, hogy $\sigma(\mathcal{A}) \leq 0$. De mivel $\sigma(\mathcal{A})$ nemnegatív szám, így $\sigma(\mathcal{A}) = 0$, amely ellentmondás. Tehát $1 \in \mathcal{A}$. Másrészt, ha $\sigma(\mathcal{A}) > 0$, akkor $c = \sigma(\mathcal{A})$-t írva azt kapjuk, hogy

$$c = \inf_{n \in \mathbb{N}^+} \frac{\mathcal{A}(n)}{n} \leq \frac{\mathcal{A}(n)}{n}$$

minden $n \in \mathbb{N}^+$-re. Azaz

$$cn \leq \mathcal{A}(n)$$

minden $n \in \mathbb{N}^+$-re.

Következőben tegyük fel, hogy $1 \in \mathcal{A}$ és $\mathcal{A}(n) > cn$ minden n-re. Ekkor

$$\sigma(\mathcal{A}) = \inf_{n \in \mathbb{N}^+} \frac{\mathcal{A}(n)}{n} > \inf_{n \in \mathbb{N}^+} c = c > 0.$$

A 14.3 Propozíció bizonyítása. Tegyük fel, hogy $\sigma(\mathcal{A}) = 1$. Bebizonyítjuk, hogy $\mathcal{A} = \mathbb{N}^+$ vagy $\mathcal{A} = \mathbb{N}^+ \cup \{0\}$. Valóban, legyen $n \in \mathbb{N}^+$. Ekkor

$$1 = \sigma(\mathcal{A}) = \inf_{n \in \mathbb{N}^+} \frac{\mathcal{A}(n)}{n} \leq \frac{\mathcal{A}(n)}{n}.$$

Így

$$n \leq \mathcal{A}(n).$$

Az $\mathcal{A}(n)$ definíciójából adódóan azt kapjuk, hogy $1, 2, 3, \ldots, n \in \mathcal{A}$. Így minden $n \in \mathbb{N}^+$ esetén bebizonyítottuk, hogy $n \in \mathcal{A}$, amiből következik az állítás. Az is világos, hogy ha $\mathcal{A} = \mathbb{N}^+$ vagy $\mathcal{A} = \mathbb{N}^+ \cup \{0\}$, akkor

$$\sigma(\mathcal{A}) = \inf_{n \in \mathbb{N}^+} \frac{\mathcal{A}(n)}{n} = \inf_{n \in \mathbb{N}^+} \frac{n}{n} = 1.$$

Ezután bebizonyítjuk Schnirelmann főtételeit.

14.4 Tétel. (Schnirelmann) *Ha $\mathcal{A}, \mathcal{B} \subseteq \mathbb{N} \cup \{0\}$ és $0 \in \mathcal{A} \cap \mathcal{B}$, akkor*

$$\sigma(\mathcal{A} + \mathcal{B}) \geq \sigma(\mathcal{A}) + \sigma(\mathcal{B}) - \sigma(\mathcal{A})\sigma(\mathcal{B}).$$

A 14.4 Tétel bizonyítása. Ha $\sigma(\mathcal{A}) = 0$, akkor a következőt kell bizonyítanunk:

$$\sigma(\mathcal{A} + \mathcal{B}) \geq \sigma(\mathcal{B}).$$

Mivel $0 \in \mathcal{A}$, így

$$\mathcal{A} + \mathcal{B} \supseteq \mathcal{B},$$

azaz az állítás triviális. Feltehetjük, hogy $\sigma(\mathcal{A}) > 0$. A 14.2 Propozíció szerint $1 \in \mathcal{A}$. Tekintsünk egy tetszőleges $n \in \mathbb{N}$-et, és jelöljük $\mathcal{A} \cap [1, n]$ elemeit rendre

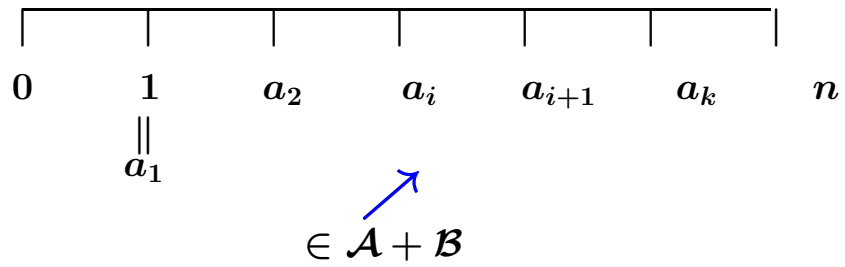
$$1 = a_1 < a_2 < \ldots < a_k \leq n.$$

számokkal. Ekkor $k = \mathcal{A}(n)$.

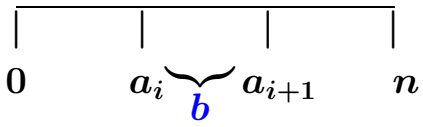
Ezután felsorolunk néhány (de nem az összes) elemet $\mathcal{A} + \mathcal{B}$ halmazból.

Mivel $0 \in \mathcal{B}$

$$a_i + 0 = a_i \in \mathcal{A} + \mathcal{B} \quad \text{ha} \quad i = 1, \ldots, k.$$



Vannak további elemek is $\mathcal{A}+\mathcal{B}$ halmazban. Az $i = 1, 2, \ldots, k-1$ számokra tekintsük az $a_i + b$ elemeket, ahol $b \in \mathcal{B}$ és $0 < b < a_{i+1} - a_i$.



A fenti elemek mindegyike az (a_i, a_{i+1}) részintervallumba esik és $\in \mathcal{A} + \mathcal{B}$.

Végül tekintsük azokat az elemeket, amelyekre

$$a_k + b, \quad b \in \mathcal{B}, \quad b \leq n - a_k.$$

Minden ilyen típusú elem az $(a_k, n]$ részintervallumba esik és $\in \mathcal{A} + \mathcal{B}$.

Hány elemet soroltunk fel eddig?

$a_i \in \mathcal{A} + \mathcal{B}$, $i = 1, \ldots, k$, $k = \mathcal{A}(n)$ darab elem,

$a_i + b \in \mathcal{A} + \mathcal{B}$, $i = 1, \dots, k-1$, $b \in \mathcal{B}$, $0 < b < a_{i+1} - a_i$

rögzített i-re, $\mathcal{B}(a_{i+1} - a_i - 1)$ darab elem,

$a_k + b \in \mathcal{A} + \mathcal{B}$, $b \in \mathcal{B}$, $0 < b \le n - a_k$, $\mathcal{B}(n - a_k)$ darab elem.

Így az $\mathcal{A} + \mathcal{B} \cap [1, n]$ halmazban az elemek száma legalább

$$(\mathcal{A} + \mathcal{B})(n) \ge \mathcal{A}(n) + \sum_{i=1}^{k-1} \mathcal{B}(a_{i+1} - a_i - 1) + \mathcal{B}(n - a_k).$$

Ekkor

$$\begin{aligned}(\mathcal{A} + \mathcal{B})(n) &\ge \mathcal{A}(n) + \sigma(\mathcal{B}) \cdot \left(\sum_{i=1}^{k-1} (a_{i+1} - a_i - 1) \right) + \sigma(\mathcal{B}) \cdot (n - a_k) \\ &= \mathcal{A}(n) + \sigma(\mathcal{B}) \cdot (n - \mathcal{A}(n)) \\ &= \mathcal{A}(n)(1 - \sigma(\mathcal{B})) + \sigma(\mathcal{B}) \cdot n.\end{aligned}$$

Itt $1 - \sigma(\mathcal{B})$ pozitív vagy 0 és $\mathcal{A}(n) \ge \sigma(\mathcal{A})n$, azaz

$$\begin{aligned}(\mathcal{A} + \mathcal{B})(n) &\ge \sigma(\mathcal{A}) \cdot n \cdot (1 - \sigma(\mathcal{B})) + \sigma(\mathcal{B}) \cdot n \\ &= \big(\sigma(\mathcal{A}) + \sigma(\mathcal{B}) - \sigma(\mathcal{A})\sigma(\mathcal{B})\big) \cdot n.\end{aligned}$$

Ekkor $\mathcal{A}(n) \ge \sigma(\mathcal{A})n$-t használva kapjuk, hogy

$$\frac{(\mathcal{A} + \mathcal{B})(n)}{n} \ge \sigma(\mathcal{A}) + \sigma(\mathcal{B}) - \sigma(\mathcal{A})\sigma(\mathcal{B}) \text{ minden } n \ge 1\text{-re},$$

$$\sigma(\mathcal{A} + \mathcal{B}) \ge \sigma(\mathcal{A}) + \sigma(\mathcal{B}) - \sigma(\mathcal{A})\sigma(\mathcal{B}).$$

Ezután a következőt bizonyítjuk:

14.5 TÉTEL. (Schnirelmann) *Ha $\mathcal{A}, \mathcal{B} \subseteq \mathbb{N} \cup \{0\}$, $0 \in \mathcal{A} \cap \mathcal{B}$ és*

$$\sigma(\mathcal{A}) + \sigma(\mathcal{B}) \ge 1,$$

akkor

$$\sigma(\mathcal{A} + \mathcal{B}) = 1.$$

A 14.5 Tétel bizonyítása. A 14.3 Propozíció szerint:

$$\sigma(\mathcal{A}+\mathcal{B})=1 \iff \forall n\in\mathbb{N}^+,\ n\in\mathcal{A}+\mathcal{B}.$$

Ez utóbbit fogjuk bizonyítani.

I. Eset: $n\in\mathcal{A}\cup\mathcal{B}$.

$$\text{Ha } n\in\mathcal{A},\ \text{akkor } n=n+0\in\mathcal{A}+\mathcal{B}.$$
$$\cap \quad \cap$$
$$\mathcal{A} \quad \mathcal{B}$$

Ha $n\in\mathcal{B}$, hasonlóan kapjuk, hogy $n\in\mathcal{A}+\mathcal{B}$.

