Bevezetés

Ezt a könyvet olyan olvasóknak szánom, akik járatosak a matematikában, bevezetés nélkül felhasználjuk a számelmélet, kombinatorika, analízis, geometria fogalmait. Például ismertnek tételezem fel a számelmélet elemeit a Legendre-szimbólum alaptulajdonságaival bezárólag, a Fibonacci-sorozat alaptulajdonságait, az egységgyököket, a lineáris algebra módszereit, a gráfelmélet alapfokú ismeretét, integrálok kiszámításának trükkjeit. Használom az ordó-szimbolikát.

Azt is lehet mondani, a matematika középhaladóinak szól a könyv: érdeklődő gimnazistáknak, egyetemistáknak, matematika-tanároknak, matematikusoknak.

A könyv számos egymással csak ritkán kapcsolatban álló fejezetből áll, ezek mindegyike egy vagy több számomra meglepő, szép vagy furcsa bizonyítást tartalmaz.

Szeretnék néhány figyelmeztető megjegyzést tenni. Először is e válogatás szubjektív: biztos vagyok benne, hogy egyes tételek az olvasók rosszallását vívják ki, másrészt sok olvasó tud mondani olyan itt nem szereplő bizonyítást, ami itt joggal szerepelhetne, esetleg több joggal, mint ami itt van.

Bár igyekeztem elkerülni azt, hogy az olvasó számára jól hozzáférhető bizonyításokat publikáljak, erre nem törekedtem minden körülmények között, tippem szerint egy tájékozott matematikus olvasó felét-harmadát ismerheti ezeknek a gyöngyszemeknek.

Elem rendje mod p

Ha 2 hatványainak egy páratlan prímmel vett maradékait vizsgáljuk, akkor, mint jól ismert, periodikus sorozatot kapunk. Van tehát egy olyan legkisebb $d > 1$ szám, hogy

$$2^d \equiv 1 \pmod{p}$$

és ekkor 2 hatványainak maradékai egy d hosszúságú periódussal periodikus sorozatot alkotnak ezért pontosan $n = d, 2d, \ldots$-ra teljesül, hogy $2^n \equiv 1 \pmod{p}$. Ezt 2 mod p vett *rendjének* nevezzük (ez ugyanis a redukált maradékrendszer multiplikatív csoportjában vett rend). Annyit tudhatunk d-ről, hogy $d > 1$ és persze Fermat kis tétele miatt d osztója $p - 1$-nek.

Van olyan eset, amikor ennél pontosabban meg tudjuk adni ezt a rendet. Legyen ugyanis p az n-edik Fermat-szám osztója, tehát $p|F_n = 2^{2^n} + 1$. Ezt átírhatjuk a következőkképpen:

$$2^{2^n} \equiv -1 \pmod{p}.$$

Négyzetreemelve

$$2^{2^{n+1}} \equiv 1 \pmod{p}.$$

adódik, és innen azt kapjuk, hogy 2 rendje mod p egy olyan d szám, ami osztója 2^{n+1}-nek de nem osztója 2^n-nek. Ilyen szám azonban csak egy van: $d = 2^{n+1}$. Ha viszont tudjuk ezt, akkor fenti megjegyzésünk miatt azonnal adódik, hogy $2^{n+1}|p - 1$.

Ezt az észrevételt egy picit javíthatjuk.

1. Tétel. *Ha $n \geq 2$, p prímosztója $2^{2^n} + 1$-nek, akkor*

$$p \equiv 1 \pmod{2^{n+2}}.$$

Bizonyítás. A fentiek szerint elég annyit bebizonyítani, hogy

$$2^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

hiszen abból $d|(p-1)/2$ adódik, de d-ről már tudjuk, hogy 2^{n+1}-gyel egyenlő. Ez viszont Euler lemmája miatt azonos azzal, hogy

$$\left(\frac{2}{p}\right) \equiv 1 \pmod{p}.$$

Ez viszont igaz, hiszen az $n \geq 2$ kikötés és fenti megjegyzésünk szerint $p \equiv 1 \pmod 8$ és a kvadratikus reciprocitási tétel kiegészítése szerint ekkor ez teljesül.

De be tudjuk ezt egyszerűen is bizonyítani. Tegyük fel ugyanis, hogy nem teljesül. Azt tudjuk, például az Euler-lemmából, hogy mindenképpen

$$2^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$$

így azt kapjuk, hogy a $p = 8k + 1$ prímre

$$2^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Vegyük ekkor az $a \equiv 2^{2k} + 1 \pmod p$ maradékot. Ekkor, Fermat kis tétele szerint

$$1 \equiv a^{p-1} \equiv (1 + 2^{2k+1} + 2^{4k})^{\frac{p-1}{2}} \pmod{p}.$$

Amit feltettünk, az az, hogy $2^{4k} \equiv -1 \pmod p$, ezért a fenti kongruencia továbbírható, mint

$$(1 + 2^{2k+1} - 1)^{\frac{p-1}{2}} \equiv (2^{2k+1})^{\frac{p-1}{2}} \equiv 2^{\frac{p-1}{2}} \equiv -1 \pmod{p},$$

de ez ellentmondás. □

Ez az ötlet azonnal igazol egy, a Fermat-számokra vonatkozó prímtesztet is.

2. Tétel. *Ha $n \geq 1$, akkor az $F_n = 2^{2^n} + 1$ Fermat-szám pontosan akkor prím, ha*

$$3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$$

teljesül.

Bizonyítás. Ha F_n prím, akkor az Euler-lemma miatt

$$3^{\frac{F_n-1}{2}} \equiv \left(\frac{3}{F_n}\right) \pmod{F_n}$$

lesz igaz, továbbá, mivel az $n \geq 1$ feltétel miatt $F_n \equiv 1 \pmod 4$, a kvadratikus reciprocitási tétel miatt

$$\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right) = \left(\frac{-1}{3}\right) = -1,$$

hiszen F_n nyilván -1 maradékot ad 3-mal osztva.

A másik irányhoz tegyük fel, hogy teljesül

$$3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}.$$

Legyen p tetszőleges prímosztója F_n-nek. Ekkor persze

$$3^{\frac{F_n-1}{2}} \equiv -1 \pmod{p}$$

is teljesül, ebből viszont, ahogy korábban végiggondoltuk, következik, hogy 3 rendje F_n-1 lesz mod p. Megint Fermat kis tételéből adódik, hogy $F_n-1|p-1$, tehát $p-1 \geq F_n-1$, vagyis $p = F_n$. De ekkor készen vagyunk. □

Egy további alkalmazás a következő.

3. Tétel. *Ha $n \geq 2$, $m = n$ vagy $n+1$, $p|F_n$, $q|F_m$, $p \neq q$, akkor pq álprím 2-re.*

Bizonyítás. Azt kell tehát bebizonyítanunk, hogy a fenti esetben

$$2^{pq-1} \equiv 1 \pmod{pq}$$

teljesül. A fentiekből tudjuk, hogy $2^{n+2}|p-1$, $2^{m+2}|q-1$. Feltettük, hogy n és m egyenlő, vagy egymásutáni számok, ezért $2^{m+1}|p-1$, $2^{n+1}|q-1$ is teljesülni fog. Mivel 2 rendje p-vel osztva 2^{n+1} és q-val osztva 2^{m+1}, ezért a fentiekből következik

$$2^{p-1} \equiv 1 \pmod{q}, \quad 2^{q-1} \equiv 1 \pmod{p}$$

de ekkor

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

és hasonlóan $2^{pq-1} \equiv 1 \pmod{p}$. □

Jegyezzük meg, hogy a tételből következik, hogy van végtelen sok álprím, hiszen vehetjük egymásutáni Fermat-számok egy-egy prímosztóját (különböző Fermat-számok mindig relatív prímek).

Számtani sorozat, amiben nincs $p + 2^n$ alakú elem

Romanov 1934-ben bebizonyította, hogy van olyan $c > 0$ konstans, hogy minden $x \geq 3$-ra x-ig legalább cx olyan páratlan szám van, ami egy prímszám

és egy 2-hatvány összege. Ez azért rendkívül meglepő, mert az ilyen típusú párok, tehát a $(p, 2^n)$ alakú párok száma sem sokkal több: prímszám $x/\log x$, 2-hatvány pedig $\log x/\log 2$ van, összesen ilyen pár tehát nem sokkal több mint x van. Tehát a nem túl sok $p + 2^n$ alakú szám eléggé egyenletesen oszlik szét a különböző értékek között. Romanov azt is megkérdezte, nem áll-e minden 1-nél nagyobb páratlan szám elő, mint egy prímszám és egy 2-hatvány összege. Ezt előtte már de Polignac is megkérdezte 1849-ben. Maga Polignac nem sokkal ezután talált ellenpéldát (959), de annak igazolása, hogy végtelen sok ellenpélda van, csak 1950-ben sikerült Van der Corputnak és Erdősnek. Mindketten ennél lényegesen többet bizonyítottak. Van der Corput azt, hogy az ellenpéldák pozitív sűrűségű sorozatot alkotnak, Erdős pedig ennél is sokkal többet: hogy van csupa ellenpéldából álló végtelen számtani sorozat.

4. Tétel. (Erdős Pál) *Van páratlan számokból álló végtelen számtani sorozat, amelynek egyik tagja sem áll elő egy prímszám és egy 2-hatvány összegeként.*

1. Bizonyítás. Vegyük a $p_1, p_2, p_3, p_4, p_5, p_6, p_7$ prímszámokat a következő módon:

i	a_i	m_i	p_i
1	1	2	3
2	2	4	5
3	4	8	17
4	8	16	257
5	16	32	65537
6	0	64	641
7	32	64	6700417

Korábbi megjegyzéseink szerint 2 rendje pontosan m_i mod p_i. Továbbá, ha n természetes szám, akkor van egy és pontosan egy olyan i, hogy $n \equiv a_i \pmod{m_i}$ teljesül.

Legyen

$$A_0 = \{x : x \equiv 7 \pmod 8\}, \quad A_i = \{x : x \equiv 2^{a_i} \pmod{p_i}\} (1 \le i \le 7).$$

Ha a pozitív egészekre szorítkozunk, akkor minden A_i számtani sorozat és $B = A_0 \cap \cdots \cap A_7$ metszete is, ez utóbbi differenciája

$$8p_1p_2p_3p_4p_5p_6p_7 = 8(2^{64} - 1).$$

Jegyezzük meg, hogy B csupa páratlan számból áll, és a legkisebb is legalább $p_7 + 2^{32}$.

Tegyük most fel, hogy valamelyik $x \in B$ szám $x = 2^n + q$ alakú, ahol q (nyilván páratlan) prímszám. Valamelyik $1 \leq i \leq 7$-re teljesül $n \equiv a_i \pmod{m_i}$, így p_i-vel osztva x egyrészt $2^{a_i} + q$-val másrészt (mivel $x \in A_i$) 2^{a_i}-vel kongruens. Azaz q osztható p_i-vel, tehát $q = p_i$. A feltevések szerint $x \geq 4 + p_7$, ezért mindenképpen $n \geq 3$. De ekkor a 8-cal vett maradék vizsgálata ellentmondásra vezet: egyrészt a feltevés szerint $x \equiv 7 \pmod 8$, másrészt 2^n maradéka 0, p_i maradéka pedig 1, 3 vagy 5, ebből nem tudunk 7-et összerakni. □

2. Bizonyítás. Erdős eredeti bizonyítása ettől kissé eltérően *Bang tételét* használta. Eszerint minden $n > 1$, $n \neq 6$ számra van olyan p prím, hogy $p \mid 2^n - 1$, de $p \nmid 2^m - 1$ $(m < n)$. Ezért Erdős készített egy olyan kongruenciarendszert, hogy minden természetes szám kielégíti valamelyiket (tehát a rendszer *lefedő kongruenciarendszer*) és amelynek modulusai egymástól különböznek, és egyik sem 1 vagy 6:

$$\begin{aligned} x &\equiv 0 \pmod 2 \\ x &\equiv 0 \pmod 3 \\ x &\equiv 1 \pmod 4 \\ x &\equiv 7 \pmod 8 \\ x &\equiv 11 \pmod{12} \\ x &\equiv 19 \pmod{24}. \end{aligned}$$

Majd vett olyan prímeket, melyekre nézve 2 rendje sorra 2, 3, 4, 8, 12, és 24: $p_1 = 3$, $p_2 = 7$, $p_3 = 5$, $p_4 = 17$, $p_5 = 13$, $p_6 = 241$.

Ha most tekintjük az

$$\begin{aligned}
x &\equiv 2^0 \pmod{p_1}\\
x &\equiv 2^0 \pmod{p_2}\\
x &\equiv 2^1 \pmod{p_3}\\
x &\equiv 2^7 \pmod{p_4}\\
x &\equiv 2^{11} \pmod{p_5}\\
x &\equiv 2^{19} \pmod{p_6}\\
x &\equiv 2^9 + 2^8 + 1 \pmod{2^{10}}
\end{aligned}$$

kongruenciákat, akkor ezek megoldásai olyan számtani sorozatot alkotnak, ami nem tartalmaz $p + 2^n$ alakú számot. A bizonyítás ugyanúgy halad, mint az 1. Bizonyításban. Az utolsó kongruencia annak biztosítására szolgál, hogy x nem lehet $x = p_i + 2^n$ alakú a fenti p_i prímekkel. Valóban, ekkor $p_i < 2^8 = 256$, a második tag maradéka 0 és 2^9 közé esik moduló 2^{10}, így összegük nem elégítheti ki az utolsó kongruenciát. □

Ezzel az ötlettel egy másik tétel is könnyen bizonyítható.

5. Tétel. (W. Sierpiński) *Van végtelen sok olyan $k > 1$ természetes szám, hogy $k2^n + 1$ mindig összetett ($n = 1, 2, \ldots$).*

Bizonyítás. Vegyük a fenti a_i, m_i, p_i számokat. Hasonlóan az előző bizonyításokhoz, azt szeretnénk elérni, hogy ha n-re $n \equiv a_i \pmod{m_i}$ teljesül, akkor legyen igaz $p_i \mid k2^n + 1$. Mivel ekkor $2^n \equiv 2^{a_i} \pmod{p_i}$, ez tovább alakítható, mint

$$k2^{a_i} + 1 \equiv 0 \pmod{p_i},$$

azaz vegyük a

$$k \equiv -2^{m_i - a_i} \pmod{p_i}$$

kongruenciarendszert. Ha k ennek megoldása, akkor minden n-re $k2^n + 1$ osztható $p_1, \ldots, p_6$ valamelyikével. Ha még kikötjük, hogy $k > p_6$, akkor egyenlőség nem állhat, tehát csupa összetett számról van szó. □

Ez az ötlet használható egy, a Fibonacci sorozattal kapcsolatos probléma megoldására. Tekintsük a Fibonacci típusú sorozatokat, tehát az olyan egész számokból álló $T_0, T_1, \ldots$ sorozatokat, amelyekre a $T_{n+1} = T_n + T_{n-1}$ rekurzió

teljesül. Könnyű látni, hogy T_0, T_1 meghatározza a sorozatot, sőt indukcióval a

$$T_n = T_1 F_n + T_0 F_{n-1}$$

formula is belátható. Ha azt a problémát vizsgáljuk, van-e végtelen sok prímszám egy ilyen sorozatban (ez az eredeti Fibonacci sorozatra megoldatlan), nyilván ki kell kötni a $(T_0, T_1) = 1$ feltételt, hiszen, ha T_0-nak és T_1-nek lenne 1-nél nagyobb közös osztója, az a sorozat valamennyi tagját osztaná. De ha ez a feltétel teljesül, mint Graham felfedezte, akkor is lehet a sorozat minden tagja összetett. Valóban, mivel a Fibonacci sorozat a 2-hatványokhoz hasonlóan periodikus bámilyen modulusra nézve, találhatók olyan a_i, m_i, p_i számok, hogy a p_i-k különböző prímszámok, az $n \equiv a_i \pmod{m_i}$ rendszer lefedő, és ha $m_i \mid n$, akkor $p_i \mid F_n$. Ebből ki lehet számolni T_0, T_1 értékeket, hogy minden T_n-et valamelyik p_i oszt. Graham eredeti (számolási hibát tartalmazó) példáját Knuth javította és a

$$T_0 = 62638280004239857,$$

$$T_1 = 49463435743205655$$

értékeket találta.

Irodalom

[1] J. G. Van der Corput: On de Polignac's conjecture, *Simon Stevin*, **27**(1950), 99–105.

[2] P. Erdős: On integers of the form $2^k + p$ and some related problems, *Summa Brasil. Math.*, **2**(1950), 113–123.

[3] Erdős Pál: Egy kongruenciarendszerekről szóló problémáról, *Matematikai Lapok*, **3**(1952), 122–128.

[4] R. L. Graham: A Fibonacci-like sequence of composite numbers, *Math. Magazine*, **37**(1964), 322–324.

[5] D. E. Knuth: A Fibonacci-like sequence of composite numbers, *Math. Magazine*, **63**(1990), 21–25.

[6] N. P. Romanoff: Über einige Sätze der additiven Zahlentheorie, *Math. Ann.*, **109**(1934), 668–678.

[7] W. Sierpiński: Sur un problème concernant les nombres $k2^n+1$, *Elem. Math.*, **15**(1960), 73–74.

Az Erdős-Ginzburg-Ziv tétel

A skatulyaelv egyik jólismert alkalmazása a következő z állítás.

6. Tétel. *Ha $n \geq 1$, akkor n szám közül mindig kiválasztható egy vagy több, amelyeknek az összege osztható n-nel.*

Bizonyítás. Tegyük fel, hogy adottak az $a_1, \ldots, a_n$ egész számok. Ha van az $a_1, a_1+a_2, \ldots, a_1+a_2+\cdots+a_n$ számok között kettő, ami azonos maradékot ad n-nel osztva, akkor különbségük számaink n-nel osztható részösszegét adja. Ha nincs, akkor az $a_1, a_1+a_2, \ldots, a_1+\cdots+a_n$ számok n-nel vett maradékai különbözők, tehát előfordul 0 is.

Ennek egy érdekes változata a következő tétel.

7. Tétel. (Erdős-Ginzburg-Ziv) *$2n-1$ egész szám közül mindig kiválasztható pontosan n aminek az összege osztható n-nel.*

Bizonyítás. Először is belátjuk, hogy ha az állítás igaz n-re és m-re, akkor nm-re is. Legyen adva tehát $2nm-1$ szám. Ezek közül, nézve például az első $2n-1$ számot, kiválasztható n, amelyeknek az összege osztható n-nel. Ezt az n számot félretéve, a maradékban ismét találhatunk n-et, aminek az összege osztható n-nel. Ezeket ismét félretéve, az eljárást addig folytathatjuk, amíg a megmaradt számok száma $2n-1$ alá nem csökken. Amikor ez előfordul, már $2m-1$ olyan csoportot választottunk ki, amelyek mindegyike n darab számból áll úgy, hogy összegeik az n-nel osztható $na_1, \ldots, na_{2m-1}$ számok. Ezután az állítás m-re vonatkozó esetét $a_1, \ldots, a_{2m-1}$-re alkalmazva találhatunk az $a_1, \ldots, a_{2m-1}$ számok között m-et, aminek az összege osztható m-mel. Ez az eredeti számokra azt jelenti, hogy van mn, aminek az összege osztható mn-nel.

A fenti megjegyzés miatt elég az állítást prímekre igazolni.

Legyen tehát adva a p prímszám. A következőkben ha A (különböző) mod p maradékosztályokból álló halmaz, x mod p maradékosztály, jelölje $x+A$ illetve $A+x$ az $\{x+a : a \in A\}$ halmazt, ha pedig A és B mod p maradékosztályokból álló halmazok, legyen

$$A+B = \{x+y : x \in A, y \in B\}.$$

Lemma. *Ha A, B mod p maradékosztályokból álló halmazok, $|A| = k < p$, $|B| = 2$, akkor $|A+B| \geq k+1$.*

Bizonyítás. Legyen $A = \{a_1, \ldots, a_k\}$, $B = \{b, b'\}$. Mivel $A + B$ tartalmazza a különböző $a_1 + b, \ldots, a_k + b$ maradékokat, $|A + B| \geq k$. Ha itt egyenlőség van, azaz $|A + B| = k$, az azt jelenti, hogy az $a_1 + b', \ldots, a_k + b'$ maradékok mindegyike azonos valamelyik $a_1 + b, \ldots, a_k + b$ alakú maradékkal. Másként fogalmazva, ha $Z = A + b$, akkor $b' - b$-t hozzáadva, Z önmagára képeződik. Ha viszont Z egy tetszőleges eleméhez sorra hozzáadjuk a (teljes maradékrendszert alkotó) $b' - b, 2(b' - b), \ldots, (p-1)(b' - b)$ maradékokat, akkor teljes maradékrendszert kapunk, azaz $Z = \{0, 1, \ldots, p-1\}$, $k = p$, ellentmondás.

A Tétel bizonyításához tegyük fel, hogy adottak az $a_1, \ldots, a_{2p-1}$ számok. Feltehetjük, hogy közöttük nincs p olyan, aminek azonos lenne a maradéka p-vel osztva, hiszen ekkor ezek összege p-vel osztható lenne. A számokat p-vel vett maradékaikkal helyettesítve feltehetjük, hogy

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

Legyen $A = \{a_p\}$, $B_1 = \{a_1, a_{p+1}\}, \ldots, B_{p-1} = \{a_{p-1}, a_{2p-1}\}$. Jegyezzük meg, hogy minden B_i két, mod p, különböző elemből áll, hiszen, ha például $a_1 = a_{p+1}$, akkor a fentiek szerint $a_1 = \cdots = a_{p+1}$ tehát számaink között lenne $p + 1$ kongruens, amit kizártunk.

Ezek szerint alkalmazhatjuk a Lemmát, innen indukcióval

$$|A + B_1| \geq 2, |A + B_1 + B_2| \geq 3, \ldots, |A + B_1 + \cdots + B_{p-1}| \geq p$$

adódik. Az utolsó egyenlőtlenség szerint $A + B_1 + \cdots + B_{p-1}$ tartalmaz minden mod p maradékosztályt, így a 0-t is. Vannak tehát $x, y_1, \ldots, y_{p-1}$ elemek úgy, hogy $x + y_1 + \cdots + y_{p-1} \equiv 0 \pmod{p}$ és $x \in A$, $y_1 \in B_1, \ldots, y_{p-1} \in B_{p-1}$. De ezzel készen vagyunk, mert $x, y_1, \ldots, y_{p-1}$ sorozatunk különböző elemei.

N. Zimmermantól ered a következő alternatív bizonyítás. Legyen ismét p prímszám, $a_1, \ldots, a_{2p-1}$ adott egész számok. Készítsük el az

$$S = \sum_A \left(\sum_{i \in A} a_i \right)^{p-1}$$

összeget, ahol A végigfut az $\{1, \ldots, 2p-1\}$ indexhalmaz összes p elemű részhalmazán. Ha nincs p tagú, p-vel osztható részösszeg, akkor minden A-ra a belső tag, az Euler-Fermat tétel szerint p-vel osztva 1-et ad maradékul,

tehát S maradéka p-vel osztva annyi, amennyi a lehetséges A-k számának, azaz

$$\binom{2p-1}{p} = \frac{(2p-1)\cdots(p+1)}{(p-1)!}$$

ami nem osztható p-vel, mert a számlálóban csupa p-vel nem osztható szám szorzata áll.

Másrészt vizsgáljuk meg az

$$f(x_1,\ldots,x_{2p-1}) = \sum_A \left(\sum_{i\in A} x_i\right)^{p-1}$$

polinomot.

A kiszorzásokat elvégezve az adódik, hogy $f(x_1,\ldots,x_{2p-1})$ olyan polinom, aminek minden együtthatója nemnegatív egész szám és monomjai

$$x_{i_1}^{t_1}\cdots x_{i_k}^{t_k}$$

alakúak, ahol $1 \le k \le p-1$ és $t_1+\cdots+t_k = p-1$. Egy adott A-ra ezt elvégezve a fenti szorzat kap egy valamilyen M nemnegatív egész együtthatót. Ha ezt minden A halmazra összegezzük, akkor az együttható annyiszor M lesz, ahány $i_1,\ldots,i_k$-t tartalmazó A halmaz van, azaz

$$\binom{2p-1-k}{p-k}.$$

Ez viszont mindig osztható p-vel, mivel

$$\binom{2p-1-k}{p-k} = \frac{(2p-1-k)!}{(p-k)!(p-1)!}$$

és itt a számlálóban van p-vel osztható tényező, a nevezőben pedig nincs. Ezzel készen vagyunk, hiszen azt kaptuk, hogy az $f(x_1,\ldots,x_{2p-1})$ polinom minden együtthatója osztható p-vel, ezért az $S = f(a_1,\ldots,a_{2p-1})$ szám is, ami ellentmondás.

A felhasznált lemma speciális esete a következő tételnek.

8. Tétel.(Cauchy-Davenport lemma.) *Legyen p prímszám, A, B mod p maradékosztályok nemüres halmazai. Ekkor, ha $|A|+|B| > p$, akkor $A+B$ a teljes maradékrendszer, ha pedig $|A|+|B| \le p+1$, akkor $|A+B| \ge |A|+|B|-1$.*

Bizonyítás. Először az első állítást igazoljuk. Legyen x tetszőleges mod p maradékosztály, belátjuk, hogy egy A-beli és egy B-beli maradékosztály összege. Az A és az $\{x-b : b \in B\}$ maradékrendszerek elemszámainak összege $|A|+|B| > p$, van tehát közös elemük. Azaz $a \equiv x-b \pmod p$ valamilyen $a \in A$-ra és $b \in B$-re,tehát $x \equiv a+b \pmod p$.

A második állítást $|B|$-re vonatkozó indukcióval igazoljuk. A $|B|=1$ eset nyilvánvaló: ha $B=\{b\}$, akkor $A+b$ elemszáma nyilván azonos $|A|$-vel. Tegyük fel, hogy $|B| \geq 2$.

Lemma. *Van olyan c maradékosztály, hogy ha $A' = A+c$, akkor $\emptyset \neq A' \cap B \neq B$.*

Bizonyítás. Válasszuk B-ből a különböző b, b' elemeket. Van $a \in A$, amire $a+(b'-b) \notin A$, mert, ahogy az előző lemma bizonyításánál láttuk, ha A zárt lenne a $x \mapsto x+(b'-b)$ leképezésre, akkor A tartalmazna minden mod p maradékosztályt, ami $|A| < p$ miatt kizárt. Azt állítjuk, hogy a $c \equiv b-a$ választás jó. Valóban, $A' \cap B \neq \emptyset$, mivel $b = a+(b-a)$ közös elem. Másrészt $b' \notin A' \cap B$, hiszen, ha lenne olyan $a' \in A$, amire $a'+(b-a) \equiv b'$ teljesülne, akkor $a' \equiv a+(b'-b)$ lenne, amit kizártunk.