II. Eset: $n\notin\mathcal{A}\cup\mathcal{B}$. Ekkor $n>1$, különben

$$1\notin\mathcal{A}\cup\mathcal{B}$$
$$1\notin\mathcal{A}\quad 1\notin\mathcal{B}$$
$$\mathcal{A}(1)=\mathcal{B}(1)=0$$
$$\sigma(\mathcal{A})=\sigma(\mathcal{B})=\frac{\mathcal{A}(1)}{1}=\frac{\mathcal{B}(1)}{1}=0$$

Ekkor $\sigma(\mathcal{A})+\sigma(\mathcal{B})=0$, de a tétel feltételei miatt $\sigma(\mathcal{A})+\sigma(\mathcal{B})\geq 1$. Így beláttuk, hogy $n>1$. Ekkor

$$\mathcal{A}(n)+\mathcal{B}(n)\geq\sigma(\mathcal{A})\cdot n+\sigma(\mathcal{B})\cdot n=(\sigma(\mathcal{A})+\sigma(\mathcal{B}))\cdot n\geq n.$$

A fenti alapján és $n\notin\mathcal{A}\cup\mathcal{B}$ miatt

$$\mathcal{A}(n)=\mathcal{A}(n-1),\ \ \mathcal{B}(n)=\mathcal{B}(n-1),\ \ \mathcal{A}(n-1)+\mathcal{B}(n-1)\geq n.$$

Minden $a\in\mathcal{A}$, $0<a\leq n-1$-re tekintsük a-t, és minden $b\in\mathcal{B}$, $0<b\leq n-1$-re tekintsük $n-b$-t. Ezek a számok az $\{1,2,\ldots,n-1\}$ halmazban vannak és számuk

$$\mathcal{A}(n-1)+\mathcal{B}(n-1)\geq n.$$

A skatulyaelv szerint létezik $a \in \mathcal{A}$ és $b \in \mathcal{B}$, melyekre

$$a = n - b \implies a + b = n, \quad n \in \mathcal{A} + \mathcal{B},$$

ezzel a tétel bizonyítását befejeztük.

Sok-sok éven át fennállt a sejtés, hogy vajon az

$$\sigma(\mathcal{A} + \mathcal{B}) \geq \sigma(\mathcal{A}) + \sigma(\mathcal{B}) - \sigma(\mathcal{A})\sigma(\mathcal{B})$$

egyenlőtlenségben a „$-\sigma(\mathcal{A})\sigma(\mathcal{B})$" tag elhagyható-e.

1932-ben Khintchin [3] jelentős részeredményt ért el abban az esetben, amikor $\sigma(\mathcal{A}) = \sigma(\mathcal{B})$. Végül Mann [4] bizonyította be a sejtést 1942-ben.

14.6 TÉTEL. (Mann, 1942) *Ha* $\mathcal{A}, \mathcal{B} \subseteq \mathbb{N} \cup \{0\}$ *és* $0 \in \mathcal{A} \cap \mathcal{B}$*, akkor*

$$\sigma(\mathcal{A} + \mathcal{B}) \geq \min\{1, \sigma(\mathcal{A}) + \sigma(\mathcal{B})\}.$$

Minden bizonnyal a kombinatorikus számelmélet egyik leghasznosabb tétele, ugyanakkor nagyon komplikált, így itt kihagyjuk a bizonyítást.

Hivatkozások

[1] L. G. Schnirelmann, *On the additive properties of numbers*, first published in „Proceedings of the Don Polytechnic Institute in Novocherkassk" (oroszul), vol XIV (1930), 3-27, és újra kiadva „Uspekhi Matematicheskikh Nauk"-ben (oroszul), 1939, no. 6, 9–25.

[2] L. G. Schnirelmann, First published as "Über additive Eigenschaften von Zahlen" in "Mathematische Annalen" (németül), vol 107 (1933), 649-690, és újra kiadva "On the additive properties of numbers" "Uspekhin. Matematicheskikh Nauk"-ban (oroszul), 1940, no. 7, 7–46.

[3] A. Y. Khinchin, *Zur additiven Zahlentheorie*, Mat. Sb., 39:3 (1932), 27–34.

[4] H. B. Mann, *A Proof of the Fundamental Theorem on the Density of Sets of Positive Integers*, Ann. Math. 43 (1942), 523-527.

[5] A. Sárközy, Kombinatorikus Számelmélet, egyetemi előadás.

[6] Kép, Lev Schnirelmann, link.

[7] Kép, a sűrűség illusztrációja, link.

15. Brun szita

Viggo Brun kifejlesztette Eratoszthenész szitájának egy általánosítását a század első negyedében, amelynek segítségével jó becslések adhatóak egy $\mathcal{A}$ halmaz elemszámáról, ahol az elemek nem oszthatók a $p_1, ..., p_k$ prímszámok egyikével sem feltéve, hogy a $\mathcal{A}$ "szabályosan van eloszolva" modulo a fenti prímek (lásd [1] és [2]).

Brun szitáját használva jó néhány Goldbach sejtéshez kötődő eredmény igazolható. Így például, hogy minden természetes szám felírható két olyan szám összegeként, melyeknek prímtényezős felbontásában legfeljebb 9 darab prím szerepel (ld. [3]).

Továbbá, Schnirelmann bebizonyította, hogy minden egész szám felírható legfeljebb $800\,000$ darab prím összegeként. Ezt az eredményt a következő fejezetben tárgyaljuk részletesen.

A fejezet megírása során főképpen [5]-t és [6]-t használtam.

A jól ismert logikai-szita formula az első lépés Brun becslésének bizonyításához.

15.1 Lemma. *Tegyük fel, hogy adott egy véges $\mathcal{A}$ halmaz, N darab elemmel, ahol bizonyos elemek rendelkeznek a $T_1, T_2, ..., T_r$ rossz*

tulajdonságok közül néhánnyal. Jelölje $N_{i_1,i_2,\ldots,i_k}$ *azon elemek számát, amelyek a* $T_{i_1}, T_{i_2}, \ldots, T_{i_k}$ *rossz tulajdonságokkal rendelkeznek. Ekkor a jó elemek számára (amelyek nem rendelkeznek rossz tulajdonsággal) tudjuk, hogy*

$$G = N + \sum_{k=1}^{r} (-1)^k \sum_{\leq i_1 < i_2 < \cdots < i_k \leq r} N_{i_1,i_2,\ldots,i_k}. \tag{15.1}$$

A 15.1 Lemma bizonyítása. Két tényt kell igazolnunk:

1. Minden jó elemet egyszer számoltunk.
2. A rossz elemeket 0-szor számoltuk.

Az 1. állítás triviális, hiszen a jó elemek csak az első tagban szerepelnek.

A 2. állítás igazolásához, tegyük fel, hogy egy rossz elemnek pontosan ℓ darab rossz tulajdonsága van (ekkor $r \geq \ell > 0$).

Ezek a rossz tulajdonságok: $T_{j_1}, \ldots, T_{j_\ell}$. Az (15.1) képletben szereplő multiplicitást úgy kapjuk, hogy megnézzük, hogy hányféleképpen vehetünk egy $i_1, \ldots, i_k$ részhalmazt a $j_1, \ldots, j_\ell$ halmazból, s ezt $(-1)^k$ súllyal vesszük.

Ez összesen $\binom{\ell}{k}$ lehetőség, ami azt jelenti, hogy egy rossz elemet összesen

$$\sum_{k=0}^{\ell} (-1)^k \binom{\ell}{k}$$

darabszámszor számoltunk. De a binomiális tétel szerint a fenti kifejezés $(1-1)^\ell = 0$, amely bizonyítja a 2. állításunk.

Ha ránézünk (15.1)-re, azt látjuk, hogy a szumma rengeteg tagot tartalmaz (összesen 2^r darabot), amely túl soknak bizonyult a

lemma alkalmazásai során. Habár egy ügyes ötlettel jelentősen lecsökkenthetjük a tagok számát.

15.2 Lemma. *A logikai szita formula jelöléseit használva, a jó elemek G számára azt kapjuk, hogy*

$$N + \sum_{k=1}^{2t-1} (-1)^k \sum_{\leq i_1 < i_2 < \cdots < i_k \leq r} N_{i_1,i_2,\ldots,i_k} \leq G$$
$$\leq N + \sum_{k=1}^{2t} (-1)^k \sum_{\leq i_1 < i_2 < \cdots < i_k \leq r} N_{i_1,i_2,\ldots,i_k}.$$

minden $t \in \mathbb{N}^+$-re.

Ezt akár úgy is mondhatjuk durván, hogy a "-"-ok után megállva alulról, a "+"-ok után megállva felülről becsülünk.

A 15.2 Lemma bizonyítása.: Két tényt kell igazolnunk:

1. Mindkét szummában minden jó elemet egyszer számoltunk.
2. Minden rossz elemet a baloldali szummában ≤ 0 súllyal, a jobboldali szummában ≥ 0 súllyal számoltunk.

Itt az 1. állítás triviális.

A 2. állításhoz azt kell igazolnunk, hogy:

$$\sum_{k=0}^{j} (-1)^k \binom{\ell}{k} = (-1)^j \binom{\ell - 1}{j}.$$

A bizonyítás nagyon egyszerűen látható j szerinti indukcióval, és a $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$ összefüggéssel. Ezzel a lemma bizonyítását befejeztük.

Ezután ténylegesen rátérünk a Brun szita leírására.

A következőkben a logikai szita formulát használjuk (ld. Lemma 15.2), de kissé új jelölésekkel.

Legyen $\mathcal{A}$ egész számok egy halmaza, és jelölje A_d az $\mathcal{A}$ halmaz azon elemeinek a számát, melyek oszthatóak d-vel. Továbbá jelölje $\omega(d)$ a d szám különböző prímosztóinak a számát.

Tegyük fel, hogy szeretnénk $\mathcal{A}$ azon elemeinek a számát becsülni, melyek nem oszthatóak a $p_1, p_2, \ldots, p_k$ prímek egyikével sem. Jelölje T_i azt a „rossz” tulajdonságot, ha $\mathcal{A}$ egy eleme osztható a p_i prímmel. Ekkor a 15.2 Lemma szerint:

$$\sum_{\substack{d \mid p_1 p_2 \cdots p_k \\ \omega(d) \leq 2t-1}} \mu(d) A_d \leq \sum_{a \in \mathcal{A}} \sum_{p_1 \nmid a, p_2 \nmid a, \ldots, p_k \nmid a} 1 \leq \sum_{\substack{d \mid p_1 p_2 \cdots p_k \\ \omega(d) \leq 2t}} \mu(d) A_d. \tag{15.2}$$

Ideális esetben A_d elemszáma a következővel becsülhető:

$$X \frac{m(d)}{d} + R_d, \tag{15.3}$$

ahol $m(d)$ egy multiplikatív függvény, X egy konstans, amely értéke csak az $\mathcal{A}$ halmaztól függ, R_d pedig a „hibatag”, amely a „főtag” $X \frac{m(d)}{d}$-hez képest kicsi.

Mielőtt továbbmennénk két példát mutatunk A_d becslésére.

Először legyen $\mathcal{A} = \{a : \ 1 \leq a \leq x\}$. Világos, hogy

$$A_d = \frac{x}{d} + R_d, \tag{15.4}$$

ahol $|R_d| \leq 1$. Azaz (15.3)-ban vehetjük $X = x$-nek és $m(d) = 1$-nek.

A második példában $\mathcal{A} = \{n(n+2) : \ n \in \{y, y+1, \ldots, x\}\}$. Legyen d négyzetmentes egész szám. Ekkor az

$$n(n+2) \equiv 0 \pmod{d}$$

kongruenciának $m(d)$ darab megoldása van a kínai maradéktétel alapján, ahol m egy multiplikatív függvény, és $m(2) = 1$ valamint $m(p) = 2$ ha a p prímre $p \geq 3$. Világos, hogy

$$A_d = (x - y)\frac{m(d)}{d} + R_d, \tag{15.5}$$

ahol $|R_d| \leq 2^{\omega(d)}$.

Térjünk vissza az általános esetre. Ha (15.3) fennáll, akkor:

$$\begin{aligned}\sum_{\substack{d|p_1p_2\cdots p_k\\ \omega(d)\leq h}} \mu(d)A_d &= \sum_{\substack{d|p_1p_2\cdots p_k\\ \omega(d)\leq h}} \mu(d)\left(X\frac{m(d)}{d} + R_d\right)\\ &= X\sum_{\substack{d|p_1p_2\cdots p_k\\ \omega(d)\leq h}} \mu(d)\frac{m(d)}{d} + O\left(\sum_{\substack{d|p_1p_2\cdots p_k\\ \omega(d)\leq h}} R_d\right).\end{aligned} \tag{15.6}$$

A következőkben $\sum_{\substack{d|p_1p_2\cdots p_k\\ \omega(d)\leq h}} \mu(d)\frac{m(d)}{d}$-t becsüljük. Legyen egyelőre $u > 1$ tetszőleges valós szám, amelynek értékét később rögzítjük. Ekkor $u^{\omega(d)-h} > 1$ ha $\omega(d) > h$. Így:

$$\begin{aligned}\sum_{\substack{d|p_1p_2\cdots p_k\\ \omega(d)\leq h}} \mu(d)\frac{m(d)}{d} &= \sum_{d|p_1p_2\cdots p_k} \mu(d)\frac{m(d)}{d} + O\left(\sum_{\substack{d|p_1p_2\cdots p_k\\ \omega(d)> h}} \frac{m(d)}{d}\right)\\ &= \sum_{d|p_1p_2\cdots p_k} \mu(d)\frac{m(d)}{d} + O\left(\sum_{d|p_1p_2\cdots p_k} \frac{m(d)}{d}u^{\omega(d)-h}\right)\\ &= \sum_{d|p_1p_2\cdots p_k} \mu(d)\frac{m(d)}{d} + O\left(u^{-h}\sum_{d|p_1p_2\cdots p_k} \frac{m(d)}{d}u^{\omega(d)}\right).\end{aligned}$$

Itt az összegek felírhatóak mint Euler szorzatok, azaz:

$$\sum_{\substack{d|p_1p_2\cdots p_k\\ \omega(d)\le h}} \mu(d)\frac{m(d)}{d} =$$

$$= \prod_{p\in\mathcal{P}}\left(1-\frac{m(p)}{p}\right) + O\left(u^{-h}\prod_{p\in\mathcal{P}}\left(1+u\frac{m(p)}{p}\right)\right)$$

$$= \prod_{p\in\mathcal{P}}\left(1-\frac{m(p)}{p}\right) + O\left(u^{-h}\prod_{p\in\mathcal{P}}\left(1+\frac{m(p)}{p}\right)^u\right),$$

ahol $\mathcal{P}$ jelöli a $p_1, p_2, \dots, p_k$ prímek halmazát.

Ezután rögzítsük u-t az $u = h/\left(\sum_{p\in\mathcal{P}} \log\left(1+\frac{m(p)}{p}\right)\right)$ képlettel acélból, hogy a hibatagot minimalizáljuk. Ekkor

$$\sum_{\substack{d|p_1p_2\cdots p_k\\ \omega(d)\le h}} \mu(d)\frac{m(d)}{d} = \prod_{p\in\mathcal{P}}\left(1-\frac{m(p)}{p}\right) + O\left(\frac{1}{h}\sum_{p\in\mathcal{P}}\frac{m(p)}{p}\right)^h.$$

A fentit, (15.2)-t és (15.6)-t használva kapjuk, hogy

$$\sum_{a\in\mathcal{A}}\sum_{p_1\nmid a, p_2\nmid a,\dots,p_k\nmid a} 1 = X\prod_{p\in\mathcal{P}}\left(1-\frac{m(p)}{p}\right) + X\cdot O\left(\frac{1}{h}\sum_{p\in\mathcal{P}}\frac{m(p)}{p}\right)^h + O\left(\sum_{\substack{d|p_1p_2\cdots p_k\\ \omega(d)\le h}} R_d\right) \tag{15.7}$$

ha $u = h/\left(\sum_{p\in\mathcal{P}} \log\left(1+\frac{m(p)}{p}\right)\right) \ge 1$.

A következőkben két alkalmazást mutatunk be. Először csak az x-nél kisebb prímek számát becsüljük.

Ha P jelöli azon prímek halmazát, melyek y-nál kisebbek és $\mathcal{A} = \{1, 2, ..., x\}$, akkor (15.7) jobboldala felső becslést ad a prímek számára y és x között.

De (15.4)-ben láttuk, hogy $m(d) = 1$ és $|R_d| \leq 1$. Először a két hibatagot becsüljük. Itt Mertens tételeire [4] lesz szükségünk. A következőkben a szumma prímeken fut.

15.3 LEMMA. (Mertens első tétele)

$$\left| \sum_{p \leq n} \frac{\log p}{p} - \log n \right| \leq 2$$

ha $n \geq 2$.

15.4 LEMMA. (Mertens második tétele)

$$\lim_{n \to \infty} \left(\sum_{p \leq n} \frac{1}{p} - \log \log n - M \right) = 0.$$

Itt M *az ún. Meissel-Mertens konstans (ld. A077761). Még pontosabban igaz, hogy a limesz alatti kifejezés abszolút értékben nem haladja meg*

$$\frac{4}{\log(n+1)} + \frac{2}{n \log n}$$

értéket bármilyen $n \geq 2$ *esetén.*

15.5 LEMMA. (Mertens harmadik tétele)

$$\lim_{n \to \infty} \log n \prod_{p \leq n} \left(1 - \frac{1}{p} \right) = e^{-\gamma} \approx 0.561459483566885,$$

ahol γ *az ún. Euler–Mascheroni konstans (ld. A001620).*

Mertens tételei itt nincsenek bizonyítva, de megjegyezzük, hogy pl. az első két tétel bizonyítása megtalálható a kapcsolódó Wikipédia oldalon: link.

Térjünk vissza a y és x közötti prímszámok becsléséhez. Ehhez az (15.7)-t használjuk, megfelelő h választással.

A (15.7) képletben a második hibatag y^t-val becsülhető, és Mertens tételeit használjuk a többi tag becslésére. (Ekkor ugye tudjuk, hogy $m(d) = 1$). Azaz:

$$\pi(x) - \pi(y) \leq x\frac{e^{-\gamma} + o(1)}{\log y} + x \cdot O(\frac{1}{h}\log\log y)^h + O(y^h).$$

Ha csak olyan prímszámokra vagyunk kíváncsiak, amelyek nem haladják meg az x-t, akkor y-t is rögzíthetjük pl. a következővel: $y = x^{1/(2c)\log\log x}$, legyen továbbá $h = c\log\log x$ (így egy közel optimális felső becslés kapunk a fenti egyenlőtlenségben). Ez alapján:

$$\pi(x) = O(\frac{x\log\log x}{\log x}),$$

amely ugyan a vártnál egy $\log\log x$ szorzóval rosszabb, de már messze nem triviális eredmény.

A következőkben az ikerprímek számára adunk felső becslést.

Jelölje $\mathcal{P}$ megint az y-nál kisebb prímek halmazát, és definiáljuk $\mathcal{A}$ halmazt $\mathcal{A} = \{n(n+2) : n \in [y, x]\}$-val.

Megjegyezzük, hogy ha $p \mid n(n+2)$ egy $p \in \mathcal{P}$ prímre, akkor n és $n+2$ nem lehet egyszerre prím. Ezután a (15.7)-ben szereplő becslést használjuk, ahol $m(2) = 1$ is $m(p) = 2$ ha $p > 2$. Szintén tudjuk, hogy $|R_d| \leq 2^{\omega(d)}$. Akárcsak az előbb azt kapjuk, hogy

$$\pi_2(x) - \pi_2(y) \leq x\frac{c}{(\log y)^2} + xO(\frac{1}{h}\log\log y)^h + O((2y)^h),$$

ahol $\pi_2(x)$ jelöli az x-et meg nem haladó ikerprímek számát. Rögzítsük $h = c\log\log x$-t és $y = x^{1/(2c)\log\lg x}$-t. Ekkor azt kapjuk,

hogy

$$\pi_2(x) \leq O\left(\frac{x(\log\log x)^2}{(\log x)^2}\right).$$

(Itt azt is használtuk, hogy $1 - \frac{2}{p} \leq e^{-2/p}$ valamint Mertens tételeit.)

A fenti eredményből Ábel átrendezéssel Brun levezette, hogy a $\sum_{p,p+2 \text{ prímek}} \frac{1}{p} + \frac{1}{p+2}$ kifejezés konvergens:

$$\begin{aligned}
\sum_{p,p+2 \text{ prímek}} \frac{1}{p} + \frac{1}{p+2} &\ll \sum_{p,p+2 \text{ prímek}} \frac{1}{p} \\
&\leq \sum_x \frac{\pi_2(x) - \pi_2(x-1)}{x} \\
&\leq \sum_x \pi_2(x)\left(\frac{1}{x} - \frac{1}{x+1}\right) \\
&\ll \sum_x \frac{\pi_2(x)}{x^2} \\
&\ll \sum_x \frac{(\log\log x)^2}{x(\log x)^2} \\
&\ll \infty.
\end{aligned}$$

Az ikerprímekre adott felső becslés: $(\log\log x)^2$ rosszabb a várhatóan legjobb értéknél. Tovább fejlesztve a fenti "egyszerű" Brun szitát, amint azt Brun tette, a $(\log\log x)^2$ tényező elhagyható. Ez a "teljes" Brun szita jóval komplikáltabb.