Mivel $|A'| = |A|$ és $|A'+B| = |A+B|$, elég belátni, hogy $|A'+B| \geq |A'|+|B|-1$.

Legyen $A^* = A' \cup B$, $B^* = A' \cap B$. Ekkor, a szita-formula alapján $|A^*|+|B^*| = |A'|+|B|$. Nyilván $A^*+B^* \subseteq A'+B$ és A^*, B^* nemüres halmazok, továbbá $|B^*| < |B|$. Ezért, mivel $|B|$-re vonatkozó indukciót használunk, $|A^*+B^*| \geq |A^*|+|B^*|$. Ezzel készen vagyunk, mert

$$|A'+B| \geq |A^*+B^*| \geq |A^*|+|B^*|-1 = |A'|+|B|-1.$$

Megfogalmazhatunk, legalábbis prímmodulus esetére, a 7. Tételnek egy olyan általánosítását, ami az 6. Tételhez hasonló állítást ad: ha p prím és a $\mathbf{Z}_p \times \mathbf{Z}_p$ Abel-csoportban (tehát a p elemű ciklikus csoport két példányának direkt szorzatában) veszünk $2p-1$ elemet, akkor ezek közül néhány összege a $(0,0)$ elem. Az említett direkt szorzat elemei (x,y) alakú vektorok, ahol x, y mod p maradékosztályok. Két ilyen vektort természetesen koordinátánként adunk össze, a mod p számolás szabályai szerint. A fenti állítás valóban tartalmazza az Erdős-Ginzburg-Ziv tétel mod p esetét: ha $a_1, \ldots, a_{2p-1}$ mod p maradékosztályok, akkor készítsük el a $\mathbf{b}_1 = (1,a_1), \ldots, \mathbf{b}_{2p-1} = (1,a_{2p-1}) \in \mathbf{Z}_p \times \mathbf{Z}_p$ vektorokat. Ha ezek közül valahány összege a $(0,0)$ nullvektor, akkor

ezek k száma az első koordinátát figyelembe véve csak p-vel osztható lehet, de mivel $k \leq 2p-1$, csak $k = p$ jöhet szóba.

9. Tétel. (J. E. Olson) *Ha az r tényezős $\mathbf{Z}_p \times \cdots \times \mathbf{Z}_p$ csoportban kiválasztunk $r(p-1)+1$ (nem feltétlenül különböző) elemet, akkor ezek közül néhány összege a $(0,\ldots,0)$ nullvektor.*

Bizonyítás. Először megjegyezzük, hogy a tételbeli korlát éles: ha vesszük azt a rendszert, ami az

$$(1,0,\ldots,0),(0,1,\ldots,0),\ldots,(0,\ldots,1)$$

báziselemek mindegyikét $(p-1)$-szer tartalmazza, akkor nem tudunk úgy elemeket kiválasztani, hogy összegük a $(0,\ldots,0)$ vektor legyen.

Jelölje G a $\mathbf{Z}_p \times \cdots \times \mathbf{Z}_p$ csoportot, a csoportműveletet multiplikatívan írva, tehát G a $g = g_1^{i_1} \ldots g_r^{i_r}$ elemekből áll, ahol $0 \leq i_1,\ldots,i_r < p$ és két elem összeszorzásánál a kitevőket mod p redukáljuk.

Szükségünk lesz G-nek a $\mathbf{Z}_p$ fölötti csoportalgebrájára. Ennek a gyűrűnek az elemei a formális

$$\sum_{g \in G} k_g g$$

alakú összegek, ahol minden g-re k_g egy mod p maradékosztály. Két ilyen formális összeget tagonként adunk össze, a k_g együtthatókat mod p redukálva. Szorzásnál a csoportelemeket a csoportbeli szorzással szorozzuk össze és természetesen figyelembe vesszük a disztributivitást. Jelöljük a gyűrűt R-rel.

1. Lemma *Ha $g \in G$, akkor*

$$(1-g)^p = 0.$$

Bizonyítás. Kiszorozva

$$(1-g)^p = 1 - \binom{p}{1} g + \binom{p}{2} g^2 \cdots + \binom{p}{p-1} g^{p-1} - g^p.$$

Itt a közbülső tagok együtthatói p-vel oszthatóak, tehát az R gyűrű számolási szabályai szerint nullák. Marad $1 - g^p$ ami nulla, mivel $g^p = 1$. □

2. Lemma *Ha $u_1,\ldots,u_n \in R$, akkor*

$$1 - u_1 \cdots u_n = h_1(1-u_1) + \cdots + h_n(1-u_n)$$

alkalmas $h_1, \ldots, h_n \in R$ elemekre.

Bizonyítás.

$$1 - u_1 \cdots u_n = (1 - u_1) + u_1(1 - u_2) + u_1u_2(1 - u_3) + \cdots + u_1 \cdots u_{n-1}(1 - u_n).$$

□

3. Lemma. *Ha $a_1, \ldots, a_{r(p-1)+1} \in G$, akkor*

$$(1 - a_1) \cdots (1 - a_{r(p-1)+1}) = 0.$$

Bizonyítás. A 2. Lemma szerint minden a_i-ra

$$1 - a_i = \sum_{j=1}^{r} h_j(1 - g_j)$$

alakban írható, ahol $g_1, \ldots, g_r$ a G csoport generátorai és $h_1, \ldots, h_r \in R$. Ezután kiszorozva az $(1 - a_1) \cdots (1 - a_{r(p-1)+1})$ szorzatot olyan összeget kapunk, ahol minden tag

$$h(1 - g_1)^{i_1} \cdots (1 - g_r)^{i_r}$$

alakú, ahol $h \in R$, az $i_1, \ldots, i_r$ kitevők összege pedig $r(p-1)+1$. Ez utóbbi csak úgy lehet, ha valamelyik i_j kitevőre $i_j \geq p$ teljesül, de ekkor az 1. lemma miatt $(1 - g_j)^{i_j} = 0$, ezért az egész szorzat 0.

A tétel bizonyításához szorozzuk ki a 3. Lemmában szereplő szorzatot:

$$(1 - a_1) \cdots (1 - a_{r(p-1)+1}) = 1 - (a_1 + \cdots + a_{r(p-1)+1}) + (a_1a_2 + \cdots) - \cdots .$$

Itt a jobboldalon R olyan elemei szerepelnek, amelyek

$$a_{i_1} \cdots a_{i_k} \quad (i_1 < \cdots < i_k)$$

alakban írhatók, tehát az $a_1 \cdots a_{r(p-1)+1}$ szorzat részszorzatai ($\pm$ előjelekkel). számolási szabályaink szerint ez az összeg csak akkor lehet nulla, ha az 1 tagot másik tag (vagy tagok) kiejti, azaz $1 = a_{i_1} \cdots a_{i_k}$ alkalmas $1 \leq k \leq r(p-1)+1$-re.

Irodalom

[1] N. Alon, M. Dubiner: Zero-sum subsets of prescribed size, **Combinatorics, Paul Erdős is Eighty**, (Vol. 1), Keszthely, 1993, 33–50.

[2] A.-L. Cauchy: Recherches sur les nombres, *J. Ecole Polytechniques*, **9**(1813), 99–123.

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

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

[5] J. E. Olson: A combinatorial problem on finite abelian groups, I, *Journal of Number Theory*, **1**(1969), 8–10.

A Fibonacci számok gyors kiszámítása

Egy érdekes trükkel gyorsan hatványozhatunk természetes számokat.

10. Tétel. *Tetszőleges természetes szám n-edik hatványra emelhető $O(\log n)$ szorzással.*

Bizonyítás. Ha a^n-t a kiszámítandó hatvány, akkor ismételt négyzetreemelésekkel egyre nagyobb hatványait számítjuk ki, majd ezekből szorzással kapjuk a kívánt számot. Legyen tehát

$$n = 2^{k_r} + 2^{k_{r-1}} + \cdots + 2^{k_0},$$

ahol $k_r > \cdots > k_0$. Ismételt négyzetreemelésekkel kiszámítjuk $a, a^2, \cdots, a^{2^{k_r}}$-et, majd az így kapott hatványokból kiszorozzuk a^n-et:

$$a^n = a^{2^{k_r}} \cdot 2^{2^{k_{r-1}}} \cdot \cdots \cdot a^{2^{k_0}}.$$

A négyzetreemelések száma k_r a szorzásoké r, mindkettő legfeljebb akkora, mint n (2-es alapú) logaritmusa. □

Meg lehet jegyezni, hogy programozási szempontból kissé illuzórikus két szám összeszorzását *mindig* egy lépésnek nevezni, hiszen például többmillió jegyű számoriásoknál a szorzás végrehajtása (sőt már a számok tárolása

is) jelentős gondokat okozhat. Abban az esetben mégis hasznos az algoritmus, amikor a kapott számok mindig egy korlát alatt maradnak: amikor egy valamilyen m modulusra vett maradékokkal dolgozunk.

Nézzük most meg, hogan lehet számolni a Fibonacci-sorozat tagjait! A szokásos módon, a Fibonacci-sorozat hogy definíciója az, hogy $F_0 = 0$, $F_1 = 1$ és a nagyobb indexű tagokra $F_{n+1} = F_n + F_{n-1}$.

11. Tétel. *F_n kiszámítható $O(\log n)$ szorzással.*

Bizonyítás. Bármennyire is különös, az n-edik Fibonacci-számot előállíthatjuk n-edik hatványként, ha nem is számként, de mátrixként.

Indukcióval könnyen igazolható a következő képlet:

$$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}^n = \begin{bmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{bmatrix}.$$

Mivel két 2×2-s mátrix összeszorzása végrehajtható nyolc szorzással (és négy összeadással) a baloldali hatvány kiszámítható az előző tételhez hasonló módon $O(\log n)$ szorzással. □

Négyzetgyökvonás gyorsan

A négyzetgyökvonásra jól ismert egy kvadratikus közelítő algoritmus (tulajdonképpen Newton gyökközelítő eljárása).

Tegyük fel, hogy $\sqrt{d}$-t akarjuk kiszámítani, ahol d olyan természetes szám, ami nem négyzetszám. Legyen $M = [\sqrt{d}]$, és készítsük el a következő sorozatot:

$$c_0 = M + 1$$

és, ha $n \geq 0$, akkor legyen

$$c_{n+1} = \frac{1}{2}\left(c_n + \frac{d}{c_n}\right).$$

Nyilván

$$c_0 > c_1 > c_2 \cdots > \sqrt{d}.$$

Tehát c_n felülről konvergál egy számhoz, ami csak $\sqrt{d}$ lehet. Ez a konvergencia kvadratikus:

$$c_{n+1} - \sqrt{d} = \frac{1}{2}\left(c_n - 2\sqrt{d} + \frac{d}{c_n}\right) = \frac{1}{2}\frac{(c_n - \sqrt{d})^2}{c_n} < \frac{1}{2M}(c_n - \sqrt{d})^2.$$

Ha kiírjuk a fenti $c_0, c_1, \ldots$ sorozatra, mint $c_n = a_n/b_n$ racionális számokra a rekurziót, akkor

$$a_{n+1} = a_n^2 + db_n^2, \qquad b_{n+1} = 2a_n b_n$$

adódik. Ezt úgy is írhatjuk, hogy

$$a_n - b_n\sqrt{d} = (a_0 - b_0\sqrt{d})^{2^n} = (M + 1 - \sqrt{d})^{2^n},$$

ahol a jobboldalon egy 0 és 1 közötti valós szám 2^n-edik hatványa áll, ami persze kvadratikusan tart 0-hoz.

Még egy kicsit átalakítva ezt az okoskodást, azt mondhatjuk, hogy a

$$\begin{bmatrix} a_n & b_n \\ db_n & a_n \end{bmatrix} = \begin{bmatrix} M+1 & 1 \\ d & M+1 \end{bmatrix}^{2^n}$$

mátrixot számítjuk ki ismételt négyzetreemeléssel, és ekkor lényegében visszajutottunk a a Fibonacci számok gyors kiszámítására adott érveléshez.

Fermat kis tétele a Fibonacci sorozatra

A skatulyaelv egyik jólismert alkalmazása az az állítás, hogy minden k pozitív egész számra van a Fibonacci sorozatnak olyan tagja, ami osztható k-val.

Az is könnyen belátható, hogy van olyan $d(k)$ érték, hogy k pontosan akkor osztója F_n-nek, ha $d(k)$ osztja n-et. Kérdés, mit mondhatunk erről a $d(k)$ számról. A pontos meghatározás persze nem várható, de talán a prímszámok esetén Fermat kis tételéhez hasonlóan adhatunk egy olyan értéket, aminek az adott szám mindig osztója.

Nézzük meg az első néhány p prímszámra $d(p)$ értékét!

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43
$d(p)$	3	4	5	8	10	7	9	18	24	14	30	19	20	44

Ebből látszik, hogy $p > 5$-re p mindig osztója F_{p-1}, F_{p+1} valamelyikének. A pontos feltételt az alábbi tétel tartalmazza.

12. Tétel. *Ha $p \neq 5$ páratlan prímszám, akkor $p|F_{p-1}$ ha $p \equiv \pm 1 \pmod 5$ és $p|F_{p+1}$ ha $p \equiv \pm 3 \pmod 5$.*

Bizonyítás. Írjuk fel F_n explicit alakját:

$$F_n = \frac{1}{\sqrt{5}}\left(\alpha^n - \beta^n\right),$$

ahol

$$\alpha = \frac{1+\sqrt{5}}{2}, \quad \beta = \frac{1-\sqrt{5}}{2} < 0,$$

Ezekről a számokról még tudjuk, hogy

$$\alpha + \beta = 1, \quad \alpha\beta = -1, \quad \alpha - \beta = \sqrt{5}.$$

A Fibonacci-sorozatos példák megoldásával kapcsolatos rutin azt sugallja, hogy a fenti, irracionális számokat alkalmazó képlet nem alkalmazható osztthatósági állítások igazolására. Ez azonban nincs így.

Legyen $p \neq 5$ páratlan prímszám. Először kiszámítjuk F_p p-vel vett maradékát. Felírva a képletet és az egymást kioltó tagokat kihagyva a következőt adódik.

$$F_p = \frac{(1+\sqrt{5})^p - (1-\sqrt{5})^p}{\sqrt{5}2^p} = \frac{2}{\sqrt{5}2^p}\left(\binom{p}{1}\sqrt{5} + \binom{p}{3}\sqrt{5}^3 + \cdots + \sqrt{5}^p\right) =$$

$$= \frac{2}{2^p}\left(\binom{p}{1} + 5\binom{p}{3} + \cdots + 5^{\frac{p-1}{2}}\right).$$

Az utolsó zárójelben egy kivételével csupa p-vel osztható tagunk van. Ezért azt kapjuk, hogy F_p, ami egész szám, olyan tört alakjában írható, aminek nevezője, Fermat kis tétele miatt, p-vel osztva 2-t ad maradékul, számlálója pedig annyit, mint

$$2 \cdot 5^{\frac{p-1}{2}}.$$

Innen adódik, hogy $F_p \equiv 5^{\frac{p-1}{2}} \pmod{p}$. Ezt viszont ki tudjuk számolni: a Legendre-szimbólummal kapcsolatos Euler-lemmából és a kvadratikus reciprocitás tételéből adódik, hogy

$$5^{\frac{p-1}{2}} \equiv \left(\frac{5}{p}\right) \equiv \left(\frac{p}{5}\right) \pmod{p}$$

ez pedig 1, ha $p \equiv \pm 1 \pmod 5$ és -1, ha $p \equiv \pm 2 \pmod 5$.

Ezután kiszámítjuk az $F_{p-1} + F_{p+1}$ összeg p-vel vett maradékát.

$$F_{p-1}+F_{p+1}=\frac{1}{\alpha-\beta}\left(\alpha^p\underbrace{\left(\alpha+\frac{1}{\alpha}\right)}_{\alpha-\beta}-\beta^p\underbrace{\left(\beta+\frac{1}{\beta}\right)}_{\beta-\alpha}\right)=\alpha^p+\beta^p$$

felhasználva $\alpha\beta=-1$-et.
Ez a fentihez hasonlóan kifejthető:

$$=\frac{2}{2^p}\left(1+\binom{p}{2}5+\binom{p}{4}5^2+\cdots\right)$$

Itt megint a p-vel vett maradékot véve, adódik, hogy $F_{p-1}+F_{p+1}\equiv 1 \pmod p$. Ezzel készen is vagyunk, hiszen, ha $p\equiv\pm1 \pmod 5$, akkor egyrészt $F_p\equiv 1 \pmod p$, másrészt $F_{p-1}+F_{p+1}\equiv 1 \pmod p$ is igaz, de ez úgy is írható, hogy $1\equiv F_{p-1}+F_{p+1}=2F_{p-1}+F_p\equiv 2F_{p-1}+1 \pmod p$, azaz $F_{p-1}\equiv 0 \pmod p$. Hasonlóképpen kezelhető a $p\equiv\pm2 \pmod 5$ eset is. □

Generátorfüggvények

Kongruenciák egy

$$x\equiv a_1 \pmod{m_1}$$
$$\cdots$$
$$x\equiv a_n \pmod{m_n}$$

rendszerét *lefedő*nek nevezünk, ha minden természetes szám kielégíti legalább az egyiket. Akkor viszont, ha minden természetes szám legfeljebb az egyiket oldja meg, *idegen* kongruencia-rendszerről beszélünk. Erdős Pál 1950-ben sejtette, hogy egy különböző modulusokkal rendelkező kongruencia-rendszer nem lehet egyszerre lefedő és idegen is (persze feltesszük, hogy legalább 2 kongruenciából áll).

13. Tétel. (L. Mirsky, D. J. Newman, H. Davenport, R. Rado) *Különböző modulusokkal rendelkező (véges) kongruencia-rendszer nem lehet egyszerre lefedő és idegen.*

Bizonyítás. Tegyük fel, hogy az $x\equiv a_1 \pmod{m_1},\ldots,x\equiv a_n \pmod{m_n}$ rendszer ellenpélda. Feltehetjük, hogy $0\le a_t<m_t$ minden $1\le t\le n$-re. Ekkor, ha összeadjuk az x változó azon hatványait, amelyek kitevői egy adott $x\equiv a_t \pmod{m_t}$ kongruenciát kielégítenek, az

$$x^{a_t}+x^{a_t+m_t}+x^{a_t+2m_t}+\cdots=x^{a_t}\frac{1}{1-x^{m_t}}$$

sort kapjuk. Ha ezeket összeadjuk, a feltevés szerint x minden nemnegatív egész kitevős hatványát pontosan egyszer kapjuk meg, azaz

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + \cdots = x^{a_1}\frac{1}{1-x^{m_1}} + \cdots + x^{a_n}\frac{1}{1-x^{m_n}}.$$

Mondhatjuk persze, hogy ez, mint képlet persze igaz, de vajon konkrét behelyettesítéskor mikor teljesül. Mint általában sorok átrendezéseinél, a fenti egyenlőség teljesülni fog, ha a fenti sor abszolút konvergens, ami példánkban akkor igaz, ha $|x| < 1$. És x valós. Vagy *komplex*. És itt jön az ötlet, ugyanis a komplex számok között már tudunk olyat találni, amelyre ez nem teljesülhet.

Legyen a modulusok között mondjuk m_n a legnagyobb, ω pedig az ,,első" m_n-edik egységgyök, azaz

$$\omega = \cos\left(\frac{2\pi}{m_n}\right) + i\sin\left(\frac{2\pi}{m_n}\right).$$

Ha 0-ból a sugár mentén tartunk ω-hoz, akkor a baloldal $1/(1-\omega)$-hoz konvergál.

A jobboldal tagjai közül az utolsót kivéve mindegyik a megfelelő konkrét komplex számhoz, azaz a t-edik $1/(1-\omega^{m_t})$-hoz konvergál. (Mivel $\omega^{m_t} \neq 1$, ha $t = 1, \ldots, n-1$ itt nincs semmi baj.) Az utolsó azonban ,,felrobban", $1/(1-x^{m_n})$ végtelenhez tart, ha $x \to \omega$, ez viszont ellentmondás, hiszen két egyenlő kifejezés közül csak az egyik végtelenhez nem tarthat. □

14. Tétel. *A nemnegatív egészek halmaza pontosan egyféleképpen bontható két halmazra, A-ra és B-re úgy, hogy minden nemnegatív egész ugyanannyi féleképpen írható két különböző A-beli szám öszegeként, mint két különböző B-beli öszegeként.*

Bizonyítás. Tegyük fel, hogy $0 \in A$, $0 \notin B$. Legyen A illetve B generátorfüggvénye $f(x)$ és $g(x)$ tehát

$$f(x) = \sum_{a\in A} x^a = 1 + \cdots, \quad g(x) = \sum_{b\in B} x^b = x + \cdots.$$

Mivel partícióról van szó,

$$f(x) + g(x) = 1 + x + x^2 + x^3 + \cdots = \frac{1}{1-x}$$

Ha $f(x)^2$-et sorba fejtjük, akkor egy x^n tag együtthatója az $n = a + a'$ $(a, a' \in A)$ egyenlet megoldásainak száma. Ha olyan hatványsort akarunk, ahol x^n együtthatója annyi, ahányféleképpen n-et két különböző A-beli szám összegeként tudjuk előállítani, akkor az

$$f(x)^2 - \sum_{a \in A} x^{2a} = f(x)^2 - f(x^2)$$

sort kell vennünk.

A tétel feltétele tehát így fogalmazható:

$$f(x)^2 - f(x^2) = g(x)^2 - g(x^2)$$

azaz

$$f(x)^2 - g(x)^2 = f(x^2) - g(x^2).$$

A baloldal így alakítható:

$$f(x)^2 - g(x)^2 = (f(x) - g(x))(f(x) + g(x)) = (f(x) - g(x))\frac{1}{1-x}.$$

Felszorozva a fenti egyenlőség így alakíthtató:

$$f(x) - g(x) = (1 - x)(f(x^2) - g(x^2)).$$

Itt x helyébe x^2-et helyettesítve és visszaírva azt kapjuk, hogy

$$f(x) - g(x) = (1 - x)(f(x^2) - g(x^2)) = (1 - x)(1 - x^2)(f(x^4) - g(x^4)),$$

amit folytathatunk,

$$f(x) - g(x) = (1 - x)(1 - x^2) \cdots (1 - x^{2^t})(f(x^{2^{t+1}}) - g(x^{2^{t+1}})).$$

Ha t értéke egyre nagyobb, az $(f(x^{2^{t+1}}) - g(x^{2^{t+1}}))$ tényező az 1 főtagon kívül csak olyan tagokból áll amelyekben x legalább a 2^{t+1}-edik hatványon van. Ezért igaz lesz az

$$f(x) - g(x) = (1 - x)(1 - x^2)(1 - x^4) \cdots$$

előállítás. Ebből nagyon könnyen kiolvasható, hogy $f(x) - g(x)$-ben mennyi lesz egy adott n-re x^n együtthatója: ha n kettes számrendszerbeli előállítása

$$n = 2^{k_t} + \cdots + 2^{k_1}, \quad k_t > \cdots > k_1,$$

akkor x^n-t csak úgy kaphatjuk, ha az $(1-x^{2^{k_t}}),\dots(1-x^{2^{k_1}})$ tényezőkből a második tagot, a többiből az elsőt vesszük, azaz x^n együtthatója $(-1)^t$ lesz.

Ebből az adódik, hogy A pontosan azokat a számokat tartalmazza, amelyek kettedes előállításában a jegyek összege (tehát az 1-esek száma) páros, B azokat, amelyekben páratlan. Megkaptuk tehát, hogy csak egy felbontása lehet a természetes számoknak, ami kielégíti a feltételeket. De ez meg is felel, hiszen, ha

$$f(x)-g(x)=(1-x)(1-x^2)(1-x^4)\cdots$$

akkor nyilván

$$f(x)-g(x)=(1-x)(f(x^2)-g(x^2))$$

és a fenti okoskodás megfordítható. □

Irodalom

[1] D. J. Newman: *Analytic Number Theory*, Springer, 1998.

A kvadratikus reciprocitás tétele

A Legendre-szimbólummal kapcsolatban használni fogjuk Euler észrevételét:

$$\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}} \pmod p.$$

15. Tétel. *Ha $p\neq q$ páratlan prímszámok, akkor*

$$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Bizonyítás. Legyen

$$\Phi=\Big\{1\le k\le\frac{pq-1}{2}:(k,pq)=1\Big\}.$$

Legyen továbbá A a Φ-beli maradékosztályok szorzata modulo pq.

1. Lemma. $A\equiv\pm1 \pmod{pq}$ *akkor és csak akkor, ha* $p\equiv q\equiv 1 \pmod 4$.

Bizonyítás. Először is jegyezzük meg, hogy a mod pq redukált maradékrendszer minden x eleme esetén x és $-x$ közül pontosan az egyik van Φ-ben.

Ezért, minden $a \in \Phi$ maradék esetén van pontosan egy $a' \in \Phi$, hogy $aa' \equiv \pm 1 \pmod{pq}$. Az $a \mapsto a'$ hozzárendelés párokba osztja Φ elemeit, ekkor

$$\Psi = \left\{ a \in \Phi : a^2 \equiv \pm 1 \pmod{pq} \right\}$$

azoknak az elemeknek a halmaza, amik önmagukkal alkotnak párt. Ezért a Φ-beli maradékosztályok A szorzatára igaz, hogy $A \equiv \pm B \pmod{pq}$, ahol B a Ψ-beli maradékosztályok szorzata.

B kiszámításához tegyük fel először, hogy $p \equiv q \equiv 1 \pmod 4$. $x^2 \equiv 1 \pmod{pq}$ gyökei $\pm 1, \pm N$ alakúak egy bizonyos N maradékosztályra, $x^2 \equiv -1 \pmod{pq}$ gyökei pedig $\pm I, \pm NI$ alakúak a fenti N és egy I maradékosztály segítségével. Itt a Φ-be esők szorzatát kell venni, tehát minden $\pm$ pár közül az egyiket, ez $\pm(1 \cdot N \cdot I \cdot NI) = \mp 1$ lesz pq-val osztva.

Tegyük most fel, hogy p és q közül nem mindkettő ad 1-et maradékul 4-gyel osztva. Ekkor Ψ csak $x^2 \equiv 1 \pmod{pq}$ gyökeit tartalmazza, tehát, mint az előbb, 1 és -1 közül az egyiket és N és $-N$ közül az egyiket. B, ezek szorzata, $\pm(1 \cdot N) \neq \pm 1$ lesz pq-val osztva.

2. Lemma. *$A \equiv (-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) \pmod p$ és $A \equiv (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) \pmod q$.*

Bizonyítás. Szimmetria okokból elég az első állítást igazolni. A-nak p-vel vett maradékát $\frac{B}{C}$ alakban állíthatjuk elő, ahol B az összes, p-vel nem osztható szám szorzatának p-vel vett maradéka 1-től $\frac{pq-1}{2}$-ig, C pedig ezek közül a q-val oszthatók szorzatának. Mivel $\frac{pq-1}{2} = p\frac{q-1}{2} + \frac{p-1}{2}$, B előáll, mint $\frac{q-1}{2}$ teljes redukált maradékrendszert alkotó szám szorzata és még egy redukált maradékrendszer fele, azaz $1 \cdot \dots \cdot \frac{p-1}{2}$. Az előbbi faktorok szorzata Wilson tétele miatt $(-1)^{\frac{q-1}{2}}$-t ad p-vel osztva. Annyit kaptunk tehát, hogy

$$B \equiv (-1)^{\frac{q-1}{2}} \left(\frac{p-1}{2}\right)! \pmod p.$$

C egyszerűen felírható:

$$C = q \cdot (2q) \cdots \left(q\frac{p-1}{2}\right) \equiv q^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod p$$

és itt Euler tétele miatt $q^{\frac{p-1}{2}} \equiv \left(\frac{q}{p}\right) \pmod p$. □

A két lemmából már könnyen befejezhetjük a tétel bizonyítását. Ha $p \equiv q \equiv 1 \pmod 4$, akkor az A szám pq-val osztva 1-et vagy -1-et ad, továbbá

p-vel vett maradéka $(-1)^{\frac{q-1}{2}}\left(\frac{q}{p}\right)$ míg q-val vett maradéka $(-1)^{\frac{p-1}{2}}\left(\frac{p}{q}\right)$. Ez csak úgy lehet, ha e két utóbbi szám azonos.

Ha pedig p és q valamelyike 3-mal kongruens modulo 4, akkor A p-vel és q-val vett maradékainak értéke nem lehet azonos, hiszen akkor a közös érték, ami csak 1 vagy -1 lehet, szükségképpen A pq-val vett maradéka is lenne, ellentmondva az 1. Lemmának.

Véges testekre vonatkozó ismeretekkel másik bizonyítás is adható.

2. bizonyítás. Vegyük az $F = \mathrm{GF}(p^{q-1})$ testet, ez tehát p^{q-1} elemű és minden elem önmagával vett p-szeres összege 0. Innen, a binomiális tétel segítségével adódik, hogy ha a, b a test elemei, akkor

$$(a+b)^p = a^p + b^p.$$

Egy fontos tétel szerint a test multiplikatív csoportja ciklikus, van tehát olyan ω eleme, amire

$$\omega^{p^{q-1}-1} = 1,$$

de minden kisebb kitevős hatványa 1-től különböző. Legyen

$$f = \frac{p^{q-1}-1}{q},$$

ez Fermat kis tétele miatt egész szám. Ha most $\xi = \omega^f$, akkor ξ rendje pontosan q. Ezért $1 + \xi + \cdots + \xi^{q-1} = 0$.

Legyen

$$G = \sum_{j=1}^{q-1} \left(\frac{j}{q}\right) \xi^j.$$

1. Lemma. $G^2 = (-1)^{\frac{q-1}{2}} q$.

Bizonyítás. A $G \cdot G$ szorzatban a második tényezőben j helyett $-k$ szerint összegezve:

$$\begin{aligned} G^2 &= \left(\sum_{j=1}^{q-1} \left(\frac{j}{q}\right)\xi^j\right)\left(\sum_{k=1}^{q-1}\left(\frac{-k}{q}\right)\xi^{-k}\right) \\ &= \sum_{j=1}^{q-1}\sum_{k=1}^{q-1}\left(\frac{j}{q}\right)\xi^j\left(\frac{-k}{q}\right)\xi^{-k} = \left(\frac{-1}{q}\right)\sum_{j=1}^{q-1}\sum_{k=1}^{q-1}\left(\frac{jk}{q}\right)\xi^{j-k} \end{aligned}$$

adódik. Ha k helyett jn-et írunk, akkor ez

$$\left(\frac{-1}{q}\right)\sum_{j=1}^{q-1}\sum_{n=1}^{q-1}\left(\frac{j^2n}{q}\right)\xi^{j(1-n)} = (-1)^{\frac{q-1}{2}}\sum_{n=1}^{q-1}\left(\frac{n}{q}\right)\sum_{j=1}^{q-1}\xi^{j(1-n)}$$

alakban írható, és itt a belső összeg $n = 1$-re $q-1$, egyébként pedig -1. Ezért a szereplő kettős összeg így alakítható tovább:

$$(q-1) + (-1)\sum_{n=2}^{q-1}\left(\frac{n}{q}\right) = (q-1)+1 = q,$$

hiszen

$$\sum_{n=1}^{q-1}\left(\frac{n}{q}\right) = 0.$$

□

A Lemmából adódik, hogy

$$G^p = (G^2)^{\frac{p-1}{2}}G$$

$$= \left((-1)^{\frac{q-1}{2}}q\right)^{\frac{p-1}{2}}G = (-1)^{(p-1)(q-1)/4}q^{(p-1)/2}G = (-1)^{(p-1)(q-1)/4}\left(\frac{q}{p}\right)G$$

mivel F-ben p többszöröseit elhagyhatjuk.

Ezt a hatványt kiszámíthatjuk úgy is, hogy felhasználjuk, hogy F-ben szabad tagonként p-edik hatványra emelni:

$$G^p = \sum_{j=1}^{q-1}\left(\frac{j}{q}\right)\xi^{jp} = \sum_{j=1}^{q-1}\left(\frac{p}{q}\right)\left(\frac{pj}{q}\right)\xi^{jp}.$$

Átcserélve az indexelést $k = jp$-re ez

$$\left(\frac{p}{q}\right)\sum_{k=1}^{q-1}\left(\frac{k}{q}\right)\xi^k = \left(\frac{p}{q}\right)G.$$

Azaz

$$(-1)^{(p-1)(q-1)/4}\left(\frac{q}{p}\right)G = \left(\frac{p}{q}\right)G$$

és mivel G nyilván nem 0 (hiszen a Lemma szerint négyzete sem 0), G-vel egyszerűsíthetünk és adódik a tétel. □

Irodalomjegyzék

[1] S.Y. Kim: An elementary proof of the quadratic reciprocity law, *American Math. Monthly*, **111**(2004), 48–50.
[2] George Rousseau: On the quadratic reciprocity law, *Journal of Australian Math. Soc.*, **51**(1991), 423–425.

Prímszámok előállítása két négyzetszám összegeként

Jól ismert, sok helyen szereplő az a Fermat-tól eredő, először Euler által igazolt tétel, hogy minden $p = 4n + 1$ alakú prímszám két négyzetszám összege. Ennél jóval többet igazolt Gauss, ő ugyanis pontosan meg tudta mondani mi az a két négyzetszám.

16. Tétel. *Ha $p = 4n + 1$ prím, akkor $p = A^2 + B^2$, ahol A és B $\binom{2n-1}{n-1}$ illetve $(2n)!\binom{2n-1}{n-1}$ legkisebb abszolút értékű maradéka mod p.*

Ennek egy Jacobstahltól eredő bizonyítását adjuk.

1. Lemma. *Ha p prímszám, $k > 0$ nem osztható $p-1$-gyel, akkor*

$$1^k + \cdots + (p-1)^k \equiv 0 \pmod{p}.$$

Bizonyítás. Feltehetjük, hogy $0 < k < p - 1$. Legyen g primitív gyök mod p, ekkor a vizsgált összeg

$$g^k + g^{2k} + \cdots + g^{(p-1)k} = g^k \frac{g^{(p-1)k} - 1}{g^k - 1} \equiv 0 \pmod{p}.$$

□

2. Lemma. *Ha a $p > 2$ prím nem osztja a-t, akkor*

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

Bizonyítás. Az Euler-lemma szerint kifejtve

$$\sum_{x=1}^{p} (x^2 + a)^{\frac{p-1}{2}} = \sum_{x=1}^{p} \left(x^{p-1} + \frac{p-1}{2} x^{p-3} a + \cdots + a^{\frac{p-1}{2}} \right) \equiv -1 \pmod{p}$$

felhasználva az 1. Lemmát. Az összeg nyilván páratlan (mivel x és $-x$ azonos értékű tagot ad) továbbá az abszolút értéke legfeljebb p. Innen már adódik, hogy az összeg pontosan -1. □

A továbbiakban $a = 1, \ldots, p$-re legyen

$$f(a) = \sum_{x=1}^{p} \left(\frac{x}{p}\right)\left(\frac{x^2 - a}{p}\right).$$

3. Lemma. *Ha a és b mindketten kvadratikus maradékok vagy pedig mindketten kvadratikus nemmaradékok, akkor $f(a) = \pm f(b)$.*

Bizonyítás. Ekkor $a \equiv br^2 \pmod{p}$ alkalmas $1 \leq r \leq p-1$-re, innen

$$f(a) = \sum_{x} \left(\frac{x}{p}\right)\left(\frac{x^2 - br^2}{p}\right) = \left(\frac{r}{p}\right) \sum_{y} \left(\frac{y}{p}\right)\left(\frac{y^2 - b}{p}\right) = \left(\frac{r}{p}\right) f(b)$$

ahol az $x \equiv yr$ helyettesítést végeztük el. □

Ha $f(a)$-t négyzetreemeljük, akkor a következőt kapjuk:

$$\sum_{x}\sum_{y} \left(\frac{xy}{p}\right)\left(\frac{(a-x^2)(a-y^2)}{p}\right) = \sum_{x}\sum_{y} \left(\frac{xy}{p}\right)\left(\frac{a^2 - a(x^2+y^2) + x^2y^2}{p}\right)$$

Ha ezeket $a = 1, \ldots, p$-re összeadjuk, a következőt kapjuk:

$$\sum_{x}\sum_{y}\sum_{a} \left(\frac{xy}{p}\right)\left(\frac{\left(a - \frac{x^2+y^2}{2}\right)^2 - \left(\frac{x^2-y^2}{2}\right)^2}{p}\right)$$

Ha itt most a belső összegben végrehajtjuk a következő helyettesítést:

$$b = a - \frac{x^2 + y^2}{2}$$

akkor ez adódik:

$$\sum_{x}\sum_{y} \left(\frac{xy}{p}\right) \sum_{b} \left(\frac{b^2 - \left(\frac{x^2-y^2}{2}\right)^2}{p}\right).$$

Itt a belső összeg $p-1$, ha $x \equiv \pm y \pmod p$, egyébként, a 2. Lemma szerint, -1. Innen adódik, hogy

$$\sum_{a=1}^{p} f^2(a) = 2p(p-1).$$

Itt

$$f(p) = \sum_{x=1}^{p-1} \left(\frac{x}{p}\right) = 0,$$

a többi tag közül $\frac{p-1}{2}$ $f(1)^2$-tel, $\frac{p-1}{2}$ pedig $f(n)^2$-tel azonos, ahol n tetszőleges kvadratikus nemmaradék mod p. Azaz

$$2p(p-1) = \frac{p-1}{2}\big(f(1)^2 + f(n)^2\big)^2,$$

tehát $p = A^2 + B^2$, ahol

$$A \equiv \frac{1}{2}\sum \left(\frac{x}{p}\right)\left(\frac{x^2-1}{p}\right) \pmod p.$$

Ismét az Euler-lemmát alkalmazva (ne felejtsük, $p = 4n+1$)

$$2A \equiv \sum_{x=1}^{p-1} x^{2n}\big(x^2-1\big)^{2n} = \sum_{x=1}^{p-1}\left(x^{6n} - \cdots + (-1)^n\binom{2n}{n}x^{4n} + \cdots\right)$$

ez pedig az 1. Lemmát alkalmazva $(-1)^{n+1}\binom{2n}{n}$-nel kongruens.

Ha A értékét ismerjük, akkor B-ét is, hiszen ekkor $B \equiv xA \pmod p$ lehet csak, ahol x az $x^2+1 \equiv 0 \pmod p$ kongruencia megoldása. Ez viszont $x \equiv \pm(2n)! \pmod p$, hiszen a Wilson-tétel miatt

$$-1 \equiv (4n)! \equiv (2n)!(-2n)\cdots(-1) = (2n)!^2 \pmod p.$$

□

Számos hasonló eredmény született. 1846-ban M. A. Stern például azt igazolta, hogy ha $p = 8n+3$ prím, akkor $p = A^2 + 2B^2$, ahol $\pm 2A \equiv \binom{4n+1}{n} \pmod p$. Ezt Eisenstein azzal egészítette ki, hogy $A = 4r + 1 - 2n$, ahol r azon $1 \le z \le \frac{p-1}{2}$ egészek száma, amikre $1 + zi$ nyolcadik hatványmaradék mod p. Stickelberger azt bizonyította, hogy ha $p = 15n+4$ prím, akkor $p = A^2 + 15B^2$ alakban írható, ahol

$$2A \equiv 5^{\frac{p-1}{3}}\binom{5n+1}{n} \pmod p.$$

A kvadratikus maradékok eloszlása

Ha $p > 2$ prámszám, akkor a mod p redukált maradékosztályok között ugyanannyi kvadratikus maradék és kvadratikus nemmaradék van. Kérdés, hogy ezek hogyan oszlanak el. Mivel semmi okunk nincs annak feltételezésére, hogy valami struktúra lenne, hajlamosak vagyunk azt tippelni, véletlenszerűen. Ennek egy lehetséges tesztje az lehet, ha igaz, hogy azon i maradékosztályok száma, amikre i és $i+1$ is kvadratikus maradék, aszimptotikusan $p/4$, sőt általában, annak valószínűsége, hogy k egymásutáni maradék kvadratikus karaktere egy adott mintát ad, $1/2^k$, minden mintára. Ezt $k = 2$-re gyorsan bebizonyítjuk.

17. Tétel. *Ha p prímszám, akkor, ha ε_0 és ε_1 is $+1$ vagy -1, akkor az*

$$E(\varepsilon_0, \varepsilon_1) = \left\{ 0 < i < p-1 : \left(\frac{i}{p}\right) = \varepsilon_0, \left(\frac{i+1}{p}\right) = \varepsilon_1 \right\}$$

halmaz elemszáma aszimptotikusan $p/4$.

Bizonyítás. Legyen $a = |E(+1,+1)|$, $b = |E(+1,-1)|$, $c = |E(-1,+1)|$, $d = |E(-1,-1)|$. Azaz, a azon $0 < i < p-1$ maradékok száma, amikre i és $i+1$ is kvadratikus maradék, stb. Az összes ilyen maradék közül a kvadratikus maradékok száma

$$a + b = \begin{cases} \frac{p-3}{2}, & \text{ha } p \equiv 1 \mod 4, \\ \frac{p-1}{2}, & \text{ha } p \equiv 3 \mod 4 \end{cases}$$

(mivel -1-et kihagytuk).

Hasonlóan adódik

$$a + c = \frac{p-3}{2}.$$

Az előző fejezet 2. Lemmáját használva

$$\sum \left(\frac{i}{p}\right)\left(\frac{i+1}{p}\right) = \sum \left(\frac{i^2+i}{p}\right) = \sum \left(\frac{4i^2+4i}{p}\right) = \sum \left(\frac{i^2-1}{p}\right) = -1,$$

hiszen, ha i egy teljes maradékrendszeren megy végig, akkor $2i+1$ is. Ebből azt kapjuk, hogy $a - b - c + d = -1$. Innen már adódik, hogy

$$a = \begin{cases} \frac{p-5}{4}, & \text{ha } p \equiv 1 \mod 4, \\ \frac{p-3}{4}, & \text{ha } p \equiv 3 \mod 4 \end{cases}$$

stb. □

18. Tétel. (A. Brauer) *Ha k természetes szám és a p prímszám k-tól függően elég nagy, akkor van modulo p k egymásutáni maradékosztály, ami kvadratikus maradék.*

Bizonyítás. Van der Waerden tételére hivatkozunk. Eszerint, ha k és r természetes számok, akkor van olyan $W(k,r)$ természetes szám, hogy ha az $\{1,\dots,W(k,r)\}$ halmazt r részre osztjuk, akkor valamelyik tartalmaz k-tagú számtani sorozatot. Legyen $p > W(k^2,2)$ prímszám. Ha az $1,\dots,W(k^2,2)$ számokat aszerint színezzük két színnel, hogy kvadratikus maradékok-e vagy sem, a tétel szerint kapunk egy k^2 hosszúságú számtani sorozatot csupa azonos karaterű számból: vagy mind kvadratikus maradék vagy mind kvadratikus nemmaradék. Legyen d a sorozat differenciája, nyilván d nem osztható p-vel. Ha a sorozat minden tagját modulo p leosztjuk d-vel, akkor egymásutáni maradékokat kapunk. Továbbá még mindig azonos lesz a számok kavdratikus karaktere, nevezetesen, ha d kvadratikus maradék, akkor az osztással a számok kvadratikus karaktere nem változott, ha pedig nemmaradék, akkor mindegyiké megváltozott.

Legyenek számaink $a, a+1, \dots, a+(k^2-1)$. Ha mind kvadratikus maradék, készen vagyunk, hiszen kaptunk k (sőt k^2) egymásutáni kvadratikus maradékot.

Feltehetjük tehát, hogy mindegyik kvadratikus nemmaradék. Legyen c a legkisebb kvadratikus nemmaradék modulo p. Ha $c > k$ készen vagyunk, hiszen ekkor $1,\dots,k$ egymásutáni kvadratikus maradékok k hosszúságú sorozata. Feltehetjük tehát, hogy $c \le k$. Vegyük k^2 hosszúságú sorozatunkban a c-vel oszthatókat, ezekből legalább k van. Ha ezeket c-vel végigosztjuk, egymásutáni számokat kapunk és persze mindegyik kvadratikus maradék lesz, mivel két kvadratikus nemmaradék hányadosa. □

Felvetett problémánkat végül B. Z. Moroz és René Peralta igazolta:

19. Tétel. *Ha p prímszám és $\varepsilon_1,\dots,\varepsilon_k$ mindegyike $+1$ vagy -1, $0 < a < p$, és $E(a,\varepsilon_1,\dots,\varepsilon_k)$ jelöli a*

$$\left\{0 < i < p : \left(\frac{i+a}{p}\right) = \varepsilon_1, \left(\frac{i+2a}{p}\right) = \varepsilon_2, \dots, \left(\frac{i+ka}{p}\right) = \varepsilon_k\right\}$$

halmazt, akkor

$$\left| |E(a,\varepsilon_1,\dots,\varepsilon_k)| - \frac{p}{2^k} \right| \le (3+\sqrt{p})k.$$

□

20. Tétel. *Van olyan $c > 0$ konstans, hogy minden elég nagy p prímszámra az $[1, \sqrt{p}]$ intervallumban legalább $c\sqrt{p}$ kvadratikus maradék és legalább $c\sqrt{p}$ kvadratikus nemmaradék van. Speciálisan a legkisebb kvadratikus nemmaradék $\sqrt{p}$-nél kisebb.*

Bizonyítás. Azt a tételt használjuk, hogy azon (a, b) párok aszimptotikus száma, amire $1 \leq a, b \leq N$ és $(a, b) = 1$,

$$\frac{6}{\pi^2} N^2.$$

Legyen most p egy elég nagy prím,

$$X = \{(a, b) : 1 \leq a, b < \sqrt{p}, (a, b) = 1\}.$$

A hivatkozott tétel szerint $|X| \sim \frac{6}{\pi^2} p$. Továbbá az $(a, b) \mapsto \frac{a}{b}$ leképezés injektív X-ből a racionális számok halmazába.

Belátjuk, hogy ha $(a, b) \neq (c, d)$, akkor

$$\frac{a}{b} \not\equiv \frac{c}{d} \pmod{p}.$$

Valóban, tegyük fel, hogy $\frac{a}{b} \equiv \frac{c}{d} \pmod{p}$. Felszorozva ebből $p | ad - bc$ adódik, ami lehetetlen, mivel $(a, b) = (c, d) = 1$ miatt $ad - bc \neq 0$, viszont abszolút értéke $a, b, c, d < \sqrt{p}$ miatt kisebb p-nél, tehát nem lehet osztható p-vel. Ezért, ha $(a, b) \in X$-hez hozzárendeljük az $\frac{a}{b} \pmod{p}$ értéket, akkor mod p vett maradékok egy $\frac{6}{\pi^2} p$ elemű Y halmazát kapjuk.

Mivel $\frac{6}{\pi^2} > \frac{1}{2}$, Y tartalmaz legalább $(\frac{6}{\pi^2} - \frac{1}{2})p$ kvadratikus nemmaradékot.

Legyen a $\sqrt{p}$ alatti kvadratikus maradékok száma R, a nemmaradékok száma N. Ekkor $R + N = \sqrt{p}$, továbbá $2RN \geq (\frac{6}{\pi^2} - \frac{1}{2})p$. Innen azonnal adódik, hogy $R, N > c\sqrt{p}$ alkalmas $c > 0$-ra. □

A számelmélet egyik nevezetes problémája, hogy minden $\varepsilon > 0$-ra, ha p elég nagy, a legkisebb kvadratikus nemmaradék kisebb, mint p^ε. Vinogradov elég nagy p-re $p^\theta (\log p)^2$ korlátot adta, ahol $\theta = \frac{1}{2\sqrt{e}}$. Ezt Burgess $O(p^{\theta/2+\varepsilon})$-ra javította.

Irodalom

[1] D. A. Burgess: The distribution of quadratic residues and non-residues. *Mathematika*, **4**(1957), 106–112.
[2] B. Z. Moroz: The distribution of power residues and non-residues, *Vestnik of the Leningrad University*, **16**(1961), 164–169. .
[3] R. Peralta: On the distribution of quadratic residues and nonresidues modulo a prime number, *Mathematics of Computation*, **58**(1992), 433–440.

A Prouhet-Tarry-Escott probléma

A következő tétel Schweitzer-feladat volt.

21. Tétel. *Ha $a_1, \dots, a_n$ páratlan, $b_1, \dots, b_n$ páros természetes számok, amikre*

$$\begin{aligned} a_1 + \cdots + a_n &= b_1 + \cdots + b_n \\ a_1^2 + \cdots + a_n^2 &= b_1^2 + \cdots + b_n^2 \\ &\dots \\ a_1^k + \cdots + a_n^k &= b_1^k + \cdots + b_n^k \end{aligned} \tag{1}$$

teljesül, akkor $n \geq 2^k$.

1. Bizonyítás. (Jonathan M. Borwein) Legyen

$$f(x) = x^{a_1} + \cdots + x^{a_n} - x^{b_1} + \cdots + x^{b_n}.$$

Ekkor $f(1) = n - n = 0$. Továbbá

$$f'(1) = (a_1 + \cdots + a_n) - (b_1 + \cdots + b_n) = 0,$$

$$f''(1) = \big(a_1(a_1-1) + \cdots + a_n(a_n-1)\big) - \big(b_1(b_1-1) + \cdots + b_n(b_n-1)\big) = 0,$$

és így tovább, egészen az

$$f^{(k)}(1) = 0$$

egyenlőségig. Tehát $f(1) = f'(1) = \cdots = f^{(k)}(1) = 0$, ezért $f(x)$ osztható $(x-1)^{k+1}$-nel. Mivel $(x-1)^{k+1}$ főegyütthatója 1, az $f(x) = (x-1)^{k+1}g(x)$ egyenlőségben $g(x)$ egész együtthatós. Ha most $x = -1$ et helyettesítünk, akkor $-2n = 2^{k+1}A$ adódik, ahol A egész, tehát n osztható 2^k-nal. □

2. Bizonyítás. (Károlyi Gyula) Belátjuk, hogy van olyan legfeljebb k-adfokú $p(x)$ polinom, ami páros helyen 2^k-nal osztható, páratlan helyen

2^k-nal osztva 1-et maradékul adó egész értéket vesz fel. Ez elég, hiszen kiszorozva és csoportosítva

$$p(a_1) + \cdots + p(a_n) = p(b_1) + \cdots + p(b_n)$$

adódik, márpedig 2^k-nal osztva a baloldal 0-val, a jobboldal n-nel kongruens, tehát n osztható 2^k-nal.

Ha $k = 1$, a $p(x) = x$ polinom nyilván megfelelő. Tegyük fel, hogy az $f(x)$ polinom megfelelő k-ra. Legyen $g(x) = 2f(x) - 1$. Ekkor

$$g(x) \equiv \begin{cases} -1 & (2^k) \quad \text{ha } x \text{ páros} \\ 1 & (2^k) \quad \text{ha } x \text{ páratlan.} \end{cases}$$

Legyen $p(x) = g(1) + \cdots + g(x)$. Ekkor $p(x)$ könnyen láthatóan valóban 0-át és 1-et ad 2^k-nal osztva aszerint, hogy x páros vagy páratlan.

Be kell látnunk, hogy $p(x)$ (legfeljebb) $k+1$-edfokú polinom. Ehhez azt jegyezzük meg, hogy $g(x)$-et felírható

$$g(x) = a_k \binom{x}{k} + \cdots + a_0 \binom{x}{0}$$

alakban. Valóban, mivel a szereplő binomiális együtthatók rendre $k, k-1, \ldots, 0$-fokú polinomok, ezt maradékos osztással beláthatjuk.

Ekkor viszont a Pascal-háromszög tulajdonságaiból az adódik, hogy

$$p(x) = a_k \binom{x}{k+1} + \cdots + a_0 \binom{x}{1}$$

teljesül és ez egy legfeljebb $k+1$-edfokú polinom. □

A számelmélet egyik régi megoldatlan problémája a következő:

Prouhet-Tarry-Escott probléma. *Minden $n \geq 2$ természetes számra van természetes számoknak két különböző $\{a_1, \ldots, a_n\}$ és $\{b_1, \ldots, b_n\}$ halmaza, hogy*

$$\begin{gathered} a_1 + \cdots + a_n = b_1 + \cdots + b_n \\ a_1^2 + \cdots + a_n^2 = b_1^2 + \cdots + b_n^2 \\ \cdots \\ a_1^{n-1} + \cdots + a_n^{n-1} = b_1^{n-1} + \cdots + b_n^{n-1} \end{gathered}$$

teljesül.

Erdős számos tételben vizsgálta, hány tagja lehet egy sorozatnak, amely rendelkezik egy tulajdonsággal, ami megvan a prímszámok sorozatának. Mivel a prímszámok eleve példát adnak ilyen tulajdonságú sorozatra, a kérdés általában az, hogy hogy ha a sorozat tagjai x-nél kisebbek, a sorozat hossza mennyivel haladhatja meg $\pi(x)$-et, a prímszámok számát. Ha például az adott tulajdonság az, hogy a sorozat egyik tagja sem osztója a többi szorzatának, akkor a sorozat hosza legfeljebb $\pi(x)$.