Az alapgondolat röviden: kiinduló formulánk volt

$$\sum_{\substack{d \mid p_1 p_2 \cdots p_k \\ \omega(d) \leq 2t-1}} \mu(d) A_d \leq S(\mathcal{A}, \mathcal{P}) \leq \sum_{\substack{d \mid p_1 p_2 \cdots p_k \\ \omega(d) \leq 2t}} \mu(d) A_d,$$

ahol $S(\mathcal{A}, \mathcal{P}) = \sum_{a \in \mathcal{A}} \sum_{p_1 \nmid a, p_2 \nmid a, \ldots, p_k \nmid a} 1$. Ez a következő alakban

is írható:

$$\sum_{d|p_1p_2\cdots p_k} \chi_1(d)\mu(d)A_d \le S(\mathcal{A},\mathcal{P}) \le \sum_{d|p_1p_2\cdots p_k} \chi_2(d)\mu(d)A_d, \tag{15.8}$$

ahol

$$\chi_1(d) = \begin{cases} +1 & \text{ha } \omega(d) \le 2t-1, \\ 0 & \text{ha } \omega(d) > 2t-1, \end{cases} \quad \chi_2(d) = \begin{cases} +1 & \text{ha } \omega(d) \le 2t, \\ 0 & \text{ha } \omega(d) > 2t. \end{cases} \tag{15.9}$$

Cél e χ_1, χ_2-t olyan más χ_1, χ_2-vel helyettesíteni, melyre:

a) A χ_1, χ_2 továbbra is eleget tesz (15.8)-nak.

b) $\chi_1(1) = \chi_2(2) = 1$.

c) $\chi_i(d) \in \{0,1\}$ minden $d \mid p_1p_2\cdots p_k$-ra és $i = 1$-re vagy $i = 2$-re.

d) Ez az új χ_1, χ_2 jobb becslést ad $S(\mathcal{A},\mathcal{P})$-ra.

Brun talált ilyen χ_1, χ_2-t, de a bizonyítása rendkívül komplikált. Itt csak egy olyan különösen fontos és általános esetet mutatunk, mely a fenti módon bizonyítható:

15.6 TÉTEL. *Legyen* $k \in \mathbb{N}$, $a_1, b_1, \ldots, a_k, b_k \in \mathbb{Z}$ *és* $(a_i, b_i) = 1$ $i = 1, 2, \ldots, k$*-ra. Továbbá*

$$E \overset{\text{def}}{=} \prod_{i=1}^{k} a_i \prod_{1\le r<s\le k} (a_r b_s - a_s b_r) \ne 0,$$

$0 < \varepsilon < 1$, $y \in \mathbb{R}$, $2 \le y \le x$, $z \overset{\text{def}}{=} y^{\varepsilon}$,

$$\mathcal{A} \overset{\text{def}}{=} \{\prod_{i=1}^{k}(a_i n + b_1) : \ n \in \mathbb{N},\ x - y < n \le x\}$$

és

$$\mathcal{P} \stackrel{\text{def}}{=} \{p:\ 0 < p \le z,\ p \text{ prím}\}.$$

Tegyük fel, hogy a

$$\prod_{i=1}^{k}(a_i n + b_1) \equiv 0 \pmod{h}$$

kongruenciának $m(p)$ darab megoldása van. Ekkor

$$\begin{aligned} S(\mathcal{A},\mathcal{P}) &= \left|\{a:\ a\in\mathcal{A},\ (a,\prod_{p\in\mathcal{P}} p)=1\}\right| \\ &\le c\left(\prod_{p|E,\ p\le y}\left(1-\frac{1}{p}\right)^{m(p)-k}\right)\frac{y}{(\log y)^k}, \end{aligned}$$

ahol a c konstans csak k-tól és ε-tól függ.

Nem bizonyítjuk a tételt, de mutatunk két fontos alkalmazást. Az elsőben legyen $k=2, a_1=1, b_1=0, a_2=1, b_2=2, y=x, \varepsilon = 1/2$. Ekkor azt kapjuk, hogy:

15.7 KÖVETKEZMÉNY.

$$\pi_2(x) \stackrel{\text{def}}{=} \{p:\ 0<p\le x,\ p, p+2 \text{ prímek}\} \ll \frac{x}{(\log x)^2}.$$

A második alkalmazásban $k=2, a_1=1, b_1=0, a_2=-1, b_2=x, y=x, \varepsilon=1/2$-t választunk, és ekkor a következőt kapjuk:

15.8 KÖVETKEZMÉNY.

$$|\{(p,q):\ p+q=x, 0<p,q \text{ prímek}\}| \ll \prod_{p|x}\left(1+\frac{1}{p}\right)\frac{x}{(\log x)^2}.$$

Ez utóbbi következmény fontos szerepet fog játszani a következő fejezetben.

Hivatkozások

[1] V. Brun, *Über das Goldbachsche Gesetz und die Anzahl der Primzahlpaare*. Archiv for Mathematik og Naturvidenskab. B34 (8) (1915).

[2] V. Brun, *La série* $\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13}+\frac{1}{17}+\frac{1}{19}+\frac{1}{29}+\frac{1}{31}+\frac{1}{41}+\frac{1}{43}+\frac{1}{59}+\frac{1}{61}+\cdots$ où *les dénominateurs sont "nombres premiers jumeaux" est convergente ou finie*, Bulletin des Sciences Mathématiques. 43 100–104, 124–128 (1919).

[3] V. Brun, *Le crible d'Eratosthène et le théorème de Goldbach*, Christiania Vidensk. Selsk. Skr. 1920, Nr. 3.

[4] F. Mertens, *Ein Beitrag zur analytischen Zahlentheorie*, J. reine angew. Math. 78 (1874), 46–62.

[5] Planemath, Brun's pure sieve, link.

[6] A. Sárközy, Kombinatorikus Számelmélet, egyetemi előadás.

[7] Kép, Viggo Brun, link.

[8] Kép, Eratosthenes, link.

16. Részeredmények a Goldbach sejtéshez vezető úton

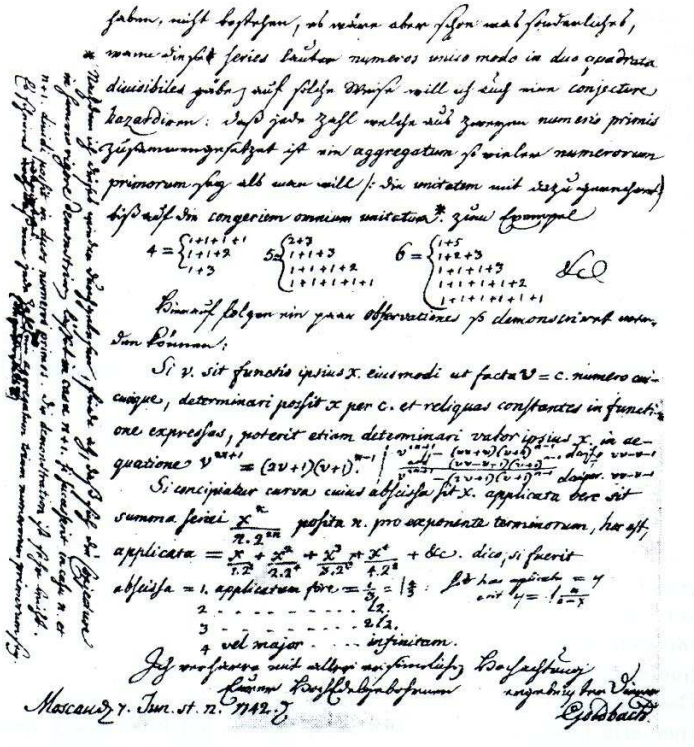
Christian Goldbach, német matematikus többek közt a prímszámok összegét is tanulmányozta. 1742. június 7-én Leonhard Eulernek írt levelében vetette fel a híres Goldbach-sejtést. Az alábbiak az akkori Goldbach-sejtés modern változata:

16.1 SEJTÉS. (erős Goldbach-sejtés) *Minden $n \geq 4$ páros szám felírható két prímszám összegeként.*

16.2 SEJTÉS. (gyenge Goldbach-sejtés) *Minden $n \geq 4$ szám felírható legfeljebb három prímszám összegeként.*

Fontos megjegyezni, hogy a gyenge sejtés következik az erősből: ha n páros, akkor az erős Goldbach sejtés azt állítja, hogy n két prím összege. Ha n páratlan, akkor $n-3$ páros szám, így $n-3$ két prím összege, és ekkor n három prím összege.

Alább Goldbach egy levele olvasható, melyet Eulernek írt (bár ez nem az a levél, amelyben híres sejtését megfogalmazta, de mindenképpen van történeti érdekessége).



A Goldbach-sejtésről és kapcsolódó részeredményekről bővebben a kapcsolódó Wikipedia oldalon [8] is olvashatunk. Most pusztán annyit említünk meg, hogy a gyenge sejtést Vinogradov [7] bizonyította elegendően nagy prímekre, és később Helfgott [1], [2] minden 4-nél nagyobb számra, de ez utóbbi eredmények még lektorálás alatt vannak.

Habár Helfgott eredménye megoldja a gyenge Goldbach sejtést, történelmileg számos azt megelőző lépés született a sejtés megoldása felé vezető úton. Ezek közül talán leghíresebb Schnirelmann [5], [6] eredményei, aki bebizonyította, hogy minden 1-nél nagyobb szám felírható legfeljebb $800\,000$ darab prím összegeként.

Ebben a fejezetben ezt az eredményt tárgyaljuk [4] alapján.

16.3 Definíció. *Ha $\mathcal{A} \subseteq \mathbb{N} \cup \{0\}$ olyan halmaz, hogy minden természetes szám felírható legfeljebb k darab $\mathcal{A}$-beli elem összegeként, akkor $\mathcal{A}$-t k-adrendű bázisnak hívjuk. Ha ez csak elegendően nagy természetes számokra igaz, akkor $\mathcal{A}$-t k-adrendű aszimptotikus bázisnak hívjuk.*

16.4 Tétel. (Schnirelmann) *A prímek aszimptotikus bázist alkotnak. Más szóval, létezik olyan k, hogy minden elegendően nagy n természetes szám felírható legfeljebb k darab prímszám összegeként.*

A bizonyítás a következő két önmagában is érdekes tételen alapul:

16.5 Tétel.

$$|\{(p,q) : \ p+q=x, 0<p,q \text{ prímek}\}| \ll \prod_{p|x}\left(1+\frac{1}{p}\right)\frac{x}{(\log x)^2}.$$

Ez a tétel a 15. fejezetbeli 15.8 Következménye, amelyet bár nem igazoltuk teljes részletességgel, de ismertettük a szükséges eszközöket.