Egy másik karakterisztikus példa a következő.

22. Tétel. (Erdős) *Legyen $c_1 < \cdots < c_m \leq x$ természetes számok sorozata, amiben nincs két azonos hosszúságú, azonos szorzatú részsorozat, tehát, ha $i_1, \ldots, i_r, j_1, \ldots, j_r \leq m$ különböző elemek, akkor $c_{i_1} \cdots c_{i_r} \neq c_{j_1} \cdots c_{j_r}$. Ekkor*

$$m \leq \pi(x) + 2x^{2/3}.$$

Bizonyítás. Egy lemmával kezdjük.

Lemma. *Minden $n \leq x$ természetes szám felírható két természetes szám $n = ab$ szorzataként, ahol $a \leq x^{2/3}$ vagy prímszám és $b \leq x^{2/3}$.*

Bizonyítás. Az állítás nyilvánvaló, ha $n \leq x^{2/3}$ (ekkor vehetjük $a = 1$, $b = n$-et). Legyen tehát $x^{2/3} < n \leq x$. Ismét készen vagyunk, ha n-nek van $x^{1/3}$-nál nagyobb prímosztója: ekkor választhatjuk ezt a-nak, társosztóját pedig b-nek. Tegyük tehát fel, hogy ilyen prímosztó nincs. Állítsuk elő n-t prímszámok (esetleg ismétléses) szorzataként: $n = p_1 \cdots p_s$. Legyen $r < s$ a legnagyobb index, amire a $p_1 \cdots p_r$ részszorzat értéke legfeljebb $x^{1/3}$. Legyen $a = p_1 \cdots p_{r+1}$, $b = p_{r+2} \cdots p_s$. Ekkor a fentiek szerint $a > x^{1/3}$ tehát $b < x^{2/3}$. Továbbá a két $x^{1/3}$-nál kisebb tényező szorzata, nevezetesen $p_1 \cdots p_r$-é és p_{r+1}-é, ezért $a < x^{2/3}$. □

Ezután a Tétel bizonyításához legyen $c_1 < \cdots < c_m \leq x$ olyan sorozat, amire a Tétel feltevése teljesül. Tekintsük a következő páros gráfot: a gráf osztályai A és B ahol A az x-nél nem nagyobb prímszámokból és a legfeljebb $\leq x^{2/3}$ nagyságú természetes számokból áll, míg B a legfeljebb $x^{2/3}$ nagyságú természetes számokat tartalmazza (tehát minden $\leq x^{2/3}$ természetes szám két példányban szerepel, egyszer A-ban, egyszer B-ben).

A sorozat minden elemét reprezentáljuk egy éllel: ha $c_i = ab$, ahol $a \in A$, $b \in B$, akkor feleltessük meg a_i-nek az $\{a, b\}$ élt. Így keletkezik egy páros

gráf $\pi(x)+2x^{2/3}$ szögponttal és m éllel. Ha az élek száma annyi, vagy több, mint a pontok száma, akkor keletkezik kör, ami csak páros lehet (lévén a gráf páros): pontjai $a_1, b_1, \ldots, a_r, b_r$, ahol $a_i \in A$, $b_i \in B$ és az egymásutáni pontok ciklikusan össze vannak kötve. De ekkor $a_1b_1, \ldots, a_rb_r$ illetve $b_1a_2, \ldots, b_ra_1$ sorozatbeli elemek, amelyek szorzata ugyanaz, $a_1b_1 \cdots a_rb_r$. Mivel ez pontosan a kizárt konfiguráció, ilyen nincs, tehát az élek száma, azaz $m < \pi(x)+2x^{2/3}$. □

Irodalom

[1] P. Erdős: On sequences of integers no one of which divides the product of two others and on some related problems, *Mitteil. Forsch.-Inst. Math. Mech. Univ. Tomsk*, **2**(1938), 74–82.

A 2-hatványok sorozatának kiegészítője

Erdős egyik kedvelt témaköre az volt, hogy egy adott sorozatnak milyen kis komplementere lehet. Ezen a következőt értjük. Természetes számok $A = \{a_0, a_1, \ldots\}$ sorozatához keresünk egy másik $B = \{b_0, b_1, \ldots\}$ sorozatot, amire az

$$A + B = \{a_i + b_j : i, j = 0, 1, \ldots\}$$

összegsorozat minden természetes számot tartalmaz (esetleg minden elég nagy számot, esetleg számok pozitív sűrűségű részhalmazát). Az érdekes eset az, amikor konkrét A sorozatról van szó, aminek sűrűségét pontosan ismerjük. Például lehet A a prímszámok sorozata, vagy a 2-hatványoké. (Könnyű észrevenni, hogy Erdőst a 4. oldalon említett Romanov-féle tétel vezette ehhez a kérdéshez.) Mivel x-ig kb. $c\log x$ 2-hatvány van, ahol $c = 1/\log 2$, ha kiegészítő sorozatot keresünk hozzá, annak x-ig legalább $dx/\log x$ tagjának kell lennie, ahol $d = 1/c$. Azt a problémát, hogy ez, akár nagyobb d-vel is, lehetséges, a gimnazista Ruzsa oldotta meg.

23. Tétel. (Ruzsa) *Van természetes számoknak olyan A sorozata, aminek x-ig legfeljebb $40\frac{x}{\log x}$ eleme van és minden $n \geq 1$ természetes szám $n = a+2^k$ alakban írható, ahol $a \in A$.*

Bizonyítás. Elég egy olyan sorozatot készíteni, aminek x-ig legfeljebb $20\frac{x}{\log x}$ eleme van és minden 5-tel nem osztható szám az említett módon előállítható. Valóban, ha A ilyen tulajdonságú sorozat, és a B sorozat tartalmazza A

elemeit, valamint A elemeinek rákövetkezőit, akkor egyrészt B-nek legfeljebb kétszer annyi eleme van, mint A-nak, másrészt minden $n \geq 1$ természetes szám vagy a megelőzője nem osztható 5-tel, ezért előállítható $n = a+2^k$ vagy $n = a+1+2^k$ alakban ahol $a \in A$, tehát mindenképpen $n = b+2^n$ alakban, ahol $b \in B$.

Legyen A az $5^u v$ alakú számok sorozata, ahol $5^u > \frac{1}{5}\log v$.

1. Lemma. *Ha $x \geq 5$, akkor A-nak $x/5$ és x között legfeljebb $10\frac{x}{\log x}$ eleme van.*

Bizonyítás. Valóban, ekkor

$$v < \frac{x}{5^u} < \frac{5x}{\log v}.$$

De, ha $v \log v < 5x$, akkor, mint kis számítás mutatja, $v < 10\frac{x}{\log x}$ és minden v-hez csak egy 5^u alakú tényező lehet. □

2. Lemma. *Ha $x \geq 1$, akkor A-nak x-ig legfeljebb $20\frac{x}{\log x}$ eleme van.*

Bizonyítás. Ezt x-re indukcióval bebizonyítjuk. Az állítás nyilvánvaló, ha $x < e^{20}$, ekkor ugyanis $20\frac{x}{\log x}$ nagyobb mint x. Tegyük fel, hogy $x > e^{20}$ és az állítás már be lett látva $x/5$-re. Az indukcióhoz az 1. Lemmát használva elég annyit belátni, hogy ekkor

$$20\frac{x/5}{\log(x/5)} + 10\frac{x}{\log x} \leq 20\frac{x}{\log x}$$

teljesül. Kiszorozva és egyszerűsítve ez a

$$\log 5 \leq \frac{3}{5}\log x$$

alakot ölti, ami igaz, ha $x \geq 25$. □

Végül belátjuk, hogy ha n 5-tel nem osztható természetes szám, akkor $n = a + 2^k$ alakban írható, ahol $a \in A$. Válasszuk r-et úgy, hogy

$$5^r \leq \log n < 5^{r+1}$$

teljesül. Mivel 2 primitív gyök mod 5^r, van $k < 5^r$, hogy $2^k \equiv n \pmod{5^r}$, azaz $n - 2^k = 5^r v$. Itt $v < n$, tehát

$$5^r \geq \frac{1}{5}\log n > \frac{1}{5}\log v,$$

azaz $5^r v$ az A sorozat eleme. □

Irodalom

[1] I. Ruzsa, Jr.: On a problem of P. Erdős. *Canad. Math. Bull.*, **15**(1972), 309–310.

Téglalap felbontása téglalapokra

Egy adott T téglalapot felbontjuk a $T_1, \ldots, T_n$ kisebb téglalapokra (a kis téglalapok oldalai szükségképpen párhuzamosak a nagyéival). A következő tétel azt vizsgálja, mikor lehetséges, hogy mindegyik $T_1, \ldots, T_n$ téglalap egyik oldala egész hosszúságú.

24. Tétel. *Ha a T téglalapot felbontjuk a $T_1, \ldots, T_n$ kisebb téglalapokra és mindegyik T_i téglalapnak van egész hosszúságú oldala, akkor T-nek is van.*

1. Bizonyítás. Tegyük fel, hogy a T téglalap a sík első negyedében helyezkedik el, úgy, hogy egyik csúcsa az origó. A feltevés szerint minden T_i téglalapnak van két, párhuzamos (vagy esetleg négy) egész hosszúságú oldala, vastagítsuk meg ezeket az oldalakat. Így egy gráfot kapunk, amiben, mint rövid megfontolás mutatja, T négy csúcsa páratlanfokú, a többi csúcs párosfokú. Ekkor viszont, mint a jólismert okoskodás mutatja, van út, ami összeköti T origóban levő csúcsát T egy másik csúcsával, s mivel az összekötő szakaszok egész hosszúságú, tengelyekkel párhuzamos szakaszok, az adódik, hogy a T egy másik csúcsa is rácspont, tehát készen vagyunk. □

2. Bizonyítás. Ismét feltesszük, hogy téglalapjaink az xy koordinátasíkon a tengelyekkel párhuzamos oldalakkal rendelkeznek. Olyan $F(x, y)$ függvényt keresünk, aminek egy S tengelypárhuzamos téglalapon vett integrálja pontosan akkor 0, ha S egyik oldalának hossza egész. Ez elég, hiszen ekkor F integrálja valamennyi $T_1, \ldots, T_n$ téglalapon 0, ezért T-n is az, így az F-re kikötött feltevés miatt T egyik oldala egész.

Ha F-et $F(x, y) = f(x)f(y)$ alakban keressük, akkor az $S = I \times J$ téglalapra, ahol I, J valós intervallumok,

$$\int_S F = \int_I f(t)dt \int_J f(t)dt$$

teljesül, elég tehát egy olyan, a valós számokon megadott f függvényt keresni, amire $\int_I f = 0$ pontosan akkor, ha I egész hossúságú.

Ilyen függvény pedig a (komplex értékeket felvevő)

$$f(t) = e^{2\pi it}$$

függvény. Valóban,

$$\int_a^b f(t)dt = \left[\frac{1}{2\pi i}e^{2\pi it}\right]_a^b = \frac{e^{2\pi ib} - e^{2\pi ia}}{2\pi i}$$

ez pedig pontosan akkor 0, ha $b - a$ egész. □

Irodalom

[1] S. Wagon: Fourteen proofs of a result about tiling a rectangle, Amer. Math. Monthly, **94**(1987), 601–617.

Négyzet lefedése kisebb négyzetekkel

Ebben a fejezetben azt vizsgáljuk, mikor lehet adott négyzetekkel az egységnégyzetet lefedni. Megengedjük, hogy a négyzetek egymást átfedjék, de ragaszkodunk ahhoz, hogy azonos állásúak legyenek az egységnégyzettel.

25. Tétel. *Ha adottak az $a_1, \ldots, a_n$ oldalú négyzetek és $a_1^2 + \cdots + a_n^2 \geq 4$, akkor a négyzetekkel lefedhető az egységnégyzet.*

Bizonyítás. Feltehetjük, hogy nincs 1, vagy hosszabb oldalú négyzet, hiszen ekkor már ez lefedi az egységnégyzetet. Legyenek a négyzetek oldalai csökkenő sorrendben felsorolva: $1 > a_1 \geq \cdots \geq a_n$.

Minden a_i szám 2 két egymásutáni hatványa közé esik:

$$\frac{1}{2^{k_i}} \leq a_i < \frac{1}{2^{k_i-1}}.$$

Zsugorítsuk valamennyi kis négyzetet: az a_i oldalhosszúságút $1/2^{k_i}$ oldalhosszúságúra. Ha a zsugorított négyzetekkel le tudjuk fedni az egységnégyzetet, akkor az adja az egységnégyzet lefedését az eredeti négyzetekkel, tehát elég az új négyzetekkel foglalkoznunk. Mivel $1/2^{k_i}$ több, mint fele a_i-nak, az új négyzetek területei nagyobbak, mint negyedei a megfelelő régi négyzetek területeinek.

Ezzel visszavezettük a feladatot a következőre: ha az $1/2^{k_1}, \ldots, 1/2^{k_n}$ oldalhosszúságú négyzetek összterülete 1-nél nagyobb, akkor lefedhető velük az egységnégyzet.

Ha az $1/2^{k_1}, \ldots, 1/2^{k_n}$ sorozatban ugyanazon $1/2^k$ érték négyszer szerepel, akkor ezeket áthelyettesíthetjük egy $1/2^{k-1}$ értékkel ez annak felel meg, hogy a négy azonos négyzetet egy kétszerakkorává forrasztjuk össze.

Ezt a műveletet addig elvégezve, amíg lehet (egyszer el kell akadnunk, mert ilyenkor a négyzetek száma csökken) egy olyan sorozathoz jutunk, amiben minden 2-hatvány legfeljebb háromszor szerepel.

Ha szerepel 1 vagy nagyobb szám, akkor persze készen vagyunk, lefedtük az egységnégyzetet. Különben, a négyzetek öszterülete kisebb, mint

$$\frac{3}{4}+\frac{3}{4^2}+\frac{3}{4^3}+\frac{3}{4^4}+\cdots=1,$$

ami ellentmond feltevéseinknek. □

26. Tétel. (Bezdek András, Bezdek Károly) *Ha adottak az $a_1,\ldots,a_n$ oldalú négyzetek és $a_1^2+\cdots+a_n^2\geq 3$, akkor a négyzetekkel lefedhető az egységnégyzet.*

Bizonyítás. Ismét feltehetjük, hogy nincs 1 vagy annál hosszabb oldalú négyzet és hogy a négyzetek nagyság szerint csökkenő sorrendben vannak felsorolva: $1>a_1\geq\cdots\geq a_n$. Kezdjük egymás mellé helyezni a négyzeteket addig, amíg egy 1 hosszúságú sávot nem kapunk. Ez először annál az n_1 indexnél fog bekövetkezni, amire

$$a_1+\cdots+a_{n_1-1}<1\leq a_1+\cdots+a_{n_1}$$

teljesül. Ezzel a sávval le tudjuk fedni az egységnégyzet egy a_{n_1} szélességű sávját. Ezután addig haladunk tovább, amíg a kis négyzetek összoldalhossza ismét meg nem haladja az 1-et, ehhez ahhoz az n_2 indexhez kell eljutni, amire

$$a_{n_1+1}+\cdots+a_{n_2-1}<1\leq a_{n_1+1}+\cdots+a_{n_2}$$

teljesül. Ezekkel egy a_{n_2} széles sávját tudjuk lefedni az egységnégyzetnek. Végül kapunk egy utolsó $n_k\leq n$ indexet, a maradék négyzetekből (ha vannak) már nem tudunk 1 hosszú sávot összeállítani:

$$a_{n_k+1}+\cdots+a_n<1.$$

Ezzel végül is lefedtük az egységnégyzet egy darabját $b=a_{n_1}+\cdots+a_{n_k}$ öszhosszúságú sávokkal, annyit kell megmutatnunk, hogy $b\geq 1$.

Mivel 0 és 1 közötti szám négyzete kisebb a számnál,

$$a_1^2+\cdots+a_{n_1-1}^2<1$$

fog teljesülni. Mivel az oldalak csökkenő hosszúságúak, minden $1\leq i\leq k$-ra

$$a_{n_i+1}^2+\cdots+a_{n_{i+1}-1}^2\leq(a_{n_i+1}+\cdots+a_{n_{i+1}-1})a_{n_i}<a_{n_i}$$

igaz. Ez az utolsó, „csonka" összegre is igaz. Ha a baloldalakat összeadjuk és hozzáadjuk az $a_{n_1}^2 + \cdots + a_{n_k}^2$ összeget, akkor azt kapjuk, hogy

$$a_1^2 + \cdots + a_n^2 < 1 + (a_{n_1} + \cdots + a_{n_k}) + a_{n_1}^2 + \cdots + a_{n_k}^2$$

$$\leq 1 + (a_{n_1} + \cdots + a_{n_k}) + (a_{n_1} + \cdots + a_{n_k})^2 = 1 + b + b^2$$

de feltevésünk szerint a baloldal legalább 3, innen $3 < 1 + b + b^2$ azaz $b \geq 1$. □

Irodalom

[1] A. Bezdek, K. Bezdek: Eine hinreichende Bedingung für die Überdeckung des Einheitwürfels durch homotetische Exemplare im n-dimensionalen euklidischen Raum, *Beiträge Algebra Geom.*, **17**(1984), 5–21.

Gráfok felbontásai

27. Tétel. (Erdős Pál) *Minden véges $G = (V, E)$ gráf ponthalmaza két részre bontható úgy, hogy e részek között halad az éleknek legalább fele.*

Bizonyítás. Vegyük a V szögponthalmaz összes lehetséges $V_1 \cup V_2 = V$ partícióját, jelölje e_1 illetve e_2 az ezeken belül haladó élek számát, legyen (V_1, V_2) az a partíció, amire $e_1 + e_2$ minimális. Ha több lenne, akkor legyen az egyik. Belátjuk, hogy ez megfelel a tétel feltételeinek. Be kell látnunk, hogy $e_1 + e_2 \leq e/2$, ahol e az élek száma. Legyen $p \in V_1$ tetszőleges pont, legyen a p-ből V_1-be futó élek száma x, a p-ből V_2-be induló élek száma y. Ha a (V_1, V_2) felbontás helyett a $(V_1 - \{p\}, V_2 \cup \{p\})$ felbontást vesszük, akkor az új részeken belüli élek száma $(e_1 - x) + (e_2 + y)$, és a feltevés szerint

$$e_1 + e_2 \leq (e_1 - x) + (e_2 + y),$$

ami ekvivalens azzal, hogy $x \leq y$. Ha ezt minden $p \in V_1$ pontra összeadjuk, akkor $2e_1 \leq f$-et kapunk, ahol f a keresztélek száma. Hasonlóan adódik $2e_2 \leq f$, azaz $e_1 + e_2 \leq f = e - (e_1 + e_2)$, innen adódik a kívánt egyenlőtlenség. □

28. Tétel. (Lovász László) *Ha egy véges (V, E) gráfban minden pont foka $\leq k$ és $k = k_1 + k_2 + 1$, akkor V partíciónálható két részre: $V = V_1 \cup V_2$ úgy, hogy V_1-ben minden pont foka $\leq k_1$ és V_2-ben minden pont foka $\leq k_2$.*

Bizonyítás. Egy $V = V_1 \cup V_2$ partíció esetén jelölje e_1 a V_1-ben, e_2 a V_2-ben haladó élek számát. Legyen (V_1, V_2) egy olyan partíció, amire

$$(2k_2 + 1)e_1 + (2k_1 + 1)e_2$$

minimális. Belátjuk, hogy ez megfelel a tétel követelményeinek. Legyen ismét $p \in V_1$ egy pont, jelölje x a p-ből V_1-be, y pedig a p-ből V_2-be futó élek számát. Ha p-t ismét áttesszük V_2-be, akkor az új felbontásra $e_1' = e_1 - x$, $e_2' = e_2 + y$ lesz és a feltevés szerint

$$(2k_2 + 1)e_1 + (2k_1 + 1)e_2 \leq (2k_2 + 1)e_1' + (2k_1 + 1)e_2'.$$

Ezt kiszámolva

$$(2k_2 + 1)e_1 + (2k_1 + 1)e_2 \leq (2k_2 + 1)(e_1 - x) + (2k_1 + 1)(e_2 + y),$$

adódik, azaz

$$x(2k_2 + 1) \leq y(2k_1 + 1).$$

Mivel $x + y \leq k$, ezt tovább írhatjuk:

$$y(2k_1 + 1) \leq (k - x)(2k_1 + 1)$$

azaz

$$x(2k_1 + 2k_2 + 2) \leq k(2k_1 + 1),$$

tehát $x \leq k_1 + \frac{1}{2}$. Persze x csak egész lehet, így $x \leq k_1$. Azt kaptuk tehát, hogy V_1-ben minden pont foka legfeljebb k_1 és hasonlóan adódik, hogy V_2-ben minden pont foka legfeljebb k_2. □

A fenti tétel egy érdekes változata, amikor maximális fokszám helyett minimális fokszámot követelünk meg. Itt a fenti módszer nem működik.

29. Tétel. (Carsten Thomassen, Hajnal Péter) *Ha egy véges gráfban minden pont foka legalább $2k_1 + k_2 + 1$, akkor a gráf ponthalmaza két valódi részre bontható, hogy az elsőben minden pont foka legalább k_1, a másodikban legalább k_2*

Bizonyítás. (Hajnal Péter) Válasszuk ki a szögpontok V halmazának összes olyan nemüres részhalmazát, aminek v elemszáma és e élszáma között $e \geq k_1 v$ fennáll. Legyen A ezek között a minimális nagyságú, vagy ha ilyen több lenne, akkor azok között az (vagy az egyik olyan), amelynek e élszáma maximális.

Mivel, ha egy pontot elhagyunk a gráfból, még minden pont foka legalább $2k_1 + k_2 > 2k_1$, így az így keletkezett gráfra a fenti egyenlőtlenség teljesül, ezért A nem lehet az egész gráf szögponthalmaza. Legyen komplementere B. Azt állítjuk, hogy A és B egy kívánt típusú felbontást adnak.

Legyen $p \in A$ tetszőleges. Jelöljük x-szel a p-ből A-ba haladó élek számát. Ha elhagyjuk A-ból p-t, akkor már nem teljesülhet a fenti feltétel, tehát

$$e - x < k_1(v-1) = k_1 v - k_1 \leq e - k_1,$$

ezért $x \leq k_1$, ahogy akartuk. Nem igaz, hogy A-ban minden pont foka $\geq 2k_1 + 1$, hiszen ekkor bármelyik pontot elhagyva még mindig minden pont foka legalább $2k_1$ lenne, ezért teljesülne a feltétel. Van tehát $p \in A$ pont, amiből A-ba $x \leq 2k_1$ él fut. Legyen q tetszőleges pont B-ben, jelölje y a q-ból az B-be, z a q-ból $A - \{p\}$-be haladó élek számát. tegyük fel, hogy $y < k_2$ (mert különben készen vagyunk). Ekkor q teljes fokszáma $y+z$ vagy $y+z+1$ aszerint, hogy p és q ösze van-e kötve. Ezért $z > (2k_1+k_2+1)-(k_2+1) = 2k_1$. Ha A helyett az $A' = A-\{p\}\cup\{q\}$ halmazt vesszük, akkor az A' által feszített gráf e' élszámára $e' = e - x + z > e$ adódik, ellentmondás. □

Irodalom

[1] P. Erdős: Gráfok páros körüljárású részgráfjairól, *Mat lapok*, **18**(1967), 283–288.

[2] P. Hajnal: Partition of graphs with condition on the connectivity and minimum degree, *Combinatorica*, **3**(1983), 95–99.

[3] L. Lovász: On decomposition of graphs, *Studia Sci. Math. Hung.*, **1**(1966), 237–238.

[4] C. Thomassen: Graph decomposition with constraints on the connectivity and minimum degree, *Journal of Graph Theory*, **7**(1983), 165–167.

Diszkrét geometria

Ha G véges gráf, jelölje $\mathrm{cr}(G)$ éleinek a G síkbarajzolásainál megkapható minimális keresztezési számát, ahol az éleket úgy rajzoljuk le, hogy egy pontban legfeljebb kettő kereszteződhet. Nyilván $\mathrm{cr}(G) = 0$ pontosan akkor, ha G síkbarajzolható. Az Euler-formulából adódik, hogy ha a v csúcsból és e élből álló gráf síkbarajzolható, akkor $e \leq 3v - 6$, azaz, ha $e \geq 3v - 5$, akkor $\mathrm{cr}(G) \geq 1$. Ezt általánosítjuk.

1. Lemma. $\mathrm{cr}(G) \geq e - 3v + 6$.

Bizonyítás. Tegyük fel, hogy G-t síkbarajzoltuk, $\mathrm{cr}(G)$ kereszteződéssel. Legyen H az a gráf, amelyben G-hez hozzáadjuk a kereszteződési pontokat és az éleket annyi új élre osztjuk, ahány részre bontják a metszéspontok. Ekkor H csúcsainak száma $v + \mathrm{cr}(G)$, míg éleinek száma $e' = e + 2\mathrm{cr}(G)$, hiszen minden új csúcs negyedfokú.

Mivel $e' \leq 3v' - 6$, az adódik, hogy $e + 2\mathrm{cr}(G) \leq 3\big(v + \mathrm{cr}(G)\big) - 6$, azaz $\mathrm{cr}(G) \geq e - 3v + 6$. □

30. Tétel. (Leighton, Ajtai, Chvátal, Newborn, Szemerédi) *Ha a G véges gráfban $e \geq 4v$, akkor*

$$\mathrm{cr}(G) \geq \frac{1}{64}\frac{e^3}{v^2}.$$

Bizonyítás. (B. Chazelle, M. Sharir, E. Welzl) Később megválasztandó $0 < p < 1$ értékkel legyen G_p G-nek az a feszített részgráfja, amibe G csúcsait egymástól függetlenül, p valószínűséggel választjuk be.

Nyilván $E[v(G_p)] = pv$. G_p élszámának várható értéke $E[e(G_p)] = p^2 e$, hiszen minden él p^2 valószínűséggel kerül be G_p-be. Végül $E(\mathrm{cr}(G_p)] \leq p^4\mathrm{cr}(G)$, mert ha G-t $\mathrm{cr}(G)$ kereszteződéssel síkbarajzoljuk, akkor ezek közül bármelyiket akkor tartalmazza G_p, ha a keresztező élekhez tartozó négy csúcs mindegyike G_p-ben van.

Innen $p^4\mathrm{cr}(G) \geq E[\mathrm{cr}(G_p)] \geq p^2 e - 3pv + 6$, azaz

$$\mathrm{cr}(G) \geq \frac{e}{p^2} - \frac{3v}{p^3}.$$

Ha p-t most $p = \frac{4v}{e} \leq 1$-nek választjuk, akkor

$$\mathrm{cr}(G) \geq \frac{1}{64}\frac{e^3}{v^2}$$

adódik. □

Ebből a tételből elegánsan vezette le Székely László a kombinatorikus geometria egyik fontos tételét.

31. Tétel. (Szemerédi Endre, W. T. Trotter) *Ha a síkon adott n pont és m egyenes, akkor a köztük levő illeszkedések száma (tehát azon (i, j) indexpárok*

száma, amikre P_i rajta van e_j-n, ahol $P_1, \dots, P_n$ a pontok, $e_1, \dots, e_m$ az egyenesek felsorolása) legfeljebb $4((mn)^{2/3} + m + n)$.

Bizonyítás. (Székely László) Legyenek a G a G gráf csúcsai $P_1, \dots, P_n$ és kössünk össze kettőt, ha egyeneseink közül valamelyiken szomszédosak. Nyilván $\mathrm{cr}(G) \leq \binom{m}{2}$. Egy egyenesen nyilván eggyel több csúcs van, mint G-beli él, így, ha a tételbeli illeszkedések száma k, G éleinek száma e, akkor $k - m = e$. Ha $k - m \leq 4n$, készen vagyunk. A másik esetben, a 26. Tétel szerint

$$\mathrm{cr}(G) \geq \frac{1}{64}\frac{(k-m)^3}{n^2},$$

innen $k \leq 4(mn)^{2/3} + m$. □

Ennek sok alkalmazása közül az alábbit Elekes György találta.

32. Tétel. (Elekes) *Ha A, B, C s-elemű valós számhalmazok, akkor*

$$|AB + C| \geq Ks^{3/2},$$

alkalmas $K > 0$ konstansra, ahol $AB + C = \{ab + c : a \in A, b \in B, c \in C\}$.

Bizonyítás. Legyen tehát $S = AB + C$, $r = |S|$. Legyen

$$P = A \times S$$

és

$$\mathcal{L} = \{L_{b,c} : b \in B, c \in C\},$$

ahol

$$L_{b,c} = \{(x, bx + c) : x \in \mathbf{R}\}.$$

Ekkor P egy síkbeli $n = sr$ elemű ponthalmaz, $\mathcal{L}$ pedig $m = s^2$ egyenesből álló halmaz. Az $L_{b,c} \in \mathcal{L}$ egyenes tartalmazza P-nek s pontját, nevezetesen az összes $(a, ab + c)$ alakút $(a \in A)$. Az illeszkedések száma tehát legalább s^3, viszont a 27. Tétel szerint

$$s^3 \leq 4\big(s^{4/3}(sr)^{2/3} + sr + s^2\big)$$

ahonnan némi számolással adódik

$$r \geq \frac{1}{10}s^{3/2}.$$

□

A következő alkalmazás a Sylvester-Gallai tétel kvantitatív változata. Nevezett tétel azt mondja ki, hogy ha adott a síkban véges sok, nem egy egyenesen fekvő pont, akkor van olyan egyenes, ami ezek közül pontosan kettőn megy keresztül. Ebből egyszerű indukcióval adódik a következő állítás: ha adott a síkban n pont, akkor vagy mind egy egyenesen van, vagy legalább n egyenest határoznak meg. Az alábbi tételben az egyik lehetőséget enyhítjük, a másikat erősítjük.

33. Tétel. (Beck József) *A síkban adott n pont között vagy $c_1 n$ egy egyenesre esik, vagy a pontok legalább $c_2 n^2$ egyenest határoznak meg (alkalmas $c_1, c_2 > 0$ konstansokkal).*

Bizonyítás. Legyen tehát adva n síkbeli pont, ami közül $n/2000$ nem esik egy egyenesre. Ha $2 \leq 2^j \leq n/1000$, nevezzünk j-egyenesnek egy olyan egyenest, amire legalább 2^j, de kevesebb, mint 2^{j+1} pont esik (az adottak közül). Legyen a j-egyenesek száma m_j. Az összes, a pontok által meghatározott egyenes száma nyilván $m = \sum m_j$.

A j-egyenesek és a pontok közötti illeszkedések száma legalább $m_j 2^j$. Ezért a 27. Tétel szerint

$$m_j 2^j \leq 4\big((m_j n)^{2/3} + m_j + n\big).$$

Hogy megkönnyítsük a számolást, a fenti, $x + y + z$ alakú felső korlátot helyettesítjük a (legalább ekkora) $\max(3x, 3y, 3z)$ korláttal. Eszerint

$$m_j 2^j \leq 12(m_j n)^{2/3}$$

vagy

$$m_j 2^j \leq 12 m_j$$

vagy

$$m_j 2^j \leq 12n.$$

Átrendezéssel azt kapjuk, hogy az első esetben

$$m_j \leq 2000 \frac{n^2}{8^j}$$

a másodikban

$$2^j \leq 12$$

a harmadikban

$$m_j \leq 12 \frac{n}{2^j}$$

teljesül. Mindenesetre, ha $j \geq 4$, akkor $2^j > 12$, ezért ekkor mindenképpen igaz

$$m_j \leq 2000\frac{n^2}{8^j} + 12\frac{n}{2^j}.$$

Az n pontból összesen $\binom{n}{2} = \frac{n(n-1)}{2} \geq \frac{n^2}{3}$ pár választható ki. Az egy j-egyenesre eső, legfeljebb $2^{j+1} - 1$ pontból kevesebb, mint $\frac{1}{2}(2^{j+1})^2 = 2 \cdot 4^j$ pár készíthető. Ezért

$$2\sum_j m_j 4^j \geq \frac{n^2}{3}$$

adódik. Itt olyan tag, amire $2^j > n/1000$, nincs. Ha csak a $15 < j$, $2^j \leq n/1000$ értékekre összegzünk, akkor

$$2\sum_{15<j,2^j\leq\frac{n}{1000}} m_j 4^j \leq 4000n^2 \sum_{j>15} \frac{1}{2^j} + 24n \sum_{2^j\leq\frac{n}{1000}} 2^j$$

adódik. A jobboldal első tagja legfeljebb

$$4000n^2\frac{1}{2^{15}} < \frac{n^2}{8}$$

a második legfeljebb

$$24n\frac{n}{500} < \frac{n^2}{20}.$$

Azt kapjuk, hogy legalább $\frac{n^2}{3} - \frac{n^2}{8} - \frac{n^2}{20} > \frac{n^2}{10}$ olyan pontpár van, ami olyan j-egyenesen fekszik, amire $j \leq 15$. Mivel egy ilyen egyenesre legfeljebb $\frac{1}{2}(2^{16})^2 < 10^{10}$ pár eshet, az ilyen egyenesek száma legalább $n^2/10^{11}$. □

Irodalom

[1] M. Ajtai, V. Chvátal, M. M. Newborn, E. Szemerédi: Crossing-free subgraphs. *Theory and practice of combinatorics,*, North-Holland Math. Stud., **60**, North-Holland, Amsterdam, 1982., 9–12.

[2] J. Beck: On the lattice property of the plane and some problems of Dirac, Motzkin, and Erdős in combinatorial geometry, *Combinatorica*, **3**(1983), 281–297.

[3] G. Elekes: On the number of sums and products, *Acta Arith.*, **81**(1997), 365–367.

[4] F. T. Leighton: New lower bound techniques for VLSI, *Math. Systems Theory*, **17**(1984), 47–70.
[5] L. A. Székely: Crossing numbers and hard Erdős problems in discrete geometry, *Combin. Probab. Comput.*, **6** (1997), 353–358.
[6] E. Szemerédi, W. Trotter: Extremal problems in discrete geometry, *Combinatorica*, **3**(1983), 381–392.

Lineáris algebra a kombinatorikában

34. Tétel. (R. L. Graham-H. O. Pollak) *A K_n teljes gráf élhalmaza nem partícionálható $n-1$-nél kevesebb teljes páros gráfra.*

Bizonyítás. Lefordítva a tétel állítását, azt kell bebizonyítanunk, hogy ha $V = \{v_1, \ldots, v_n\}$, és $A_i, B_i \subseteq V$ k darab diszjunkt halmazból álló részhalmazpár, hogy minden V beli párhoz pontosan egy olyan $1 \leq i \leq k$ van, hogy a pár egyik eleme A_i-ben, a másik B_i-ben van, akkor $k \geq n-1$. Tegyük fel, hogy $k < n-1$.

Rendeljünk hozzá a $v_1, \ldots, v_n$ pontokhoz a $x_1, \ldots, x_n$ változókat. Írjuk fel a következő egyenleteket:

$$\sum_{j=1}^{n} x_j = 0,$$

$$\sum_{j \in A_i} x_j = 0 \quad (i = 1, \ldots, k).$$

Ez $k+1 < n$ lineáris egyenlet n ismeretlenre, van tehát nemzéró megoldása, mondjuk a valós számok körében. Tekintsünk egy ilyen nemtriviális megoldást és írjuk rá minden élre egy számot mégpedig a v_j és $v_{j'}$ pontok közötti élre $x_j x_{j'}$-t. Számítsuk ki az élekre írt számok összegét! Egyrészt egy adott (A_i, B_i) párra a két halmaz közötti élekre írt számok összege

$$\sum_{j \in A_i} \sum_{j' \in B_i} x_j x_{j'} = \left(\sum_{j \in A_i} x_j \right) \left(\sum_{j' \in B_i} x_{j'} \right) = 0$$

és mivel feltevésünk szerint minden él pontosan egyszer szerepel mint valamelyik (A_i, B_i) keresztező éle, összesen is 0-t kapunk.

Másrészt számítsuk ki egy adott v_j pontra a belőle kiinduló élekre írt számok összegét. Ez nyilvánvalóan

$$x_j\left(\sum_{j'\neq j} x_{j'}\right) = -x_j^2$$

mivel $x_1 + \cdots + x_n = 0$. Ha ezt minden pontra összeadjuk, akkor az élekre írt számok összegének kétszeresét kapjuk, ami egyfelől persze 0, másrészt

$$-\left(\sum_j x_j^2\right) < 0$$

ellentmondás. □

35. Tétel. (Fisher-egyenlőtlenség) *Ha* $|S| = n$, $A_1, \ldots, A_m \subseteq S$ *olyan halmazok, hogy* $|A_i| = k$, $|A_i \cap A_j| = r$ *ha* $i \neq j$, *akkor* $m \leq n$.

Bizonyítás. Nyilván $r < k$. Legyen $S = \{s_1, \ldots, s_n\}$. Vegyünk egy n-dimenziós vektorteret, legyen benne $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ bázis.

Rendeljük hozzá az $A_i \subseteq S$ halmazhoz az $\mathbf{a}_i = \sum\{\mathbf{e}_j : s_j \in A_i\}$ karakterisztikus vektort. Ekkor az $\mathbf{a}_i\mathbf{a}_j$ skaláris szorzat értéke k, ha $i = j$, r, ha $i \neq j$.

Belátjuk, hogy az $\{\mathbf{a}_1, \ldots, \mathbf{a}_m\}$ vektorok lineárisan függetlenek, ebből persze már következik $m \leq n$ (hiszen a tér dimenziója n).

Ehhez tegyük fel, hogy

$$\sum_{i=1}^{m} \lambda_i \mathbf{a}_i = \mathbf{0}$$

ahol nem mindegyik λ_i nulla.

Skalárisan szorozva $\mathbf{a}_j$-vel a következőt kapjuk:

$$0 = \sum_{i=1}^{m} \lambda_i \mathbf{a}_i \mathbf{a}_j = \sum_{i\neq j} \lambda_i r + \lambda_j k = \lambda r + \lambda_j (k - r)$$

ahol $\lambda = \lambda_1 + \cdots + \lambda_m$. Ha $\lambda = 0$, akkor adódik, hogy $\lambda_1 = \cdots = \lambda_m$. Ha viszont $\lambda \neq 0$, akkor λ_i-k azonosak, és λ-val ellenkező előjelűek, ami lehetetlen. □

A következő tételhez előkészületként igazolunk néhány lineáris algebrai állítást, ami tetszőleges test felett igaz. A továbbiakban V egy F test felettti

véges dimenziós vektortér, amelynek bázisa $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$. A Szokásos módon értelmezzük a skaláris szorzatot. Ha M altere V-nek, akkor $M^\perp$ jelöli az M minden elemére merőleges vektorok halmazát. Könnyen látható, hogy $M^\perp$ is altér, azonban $M \cap M^\perp = \{\mathbf{0}\}$ nem feltétlenül teljesül.

1. Lemma *Ha M altér V-ben,* $\dim(M) = k$, $\dim(V) = n$, *akkor*

$$\dim(M^\perp) = n - k.$$

Bizonyítás. Ha $\{\mathbf{a}_1, \ldots, \mathbf{a}_k\}$ bázis M-ben, akkor a

$$\sum_{i=1}^{n} x_i \mathbf{e}_i \mathbf{a}_j = 0 \quad (j = 1, \ldots, k)$$

lineáris egyenletrendszer megoldásait keressük. Ennek dimenziója nagyobb $n-k$-nál akkor, ha az egyenletek között van lineáris összefüggés, azaz vannak nemnulla $\mu_1, \ldots, \mu_k$ skalárok, hogy

$$\sum_{j=1}^{k} \mu_j \mathbf{e}_i \mathbf{a}_j = 0 \quad (i = 1, \ldots, n).$$

De ez azt jelenti, hogy $\mathbf{b} = \mu_1 \mathbf{a}_1 + \cdots + \mu_k \mathbf{a}_k$-ra igaz, hogy merőleges $\mathbf{e}_1, \ldots, \mathbf{e}_n$-re, ami lehetetlen. □

2. Lemma *Ha M altér V-ben, akkor $(M^\perp)^\perp = M$.*

Bizonyítás. Ugyanis $(M^\perp)^\perp \supseteq M$ és az előző lemma miatt ugyanannyi a dimenziójuk. □

3. Lemma *Ha M altér V-ben, akkor $M + M^\perp = (M \cap M^\perp)^\perp$.*

Bizonyítás. Egy vektor akkor merőleges $M + M^\perp$-re, ha merőleges M-re és $M^\perp$-re is. Ezért

$$(M + M^\perp)^\perp = M \cap \ M^\perp.$$

Mindkét oldalra alkalmazva a $\perp$ operációt és felhasználva a 2. Lemmát kapjuk a bizonyítandót. □

4. Lemma $F = \mathrm{GF}(2)$ *esetén* $\mathbf{j} = (1, \ldots, 1) \in M + M^\perp$.

Bizonyítás. Ha $\mathbf{u} \in M \cap M^\perp$, akkor $\mathbf{uu} = 0$, tehát $\mathbf{u}$ olyan 0-1 vektor, aminek páros sok 1 koordinátája van, azaz $\mathbf{ju} = 0$. □

36. Tétel. (Gallai-Chen) *Minden véges gráf szögponthalmaza két (esetleg üres) részre partícionálható, hogy a részeken belül minden pont foka páros.*

1. Bizonyítás. (Gallai Tibor, W. K. Chen) Jelölje V a csúcsok, E az élek halmazát. Vegyük azt a GF(2) fölötti vektorteret, aminek vektorai E részhalmazai, pontosabban az E-ből $\{0,1\}$-be képező függvények. Két vektor összege a szimmetrikus differencia, ha halmaznak, a pontonkénti mod 2 összeg, ha függvénynek tekintjük őket.

Tekintsük a csillagok, tehát az egy csúcsból kiinduló élek halmazai által generált alteret. Ez könnyen láthatóan tartalmazza $\emptyset$-t, E-t, valamint éppen a *vágás*okat, tehát azokat az élhalmazokat, amelyek előállnak valamilyen $V = A \cup B$ partícióból, mint a keresztező élek halmaza. A 4. Lemma szerint E felbomlik, mint $E = \mathbf{x} + \mathbf{y}$, tehát két részhalmaza szimmetrikus differenciájára, amelyek közül az egyik vágás, a másik pedig merőleges minden vágásra.

Mivel a teljes E halmazt kapjuk meg, a szimmetrikus differencia itt csak diszjunkt unió lehet. Ha $\mathbf{x}$ V-nek az (A, B) partíciója, akkor $\mathbf{y}$ persze az A-beli, illetve B-beli belső élek halmaza. Az pedig, hogy $\mathbf{y}$ merőleges minden csillagra, pontosan azt jelenti, hogy az $\mathbf{y}$ élhalmaz minden pontban párosfokú, tehát (A, B) a kívánt tulajdonságú felbontás. □

A tétel érdekessége, hogy noha úgy tűnik, hogy a fenti „a" bizonyítás, belátható teljesen elemi okoskodással is.

2. Bizonyítás. (Pósa Lajos) Az állítást a gráf csúcsainak n száma szerinti indukcióval igazoljuk. Az állítás nyilván igaz, ha $n = 1$. Tegyük fel, hogy igaz az állítás n-re és G egy gráf $n+1$ szögponton. Megint készen vagyunk, ha G minden pontja páros fokszámú (ekkor úgy bontjuk két részre a pontokat, hogy az egyik rész az üres halmaz). Feltehető tehát, hogy az egyik pont, mondjuk p fokszáma páratlan. Jelölje N p szomszédainak halmazát, legyen M a többi pont halmaza, tehát az összes pontok V halmaza így bomlik fel: $V = \{p\} \cup N \cup M$. Vegyük most $N \cup M$-en azt a H gráfot, ami úgy keletkezik G-ből, hogy N-en a komplementerét vesszük, tehát két N-beli pontot akkor és csak akkor kötünk össze H-ban, ha nincsenek összekötve G-ben (egyébként H élei azonosak G-éivel).

Mivel H pontszáma n, feltevésünk szerint van tételbeli felbontása: $N \cup M = A \cup B$. Mivel N páratlan, A és B közül az egyikre és csak az egyikre, mondjuk A-ra igaz, hogy $|A \cap N|$ páros. Adjuk p-t A-hoz, tehát tekintsük V-nek azt a $V = A' \cup B'$ felbontását, amiben $A' = A \cup \{p\}$ és $B' = B$.

Be kell látnunk, hogy minden A'-beli pont páros sok A'-belivel van összekötve és hasonlóan B'-re is. A dolog nyilvánvaló p-re, hiszen A'-beli fokszáma $|A \cap N|$. Az M-beli pontokra teljesül az állítás, mert H egy jó felbontásából indultunk ki. Vegyünk tehát egy $q \in N \cap A$ pontot. A feltevés szerint H-beli fokszáma páros. Tegyük fel, hogy q H-ban x $N \cap A$-beli ponttal van összekötve. Ha H helyett G-t vizsgáljuk, akkor q fokszáma eggyel nő (mert be van kötve p-be), és $N \cap A$-beli fokszáma x-ről $|N \cap A| - 1 - x$-re változik, tehát lesz egy további $|N \cap A| - 1 - 2x$-es növekedése, ami páratlan. Végső soron azt kapjuk, hogy q G-ben páros sok A'-beli ponttal van összekötve. Hasonlóan intézhető el az az eset, amikor $N \cap B$-beli pont G-beli fokszámát vizsgáljuk. □

Irodalom

[1] Wai-Kai Chen: On vector spaces associated wit a graph, *SIAM Journal of Applied Math.*, **20**(1971), 526–529.

[2] R. L. Graham, H. O. Pollak: On embedding graphs in squashed cubes, in: *Graph Theory and Applications*, Lecture Notes in Mathematics, **303**, Springer, 1972, 99–110.

[3] T. W. Williams, L. M. Maxwell: The decomposition of a graph and the introduction of a new class of subgraphs, *SIAM J. Appl. Math.*, **20**(1971), 385–389.

[4] D. M. Woodall: A proof of McKee's Eulerian-bipartite characterization, *Disc. Math.*, **84**(1990), 217–220.

Mikor azonosan nulla egy polinom?

Valós polinomok esetében (vagy általában nulla karakterisztikájú esetben) akkor, ha minden együtthatója nulla. Időnként előfordulhat, hogy könnyebben tudunk egy polinomot különböző helyeken kiértékelni, mint a polinom együtthatóit megadni; ilyen polinomok adódhatnak például determinánsokból. Ezért érdemes azzal foglalkozni, hogyan tudjuk eldönteni egy polinomba történő behelyettesítésekkel, hogy azonosan nulla polinomról van-e szó.

37. Tétel. *Ha S véges (valós) halmaz, $p(x_1, \ldots, x_n)$ k-adfokú nemnulla polinom, akkor*

$$\left|\left\{(x_1, \ldots, x_n) \in S^n : p(x_1, \ldots, x_n) = 0\right\}\right| \leq k|S|^{n-1}.$$

Bizonyítás. Az állítást n-re indukcióval igazoljuk. Ha $n = 1$, egyváltozós polinomnak legfeljebb annyi gyöke van, mint a fokszáma, azaz k.

Tegyük fel, hogy az állítás igaz n változós polinomokra és adott az $n+1$-változós $p(x_1, \ldots, x_n, y)$ polinom. Fejtsük ki p-t y hatványai szerint:

$$p(x_1, \ldots, x_n, y) = q_m(x_1, \ldots, x_n)y^m + \cdots + q_0(x_1, \ldots, x_n)$$

ahol $q_m(x_1, \ldots, x_n)$ nemnulla polinom, amiben minden tag foka, nyilvánvalóan legfeljebb $k - m$.

Osszuk két halmazra azon $(x_1, \ldots, x_n, y) \in S^{n+1}$ sorozatok halmazát, amikre $p(x_1, \ldots, x_n, y) = 0$. Az elsőbe tartozzanak azok, amikre

$$q_m(x_1, \ldots, x_n) = 0,$$

a másikba a többi. Az első csoportba az indukció szerint legfeljebb $(k - m)|S|^{n-1} \cdot |S|$ sorozat tartozik (az utolsó tényező onnan adódik, hogy minden ideeső $(x_1, \ldots, x_n)$ sorozatot tetszés szerint kiegészíthetünk egy $y \in S$ elemmel). Egy adott $(x_1, \ldots, x_n)$ sorozatra, amire $q_m(x_1, \ldots, x_n) \neq 0$, legfeljebb m olyan y érték lehet, hogy $p(x_1, \ldots, x_n, y) = 0$, ezért a második csoport elemszáma legfeljebb $m|S|^n$, összesen tehát legfeljebb

$$(k - m)|S|^n + m|S|^n = k|S|^n$$

megoldásunk van. □

Ez a tétel egyszerű véletlen algoritmust ad annak eldöntésére, hogy egy polinom nulla-e: ha a polinom foka k, választunk egy $2k$ elemszámú S halmazt, és ebből véletlen választásokkal nyert elemekkel kiszámítjuk a polinom értékét. Ha a polinom nem nulla, akkor legfeljebb 50 % valószínűséggel kaphatunk 0-t, tehát ezt a kisérletet sokszor megismételve nagy valószínűséggel nem nulla eredményt kapunk.

Egy ilyen véletlen algoritmus eldöntheti, hogy van-e egy adott páros gráfban teljes párosítás (amire persze van jólismert determinisztikus algoritmus is). Valóban, legyen a G páros gráf adott az $A = \{a_1, \ldots, a_k\}$ és $B = \{b_1, \ldots, b_k\}$ halmazokon. Pontosan akkor van teljes párosítás ha van $\pi : \{1, \ldots, k\} \to \{1, \ldots, k\}$ permutáció, hogy minden $1 \leq i \leq k$-ra a_i össze van kötve $b_{\pi(i)}$-vel.

Ehhez készítsük el azt a determinánst, amiben, az i-edik sor j-edik helyén nulla áll, ha a_i nincs összekötve b_j-vel, egyébként pedig az x_{ij} változó. Ezzel

tehát olyan polinomot kapunk, amiben annyi változó szerepel, ahány éle G-nek van, a polinom pontosan a párosításoknak megfelelő kifejtési tagokból áll, ezért (ha nem azonosan nulla) k-adfokú. Könnyen meggondolható, hogy a polinom pontosan akkor azonosan nulla, ha a gráfnak nincs teljes párosítása. A fenti tételt használva kapjuk, hogy ha a gráfnak van párosítása és egy $2k$-elemű halmazból véletlenszerűen helyettesítünk, akkor legalább 50% valószínűséggel nemnullát kapunk, ami bizonyítja párosítás létezését.

A valós esettől eltérő a véges testek esete: valóban, ha F q-elemű véges test, akkor F-en az $x^q - x$ polinom azonosan nulla. Fontos alkalmazásai vannak olyan észrevételeknek, amelyek véges test feletti nemnulla polinomokról mutatják meg, hogy nem tűnhetnek mindenütt el.

Először is, ha $P(x)$ egy legfeljebb $(q-1)$-edfokú, nemnulla, F test feletti polinom, ahol $|F| = q$, akkor $P(x)$ nem tűnhet el azonosan. Valóban, ez abból az indukcióval kapható ismert állításból adódik, hogy egy d-edfokú polinomnak legfeljebb d gyöke lehet.

Ezt az állítást könnyen kiterjeszthetjük többváltozós polinomokra.

38. Tétel. *Legyen F test, $|F| = q$, $P(x_1, \ldots, x_n)$ polinom F fölött, ami minden változójában legfeljebb $(q-1)$-edfokú. Ekkor P nem azonosan nulla.*

Bizonyítás. A tételt n-re indukcióval bizonyítjuk. Az $n = 1$ esetet már láttuk. Ha $n-1$-re már tudjuk az állítást és adott $P(x_1, \ldots, x_n)$, fejtsük ki P-t x_n hatványai szerint:

$$P_0(x_1, \ldots, x_{n-1}) + P_1(x_1, \ldots, x_{n-1})x_n + \cdots + P_m(x_1, \ldots, x_{n-1})x_n^m,$$

ahol P_m nem a nulla polinom. Feltevéseink szerint $m \leq q-1$, továbbá minden $a_1, \ldots, a_{n-1} \in F$-re

$$P_0(a_1, \ldots, a_{n-1}) + P_1(a_1, \ldots, a_{n-1})x + \cdots + P_m(a_1, \ldots, a_{n-1})x^m,$$

az azonosan nulla polinom. Ez csak úgy lehet, ha a polinom együtthatói nullák, speciálisan $P_m(a_1, \ldots, a_{n-1}) = 0$. Mivel ez minden $a_1, \ldots, a_{n-1}$ behelyettesítésre teljesül, az indukció miatt P_m a nulla polinom, ellentmondás. □

Ennek fontos kiterjesztése Noga Alon kombinatorikus nullhelytétele.

39. Tétel. *Legyen F test, $f(x_1, \ldots, x_n)$ polinom F fölött. Legyenek $S_1, \ldots, S_n$ nemüres részhalmazok F-ben. Legyen f egyik (nemnulla együtthatós) tagja*

$x_1^{t_1} \cdots x_n^{t_n}$, *tegyük fel, hogy* f *foka* $t_1 + \cdots + t_n$ *és* $t_1 < |S_1|, \ldots, t_n < |S_n|$. *Ekkor vannak* $s_1 \in S_1, \ldots, s_n \in S_n$ *elemek, hogy* $f(s_1, \ldots, s_n) \neq 0$.