A másik fontos eszköz a Schnirelmann-féle összeghalmaz tétel lesz és azok kiterjesztései is. Először a következőt fogjuk bizonyítani:

16.6 Tétel. (Schnirelmann) *Létezik $c>0$ és x_0, hogy ha $x>x_0$, akkor legalább cx darab olyan n természetes szám létezik, melyre $n \in [1,x]$ és n felírható $n=p+q$ alakban, ahol p és q pozitív prímek.*

A 16.6 Tétel bizonyítása. Mincen $n \in [1,x]$-re jelölje $g(n)$ a

$$p+q=n,$$

egyenlet megoldásszámát, ahol p és q pozitív prímek. Továbbá legyen

$$\mathcal{A} = \{n : n \leq x, g(n) > 0\}.$$

Azt kell bizonyítanunk, hogy

$$|\mathcal{A}| > cx.$$

Ehhez legyen

$$S = \sum_{n \in \mathcal{A}} g^2(n) \quad \left(= \sum_{n \leq x} g^2(n) \right).$$

A bizonyítás során alsó és felső becslést adunk S-re, a két becslést összevetve adódik majd a tétel állítása.

Lássuk tehát S alsó becslését!

A Cauchy–Schwarz egyenlőtlenség szerint:

$$S = \sum_{n \in A} g^2(n) \geq \frac{1}{|A|} \left(\sum_{n \in A} g(n) \right)^2.$$

Itt

$$\sum_{n \in A} g(n) = \sum_{n=1}^{x} g(n) = \sum_{n=1}^{x} \sum_{p+q=n} 1 = \sum_{p+q \leq x} 1$$
$$\geq \sum_{p,q \leq \frac{x}{2}} 1 = \pi^2 \left(\frac{x}{2} \right)$$

A prímszám tétel szerint tudjuk, hogy $\pi(x) \geq \frac{x}{3 \log x}$, így

$$\sum_{n \in A} g(n) > \left(\frac{x}{3 \log x} \right)^2 = \frac{1}{9} \frac{x^2}{(\log x)^2}.$$

Ebből adódóan

$$S > \frac{1}{81} \frac{x^4}{(\log x)^4} \frac{1}{|\mathcal{A}|}.$$

A 16.5 Tétel alapján

$$g(n) \ll \prod_{p|n}\left(1+\frac{1}{p}\right)\cdot\frac{n}{(\log n)^2}.$$

Így

$$S=\sum_{n\le x} g^2(n) \ll \sum_{n\le x}\prod_{p|n}\left(1+\frac{1}{p}\right)^2\cdot\frac{n^2}{(\log n)^4},$$

Mivel az $\frac{n^2}{(\log n)^4}$ függvény monoton növekvő az $[1,x]$ intervallumon, így $\frac{n^2}{(\log n)^4}\le\frac{x^2}{(\log x)^4}$. Tehát

$$S \ll \frac{x^2}{(\log x)^4}\sum_{n\le x}\prod_{p|n}\left(1+\frac{1}{p}\right)^2.$$

Itt $\left(1+\frac{1}{p}\right)^2 \ll \left(1+\frac{2}{p}\right)e^{1/p^2}$ mivel

$$\begin{aligned}\frac{\left(1+\frac{1}{p}\right)^2}{1+\frac{2}{p}} &= \frac{1+\frac{2}{p}+\frac{1}{p^2}}{1+\frac{2}{p}}\\ &= 1+\frac{1}{p^2}\cdot\frac{1}{1+\frac{2}{p}} < 1+\frac{1}{p^2} < e^{1/p^2}.\end{aligned}$$

Azaz

$$S \ll \frac{x^2}{(\log x)^4}\sum_{n\le x}\prod_{p|n}\left(1+\frac{2}{p}\right)e^{1/p^2}$$

A következőkben $\prod_{p|n}\left(1+\frac{2}{p}\right)e^{1/p^2}$-t becsüljük:

$$\begin{aligned}\prod_{p|n}\left(1+\frac{2}{p}\right)e^{1/p^2} &= e^{\sum_{p|n}\frac{1}{p^2}}\prod_{p|n}\left(1+\frac{2}{p}\right)\\ &\ll \prod_{p|n}\left(1+\frac{2}{p}\right)\end{aligned}$$

$$= 1 + \sum_{p_{i_1},\dots,p_{i_k} | n} \frac{2^k}{p_{i_1} \cdots p_{i_k}}$$
$$= \sum_{\substack{d|n \\ |\mu(d)|=1}} \frac{2^{\omega(d)}}{d}.$$

Így:

$$\begin{aligned}
S &\ll \frac{x^2}{(\log x)^4} \sum_{n \le x} \sum_{\substack{d|n \\ |\mu(d)|=1}} \frac{2^{\omega(d)}}{d} \\
&\ll \frac{x^2}{(\log x)^4} \sum_{\substack{d \le x \\ |\mu(d)|=1}} \frac{2^{\omega(d)}}{d} \sum_{\substack{d|n \\ n \le x}} 1 \\
&\ll \frac{x^2}{(\log x)^4} \sum_{\substack{d \le x \\ |\mu(d)|=1}} \frac{2^{\omega(d)}}{d} \cdot \frac{x}{d} \\
&= \frac{x^3}{(\log x)^4} \sum_{\substack{d \le x \\ |\mu(d)|=1}} \frac{2^{\omega(d)}}{d^2} \\
&\ll \frac{x^3}{(\log x)^4} \sum_{d \le x} \frac{2^{\omega(d)}}{d^2} \ll \frac{x^3}{(\log x)^4} \sum_{d=1}^{\infty} \frac{2^{\omega(d)}}{d^2} \\
&= \frac{x^3}{(\log x)^4} \prod_p \left(1 + \frac{2}{p^2}\right) = \frac{x^3}{(\log x)^4} \prod_p e^{2/p^2} \\
&\ll \frac{x^3}{(\log x)^4}.
\end{aligned}$$

Az S-re adott alsó és felső becslést összevetve kapjuk, hogy:

$$\frac{x^4}{(\log x)^4} \cdot \frac{1}{|\mathcal{A}|} \ll S \ll \frac{x^3}{(\log x)^4}$$
$$\Downarrow$$
$$x \ll |\mathcal{A}|.$$

Ezzel a tétel állítását beláttuk.

A következőkben egy olyan tételre lenne szükség, mely szerint, ha egy halmaz pozitív sűrűségű és eleget tesz bizonyos feltételeknek, akkor aszimptotikus bázis. De mielőtt bevezetnénk az aszimptotikus sűrűség fogalmát, térjünk vissza egy kis időre a Schnirelmann sűrűségre. Emlékeztetőképpen:

Egy $\mathcal{A}$ halmaz Schnirelmann sűrűségét a következőképpen definiáljuk:

$$\sigma(\mathcal{A}) = \inf_{n\in\mathbb{N}^+} \frac{\mathcal{A}(n)}{n}.$$

Az alábbit fogjuk bizonyítani:

16.7 Tétel. (Schnirelmann) *Ha $\mathcal{A} \subseteq \mathbb{N}\cup\{0\}$ és $\sigma(\mathcal{A}) > 0$, akkor $\mathcal{A}\cup\{0\}$ (véges rendű) bázis.*

A 16.7 Tétel bizonyítása. Legyen $\mathcal{A}_0 = \mathcal{A}\cup\{0\}$. Ekkor $\sigma(\mathcal{A}_0) > 0$. A következőt fogjuk bizonyítani:

16.8 Lemma.

$$\sigma(k\mathcal{A}_0) \geq 1 - \big(1-\sigma(\mathcal{A}_0)\big)^k$$

A 16.8 Lemma bizonyítása. A lemmát indukcióval igazoljuk. Ha $k = 1$ a lemma állítása triviális. Tegyük fel, hogy a lemmát már beláttuk $k = n$-re és be szeretnénk bizonyítani $k = n+1$-re. Ekkor a 14.4 Tétel alapján:

$$\begin{aligned}
\sigma\big((n+1)\mathcal{A}_0\big) &= \sigma(n\mathcal{A}_0 + \mathcal{A}_0)\\
&\geq \sigma(n\mathcal{A}_0) + \sigma(\mathcal{A}_0) - \sigma(n\mathcal{A}_0)\sigma(\mathcal{A}_0)\\
&= \sigma(\mathcal{A}_0) + \sigma(n\mathcal{A}_0)(1-\sigma(\mathcal{A}_0))\\
&\geq \sigma(\mathcal{A}_0) + \big(1-(1-\sigma(\mathcal{A}_0))^n\big)(1-\sigma(\mathcal{A}_0))\\
&= 1-(1-\sigma(\mathcal{A}))^{n+1}.
\end{aligned}$$

Térjünk vissza a 16.7 Tétel bizonyításához. Mivel $\sigma(\mathcal{A}_0) > 0$ tudjuk, hogy

$$\exists\, k_0 \quad (1-\sigma(\mathcal{A}_0))^{k_0} < \frac{1}{2},$$

Ekkor:

$$\sigma(k_0\mathcal{A}_0) \geq 1-(1-\sigma(\mathcal{A}_0))^{k} > 1-\frac{1}{2} = \frac{1}{2}.$$

A 14.5 Tételt használva $\mathcal{A} = \mathcal{B} = k_0\mathcal{A}_0$-ra kapjuk, hogy

$$\sigma(2k_0\mathcal{A}_0) = 1,$$

amely szerint (ld. 14.3 Propozíció) $\mathcal{A}_0$ bázis. Ezzel a bizonyítást befejeztük.

Eddig azt bizonyítottuk, hogy ha a prímek halmazát $\mathcal{P}$-vel jelöljük, akkor $P + P = 2P$ az egész számoknak egy pozitív százalékát tartalmazza (ld. 16.6 Tétel). Most egy olyan tételre van szükség, hogy ha egy $\mathcal{A} \subseteq \mathbb{N} \cup \{0\}$ halmaz pozitív sűrűségű, akkor $\mathcal{A}$ aszimptotikus bázis.

Egy $\mathcal{A}$ halmaz k-adrendű aszimptotikus bázis, ha $\exists\, n_0$, melyre

$$k\mathcal{A} = \mathcal{A} + \mathcal{A} + \ldots + \mathcal{A} \supseteq \{n_0, n_0+1, n_0+2, \ldots\}.$$

Ha $2P$ egy k-adrendű aszimptotikus bázis, akkor P egy $2k$-adrendű aszimptotikus bázis:

$$\underbrace{(p_1+q_1)+(p_2+q_2)+\ldots+(p_k+q_k)}_{\text{Ez } 2k \text{ darab prímszám összege}} = n, \quad n > n_0.$$

Sajnos olyan tétel nincsen, hogyha

$$\mathcal{A} \subseteq \mathbb{N} \cup \{0\}$$

halmaznak pozitív a sűrűsége, akkor $\mathcal{A}$ aszimptotikus bázis.