Bizonyítás. Az állítást n-re való indukcióval igazoljuk. Az $n = 1$ eset egyszerűen az a jólismert állítás, hogy minden polinomnak legfeljebb annyi gyöke van, mint amennyi a fokszáma. Tegyük fel tehát, hogy igaz az állítás $n-1$-re és legyen adva $f, t_1, \ldots, t_n, S_1, \ldots, S_n$ mint a tételben. Fejtsük ki f-et x_n hatványai szerint:

$$f = f_0 + f_1 x_n + f_2 x_n^2 + \cdots$$

ahol $f_0, f_1, \ldots$ az $x_1, \ldots, x_{n-1}$ változók polinomjai. Tudjuk, hogy f_{t_n}-ben van legalább egy nemnulla együtthatós $x_1^{t_1} \cdots x_{n-1}^{t_{n-1}}$ tag és f_{t_n} foka pontosan $t_1 + \cdots + t_{n-1}$. Ezért az indukciós feltevés miatt megválaszthatjuk az $s_1 \in S_1, \ldots, s_{n-1} \in S_{n-1}$ értékeket, hogy $f_{t_n}(s_1, \ldots, s_{n-1}) \neq 0$ teljesüljön. Vegyük a $g(x_n) = f(s_1, \ldots, s_{n-1}, x_n)$ polinomot, ekkor ebben $x_n^{t_n}$ együtthatója nem nulla, tehát $g(x_n)$ foka legalább t_n. Mivel $|S_n| > t_n$, a bizonyítás elején említett tétel miatt van olyan $s_n \in S_n$ érték, amire $g(s_n) \neq 0$ és készen vagyunk. □

Ebből gyorsan levezethetjük a Cauchy-Davenport-tételt és az Erdős-Ginzburg-Ziv tételt is.

Az elsőhöz legyen $F = \mathrm{GF}(p)$, a mod p maradékosztályok teste. Tegyük fel, hogy A, B maradékosztályokból álló nemüres halmazok, amikre $|C| \leq |A| + |B| - 2$ és $|C| < p$ teljesül, ahol $C = A + B$. Legyen

$$f(x, y) = \prod_{c \in C} (x + y - c).$$

Ebben szerepel minden $x^n y^m$ alakú tag, ahol $n+m = |C|$, mivel az együtthatók nem oszthatók p-vel. Itt meg tudjuk választani n-et és m-et úgy, hogy $n < |A|$, $m < |B|$ is teljesüljön. Ekkor a tételt alkalmazva adódik, hogy van $a \in A$, $b \in B$, amire $f(a, b) \neq 0$, azaz $a + b \notin C$, ellentmondás.

Az Erdős-Ginzburg-Ziv-tételhez tegyük fel, hogy $a_1, \ldots, a_{2p-1}$ maradékosztályok mod p, ahol p megint prímszám. Legyen $S_1 = \cdots = S_{2p-1} = \{0, 1\}$, $t_1 = \cdots = t_{2p-1}$, és legyen

$$F = AB - C$$

ahol

$$A = 1 - \left(\sum a_i x_i\right)^{p-1}, \quad B = 1 - \left(\sum x_i\right)^{p-1}, \quad C = \prod (1 - x_i).$$

F $(2p-1)$-edfokú polinom, mivel A és B $(p-1)$-edfokúak, C pedig $(2p-1)$-edfokú és szerepel benne (és így F-ben is) az $x_1 \cdots x_{2p-1}$ tag. Megválaszthatjuk tehát a tételben $t_1 = \cdots = t_{2p-1} = 1$-et. Azt kapjuk, hogy vannak nullákkból és egyesekből álló $x_1, \ldots, x_{2p-1}$ értékek, amikre $F(x_1, \ldots, x_{2p-1}) \neq 0$. Az Euler-Fermat-tétel és feltevéseink szerint A, B és C csak 0 vagy 1 értéket vehet föl. Tehát $AB = 0$ és $C = 1$ vagy $AB = 1$ és $C = 0$.

Az első esetben $x_1 = \cdots = x_{2p-1} = 0$ de ekkor $A = B = 1$, lehetetlen. A második esetben $A = B = 1$ és $C = 0$. Az utóbbi, $C = 0$, csak úgy teljesülhet, ha valamelyik $x_i \neq 0$. Az előzőből az adódik, hogy $\sum x_i$ és $\sum a_i x_i$ is osztható p-vel. De ez csak úgy lehet, ha az x_i-k közül pontosan p értéke 1, a többié 0. Ekkor viszont az, hogy $\sum a_i x_i$ osztható p-vel, pontosan azt jelenti, hogy az a_i-k között van p, amiknek az összege osztható p-vel.

Hasonlóan röviden levezethető Dias da Silva és Hamidoune tétele, amivel Erdős és Heilbronn sejtését igazolták.

40. Tétel. *Ha p prímszám, A mod p maradékosztályrendszer, $k = |A| \geq 2$, $B = \{a_1 + a_2 : a_1, a_2 \in A, a_1 \neq a_2\}$, akkor $|B| \geq \min(p, 2k-3)$.*

Bizonyítás. A-ból elemeket elhagyva feltehetjük, hogy $2k-3 \leq p$. Rögzítsünk egy $a \in A$ elemet, nyilván igaz, hogy

$$B = \{a_1 + a_2 : a_1 \in A, a_2 \in A - \{a\}, a_1 \neq a_2\}.$$

Ha $|B| < 2k-3$, legyen $C \supseteq B$ olyan maradékrendszer, amire $|C| = 2k-4$. Legyen $f(x,y)$ a következő polinom:

$$f(x,y) = (x-y) \prod_{c \in C} (x+y-c).$$

Ennek fokszáma $n = 2k-3$. A pontosan n-edfokú tagok az

$$(x-y)(x+y)^{n-1}$$

szorzat tagjai, a binomiális tételből az adódik, hogy $x^{k-1}y^{k-2}$ együtthatója

$$\binom{2k-4}{k-2} - \binom{2k-4}{k-1} = \frac{(2k-4)!}{(k-2)!(k-3)!},$$

ami nem osztható p-vel, mivel $p > 2k-4$. Így alkalmazhatjuk a 34. Tételt, az $n = 2$, $t_1 = k-1$, $t_2 = k-2$ választással, az $A, A - \{a\}$ halmazokra. Az adódik, hogy van $x \in A$, $y \in A - \{a\}$, amire $f(x,y) \neq 0$, ami ellentmondás. □

Irodalom

[1] N. Alon: Combinatorial Nullstellensatz, *Combinatorics, Probability, and Computing*, **8**(1999), 7–29.

[2] N. Alon: Algebraic and probabilistic methods in discrete mathematics,

[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.

Besicovitch halmazok véges test feletti terekben

Besicovitch 1919-ben igazolta azt a meghökkentő tényt, hogy van olyan síkbeli nullmértékű halmaz, ami minden irányban tartalmaz egységhosszúságú szakaszt. Az utóbbi években felvetődött, hogy igaz-e a tétel véges test fölött is (teljes egyeneseket megkövetelve).

41. Tétel. (Zeev Dvir) *Ha F q-elemű véges test, $K \subseteq F^n$ olyan részhalmaz, ami minden irányban tartalmaz egyenest, akkor $|K| \geq c_n q^n$ alkalmas $c_n > 0$ konstansra.*

Bizonyítás. Elég belátni, hogy $|K| \geq \binom{q+n-1}{n}$. Ugyanis

$$\binom{q+n-1}{n} = \frac{(q+n-1)(q+n-2)\cdots q}{n!} \geq \frac{q \cdot q \cdots q}{n!} = \frac{1}{n!} q^n.$$

A bizonyításhoz tegyük fel indirekten, hogy $|K| < \binom{q+n-1}{n}$.

Azt állítjuk, hogy van olyan F feletti nemnulla, legfeljebb $q-1$-fokú $P(x_1, \ldots, x_n)$ polinom, ami K minden pontjában eltűnik. Valóban, a kívánt polinom

$$P(x_1, \ldots, x_n) = \sum_{i_1 + \cdots + i_n \leq q-1} c_{i_1, \ldots, i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$$

alakban írható, ahol az együtthatók nem mind nullák. A tagok száma annyi, ahány megoldása van az $i_1 + \cdots + i_n \leq q-1$ egyenlőtlenségnek a természetes számok körében. Elemi kombinatorikai számítás adja, hogy ez $\binom{q+n-1}{n}$.

Az a feltétel, hogy P eltűnik egy $(a_1, \ldots, a_n) \in K$ pontban, természetesen azt jelenti, hogy

$$\sum_{i_1 + \cdots + i_n \leq q-1} c_{i_1, \ldots, i_n} a_1^{i_1} a_2^{i_2} \cdots a_n^{i_n} = 0$$

teljesül. Ha itt a $c_{i_1,\dots,i_n}$ együtthatókat **ismeretlenek**nek tekintjük, akkor ez számukra egy homogén lineáris egyenlet. Mivel ezt K minden elemére feltesszük, a $c_{i_1,\dots,i_n}$ ismeretleneknek egy $|K|$ egyenletből álló homogén lineáris egyenletrendszert kell kielégíteniük. Az ismeretlenek száma nagyobb, mint az egyenleteké, ezért létezik nem csupa nullából álló megoldás. Létezik tehát a kívánt $P(x_1,\dots,x_n)$ polinom.

Írjuk fel P $P_0+\dots+P_m$ homogén felbontását, azaz legyen

$$P_k(x_1,\dots,x_n)=\sum_{i_1+\dots+i_n=k} c_{i_1,\dots,i_n}x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}.$$

Itt $m\le q-1$ a legnagyobb érték, amire P_m nem csupa nulla együtthatóból áll.

Most megfogalmazzuk a tételbeli feltételt: K minden irányra tartalmaz egyenest. Azaz, ha $b=(b_1,\dots,b_n)\in F^n$, akkor létezik $a=(a_1,\dots,a_n)\in F^N$, hogy minden $x\in F$-re $P(a_1+b_1x,a_2+b_2x,\dots,a_n+b_nx)=0$. Ez tehát egy egyváltozós, legfeljebb $m\le q$-adfokú polinom, ami minden x-re nulla. Ez csak úgy lehet, ha minden együtthatója nulla (38. Tétel). Az x^m-et tartalmazó tagot úgy kapjuk meg, ha a P_m-beli szorzatokban minden változóból az x-et tartalmazó tagot választjuk. Így

$$\sum_{i_1+\dots+i_n=m} c_{i_1,\dots,i_n}(b_1x)^{i_1}(b_2x)^{i_2}\cdots(b_nx)^{i_n}=P_m(b_1,\dots,b_n)x^m$$

adódik, tehát $P_m(b_1,\dots,b_n)=0$. Mivel ez minden $(b_1,\dots,b_n)\in F^n$-re igaz, ismét a 38. Tételre hivatkozva adódik, hogy P_m együtthatói valamennyien nullák, ellentmondás. □

Irodalom

[1] Zeev Dvir: On the size of Kakeya sets.

Számelmélet a kombinatorikában: a Berge-Sauer sejtés

A Chevalley-Warning tétel következő formája segítségével majdnem megoldunk egy reguláris gráfokra vonatkozó sejtést.

42. Tétel. *Ha p prímszám, $f_1(x_1,\dots,x_n),\dots,f_m(x_1,\dots,x_n)$ homogén d-fokú polinomok mod p és $n>md$, akkor van nemtriviális közös gyökrendszerük.*

Bizonyítás. Mivel homogén polinomokról van szó, egy megoldásuk mindenképpen van: a triviális

$$(x_1, \ldots, x_n) = (0, \ldots, 0).$$

A célunk belátni, hogy van legalább egy további megoldás. Legyen

$$F(x_1, \ldots, x_n) = \prod_{i=1}^{m} \bigl(1 - f_i(x_1, \ldots, x_n)^{p-1}\bigr).$$

Nyilván $F(x_1, \ldots, x_n) = 1$ akkor, ha $(x_1, \ldots, x_n)$ megoldása az egyenletrendszernek, különben 0. Ezért

$$\sum_{x_1} \cdots \sum_{x_n} F(x_1, \ldots, x_n) \equiv N \pmod{p}$$

ahol N az egyenletrendszer összes megoldásának száma, beleértve a triviális $(0, \ldots, 0)$-t is. Belátjuk, és ez elég, hogy a képlet baloldala, és így N is, osztható p-vel. A p^n darab 1-esből adódó tag összege nyilván osztható p-vel. A többi tagot úgy csoportosíthatjuk, hogy minden csoport

$$c \sum_{x_1} \cdots \sum_{x_n} x_1^{i_1} \cdots x_n^{i_n} = c \left(\sum_{x_1} x_1^{i_1} \right) \cdots \left(\sum_{x_n} x_n^{i_n} \right)$$

alakú, ahol $0 < i_1 + \cdots + i_n < n(p-1)$. Itt valamelyik i_j mindenképpen kielégíti $0 \leq i_j < p-1$-et, hiszen ha ennél nagyobbak lennének, az ellentmondana annak, hogy az összegük kisebb $n(p-1)$-nél. De ekkor a fenti szorzat, a 26. oldalon levő 1. Lemma szerint

$$\sum_{x_j} x_j^{i_j}$$

faktora osztható p-vel. □

Berge-Sauer sejtés *Minden véges reguláris negyedfokú gráfban van reguláris harmadfokú részgráf.*

43. Tétel. (N. Alon, S. Friedland, G. Kalai) *Ha egy véges, 4-reguláris gráfhoz hozzáadunk egy további élt, az új gráf tartalmaz 3-reguláris részgráfot (aminek tehát minden pontban 0 vagy 3 a foka és van éle).*

Bizonyítás. Ha az eredeti gráfnak v pontja van, akkor a 4-regularitás miatt $2v$ így az újnak $2v+1$ éle lesz. Vezessünk be minden élhez egy x_i változót és irjunk fel minden szögponthoz egy

$$\sum x_i^2 \equiv 0 \pmod 3$$

egyenletet, ahol a szumma az adott pontra illeszkedő élekhez tartozó változókat tartalmazza. Ezzel v homogén másodfokú egyenletből álló $2v+1$ ismeretlenre vonatkozó egyenletrendszerünk van mod 3, aminek az előbbi tétel szerint van nemtriviális megoldása. Ha most a nemnulla x_i-khez tartozó éleket vesszük, akkor a fenti szummákban mindenütt 1-et adnak, azaz az élek által alkotott részgráf foka minden pontban 0 vagy 3. □

Irodalom

[1] N. Alon, S. Friedland, G. Kalai: Regular subgraphs of almost regular graphs, *Journal of Combinatorial theory*(B), **37**(1984), 79–91.

[2] V. A. Tashkinov: 3-regular subgraphs of 4-regular graphs, *Mat. Zametki* **36**(1984), 239–259.

Egymástól páratlan távolságra levő pontok

44. Tétel. (R.L.Graham, B.L.Rothschild, E.G.Straus) *Az n dimenziós térben pontosan akkor lehet $n+2$ egymástól páratlan távolságra levő pontot megadni, ha $n \equiv 14 \pmod{16}$.*

Bizonyítás. Először azt igazoljuk, hogy, ha van adott tulajdonságú pontrendszer, akkor $n \equiv 14 \pmod{16}$. Ehhez szükségünk lesz egy Cayley-féle eredményre.

1. Lemma. *Ha $\mathbf{a}_1, \ldots, \mathbf{a}_{n+2}$ az n-dimenziós tér vektorai, akkor vannak nem csupa nulla $\lambda_1, \ldots, \lambda_{n+2}$ valós számok, hogy*

$$\lambda_1 \mathbf{a}_1 + \cdots + \lambda_{n+2} \mathbf{a}_{n+2} = 0$$

és

$$\lambda_1 + \cdots + \lambda_{n+2} = 0$$

is teljesül.

Bizonyítás. Vektorainknak n koordinátája van. Egészítsük ki mindegyiket egy új, $n+1$-edik koordinátával, aminek az értéke 1. Ekkor az $n+1$-dimenziós térben levő $n+2$ vektort kapunk, van tehát közöttük nemtriviális lineáris összefüggés. Ez pontosan azt jelenti, leolvasva az első n, illetve az utolsó koordinátát, amit a Lemma állít. □

2. Lemma. (Cayley) *Ha $a_1, \ldots, a_{n+2}$ az n-dimenziós tér pontjai, akkor*

$$\begin{vmatrix} 0 & d^2(a_1,a_2) & \ldots & d^2(a_1,a_{n+1}) & d^2(a_1,a_{n+2}) & 1 \\ d^2(a_2,a_1) & 0 & \ldots & d^2(a_2,a_{n+1}) & d^2(a_2,a_{n+2}) & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ d^2(a_{n+1},a_1) & d^2(a_{n+1},a_2) & \ldots & 0 & d^2(a_{n+1},a_{n+2}) & 1 \\ d^2(a_{n+2},a_1) & d^2(a_{n+2},a_2) & \ldots & d^2(a_{n+2},a_{n+1}) & 0 & 1 \\ 1 & 1 & \ldots & 1 & 1 & 0 \end{vmatrix} = 0$$

ahol $d(a_i,a_j)$ az a_i és az a_j pont távolsága.

Bizonyítás. Vektorként kezelve a pontokat, minden $d^2(a_i,a_j)$ távolságnégyzet helyébe a különbség skaláris négyzetét írhatjuk:

$$\begin{vmatrix} (\mathbf{a}_1-\mathbf{a}_1)^2 & (\mathbf{a_1}-\mathbf{a}_2)^2 & \ldots & (\mathbf{a}_1-\mathbf{a}_{n+1})^2 & (\mathbf{a}_1-\mathbf{a}_{n+2})^2 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ (\mathbf{a}_{n+1}-\mathbf{a}_1)^2 & (\mathbf{a}_{n+1}-\mathbf{a}_2)^2 & \ldots & (\mathbf{a}_{n+1}-\mathbf{a}_{n+1})^2 & (\mathbf{a}_{n+1}-\mathbf{a}_{n+2})^2 & 1 \\ (\mathbf{a}_{n+2}-\mathbf{a}_1)^2 & (\mathbf{a}_{n+2}-\mathbf{a}_2)^2 & \ldots & (\mathbf{a}_{n+2}-\mathbf{a}_{n+1})^2 & (\mathbf{a}_{n+2}-\mathbf{a}_{n+2})^2 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 \end{vmatrix}$$

Itt alkalmazva az $(\mathbf{a}_i-\mathbf{a}_j)^2 = \mathbf{a}_i^2 - 2\mathbf{a}_i\mathbf{a}_j + \mathbf{a}_j^2$ kiszorzást, észrevehetjük, hogy az i-edik sorban az utolsót kivéve minden helyen szerepel $\mathbf{a}_i^2$, amit eltüntethetünk, ha levonjuk belőle az utolsó sor $\mathbf{a}_i^2$-szeresét. Ezt minden sorral és hasonlóan az oszlopokkal megcsinálva a következő marad:

$$\begin{vmatrix} -2\mathbf{a}_1^2 & -2\mathbf{a}_1\mathbf{a}_2 & \ldots & -2\mathbf{a}_1\mathbf{a}_{n+1} & -2\mathbf{a}_1\mathbf{a}_{n+2} & 1 \\ -2\mathbf{a}_2\mathbf{a}_1 & -2\mathbf{a}_2^2 & \ldots & -2\mathbf{a}_2\mathbf{a}_{n+1} & -2\mathbf{a}_2\mathbf{a}_{n+2} & \\ \vdots & \vdots & & \ddots & \vdots & \vdots \\ -2\mathbf{a}_{n+1}\mathbf{a}_1 & -2\mathbf{a}_{n+1}\mathbf{a}_2 & \ldots & -2\mathbf{a}_{n+1}\mathbf{a}_{n+1} & -2\mathbf{a}_{n+1}\mathbf{a}_{n+2} & 1 \\ -2\mathbf{a}_{n+2}\mathbf{a}_1 & & \ldots & -2\mathbf{a}_{n+2}\mathbf{a}_{n+1} & -2\mathbf{a}_{n+2}\mathbf{a}_{n+2} & 1 \\ 1 & 1 & \ldots & 1 & 1 & 0 \end{vmatrix}$$

Alkalmazva az 1. Lemmát, olyan $\lambda_1, \ldots, \lambda_{n+2}$ való számokat kapunk, amikre egyrészt

$$\lambda_1 + \cdots + \lambda_{n+2} = 0$$

másrészt

$$\lambda_1 \mathbf{a}_1 + \cdots + \lambda_{n+2} \mathbf{a}_{n+2} = 0$$

teljesül. Az utóbbi egyenlőséget $\mathbf{a}_i$-vel skalárisan szorozva azt kapjuk, hogy

$$\lambda_1 \mathbf{a}_1 \mathbf{a}_i + \cdots + \lambda_{n+2} \mathbf{a}_{n+2} \mathbf{a}_i = 0.$$

Ebből viszont az adódik, hogy a fenti mátrix első $n+2$ oszlopát rendre $\lambda_1, \ldots, \lambda_{n+2}$-vel megszorozva és összeadva a 0 oszlopot kapjuk, innen adódik, hogy a kérdéses determináns értéke 0. □

Ez tehát szimmetrikus mátrix, a főátlóban csupa nulla elemmel. A többi helyen páratlan szám négyzete, tehát $8k+1$ alakú szám áll. Ezeket az értékeket sorra 1-re változtatjuk és megfigyeljük, hogyan változik a determináns értéke. Nézzünk egy $x = 8k+1$ értéket! Mivel x kétszer, a főátlóra tükrösen fordul elő a determinánsban, a determinánst alkotó tagokat három részre oszthatjuk: azok, amelyekben nem fordul elő, azok amelyekben előfordul de csak egyszer, és azok, amelyekben kétszer fordul elő. A második csoport tagjai párosíthatók, egymásnak megfeleltetve a főátlóra szimmetrikus tagokat. Így végül azt kapjuk, hogy a determináns értéke $A + 2Bx + Cx^2$ alakú, ahol A, B, C egész számok. Ha tehát x-et mindkét determinánsbeli előfordulásában 1-re változtatjuk, akkor a determináns értékének csökkenése

$$(A + 2Bx + Cx^2) - (A + 2B + C) = 16k(B + C(4k^2 + 1)),$$

ezért a 16-tal vett maradék nem változik. Ezt folytatva eljutunk ahhoz az $(n+3)\times(n+3)$-as determinánshoz, amiben csupa egyes áll, kivéve a főátlóban, ahol csupa nulla. A következő lépésben kiszámítjuk ennek az értékét.

3. Lemma.

$$\begin{vmatrix} 0 & 1 & \ldots & 1 \\ 1 & 0 & \ldots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \ldots & 0 \end{vmatrix} = (n+2)(-1)^{n+2}.$$

Bizonyítás. Először minden sor hozzáadunk az elsőhöz:

$$\begin{vmatrix} 0 & 1 & \dots & 1 \\ 1 & 0 & \dots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \dots & 0 \end{vmatrix} = \begin{vmatrix} n+2 & n+2 & \dots & n+2 \\ 1 & 0 & \dots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \dots & 0 \end{vmatrix} = (n+2) \begin{vmatrix} 1 & 1 & \dots & 1 \\ 1 & 0 & \dots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \dots & 0 \end{vmatrix}$$

Ezután az első sort levonjuk a többiből:

$$= (n+2) \begin{vmatrix} 1 & 1 & \dots & 1 \\ 0 & -1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & -1 \end{vmatrix} = (n+2)(-1)^{n+2}.$$

□

Végül tehát az adódik, hogy nullához 16 többszörösét adva $n+2$ többszöröséhez jutunk, azaz $n+2$ osztható 16-tal.

A konstrukcióhoz első ötletünk az, hogy alkalmas szabályos szimplexet és középpontját vesszük, ez éppen $n+2$ pont. E célból kiszámítjuk az n-dimenziós térben levő egység élhosszúságú reguláris szimplex középpontjának távolságát a csúcsoktól.

4. Lemma. *Az n-dimenziós térben levő egység élhosszúságú reguláris szimplex középpontjának távolságát a csúcsoktól: $\sqrt{n/2(n+1)}$.*

Bizonyítás. Az állítást n-re vonatkozó indukcióval látjuk be, az $n=1$ eset nyilvánvaló. Tegyük fel hogy $n-1$-re igaz az állítás: az egymástól egységnyi távolságra levő $P_1, \dots, P_{n+1}$ pontok C centruma mindegyiktől $\sqrt{(n-1)/2n}$ távolságra van. A P_{n+2} pont hozzávételével kapott rendszer centruma az a D pont ami a CP_{n+2} szakaszon van és azt $PD : CD = n : 1$ arányban osztja. Innen adódik, hogy

$$PD = \frac{n}{n+1}\sqrt{1 - CP_1^2} = \frac{n}{n+1}\sqrt{1 - \frac{n-1}{2n}} = \sqrt{\frac{n}{2(n+1)}}.$$

□

Ha valamilyen n-re úgy akarjuk az n-dimenziós térben egy szabályos szimplex csúcsait és centrumát venni, hogy bármely két pont távolsága páratlan, akkor olyan x, y páratlan számokat kell találnunk, hogy

$$\frac{x}{y} = \sqrt{\frac{n}{2(n+1)}},$$

azaz az $x^2 = n/2$, $y^2 = n+1$ egyenletrendszert kell megoldanunk. Ekkor azonban $y^2 - 2x^2 = 1$, aminek, figyelembe véve a 8-cal vett maradékokat, nincsenek páratlan egész megoldásai.

Ötletünket a következőképpen javítjuk meg. Legyen $n = 16k-2$. Először egy $n-1$-dimenziós altérben elhelyezzük egy $8k-1$ élhosszúságú szimplex $P_1, \ldots, P_n$ csúcsát. Ezután az altérre a szimplex C centrumában merőleges egyenest emelünk, és azon az altér mindkét oldalán vesszük az altértől $2k-\frac{1}{2}$ távolságra levő pontot, legyenek ezek Q illetve R. A Q és R közötti távolság nyilvánvalóan $4k-1$. A P_iP_j távolságok, mint mondtuk, $8k-1$ hosszúak. Végül pedig egy $P_iQ = P_iR$ távolság így számítható ki:

$$P_iQ^2 = \left(2k - \frac{1}{2}\right)^2 + \left(\frac{16k-3}{16k-2}\right)(8k-1)^2 = 36k^2 - 12k + 1 = (6k-1)^2,$$

azaz a pontok egymástól való távolságai $4k-1, 6k-1, 8k-1$, csupa páratlan szám. □

Irodalom

[1] R. L. Graham, B. L. Rothschild, E. G. Straus: Are there $n+2$ points in E^n with odd integral distances ? *American Math. Monthly*, (1974), 21–25.

Az n-dimenziós kocka lefedése hipersíkokkal

Az n-dimenziós térben hipersíknak az $n-1$-dimenziós alterek eltoltjait értjük. Nyilvánvaló, hogy az egységkocka két ilyennel lefedhető: a kocka két szemközti lapját elég lefedni. A dolgot megnehezítjük azzal, hogy megköveteljük: a hipersíkok pontosan egy csúcsot ne fedjenek le. Ekkor n darabra van szükségünk.

45. Tétel. (N. Alon, Z. Füredi) *Ha az n-dimenziós kocka csúcsait úgy akarjuk hipersíkokkal lefedni, hogy pontosan egy maradjon ki, akkor legalább n hipersíkra van szükségünk.*

Bizonyítás. Feltehetjük, hogy a szóbanforgó kocka csúcsai azon $\mathbf{R}^n$-beli $(x_1, \ldots, x_n)$ pontok, amikben minden x_i koordináta 0-val vagy 1-gyel egyenlő. Feltesszük, hogy $n-1$ hipersík lefedi a kocka összes csúcsát, kivéve a $(0, \ldots, 0)$ pontot. Minden hipersík egy

$$a_1x_1 + \cdots + a_nx_n = b$$

egyenletű ponthalmaz. Ha algebrai úton kívánjuk leírni, hogy $n-1$ ilyen egyenletű ponthalmaz lefedi a kocka csúcsait, kivéve az origót, akkor összeszorozzuk a megfelelő, 0-ra redukált egyenleteket, így egy olyan $p(x_1,\dots,x_n)$ polinomot kapunk, amire $p(0,\dots,0)\neq 0$, de 0-t kapunk, ha bármilyen más 0-1 sorozatot helyettesítünk be. Mivel $n-1$ lineáris polinomot szoroztunk össze, $p(x_1,\dots,x_n)$ tagjai

$$c_{i_1,\dots,i_n}x_1^{i_1}\cdots x_n^{i_n}$$

alakúak, ahol a kitevők $i_1+\cdots+i_n$ összege legfeljebb $n-1$.

A polinom összes említett tulajdonsága megmarad, ha a fenti tagokban minden 1-nél nagyobb kitevőt 1-gyel helyettesítünk. Valóban, a számunkra érdekes 0-ra és 1-re igaz, hogy $x^i=x$ $(i=2,\dots)$, és a tagok teljes fokszáma csak csökkenhet.

Így feltehetjük, hogy $p(x_1,\dots,x_n)$

$$c+(c_1x_1+\cdots+c_nx_n)+(c_{12}x_1x_2+\cdots)+\cdots+(c_{12\dots(n-1)}x_1\cdots x_{n-1}+\cdots)$$

alakú, ahol $c\neq 0$.

Ha itt elvégezzük azt a helyettesítést, amiben $x_i=1$, a többi változó 0, akkor $c+c_i=0$-t kapunk, tehát $c_i=-c$ $(i=1,\dots,n)$. Helyettesítsünk most két x_i, mondjuk az x_i és az x_j helyére 1-et, a többi helyre 0-t! Ekkor $c-2c+c_{ij}=0$-t kapunk, azaz $c_{ij}=c$ minden $1\le i<j\le n$-re. Ezt folytatva indukcióval azt kapjuk, hogy

$$c_{i_1i_2\dots i_k}=(-1)^k c.$$

Valóban, ha ezt tudjuk a k-nál kisebb értékekre, és $x_{i_1}=x_{i_2}=\cdots=x_{i_k}=1$-et helyettesítünk (a többi helyre 0-t írva), akkor azt kapjuk, hogy

$$c+\binom{k}{1}(-1)c+\binom{k}{2}(-1)^2c+\cdots+c_{i_1i_2\dots i_k}=0.$$

Ez viszont csak úgy lehetséges (egy pillantást vetve $(1-1)^k=0$ binomiális kifejtésére), ha $c_{i_1i_2\dots i_k}=(-1)^k c$. De végül $p(1,\dots,1)=0$ miatt az is igaz, hogy

$$c-\binom{n}{1}c+\binom{n}{2}c+\cdots+(-1)^{n-1}\binom{n}{n-1}c=0$$

ami képtelenség, mert megint $(1-1)^n$ binomiális kifejtésére hivatkozva egy $(-1)^n c$-es tag hiányzik a baloldalról. □

A gondolatmenet könnyen módosítható arra az esetre, amikor az egységkocka helyett az $N \times N \times \cdots \times N$ élhosszúságú kockát, azaz a

$$K = \{(x_1, \ldots, x_n) : 0 \leq x_i \leq N, i = 1, 2, \ldots, n\}$$

rácspontjait akarjuk, az origó kivételével, lefedni.

45'. Tétel. *Ha K rácspontjait úgy akarjuk hipersíkokkal lefedni, hogy pontosan $(0, 0, \ldots, 0)$ maradjon ki, akkor legalább nN hipersíkra van szükségünk.*

Bizonyítás. Tegyük fel, hogy legfeljebb $Nn - 1$ hipersíkkal le tudjuk fedni $K - \{(0, \ldots, 0)\}$-t. Az előző bizonyításhoz hasonlóan ezt úgy fordítjuk le, hogy van legfeljebb $Nn-1$ polinom, amelyek mindegyike $a_1x_1 + \cdots + a_nx_n - b$ alakú, valamelyik mindig nulla, ha $0 \leq x_i \leq N$ egészek és nem mind 0, de $x_1 = \cdots = x_n = 0$-ra egyik sem 0.

Megint összeszorozva a polinomokat egy olyan

$$F(x_1, \ldots, x_n) = \sum a_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n}$$

polinomhoz jutunk, amire igaz, hogy $F(0, 0, \ldots, 0) \neq 0$, $F(k_1, \ldots, k_n) = 0$ minden más $(k_1, \ldots, k_n) \in K$ esetben, továbbá $i_1 + \cdots + i_n \leq Nn - 1$ teljesül az indexekre.

Az előző bizonyításhoz hasonlóan először redukáljuk az N-nél nagyobb kitevőket: ha egy $a_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n}$ tagban $i_k > N$, akkor az $x_k^{i_k}$ tényezőt $q(x_k)$-val helyettesítjük, ahol

$$x_k^{i_k} = f(x_k)p(x_k) + q(x_k),$$

ahol $f(x_k)$ az $x_k(x_k - 1) \cdots (x_k - N)$ polinom, $q(x_k)$ pedig egy legfeljebb N-edfokú polinom, azaz maradékosan osztjuk $x_k^{i_k}$-t az $(N+1)$-edfokú $f(x_k)$-val. Így $F(x_1, \ldots, x_n)$ helyett kapunk egy

$$G(x_1, \ldots, x_n) = \sum b_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n}$$

polinomot, ami rendelkezik F minden számunkra fontos tulajdonságával, annyit nyerünk viszont, hogy minden i_k értéke legfeljebb N. Mivel az $i_1 + \cdots i_n \leq Nn - 1$ feltétel továbbra is fennáll, $b_{N,N,\ldots,N} = 0$ teljesül. Leosztással azt is feltehetjük, hogy $b_{00\ldots0} = 1$.

Legyen $P(x)$ az

$$\frac{(-1)^N}{N!}(x - 1) \cdots (x - N) = A_N x^N + \cdots + A_0$$

polinom. Nyilvánvaló, hogy $P(1) = \cdots = P(N) = 0$ és $p(0) = 1$. Jegyezzük meg továbbá, hogy $A_0 = 1$ és $A_N \neq 0$.

Azt állítjuk, hogy a fenti G polinomra teljesül a

$$G(x_1, \ldots, x_n) = P(x_1) \cdots P(x_n)$$

egyenlőség. Ha ezt beláttuk, akkor készen vagyunk, hiszen a $b_{N,N,\ldots,N}$ együttható egyrészt 0, másrészt a kiszorzásból adódóan A_N^n, ami nem 0.

Legyen tehát $H(x_1, \ldots, x_n) = F(x_1, \ldots, x_n) - G(x_1, \ldots, x_n)$. A H polinom eltűnik K minden rácspontjában, továbbá monomjai $c_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n}$ alakúak, ahol $i_1, \ldots, i_n \leq n$. Belátjuk, n-re való indukcióval, hogy minden ilyen tulajdonságú H polinom minden együtthatója 0.

Valóban, ha az állítást tudjuk n-re és adott $H(x_1, \ldots, x_{n+1})$, akkor fejtsük ki H-t x_{n+1} hatványai szerint:

$$H(x_1, \ldots, x_{n+1}) = H_N(x_1, \ldots, x_n) x_{n+1}^N + \cdots + H_0(x_1, \ldots, x_n).$$

Rögzítsük az egész $0 \leq k_1, \ldots, k_n \leq N$ értékeket. Ekkor a

$$H(k_1, \ldots, k_n, x_{n+1}) = B_N x_{n+1}^N + \cdots + B_0$$

polinom nulla, ha $0 \leq x_{n+1} \leq N$ egész. N-edfokú polinomnak csak úgy lehet $N+1$ különböző gyöke, ha minden együtthatója 0, azaz $B_N = \cdots = B_0 = 0$. Azt kaptuk tehát, hogy a $H_N(x_1, \ldots, x_n), \ldots, H_0(x_1, \ldots, x_n)$ polinomok valamennyien nullák, ha $0 \leq x_1, \ldots, x_n \leq N$ egész. Ekkor viszont az indukció miatt nulla együtthatós polinomoknak kell lenniük. □

Irodalom

[1] N. Alon, Z. Füredi: Covering the cube by affine hyperplanes, *European Journal of Combinatorics* **14** (1993), 79–83 .

Diszkrét téglák

Ebben a fejezetben (n-dimenziós) téglának a véges $S_1 \times \cdots \times S_n$ alakú halmazokat nevezzük. Ennek résztéglája $T_1 \times \cdots \times T_n$, ha $T_i \subseteq S_i$ teljesül $i = 1, \ldots, n$-re. Ha még $\emptyset \neq T_i \neq S_i$ is teljesül $i = 1, \ldots, n$-re, akkor $T_1 \times \cdots \times T_n$ valódi résztéglája $S_1 \times \cdots \times S_n$-nek.

46. Tétel. *Ha az n-dimenziós S téglát partícionáljuk a $T^1, \ldots, T^m$ valódi résztéglákra, akkor $m \geq 2^n$.*

Lemma. *Ha $A \subseteq B$, $\emptyset \neq A \neq B$, akkor pontosan annyi páratlan részhalmaza van B-nek, ami A-t páratlan halmazban metszi, mint ahány párosban.*

Bizonyítás. Legyen $a \in A$, $b \in B \setminus A$. Ha $Z \subseteq B$, legyen Z' az a halmaz, ami Z-től csak a és b tartalmazásában tér el: $Z' = Z \triangle \{a, b\}$. Ekkor a $Z \mapsto Z'$ leképezés a két említett halmazt egymásra képezi. □

Nevezzük az $X_1 \times \cdots \times X_n \subseteq S_1 \times \cdots \times S_n$ résztéglát *páratlan*nak, ha elemszáma páratlan. Ez nyilván pontosan akkor következik be, ha $|X_1|, \ldots, |X_n|$ mind páratlan számok. Legyen most $X = X_1 \times \cdots \times X_n$ egy véletlen páratlan résztéglája S-nek. Számítsuk ki annak valószínűségét, hogy X metszete egy adott T^i-vel páratlan! Ehhez persze annak kell teljesülnie, hogy az $|X_1 \cap T_1^i|, \ldots, |X_n \cap T_n^i|$ számok mind páratlanok, és ezek a Lemma szerint $1/2$ valószínűséggel teljesülnek, azaz pontosan $1/2^n$ a valószínűsége, hogy $X \cap T^i$ páratlan. Mivel X páratlan és $T^1, \ldots, T^m$ partíciónálják az S téglát, mindig kell lennie olyan T^i-nek, amire $X \cap T^i$ páratlan, tehát az m esemény közül, amelyek valószínűsége külön-külön $1/2^n$ valamelyik mindig bekövetkezik, tehát $m \geq 2^n$. □

Irodalom

[1] N.Alon, T.Bohman, R.Holzman, D.J.Kleitman: On partitions of discrete boxes, *Discrete Math.*, **257**(2002), 255–258.

Kommunikációs protokollok

A számítógéptudomány egyik fejezete azt vizsgálja, hogy egymással kommunikáló, de nem egy helyen levő, tehát mondjuk telefonvonallal összekötött partnerek hogyan tudnak különböző feladatokat végrehajtani úgy, hogy ne áruljanak el olyan információt, amit nem akarnak. Az ilyen kommunikációs lépéssorozatokat protokolloknak nevezzük. Ezek gyakran használják a véletlen erejét vagy ma még bizonyítatlan, de plauzibilis feltevéseket, például azt, hogy bizonyos hosszúságú számokról el tudjuk dönteni, hogy prímek, de semmilyen eljárás nem tudja faktorizálni őket.

1. Protokoll. (Pénzfeldobás telefonon) A két, telefonvonallal összekötött résztvevő, A és B pénzt szeretne feldobni, azaz olyan eljárást végrehajtani,

aminek eredményeképpen vagy A vagy B nyer, mégpedig pontosan 50 százalék valószínűséggel. Nem dobhat fel, például A egy tényleges pénzdarabot, mert B nem tudja ellenőrizni, hogy valóban mondjuk megint fejre esett a pénz és ő ismét vesztett. Olyan eljárás kell, ami szerint mindkettőjük nyerési esélye pontosan 50 százalék, és a nyertes lépései ellenőrizhetőek.

A készít két olyan nagy prímszámot, p-t és q-t, hogy B nem tudja $N = pq$-t prímtényezőkre bontani és $p \equiv q \equiv 3 \pmod 4$. Elküldi N-t B-nek. B választ egy véletlen $0 < r < N$ számot. Visszaküldi A-nak az $a \equiv r^2 \pmod N$ maradékot. Az A játékos meg tudja oldani az $x^2 \equiv a \pmod N$ kongruenciát, ugyanis ez ekvivalens az $x^2 \equiv a \pmod p$ és $x^2 \equiv a \pmod q$ kongruenciák megoldásaival, amikből a megoldás a kínai maradéktétellel megkapható. Ezek viszont p és q speciális alakja miatt könnyen megoldhatók: ha $p \equiv 3 \pmod 4$ és $x^2 \equiv a \pmod p$ megoldható, akkor megoldásai

$$x \equiv \pm a^{\frac{p+1}{4}} \pmod p.$$

Valóban, négyzetreemelve azt kapjuk, hogy

$$\left(\pm a^{\frac{p+1}{4}}\right)^2 \equiv a^{\frac{p+1}{2}} \equiv a^{\frac{p-1}{2}} a \pmod p$$

és itt az első tényező 1-gyel kongruens Euler Lemmája miatt. Hasonlóan oldhatjuk meg az egyenletet mod q is. Négy gyök adódik, az $\{r, -r\}$ pár és egy másik $\{s, -s\}$ pár. A nem tudja, hogy a négy maradék közül B melyikre gondolt. A négy gyök közül az egyiket elküldi B-nek, akinek a feladata ezután produkálni $N = pq$ prímfelbontását. Ha $\pm r$-et kapja vissza, akkor semmi új információhoz nem jutott, ezért feltevéseink szerint semmi esélye arra, hogy N felbontását megtalálja. Ha viszont $s, -s$ valamelyikét kapja, akkor N osztja az $r^2 - s^2 = (r + s)(r - s)$ szorzatot, de nem osztja egyik tényezőt sem, tehát p az egyik, q a másik tényező osztója, és mivel ekkor p (vagy q) megegyezik az $(N, r+s)$ legnagyobb közös osztóval, ami az euklideszi algoritmussal könnyen kiszámítható, ezért B felbonthatja N-et.

2. Protokoll. (Számok átlagának kiszámítása) Adott $n \geq 3$ résztvevő, akik rendre ismerik az $a_1, \ldots, a_n$ számokat. Ki akarják számítani ezek összegét anélkül, hogy bármelyikük is száma elárulására kényszerülne. Ezt a következőképpen teszik meg. Az i-edik résztvevő tetszőleges és csak őáltala ismert módon $n-1$ részre osztja számát és ezeket elküldi a többi résztvevőnek. Minden résztvevő ezután előadja az általa megkapott számokat, ezután ezeket összeadják.

3. Protokoll (Shamir titokszétosztási sémája) Adott $k \leq n$ természetes számok esetén n résztvevő között úgy akarunk szétosztani egy információt, hogy bármelyik k rekonstruálni tudja azt, de semelyik $k-1$ ne tudja. Feltesszük, hogy a közös ,,titok" egy c szám. Készítünk egy $k-1$-edfokú $p(x)$ polinomot, aminek konstans tagja c. Ezután választunk n egymástól és 0-tól különböző számot: $a_1, \ldots, a_n$ és az i-edik résztvevő megkapja a_i-t és a $p(a_i)$ számot. Ha k résztvevő összeáll, akkor az általuk ismert értékekből ki tudják számítani a $p(x)$ polinomot, hiszen minden $k-1$-edfokú polinom rekonstruálható k helyen felvett értékéből. Másrészt, ha lenne $k-1$ résztvevő, aki ki tudná számítani a konstans tagot, tehát $p(0)$-t, akkor ők ki tudnák számítani $p(x)$-et, hiszen valójában annak k helyen felvett értéke áll rendelkezésükre. Ez viszont lehetetlen: $k-1$-edfokú polinomot nem lehet $k-1$ helyen felvett értékéből meghatározni.

4. Protokoll. (Bridzsleosztás) Adott négy játékos és szét kell osztanunk közöttük az L kártyacsomag összes lapját, tehát a P_1, P_2, P_3, P_4 játékosoknak meg kell kapniuk az $L_1, L_2, L_3, L_4 \subseteq L$ lapokat. Ehhez P_1, P_2 és P_3 megállapodik egy $f : L \to L$ véletlen permutációban. Ezután P_4 tetszése szerint ad nekik 13-13 lapot, ezek lesznek $f[L_1], f[L_2], f[L_3]$ tehát P_1, P_2, P_3 elkódolt lapjai. Ekkor P_1, P_2, P_3 már ismeri lapjait, P_4 lapjai is eldőltek (hiszen ő nyilván a maradék lapokat kapja), csak ő nem ismeri azokat.

Úgy tudja meg azokat, hogy sorra lekérdezi őket. Először veszi (valamilyen sorrendben) az első kártyalapot, mindenkinek elmondja, hogy azt szeretné megtudni, kint van-e náluk ez a lap. Ezt úgy teszi, hogy generál egy véletlen 0-1 bitet. Ezt elmondja P_1-nek, aki, ha nincs nála az adott lap, akkor továbbítja P_2-nek. Ha viszont nála van, akkor megváltoztatja: 0-ról 1-re vagy fordítva. P_2 hasonlóan jár el és továbbítja az eredményt P_3-nak, aki ugyanígy cselekszik és az eredményt visszaküldi P_4-nek. Ebből P_4 megtudja, hogy az első lap nála van-e, hiszen pontosan ekkor kapja az általa elindított bitet érintetlenül vissza. hasonlóan sorra lekérdezi a többi lapot is.

5. Protokoll. (Póker) (Bárány Imre, Füredi Zoltán) A póker leosztás feladata abban különbözik a bridzsétől, hogy a $P_1, \ldots, P_k$ játékosoknál már ott vannak az L kártyacsomag $L_1, \ldots, L_k$ lapjai, és a feladat az, hogy egyet húzzunk a maradék $L - (L_1 \cup \cdots \cup L_k)$ lapokból és mondjuk odaadjuk ezt P_k-nak (természetesen úgy, hogy a többi játékos semmit ne tudjon meg róla).

Ehhez a $P_1, \ldots, P_k$ játékosok sorra választanak egy $f_1, \ldots, f_{k-1}, g : L \to L$ véletlen permutációt. Ezeket a $P_1, \ldots, P_{k-1}$ játékosok sorra elmondják a P_k játékosnak. Ezután P_k elárulja az $f_1 \circ g^{-1}, f_2 \circ g^{-1}, \ldots, f_{k-1} \circ g^{-1}$ kom-

pozíciókat rendre a $P_2, \ldots, P_{k-1}, P_1$ játékosoknak, tehát ciklikusan eggyel eltolva.

Ezt követően a $P_1, \ldots, P_{k-1}$ játékosok elküldik az $f_1[L_1], \ldots, f_{k-1}[L_{k-1}]$ kódolt lapokat rendre $P_2, \ldots, P_1$-nek tehát ismét ciklikusan, ezek a játékosok ezután, az általuk ismert permutációk segítségével kiszámítják ezekből az

$$\left(f_1 \circ g^{-1}\right)^{-1} \circ f_1[L_1] = g[L_1], \ldots, \left(f_{k-1} \circ g^{-1}\right)^{-1} \circ f_{k-1}[L_{k-1}] = g[L_{k-1}]$$

elkódolt lapokat és sorra elküldik $P_2, P_3, \ldots, P_1$-nek. Ezeket $P_2, \ldots, P_{k-1}$ elküldi P_1-nek és P_k is elküldi (az általa nyilván ismert) $g[L_k]$-t P_1-nek. P_1 most már ismeri $g[L_1], \ldots, g[L_k]$-t, ezért tud húzni egy $j \in L - \left(g[L_1], \ldots, g[L_k]\right)$ kártyát. Ezt elküldi P_k-nak aki ebből kiszámítja $g^{-1}(j)$-t az általa húzott kártyát.

Irodalom

[1] I. Bárány, Z. Füredi: Mental poker with three or more players, *Information and Control*, **59**(1983), 84–93.

[2] ifj. Bodó Zalán, Pataki János: Kártya telefonon, avagy tanuljunk nyelveket! *Középiskolai Matematikai Lapok*, **35**(1985), 145–146.
http://www.sulinet.hu/cgi-bin/db2www/lm/komal/cikk?id=198507&l=

[3] ifj. Bodó Zalán, Pataki János: Még mindig kártyajáték telefonon, avagy fő a diszkréció! *Középiskolai Matematikai Lapok*, **35**(1985), 193–196.
http://www.sulinet.hu/cgi-bin/db2www/lm/komal/cikk?id=198509&l=

[4] A. Shamir: How to share a secret. *Comm. ACM*, **22**(1979), 612–613.

A számtani közép és a mértani közép közötti egyenlőtlenség

47. Tétel. *Ha $a_1, \ldots, a_n$ pozitív valós számok, akkor*

$$\sqrt[n]{a_1 \cdots a_n} \leq \frac{a_1 + \cdots + a_n}{n}.$$

Bizonyítás. (Ezt a bizonyítást Pólya György álmában találta.) Jelöljük a számok számtani közepét A-val. Az exponenciális függvény minden valós x-re kielégíti az

$$1 + x \leq e^x$$

egyenlőtlenséget. Ezt felírva $x = \frac{a_i}{A} - 1$-re,

$$\frac{a_i}{A} \leq e^{\frac{a_i}{A}-1}$$

adódik ($1 \leq i \leq n$). Ezeket összeszorozva azt kapjuk, hogy

$$\frac{a_1 \cdots a_n}{A^n} \leq e^{\frac{\sum a_i}{A}-n} = e^{n-n} = 1.$$

Ez átrendezve $a_1 \cdots a_n \leq A^n$, amit bizonyítani akartunk.

□

Persze, ez a bizonyítás az analízis néhány komoly fogalmát használja, így mindenképpen mélyebbenfekvőbb, mint az egyenlőtlenség szokásos bizonyításai.

A Carleman-egyenlőtlenség

48. Tétel. (Carleman) *Ha $a_1, a_2, \ldots$ pozitív valós számok, akkor*

$$\sum_{k=1}^{\infty} (a_1 \cdots a_k)^{1/k} < e \sum_{k=1}^{\infty} a_k.$$

Bizonyítás. (Pólya György) Kézenfekvő ötlet a számtani közép és a mértani közép közötti egyenlőtlenséget használni, de ha ezt egyszerűen felírjuk a baloldal tagjaira, akkor

$$\sum_{k=1}^{\infty} (a_1 \cdots a_k)^{1/k} \leq \sum_{k=1}^{\infty} \frac{a_1 + \cdots + a_k}{k} = \sum_{k=1}^{\infty} a_k \left(\frac{1}{k} + \frac{1}{k+1} + \cdots \right)$$

adódik, ami használhatatlan, mert a jobboldalon divergáló sorok: a harmonikus sor végösszegei vannak. Ezért ezt a módszert egy kicsit megváltoztatjuk.

Legyen

$$c_k = \frac{(k+1)^k}{k^{k-1}} = k \left(1 + \frac{1}{k} \right)^k.$$

Ekkor a baloldal k-adig tagjára súlyozással a következőt kapjuk:

$$(a_1 \cdots a_k)^{1/k} = \frac{(c_1 a_1 \cdots c_k a_k)^{1/k}}{(c_1 \cdots c_k)^{1/k}} \leq \frac{c_1 a_1 + \cdots + c_k a_k}{k(c_1 \cdots c_k)^{1/k}}$$

a számtani közép mértani közép közötti egyenlőtlenséget a $c_1 a_1, \ldots, c_n a_n$ számokra alkalmazva.

Ezért a baloldal legfeljebb

$$\sum_{k=1}^{\infty} c_k a_k \sum_{j \geq k} \frac{1}{j(c_1 \cdots c_j)^{1/j}}$$

viszont $c_1 \cdots c_j = (j+1)^j$, így a fenti összeg a következőképpen folytatható:

$$= \sum c_k a_k \sum_{j \geq k} \frac{1}{j(j+1)} = \sum_{k \geq 1} \frac{c_k}{k} a_k = \sum \left(1 + \frac{1}{k}\right)^k a_k < e \sum a_k$$

hiszen $\left(1 + \frac{1}{k}\right)^k < e$. □

Megjegyezzük, hogy a tételben szereplő e éles, tehát nem helyettesíthető kisebb számmal.

Irodalom

[1] G. Pólya: Proof of an inequality, *Proc. London Math. Soc.*, **24**(1926), 57.