Lássunk néhány ellenpéldát.

$$\mathcal{A} = \{a : a \text{ páros}\}.$$

Ekkor $\mathcal{A}$-nak pozitív sűrűsége van, de $k\mathcal{A}$ csak a páros számokat tartalmazza. Hasonlóan látható, hogy

$$\mathcal{A} = \{a : 3 \mid a\}.$$

esetén $\mathcal{A}$ csak a 3-mal osztható számokat tartalmazza. Az ilyen típusú konstrukciókat elkerülendő, muszáj feltenni valamilyen relatív prímségi kikötést $\mathcal{A}$-ban.

A legegyszerűbb ilyen kikötés az pl., ha feltesszük, hogy $\mathcal{A}$ tartalmaz két egymást követő elemet. Először egy definíció következik.

16.9 DEFINÍCIÓ. *Ha $\mathcal{A} \subseteq \mathbb{N} \cup \{0\}$, akkor legyen*

$$\mathcal{A}(n) \overset{\text{def}}{=\!=} \big|\{a : 0 < a \leq n,\ a \in \mathcal{A}\}\big|.$$

Ezt az $\mathcal{A}(n)$ függvényt számláló függvénynek nevezzük. Ha $\mathcal{A}$ végtelen halmaz, akkor

$$\underline{d}(\mathcal{A}) \overset{\text{def}}{=\!=} \liminf_{n\to\infty} \frac{\mathcal{A}(n)}{n}$$

és

$$\overline{d}(\mathcal{A}) \overset{\text{def}}{=\!=} \limsup_{n\to\infty} \frac{\mathcal{A}(n)}{n}.$$

Ezek az értékeket aszimptotikus alsó és felső sűrűségnek nevezzük. Ha $\underline{d}(\mathcal{A}) = \overline{d}(\mathcal{A})$, akkor a közös érték az aszimptotikus sűrűség.

16.10 TÉTEL. (Schnirelmann) *Ha az* $\mathcal{A} \subseteq \mathbb{N} \cup \{0\}$ *halmazra teljesül, hogy*

a) $\underline{d}(\mathcal{A}) > 0$,

b) $\exists\, a_0$, *amelyre* $a_0, a_0 + 1 \in \mathcal{A}$,

akkor $\mathcal{A}$ *aszimptotikus bázis.*

16.11 KÖVETKEZMÉNY. *A prímszámok aszimptotikus bázist alkotnak.*

Azaz a 16.4 Tétel állítását megkapjuk, mint egy általánosabb tétel következményét.

A 16.11 Következmény bizonyítása. A 16.6 Tétel szerint $\underline{d}(2P) > 0$. Világos, hogy $4, 5 \in 2P$ mivel $4 = 2 + 2$ és $5 = 2 + 3$. A 16.10 Tétel használva megkapjuk, hogy $2P$ aszimptotikus bázis. De ekkor P is aszimptotikus bázis.

A 16.10 Tétel bizonyítása. A tétel feltételei szerint létezik a_0, melyre

$$a_0, a_0 + 1 \in \mathcal{A}.$$

Legyen

$$\mathcal{B} \overset{\text{def}}{=\!=} \{b : b \in \mathbb{N} \cup \{0\}, a_0 + b \in \mathcal{A}\},$$

Ekkor

$$\underline{d}(\mathcal{B}) = \underline{d}(\mathcal{A}),$$
$$\{0, 1\} \in \mathcal{B}$$

A 14.2 Propozíciót használva kapjuk, hogy $\sigma(\mathcal{B}) > 0$. Ezután a 16.7 Tétel szerint $\mathcal{B}$ véges rendű bázis.

Jelölje k ennek a $\mathcal{B}$ bázisnak a rendjét. Ekkor $\mathcal{A}$ egy k-adrendű aszimptotikus bázis. Valóban tegyük fel, hogy $n > ka_0$. Írjuk $n = ka_0 + x$ alakban. Mivel $\mathcal{B}$ egy k-adrendű bázis létezik

$b_1, b_2, \ldots, b_k \in \mathcal{B}$, melyekre

$$b_1 + b_2 + \cdots + b_k = x.$$

Ekkor

$$(a_0 + b_1) + (a_0 + b_2) + \cdots + (a_0 + b_k) = ka_0 + x = n.$$

A $\mathcal{B}$ halmaz definíciója miatt $a_0 + b_i \in \mathcal{A}$, azaz n felírható k darab $\mathcal{A}$-beli elem összegeként. Ez minden $n > ka_0$ számra igaz, vagyis $\mathcal{A}$ valóban aszimptotikus bázis.

Schnirelmann bizonyítása nyomán felső becslést adhatunk a a bizonyításban szereplő alkalmazott konstansokra, és így azt is megkapjuk, hogy minden 1-nél nagyobb természetes szám felírható legfeljebb $800\,000$ darab prím összegeként.

Mann tétele (ld. 14.6 Tétel) a kombinatorikus számelmélet egy alapvető tétele.

Nagyon szép tétel, de Schnirelmann sűrűséget használ, ami egy kicsit mesterséges fogalom.

Érdemes egy hasonló jellegű tételt megfogalmazni, amely a Schnirelmann sűrűség helyett az aszimptotikus sűrűséget használja.

Ez Kneser tétele [3], egy nagyon szép tétel, sok érdekes alkalmazással:

16.12 TÉTEL. (Kneser) *Ha $\mathcal{A}_0, \ldots, \mathcal{A}_k \subseteq \mathbb{N} \cup \{0\}$, akkor*

$$d(\mathcal{A}_0 + \ldots + \mathcal{A}_k) \geq \liminf \frac{\mathcal{A}_0(n) + \ldots + \mathcal{A}_k(n)}{n}$$
$$\left(\geq \underline{d}(\mathcal{A}_0) + \ldots + \underline{d}(\mathcal{A}_k)\right)$$

vagy $\exists\, g, a_0, \ldots, a_k \in \mathbb{N}$ melyekre:

1) *Minden* $\mathcal{A}_i$ *halmazt tartalmaz egy* $\mathcal{A}_i'$ *halmaz, mely* a_i *darab* mod g *maradékosztály uniója.*

2) *Az* $\mathcal{A}_0' + \ldots + \mathcal{A}_k'$ *halmazban csak véges sok olyan elem van, amely nem szerepel* $\mathcal{A}_0 + \ldots + \mathcal{A}_k$ *halmazban.*

3) $d(\mathcal{A}_0 + \ldots + \mathcal{A}_k) \geq \dfrac{a_0 + \ldots + a_k - k}{g}$.

A bizonyítás rendkívül komplikált, így kihagyjuk a jegyzetben.

Hivatkozások

[1] H. A. Helfgott, *Major arcs for Goldbach's theorem*. arXiv:1305.2897 [math.NT] (2013).

[2] H. A. Helfgott, *Minor arcs for Goldbach's problem*. arXiv:1205.5252 [math.NT] (2012).

[3] M. Kneser, *Abschätzungen der asymptotischen Dichte von Summenmengen*. Math. Z. (in German). 58 (1953), 459–484.

[4] A. Sárközy, Kombinatorikus Számelmélet, egyetemi előadás.

[5] L. G. Schnirelmann, *On the additive properties of numbers*, first published in "Proceedings of the Don Polytechnic Institute in Novocherkassk" (oroszul), vol 14 (1930), pp. 3–27, és újra kiadva "Uspekhi Matematicheskikh Nauk"-ban (oroszul), 1939, no. 6, 9–25.

[6] L. G. Schnirelmann, First published as "Über additive Eigenschaften von Zahlen" "Mathematische Annalen"-ban (németül), vol. 107 (1933), 649–690, and reprinted as "On the

additive properties of numbers" "Uspekhi Matematicheskikh Nauk"-ban (oroszul), 1940, no. 7, 7–46.

[7] I. M. Vinogradov, *The Method of Trigonometrical Sums in the Theory of Numbers*, 1954, Translated, átdolgozta és jegyzetekkel ellátta K. F. Roth és Anne Davenport.

[8] Wikipedia, Goldbach's conjecture, link

[9] Kép, Christian Goldbach, link.

[10] Kép, *Goldbach levele Eulerhez*, link.

17. Multiplikatív problemák

Ahogy az eddigiekben láthattuk a kombinatorikus számelméletben nagyon sok különböző típusú tétel szerepel. Most [10] alapján olyan problémákat fogunk tanulmányozni, amelyekben valamilyen értelemben szerepel multiplikatív vonás.

Először olyan $\mathcal{A}$ halmazokat vizsgálunk meg, melyekre a $2\mathcal{A} = \mathcal{A} + \mathcal{A}$ összeghalmaz mérete nem nő meg jelentősen.

Könnyű megadni egy ilyen $\mathcal{A}$ halmazt, vegyük például a számtani sorozatokat De vajon ők az egyetlenek? 1962-ben Freiman teljes választ adott a fenti kérdésre.

Ehhez nézzünk egy új definíciót:

17.1 Definíció. *Legyen* $k_1, \dots, k_d \in \mathbb{N}$, $k_1, \dots, k_d \geq 2$, $u, v_1, \dots, v_d \in \mathbb{Z}$ *és*

$$\mathcal{M} \stackrel{\text{def}}{=} \left\{ u + \sum_{i=1}^{d} x_i v_i : x_i \in \{1, \dots, k_i\},\ i = 1, \dots, d \right\}.$$

Ekkor $\mathcal{M}$*-et egy* d dimenziós általánosított számtani sorozatnak *hívjuk.*

Freiman a következőt bizonyította:

17.2 Tétel. (Freiman) *Minden* $\alpha > 1$*-re létezik* $c_1 = c_1(\alpha)$ *és* $c_2 = c_2(\alpha)$ *konstans, melyekre igaz, hogy ha* $|2\mathcal{A}| < \alpha|\mathcal{A}|$*, akkor létezik* d *dimenziós általánosított számtani sorozat, melyre* $d < c_1$*,* $\mathcal{A} \subseteq \mathcal{M}$ *és* $|\mathcal{M}| < c_2|\mathcal{A}|$*.*

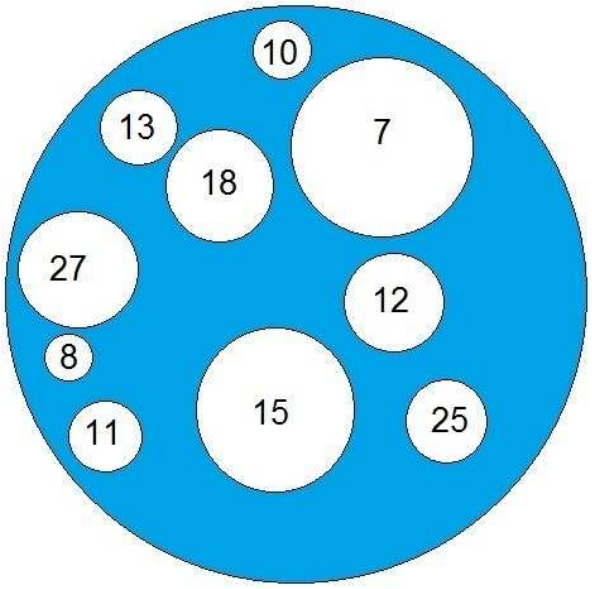
Freiman [4], [5] eredeti bizonyítása exponenciális összegeket használt, és meglehetősen komplikált volt.

Később Ruzsa [8] megadott egy egyszerűbb bizonyítást, mely gráfelméletet és a híres Ruzsa-Plünnecke egyenlőtlenséget használta.

Az érdeklődőknek szívesen ajánlom Ruzsa Imre, „Sumsets and Structure” jegyzetének tanulmányozását [9].

1935 januárjában Behrend [1] olyan halmazokat kezdett tanulmányozni, amelyekben nincs olyan elem, amely oszt egy másikat:

17.3 Definíció. *Egy $\mathcal{A} \subseteq \mathbb{N}$ halmaz akkor és csak akkor primitív, ha nem létezik $a, a' \in \mathcal{A}$, $a \neq a'$, melyre $a \mid a'$.*



Kérdés. Milyen sűrű lehet egy primitív halmaz?

A válasz nagyban függ attól, hogy melyik sűrűség fogalmat használjuk.

Kellemes feladat az olvasó számára, bizonyítást találni a következő tételre:

17.4 TÉTEL.

$$\max_{\substack{\mathcal{A}\subseteq\{1,\dots,2N\},\\ \mathcal{A}\ \text{primitív}}} |\mathcal{A}| = N.$$

Az előző tételt véges kérdésként fogalmaztuk meg. A kérdés érdekesebb a végtelen halmazok esetében. Először egy új típusú sűrűséget vezetünk be:

17.5 DEFINÍCIÓ. *Ha $\mathcal{A} \subseteq \mathbb{N}$ és $\mathcal{A}$ egy végtelen halmaz, akkor definiáljuk a logaritmikus alsó sűrűséget*

$$\underline{\delta}(\mathcal{A}) = \liminf \frac{\sum\limits_{a\in A} \frac{1}{a}}{\log N}$$

képlettel, és a logaritmikus felső sűrűséget pedig a

$$\overline{\delta}(\mathcal{A}) = \limsup \frac{\sum\limits_{a\in A} \frac{1}{a}}{\log N}$$

képlettel. Ha a két sűrűség egyenlő, azaz $\left(\underline{\delta}(\mathcal{A}) = \overline{\delta}(\mathcal{A})\right)$, akkor a közös értéket $\delta(\mathcal{A}) = \underline{\delta}(\mathcal{A}) = \overline{\delta}(\mathcal{A})$ logaritmikus sűrűségnek hívjuk.

Ismert a következő:

$$\underline{d}(\mathcal{A}) \le \underline{\delta}(\mathcal{A}) \le \overline{\delta}(\mathcal{A}) \le \overline{d}(A).$$

Behrend [1] a következőt bizonyította:

17.6 TÉTEL. (Behrend) *Ha $\mathcal{A} \subseteq \{1, 2, \dots, N\}$ és $\mathcal{A}$ primitív halmaz, akkor*

$$\sum_{a\in A} \frac{1}{a} < c\frac{\log N}{\sqrt{\log\log N}} \tag{17.1}$$

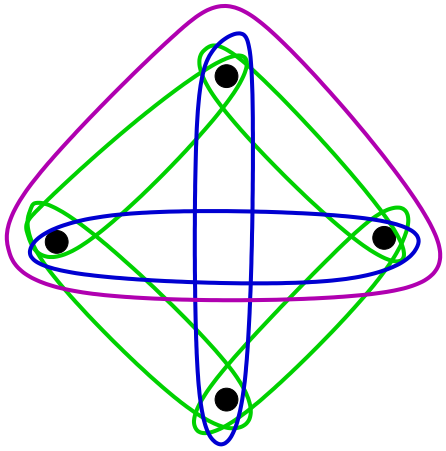
Vagyis az $\mathcal{A}$ halmaz logaritmikus sűrűsége 0. (Ez nem igaz a normál sűrűség fogalomra, amely lehet $1/2$.)

A bizonyítás érdekessége, hogy nem elég használni extremális gráfelméletet használni, hanem szükség van extremális halmazelméletre. Az egyik a fő eszköz a Sperner-tétel [11], amelyet itt nem fogunk bizonyítani.

17.7 LEMMA. (Sperner-tétel) *Ha S egy véges halmaz, $|S| = r$, $R_1, \ldots, R_t$ az S halmaz részhalmazai, és*

$$t > \binom{r}{[r/2]}, \tag{17.2}$$

akkor létezik R_i és R_j részhalmazok, melyekre $i \neq j$ és $R_i \subseteq R_j$.



Más szóval, ha elegendő számú részhalmazunk van ((17.2) állítása szerint), akkor azok között van kettő, amelyek tartalmazzák egymást.

Vegyük észre, hogy a (17.2)-ben a korlát a lehető legjobb: Nincs tartalmazási kapcsolat az $[r/2]$ elemű részhalmazok között egy r elemű halmaz esetében.

Sperner tételét nem fogjuk bizonyítani, csupán használjuk.

Behrend tételének bizonyításához, tegyük fel, hogy c elég nagy, és $N > N_0$, $\mathcal{A} \subset \{1, 2, 3, \dots, N\}$, továbbá

$$\sum_{a \in \mathcal{A}} \frac{1}{a} \geq c \frac{\log N}{\log \log N}.$$

Megmutatjuk, hogy ekkor létezik $a, a' \in \mathcal{A}$, melyekre $a < a'$ és $a \mid a'$.

Egy redukciós lépéssel kezdjük, amelyben redukáljuk a feladatot olyan halmazokra, amelyek csak négyzetmentes számokat tartalmaznak. Minden $a \in \mathcal{A}$ felírható egy négyzetszám és egy négyzetmentes szám szorzataként:

$$a = m_a^2 q_a, \qquad m_a \in \mathbb{N}, \quad |\mu(q_a)| = 1.$$

Ekkor (17.1) alapján

$$c \frac{\log N}{\sqrt{\log \log N}} \leq \sum_{a \in \mathcal{A}} \frac{1}{a} = \sum_{a \in \mathcal{A}} \frac{1}{m_a^2 q_a}$$
$$= \sum_{m=1}^{\infty} \frac{1}{m^2} \sum_{\substack{a:\ a \in \mathcal{A} \\ m_a = m}} \frac{1}{q_a}. \tag{17.3}$$

Jelöljük a belső összeget $S(m)$-mel:

$$S(m) = \sum_{\substack{a:\ a \in \mathcal{A} \\ m_a = m}} \frac{1}{q_a}.$$

Azt állítjuk, hogy létezik $m \in \mathbb{N}$, melyre

$$S(m) > \frac{c}{2} \cdot \frac{\log N}{\sqrt{\log \log N}}. \tag{17.4}$$

Ezt indirekten bizonyítjuk. Ha nincs ilyen m, akkor $\forall m \in \mathbb{N}$-re tudjuk, hogy

$$S(m) \leq \frac{c}{2} \cdot \frac{\log N}{\sqrt{\log \log N}},$$

így (17.3) alapján kapjuk

$$c\frac{\log N}{\sqrt{\log\log N}} \le \sum_{m=1}^{2} \frac{1}{m^2}\frac{c}{2}\frac{\log N}{\sqrt{\log\log N}}$$
$$= \frac{\pi^2}{6}\cdot\frac{c}{2}\frac{\log N}{\sqrt{\log\log N}} < c\frac{\log N}{\sqrt{\log\log N}},$$

amely ellentmondás. Tehát valóban létezik m, amely eleget tesz (17.4)-nak.

Rögzítsünk most egy ilyen m-et és legyen

$$\mathcal{A}(m) = \{a : \ a \in \mathcal{A},\ m_a = m\}$$
$$Q(m) = \{q : \ m^2 q \in \mathcal{A}(m)\}.$$

Vagyis $Q(m)$ azon q-k halmaza, melyre $m^2 q \in \mathcal{A}$, ahol q négyzetmentes szám. Azaz ha

$$q, q' \in \mathcal{Q}(m), \quad q < q', \quad q \mid q', \tag{17.5}$$

akkor

$$m^2 q, m^2 q' \in \mathcal{A}(m) \subset \mathcal{A},\ m^2 q < m^2 q',\ m^2 q \mid m^2 q',$$

vagyis van oszthatósági reláció $\mathcal{A}$-ban. (ld. $a = m^2 q, a' = m^2 q'$). Így elegendő olyan q, q'-t találni, amely eleget tesz (17.5)-nek.

Továbbá $q \in \mathcal{Q}(m)$ esetén $m^2 q \in \mathcal{A}(m) \subset A$, így

$$m^2 q \le N,$$

ahonnan

$$q \le N.$$

Végül, ha $q \in Q(m)$, akkor $|\mu(q)| = 1$.

Azaz, ha $Q = Q(m)$-t írunk, akkor a következő feltételek fennállnak:

$$\begin{gathered} Q \subset \{1, 2, 3, \ldots, N\}, \\ S(m) = \sum_{q \in Q} \frac{1}{q} > \frac{c}{2} \cdot \frac{\log N}{\sqrt{\log \log N}}, \\ \forall q \in Q \text{ négyzetmentes.} \end{gathered} \tag{17.6}$$

Így, ha (17.5)-t szeretnénk bizonyítani, akkor elegendő azt belátni, hogy ha Q eleget tesz a fenti három feltételnek, akkor

$$\exists q, q' \in Q,\ q < q',\ q \mid q'. \tag{17.7}$$

Ezzel sikerült a tétel bizonyítását négyzetmentes számokra redukálnunk.

Vezessük be a következő jelölést: minden $n \in \mathbb{N}$-re legyen

$$d_Q(n) \stackrel{\text{def}}{=} |\{q :\ q \in Q,\ q \mid n\}|$$

(azaz $d_Q(n)$ megszámolja, hogy n-nek hány osztója van Q-ban.)

A következőt fogjuk használni:

17.8 Lemma. *Minden $N > N_0$-ra létezik $n \in \mathbb{N}$, melyre*

1. $n \leq N$
2. $d(n) > \frac{\log N}{\log \log N}$
3. $d_Q(n) > \frac{d(n)}{\sqrt{\log d(n)}}$

A 17.8 Lemma bizonyítása. Indirekten bizonyítunk. Tegyük fel, hogy nincs ilyen n. Ekkor $\forall n \leq N$-re legyen

$$d(n) \leq \frac{\log N}{\log\log N}$$

vagy

$$d(n) > \frac{\log N}{\log\log N}.$$

De az utóbbi esetben a 3. tulajdonság nem teljesül, s így

$$\begin{aligned} d_Q(n) \leq \frac{d(n)}{\sqrt{\log d(n)}} &< \frac{d(n)}{\sqrt{\log \frac{\log N}{\log\log N}}} \\ &< 2\frac{d(n)}{\sqrt{\log\log N}}. \end{aligned}$$

Azaz:

$$\begin{aligned} \sum_{n=1}^{N} d_Q(n) &< \sum_{\substack{n\leq N \\ d(n)\leq \frac{\log N}{\log\log N}}} d_Q(n) + \sum_{\substack{n\leq N \\ d(n)<2\frac{d(n)}{\sqrt{\log\log N}}}} d_Q(n) \\ &< \sum_{n\leq N} \frac{\log N}{\log\log N} + \frac{2}{\sqrt{\log\log N}} \sum_{n\leq N} d(n). \end{aligned}$$

Ekkor

$$\begin{aligned} \sum_{n\leq N} d(n) = \sum_{n\leq N}\sum_{d|n} 1 &= \sum_{d\leq N}\sum_{\substack{n\leq N \\ d|N}} \\ &< \sum_{d\leq N} \frac{N}{d} < 2N\log N. \end{aligned}$$

Itt:

$$\begin{aligned} \sum_{n=1}^{N} d_Q(n) &< N\frac{\log N}{\log\log N} + \frac{2}{\sqrt{\log\log N}} 2N\log N \\ &< 5N\frac{\log N}{\sqrt{\log\log N}}. \end{aligned} \tag{17.8}$$

Másrészről (17.6) alapján:

$$\begin{aligned}\sum_{n=1}^{N} d_Q(n) &= \sum_{n=1}^{N}\sum_{\substack{q\mid n\\ q\in Q}} 1 = \sum_{q\in Q}\sum_{\substack{n\le N\\ q\mid n}} 1\\ &= \sum_{q\in Q}\left[\frac{N}{q}\right] > \sum_{q\in Q}\frac{1}{2}\frac{N}{q} = \frac{1}{2}N\sum_{q\in Q}\frac{1}{q}\\ &> \frac{1}{2}N\cdot\frac{c}{2}\frac{\log N}{\sqrt{\log\log N}}\\ &= \frac{c}{4}N\frac{\log N}{\sqrt{\log\log N}}.\end{aligned}$$

Amennyiben $\frac{c}{4}\ge 5$, vagyis pl. $c=20$, akkor ez ellentmond (17.8)-nek, és ezzel igazoltuk a lemmát (azaz beláttuk olyan n létezését, melyre fennállnak az 1, 2 és 3 tulajdonságok).

Tehát tekintsünk egy n-et az 1, 2, 3 tulajdonságokkal. Jelölje n különböző prímosztóinak szorzatát v és legyen $\frac{n}{v}=u$, azaz

$$n = p_1^{\alpha_1}\cdots p_r^{\alpha_r} = \left(p_1^{\alpha_1-1}\cdots p_r^{\alpha_r-1}\right)(p_1\cdots p_r) = uv,$$

ahol $u\in\mathbb{N}$, $|\mu(v)|=1$. Világos, hogyha q négyzetmentes szám, akkor $q\mid n$ esetén $q\mid v$. Tehát

$$d_Q(n) = d_Q(v). \tag{17.9}$$

Nyilvánvaló, hogy $d(n)>d(v)$, így a 2. és 3. tulajdonságok alapján (17.9)-ból következik, hogy

$$d_Q(n) = d_Q(v) > \frac{d(n)}{\sqrt{\log d(n)}}.$$

De mivel $\frac{x}{\sqrt{\log x}}$ függvény monoton növő, így

$$d_Q(n) = d_Q(v) > \frac{d(v)}{\sqrt{\log d(v)}} \tag{17.10}$$

szintén igaz.

Mivel $v = p_1 p_2 \dots p_r$, így $d(v) = 2^r$. Ezt (17.10)-be írva kapjuk, hogy

$$d_Q(v) > \frac{2^r}{\sqrt{\log 2^r}} = \frac{1}{\sqrt{\log 2}} \frac{2^r}{\sqrt{r}} > \frac{2^r}{\sqrt{r}} > \binom{r}{[r/2]}.$$

Itt az utolsó egyenlőtlenség Stirling formula következménye.

Legyen ekkor v-nek Q-beli osztói: $q_1, q_2, \dots, q_t$. Ekkor

$$t = d_Q(v) > \binom{r}{[r/2]} \tag{17.11}$$

Jelölje egy h négyzetmentes szám osztóinak halmazát $P(h)$. Ekkor:

17.9 Propozíció. *Négyzetmentes h és h' számok esetén $h \mid h'$ csak akkor áll fenn, ha $P(h) \subset P(h')$.*

Ezzel az elvvel az oszthatósági relációk vizsgálatát vissza lehet vezetni tartalmazási relációk vizsgálatára, vagyis a feladat visszavezethető kombinatorikára, speciálisan a Sperner tételre. Ez a bizonyítás fő ötlete.

Tudjuk, hogy $q_1, \dots, q_t \mid v$ esetén

$$P(q_1), P(q_2), \dots, P(q_t) \subset P(v), \tag{17.12}$$

itt jelölje a $P(q_i)$ részhalmazok számát t. Ekkor (17.11) alapján

$$t > \binom{r}{[r/2]}, \tag{17.13}$$

ahol $r = \omega(v) = |P(v)|$. Így (17.12) és (17.13) alapján alkalmazható a Sperner tétele $S, R_1, \ldots, R_t$ helyén $P(v), P(q_1), \ldots, P(q_t)$ halmazokkal. A tételt alkalmazva kapjuk, hogy

$$\exists i, j,\ i \neq j, \text{ melyekre } P(q_i) \subset P(q_j).$$

Így a propozíció alapján $q_i \mid q_j$, azaz valóban van Q-ban osztható-sági reláció, és ezzel a tételt beláttuk.

Behrend tétele szerint ha $\mathcal{A}$ primitív és $\mathcal{A} \subset \{1, 2, \ldots, N\}$, akkor

$$\sum_{a \in \mathcal{A}} \frac{1}{a} < c \frac{\log N}{\log \log N}.$$

Kérdés. Milyen messze van ez a létező legjobbtól?

Pillai [7] 1939-ban bebizonyította, hogy ha $N > N_0(\varepsilon)$ akkor létezik $\mathcal{A} \subset \{1, 2, \ldots, N\}$ primitív halmaz, melyre

$$\sum_{a \in \mathcal{A}} \frac{1}{a} > \left(\frac{1}{2\pi} - \varepsilon \right) \frac{\log N}{\log \log N}.$$

Az általa megadott $\mathcal{A}$ halmaz a következő volt:

$$\mathcal{A} = \{a :\ a \leq N,\ \Omega(a) = [\log \log N]\}.$$

Könnyű látni, hogy ez a halmaz valóban primitív, hiszen $a \neq a'$, $a \mid a'$ esetén $\Omega(a) < \Omega(a')$.

Erdős, Sárközy és Szemerédi [3] azt is igazolta, hogy Behrend tételében a konstans c vehető $\frac{1}{\sqrt{2\pi}} + \varepsilon$-nek.

Végül megjegyezzük, hogy Erdős [2] zseniális bizonyítást adott a következőre:

17.10 TÉTEL. *Létezik c konstans, hogy minden $\mathcal{A} \subset \mathbb{N}^+$ primitív halmazra*

$$\sum_{a \in \mathcal{A}} \frac{1}{a \log a} < c$$

.

Sőt, Erdős azt is sejtette, hogy

$$\sum_{a \in \mathcal{A}} \frac{1}{a \log a} < \sum_{p \text{ prím}} \frac{1}{p \log p}.$$

2022-ben Jared Duker Lichtman [6] váratlanul megoldotta a fenti reménytelennek tűnő sejtést. Munkája lektorálás alatt van.

Az Erdős sejtések iránt érdeklődő olvasók további nyitott problémákat találhatnak a következő Wikipédia oldalon: link.

Hivatkozások

[1] F. Behrend, *On sequences of numbers not divisible one by another*, Journal of the London Mathematical Society, s1-10 (1): 42–44,

[2] P. Erdős, *Note on sequences of integers no one of which is divisible by any other*, J. London Math. Soc.10 (1935), 126–128.

[3] P. Erdős, A. Sárközy, E. Szemerédi, *On divisibility properties of sequences of integers*, Collect Math.Soc. J. Bolyai 2 (1970) 35–49.

[4] G. A. Freiman, *Addition of finite sets*, Soviet Mathematics. Doklady. 5 (1964), 1366–1370.

[5] G. A. Freiman, *Foundations of a Structural Theory of Set Addition* (in Russian), Kazan: Kazan Gos. Ped. Inst. (1966) p. 140.

[6] Jared Duker Lichtman, A proof of the Erdős primitive set conjecture, arXiv:2202.02384, link.

[7] S. Pillai, *On numbers which are not multiples of any other in the set*, Proc. Indian Acad. Sci. A10 (1939) 392–394.

[8] I. Z. Ruzsa, *Generalized arithmetical progressions and sumsets*, Acta Mathematica Hungarica. 65 (4) (1994) 379–388.

[9] I. Z. Ruzsa, Sumsets and Structure, link.

[10] A. Sárközy, Kombinatorikus Számelmélet, egyetemi előadás.

[11] E. Sperner, *Ein Satz über Untermengen einer endlichen Menge*, Mathematische Zeitschrift (in German), 27 (1) (1928) 544–548.

[12] Ábra, Primitív halmaz, saját készítésű.

[13] Ábra, Sperner tétel, saját készítésű.