A Hilbert-egyenlőtlenség

49. Tétel. *Ha $n = 1, 2, \ldots$-ra a_n, b_n pozitív valós számok, akkor*

$$\sum_{m=1}^{\infty} \sum_{n=1}^{\infty} \frac{a_m b_n}{m+n} < \pi \sqrt{\sum a_m^2} \sqrt{\sum b_n^2}$$

Bizonyítás. A tétel a Cauchy-Bunyakovszkij-Schwartz egyenlőség, tehát

$$\sum a_n b_n \leq \sqrt{\sum a_n^2} \sqrt{\sum b_n^2}$$

használatát sugallja, azonban abban csak az azonos indexű tagokat szorozzuk egymással össze, míg a kívánt egyenelőtlenségben mindegyiket mindegyikkel. Ezen úgy segítünk, hogy a baloldali összeg minden tagját erőszakkal szorzatként írjuk fel:

$$\frac{a_m b_n}{m+n} = c_i d_i,$$

ahol

$$c_i = \frac{a_m}{\sqrt{m+n}} \frac{\sqrt[4]{m}}{\sqrt[4]{n}}, \quad d_i = \frac{b_n}{\sqrt{m+n}} \frac{\sqrt[4]{n}}{\sqrt[4]{m}}.$$

Ekkor a baloldal $\sum c_i d_i$, ezért a Cauchy-Bunyakovszkij-Schwartz egyenlőség adja a $\sqrt{\sum c_i^2}\sqrt{\sum d_i^2}$ felső korlátot. Ennek két tényezője a következő két összeg négyzetgyöke:

$$\sum_{m,n} \frac{a_m^2}{m+n} \frac{\sqrt{m}}{\sqrt{n}}$$

és

$$\sum_{m,n} \frac{b_n^2}{m+n} \frac{\sqrt{n}}{\sqrt{m}}.$$

Itt kézenfekvő úgy tovább haladni, hogy a_m^2 együtthatójára, tehát a

$$\sum_{n=1}^{\infty} \frac{\sqrt{m}}{(m+n)\sqrt{n}}$$

értékre adjuk a π felső becslést, és hasonlóan a másik öszegre. Mivel az $1/(m+x)\sqrt{x}$ függvény monoton csökken,

$$\frac{1}{(m+n)\sqrt{n}} < \int_{n-1}^{n} \frac{1}{m+x} \frac{1}{\sqrt{x}} dx$$

tehát végül is a

$$\sqrt{m} \int_0^{\infty} \frac{dx}{(m+x)\sqrt{x}}$$

integrált kell kiszámítani. Ha az $x = my$ helyettesítéssel élünk, akkor az integrál a következő alakot ölti:

$$\int_0^{\infty} \frac{dy}{(1+y)\sqrt{y}}$$

amit egy újabb, $y = t^2$ helyettesítéssel így írhatunk át:

$$2\int_0^\infty \frac{dt}{1+t^2} = 2\left[\operatorname{arc\,tg}\, t\right]_0^\infty = \pi$$

és készen vagyunk.

Itt is megjegyezzük, hogy a tételben szereplő π konstans nem javítható.

Irodalom

[1] G. H. Hardy, J. E. Littlewood, G. Pólya: *Inequalities*, 1934.

Sorok π-re

A híres Leibniz-féle sor

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \cdots$$

rendkívül lassan konvergál, alkalmatlan π jegyeinek kiszámítására.

Hasznosabb a arc tg függvény hatványsorát alkalmazni:

$$\operatorname{arc\,tg}(x) = x - \frac{x^3}{3} + \frac{x^5}{5} - \frac{x^7}{7} + \frac{x^9}{9} - \cdots$$

ami persze az $x = 1$ helyettesítésnél visszaadja Leibniz sorát. Ez annál gyorsabb konvergenciát ad, minél kisebb (abszolút értékű) x-re alkalmazzuk.

Mivel $\operatorname{tg}(\frac{\pi}{6}) = \frac{1}{\sqrt{3}}$, igaz a

$$\pi = 2\sqrt{3}\left(1 - \frac{1}{3\cdot 3} + \frac{1}{5\cdot 3^2} - \frac{1}{7\cdot 3^3} + \cdots\right)$$

sorfejtés (Th. F. de Lagny, 1719).

Ennél jobb az Euler által 1737-ben használt

$$\frac{\pi}{4} = \operatorname{arc\,tg}\frac{1}{2} + \operatorname{arctg}\frac{1}{3}.$$

Még ennél is jobb a John Machin átal használt azonosság (eredményét W. Jones publikálta 1706-ban)

$$\frac{\pi}{4} = 4\text{arc tg}\frac{1}{5} - \text{arctg}\frac{1}{239}.$$

A

$$\frac{\pi}{4} = \text{arc tg}\frac{1}{2} + \text{arctg}\frac{1}{5} + \text{arctg}\frac{1}{8}$$

képletet használta 1844-ben Johann Dase (1824–1861) fejszámolóművész, amikor kiszámolta π-t 200 jegyre ,,kicsit kevesebb, mint két hónap alatt".

Ramanujan egyik cikkében 17 olyan sort adott meg $1/\pi$-re, amelyek a szokásosnál gyorsabban közelítenek, mint például:

$$\frac{4}{\pi} = \sum_{n=0}^{\infty} \frac{(-1)^n(1123+21460n)(2n-1)!!(4n-1)!!}{882^{2n+1}32^n n!^3}$$

vagy

$$\frac{99^2}{\sqrt{8}\pi} = \sum_{n=0}^{\infty} \frac{(4n)!(1103+26390n)}{(n!)^4 396^{4n}}$$

Ezeknél már az első tag a 3,14158504... illetve a 3,14159273001... közelítést adja π-re!

Ma már többszáz ezekhez hasonló sor ismert π kiszámítására, ezek közül néhányat igazolunk.

50. Tétel. (a) *Ha* $|a| > 1$, *akkor*

$$\text{arc tg}\frac{1}{a} = \sum_{k=0}^{\infty} \frac{(-1)^k}{a^{2k+1}(2k+1)}$$

(b) *Ha* $a > \sqrt{2}$, *akkor*

$$\text{arc tg}\frac{1}{a-1} = \sum_{k=0}^{\infty} \frac{(-1)^n 2^{2n}}{a^{4k+3}}\left(\frac{a^2}{4k+1} + \frac{2a}{4k+2} + \frac{2}{4k+3}\right).$$

Bizonyítás. Az első formula az arc tg függvény Taylor-sora az $x = 1/a$ helyettesítéssel. Ezt úgy is megkaphatjuk, hogy az

$$\text{arc tg}(x) = \int_0^x \frac{1}{1+t^2}dt$$

integrálban az integrandust sorbafejtjük és tagonként integrálunk:

$$= \int_0^x (1 - t^2 + t^4 - t^6 + \cdots)\, dt = x - \frac{x^3}{3} + \frac{x^5}{5} - \cdots .$$

A második képlethez jegyezzük meg, hogy ha a valós, az $1 - \frac{1+i}{a}$ szám képzetes részének és valós részének hányadosa $\frac{1}{a-1}$. Ezért szögének tangense $\frac{1}{a-1}$, azaz logaritmusának képzetes része $\operatorname{arc\,tg}\frac{1}{a-1}$.

Ha $a > \sqrt{2}$, akkor $x = \frac{1+i}{a}$ abszolút értéke 1-nél kisebb, így $\log(1-x)$-et előállíthatjuk a

$$-\log(1-x) = \sum_{n=1}^{\infty} \frac{x^n}{n}$$

sorral.

A fentiekből azt kapjuk, hogy

$$\operatorname{arc\,tg}\frac{1}{a-1} = \sum_{n=1}^{\infty} \frac{1}{na^n} \operatorname{Im}\big((1+i)^n\big)$$

Ha itt az $n = 4k, 4k+1, 4k+2, 4k+3$ értékekhez tartozó tagokat csoportosítjuk, akkor azt kapjuk, hogy

$$\operatorname{arc\,tg}\frac{1}{a-1} = \sum_{k=0}^{\infty} \frac{(-1)^n 2^{2n}}{a^{4k+3}} \left(\frac{a^2}{4k+1} + \frac{2a}{4k+2} + \frac{2}{4k+3} \right)$$

. □

51. Tétel. (Adamchik, Wagon)

$$\pi = \sum_{n=0}^{\infty} \frac{(-1)^n}{4^n} \left(\frac{2}{4n+1} + \frac{2}{4n+2} + \frac{1}{4n+3} \right)$$

1. Bizonyítás. Az $a = 2$ helyettesítéssel azonnal kapjuk a 46. Tételből. □

2. Bizonyítás. A szokásos sorbafejtésekkel

$$\int_0^x \frac{1}{1+t^4}\, dt = \int_0^x \left(\sum_{n\geq 0} (-1)^n t^{4n} \right) dt = \sum_{n\geq 0} (-1)^n \frac{x^{4n+1}}{4n+1}.$$

Ezt felhasználva a tételbeli sor így írható át:

$$\int_0^{1/\sqrt{2}} \frac{2\sqrt{2}+4t+2\sqrt{2}t^2}{1+t^4}dt$$

Ez az $y=\sqrt{2}t$ helyettesítéssel így alakítható tovább:

$$\int_0^1 \frac{2\sqrt{2}+2\sqrt{2}y+2\sqrt{2}\frac{y^2}{2}}{1+\frac{y^4}{4}}\frac{dy}{\sqrt{2}} = \int_0^1 \frac{8+8y+4y^2}{y^4+4}dy$$

$$= 4\int_0^1 \frac{1}{y^2-2y+2}dy.$$

Alkalmazva a $z=y-1$ helyettesítést, a következőt kapjuk:

$$4\int_{-1}^0 \frac{1}{z^2+1}dz = 4\Big[\text{arc tg}z\Big]_{-1}^0 = \pi.$$

□

52. Tétel. (D. H. Bailey, P. Borwein, S. Plouffe, 1997)

$$\pi = \sum_{n=0}^{\infty} \frac{1}{16^n}\left(\frac{4}{8n+1}-\frac{2}{8n+4}-\frac{1}{8n+5}-\frac{1}{8n+6}\right)$$

Bizonyítás. Mivel

$$\int_0^{1/\sqrt{2}} \frac{x^{n-1}}{1-x^8}dx = \frac{1}{2^{n/2}}\sum_{k\geq 0}\frac{1}{16^k(8k+n)}$$

a jobboldali öszeget átírhatjuk, mint

$$\int_0^{1/\sqrt{2}} \frac{4\sqrt{2}-8x^3-4\sqrt{2}x^4-8x^5}{1-x^8}dx.$$

Ha itt elvégezzük az $y = \sqrt{2}x$ helyettesítést, ezt kapjuk:

$$\int_0^1 \frac{16(4 - 2y^3 - y^4 - y^5)}{16 - y^8} dy.$$

Az integrandus a következőképpen alakítható át:

$$\frac{16(y^2+2)(y^2+2y+2)(1-y)}{(2-y^2)(y^2+2)(y^2+2y+2)(y^2-2y+2)} = -\frac{4y}{2-y^2} + \frac{8-4y}{y^2-2y+2}.$$

Az első tag integrálja $-2\log 2$. A másodiké $z = 1 - y$ helyettesítással:

$$\int_0^1 \frac{4z+4}{z^2+1} dz = 2\Big[\log(z^2+1)\Big]_0^1 + 4\Big[\operatorname{ctg} z\Big]_0^1 = 2\log 2 + \pi.$$

□

Az előző formulát általánosítja a következő, Wagontól eredő formula:

$$\pi + 4\operatorname{arc\,tg}(x) + 2\log\left(\frac{1-2x-x^2}{x^2+1}\right) =$$

$$= \sum_{n=0}^{\infty} \frac{1}{16^n}\left(\frac{4(x+1)^{8n+1}}{8n+1} - \frac{2(x+1)^{8n+4}}{8n+4} - \frac{(x+1)^{8n+5}}{8n+5} - \frac{(x+1)^{8n+6}}{8n+6}\right).$$

53. Tétel. (Fabrice Bellard)

$$\pi =$$

$$\sum_{n=0}^{\infty} \frac{(-1)^n}{2^{10n+6}}\left(\frac{-32}{4n+1} - \frac{1}{4n+3} + \frac{256}{10n+1} - \frac{64}{10n+3} - \frac{4}{10n+5} - \frac{4}{10n+7} + \frac{1}{10n+9}\right)$$

Bizonyítás. Azonnal adódik a 46. Tétel első illetve második formulájából, alkalmazva a

$$\frac{\pi}{4} = 2\operatorname{arc\,tg}\frac{1}{2} - \operatorname{arc\,tg}\frac{1}{7}$$

képletet. □

Egy további sor:

54. Tétel. (S. Rabinowitz, S. Wagon)

$$\pi = \sum_{n=0}^{\infty} \frac{(n!)^2 2^{n+1}}{(2n+1)!}.$$

Bizonyítás. Az Euler-féle sortranszformációt alkalmazzuk a Leibniz-féle sorra. Eszerint, ha a

$$\sum_{n=0}^{\infty} (-1)^n a_n$$

sor konvergens, akkor

$$\sum_{n=0}^{\infty} (-1)^n a_n = \sum_{n=0}^{\infty} \frac{\Delta^n a_0}{2^{n+1}}$$

ahol $\Delta^n a_k$ az n-edik differencia sorozat, tehát $\Delta^0 a_k = a_k$, $\Delta^{n+1} a_k = \Delta^n a_k - \Delta^n a_{k+1}$ (lásd Szász Pál könyvét, I. kötet, 559. oldal). A Leibniz-sorra

$$a_k = \frac{1}{2k+1},$$

ebből indukcióval kapjuk, hogy

$$\Delta^n a_k = \frac{2 \cdot 4 \cdots (2n)}{(2k+1)(2k+3)\cdots(2k+2n+1)}$$

és ez azt adja, hogy

$$\pi = 4 \sum_{n=0}^{\infty} (-1)^n \frac{1}{2n+1} = \sum_{n=0}^{\infty} \frac{(n!)^2 2^{n+1}}{(2n+1)!}.$$

□

Egy igen gyorsan konvergáló sor pedig a következő(David, Gregory, Choodnovsky, 1994):

$$\pi = 12 \sum_{n=0}^{\infty} \frac{(-1)^k (6n)!(13591409 + 545140134n))}{(3n)!(n!)^3 640320^{3n+3/2}}$$

itt minden tag 14 új jegyet ad.

Irodalom

[1] V. Adamchik, S. Wagon: A simple formula for π, *Amer. Math. Monthly*, **104**(1997), 852–854.

[2] D. H. Bailey, D. H.; P. Borwein, S. Plouffe: On the Rapid Computation of Various Polylogarithmic Constants, *Math. Comput.*, **66**(1997), 903–913.

[3] `http://fabrice.bellard.free.fr/pi/pi_bin/pi_bin.html`

[4] S. Rabinowitz, S. Wagon: A spigot algorithm for the digits of π, *American Math. Monthly*, **102**(1995), 195–203.

[5] S. Ramanujan: Modular equations and approximations to π, *Quart. Journ. Math.*, **45**(1914), 350–372.

[6] Szász Pál: *A differenciál- és integrálszámítás elemei, I, II*, Typotex Kiadó, 2000.

[7] Collection of series for π,
`http://numbers.computation.free.fr/Constants/Pi/piSeries.html`

Még gyorsabb algoritmus π-re

A Stirling-formula segítségével könnyen megbecsülhetjük, hogy ezek a képletek milyen gyorsan konvergálnak. Az adódik, hogy az n-edik tag alkalmas $A > B > 0$ számokra A^{-n} és B^{-n} közé esik, ezért persze a részösszegek hibája is ilyen nagyságrendű, amit nevezhetnénk exponenciálisnak, de komplexitáselméleti szempontból ez lineáris, hiszen ekkor a számokat jegyeik számával mérjük.

Ugyancsak lineáris az Arkhimédesztől eredő rekurzió, ami az egység átmérőjű kör köré illetve a körbe írt szabályos $6 \cdot 2^n$-szög kerületét számolja ki: $a_0 = 2\sqrt{3}$, $b_0 = 3$, ezután indukcióval

$$a_{n+1} = \frac{2a_n b_n}{a_n + b_n}, \qquad b_{n+1} = \sqrt{a_{n+1} b_n}$$

tehát az $a_0, b_0, a_1, b_1, a_2, b_2, \ldots$ sorozatban mindig felváltva a megelőző két tag harmonikus illetve mértani közepét vesszük. Ezt könnyű igazolni, hiszen

$$a_n = 2N \frac{\sin 2\alpha}{\cos 2\alpha}, \qquad b_n = 2N \sin 2\alpha,$$

$$a_{n+1} = 4N\frac{\sin\alpha}{\cos\alpha}, \qquad b_{n+1} = 4N\sin\alpha,$$

ahol $N = 6\cdot 2^n$ és $\alpha = \pi/N$. Ezután

$$\frac{2a_nb_n}{a_n+b_n} = \frac{2}{\frac{1}{a_n}+\frac{1}{b_n}} = \frac{2}{\frac{\cos^2\alpha-\sin^2\alpha}{2N2\sin\alpha\cos\alpha}+\frac{1}{2N2\sin\alpha\cos\alpha}} = 4N\frac{\sin\alpha}{\cos\alpha} = a_{n+1}$$

és

$$\sqrt{a_{n+1}b_n} = \sqrt{4N\frac{\sin\alpha}{\cos\alpha}\cdot 2N2\sin\alpha\cos\alpha} = 4N\sin\alpha = b_{n+1}.$$

A közelítés nagyságrendjét úgy becsüljük, hogy az $a_n - b_n$ különbséget vizsgáljuk. Ha $a_n - b_n$ adott, az $a_{n+1} - b_{n+1}$ különbség így alakítható át:

$$a_{n+1} - b_{n+1} = \frac{\sqrt{a_{n+1}}}{a_{n+1}+b_{n+1}}\cdot\frac{b_n}{a_n+b_n}(a_n - b_n).$$

Itt, mivel $a_n \to \pi$, $b_n \to \pi$, a jobboldal első két tényezőjének szorzata $1/4\sqrt{\pi}$-hez konvergál, ezért

$$a_n - b_n \to c\frac{1}{(4\sqrt{\pi})^n}$$

valamilyen $c > 0$ konstanssal.

1976-ban Richard Brent és Eugene Salamin, egymástól függetlenül, az elliptikus függvények elméletének felhasználásával, olyan algoritmust készített, ami kvadratikus, azaz a hasznos jegyek száma lépésenként megduplázódik: Legyen $a_0 = 1$, $b_0 = 1/\sqrt{2}$, $s_0 = 1/2$,

$$a_{n+1} = \frac{a_n+b_n}{2}, \qquad b_{n+1} = \sqrt{a_nb_n},$$

$$c_n = a_n^2 - b_n^2, \qquad s_{n+1} = s_n - 2^{n+1}c_{n+1}.$$

Ekkor

$$p_n = \frac{2a_n^2}{s_n} \to \pi$$

kvadratikusan.

Nézzük meg ennek egy Newmantól eredő egyszerűsített verzióját! Ehhez először is a fenti a_n-re és b_n-re vonatkozó, Gauss-tól származó algoritmust vizsgáljuk meg.

Ha $a \geq b > 0$ valós számok, tekintsük a

$$T(a,b) = \left(\frac{a+b}{2}, \sqrt{ab}\right)$$

transzformációt. Ez az (a,b) párt egy hasonló párba képezi, amelyek a $[b,a]$ intervallum egy részintervallumának két végpontját adják, ráadásul ezek különbsége kisebb mint $(a+b)/2 - b = (a-b)/2$, azaz a $T(a,b)$-beli számok távolsága kevesebb mint fele a és b távolságának.

Ebből az adódik, hogy ha adott $a > b > 0$-ból elkészítjük az $a_0 = a$, $b_0 = b$, $(a_{k+1}, b_{k+1}) = T(a_k, b_k)$ rekurzív sorozatot, akkor a_k csökkenően, b_k növekvően tart ugyanahhoz az $a \geq m \geq b$ számhoz, jelöljük ezt $m(a,b)$-vel.

Ez a konvergencia kvadratikus. Ezen a következőt értjük. Tegyük fel először, hogy a/b nagy. Ha $a/b = 2^t$, egy 2-nél nagyobb szám, akkor a következő két tag hányadosa

$$\frac{a+b}{2\sqrt{ab}} = \frac{1}{2}\left(\frac{\sqrt{a}}{\sqrt{b}} + \frac{\sqrt{b}}{\sqrt{a}}\right)$$

és ez kisebb, mint $2^{t/2}$. Ez azt jelenti, hogy ha eredetileg $a/b = 2^t$, akkor $O(\log t)$ iteráció után elérjük, hogy a/b-re $1 < a/b < 2$ teljesüljön.

Ezután megnézzük, hogy az egymást követő tagok hányadosa mennyivel tér el 1-től:

$$\frac{a+b}{2\sqrt{ab}} - 1 = \frac{(\sqrt{a}-\sqrt{b})^2}{2\sqrt{ab}} = \frac{(a-b)^2}{2(\sqrt{a}+\sqrt{b})^2\sqrt{ab}}.$$
$$\leq \frac{(a-b)^2}{2(2\sqrt{b})^2 b} = \frac{(a-b)^2}{8b^2} = \frac{1}{8}\left(\frac{a}{b} - 1\right)^2,$$

tehát a sorozat konvergenciája kvadratikus.

Gauss ki is számolta $m(a,b)$ értékét:

55. Tétel. (Gauss)

$$m(a,b) = \frac{\pi}{\int_{-\infty}^{\infty} \frac{dx}{\sqrt{(x^2+a^2)(x^2+b^2)}}}$$

Bizonyítás. Legyen

$$I(a,b) = \int_{-\infty}^{\infty} \frac{dx}{\sqrt{(x^2+a^2)(x^2+b^2)}}.$$

Ha az $y = (x - \frac{ab}{x})/2$ transzformációt alkalmazzuk, akkor

$$I(a,b) = I\left(\frac{a+b}{2}, \sqrt{ab}\right)$$

adódik. Ezért $I(a,b) = I(m,m)$. De

$$I(m,m) = \int_{-\infty}^{\infty} \frac{dx}{x^2+m^2} = \frac{1}{m}\int_{-\infty}^{\infty} \frac{dy}{y^2+1} = \frac{\pi}{m}$$

ahol az $my = x$ helyettesítéssel éltünk. □

A következőben $I(N,1)$ értékét becsüljük meg egy nagy N természetes számra.

Először is

$$I(N,1) = \int_{-\infty}^{\infty} \frac{dx}{\sqrt{(x^2+1)(x^2+N^2)}} = 2\int_{0}^{\infty} \frac{dx}{\sqrt{(x^2+1)(x^2+N^2)}}$$

mivel az integrandus páros.

Továbbá az $y = \frac{N}{x}$ helyettesítéssel adódik, hogy

$$\int_{0}^{\sqrt{N}} \frac{dx}{\sqrt{(x^2+1)(x^2+N^2)}} = \int_{\sqrt{N}}^{\infty} \frac{dx}{\sqrt{(x^2+1)(x^2+N^2)}}.$$

Tehát

$$I(N,1) = 4\int_{0}^{\sqrt{N}} \frac{dx}{\sqrt{(x^2+1)(x^2+N^2)}}$$

és az utóbbi integrált kell becsülnünk.

Az integrálandó függvény második tényezője az adott intervallumban a binomiális sor segítségével

$$\frac{1}{\sqrt{N^2+x^2}} = \frac{1}{N\sqrt{1+(\frac{x}{N})^2}} = \frac{1}{N}\left(1 - \frac{x^2}{2N^2} + O\Big(\frac{x^4}{N^4}\Big)\right)$$

Továbbá differenciálással könnyen látható, hogy $T \geq 0$-ra

$$\int_{0}^{T} \frac{dx}{\sqrt{x^2+1}} = \log(T + \sqrt{T^2+1}).$$

Ezért

$$\int_0^{\sqrt{N}} \frac{dx}{\sqrt{(x^2+1)(x^2+N^2)}} = \frac{1}{N}\int_0^{\sqrt{N}} \frac{dx}{\sqrt{(x^2+1)}}\Big(1-\frac{x^2}{2N^2}+O\Big(\frac{x^4}{N^4}\Big)\Big)$$

$$= \frac{1}{N}(\log(\sqrt{N})+\log(\sqrt{N+1})) - \frac{1}{2N^3}\int_0^{\sqrt{N}} \frac{x^2}{\sqrt{x^2+1}}dx + O\Big(\frac{1}{N^3}\Big)$$

Ismét a binomiális sort alkalmazva

$$\log(\sqrt{N}+\sqrt{N+1}) = \log\Big(\sqrt{N}\Big(2+\frac{1}{2N}+O\Big(\frac{1}{N^2}\Big)\Big)\Big)$$

$$= \frac{1}{2}\log N + \log\Big(2+\frac{1}{2N}+O\Big(\frac{1}{N^2}\Big)\Big)$$

$$= \frac{1}{2}\log N + \log 2 + \log\Big(1+\frac{1}{2N}+O\Big(\frac{1}{N^2}\Big)\Big)$$

$$= \frac{1}{2}\log N + \log 2 + \frac{1}{2N}+O\Big(\frac{1}{N^2}\Big)$$

A második tag becslése:

Lemma.

$$\int_0^{\sqrt{N}} \frac{x^2}{\sqrt{1+x^2}}dx = \frac{N}{2} - \frac{1}{4}\log N + O(1).$$

Bizonyítás. Ismét a binomiális sor felhasználásával

$$\sqrt{x^2+1} = x\sqrt{1+\frac{1}{x^2}} = x\Big(1+\frac{1}{2x^2}+O\Big(\frac{1}{x^4}\Big)\Big).$$

Ezért

$$\frac{x^2}{\sqrt{1+x^2}} = x\Big(1-\frac{1}{2x^2}+O\Big(\frac{1}{x^3}\Big)\Big).$$

Innen

$$\int_0^{\sqrt{N}} \frac{x^2}{\sqrt{1+x^2}}dx = \frac{N}{2} - \frac{1}{4}\log N + O(1).$$

□

Az eddigieket összefoglalva kapjuk a következőt.

56. Tétel.

$$I(N,1) = 4\left(\frac{\log N}{2N} + \frac{\log 2}{N} + \frac{1}{4N^2} + O\left(\frac{\log N}{N^3}\right)\right).$$

Ezért

$$(N+1)I(N+1,1) - NI(N,1)$$
$$= 2(\log(N+1) - \log N) + O\left(\frac{1}{N^2}\right) = \frac{2}{N} + O\left(\frac{1}{N^2}\right).$$

Innen

$$N\left(\frac{N+1}{m(N+1,1)} - \frac{N}{m(N,1)}\right) = \frac{2}{\pi} + O\left(\frac{1}{N}\right).$$

Ezután a következőképpen számíthatjuk ki π-t n jegyre. Legyen $N = 2^n$ A fejezet elején látott Gauss-féle eljárással számítsuk ki, $\log n$ iterációval, $2n$ jegyre $m(N+1,1)$-et és $m(N,1)$-et. A fenti képlet megadja π-t n jegyre.

Irodalom

[1] R. P. Brent: Fast Multiple-Precision Evaluation of Elementary Functions, *Journal of the Association of Computing Machinery*, **23** (1976), 242–251.

[2] D. J. Newman: A simplified version of the fast algorithms of Brent and Salamin, *Journal of Computation*, **44**(1985), 207–210.

[3] E. Salamin: Computation of π Using Arithmetic-Geometric Mean, *Math. Comput.*, **30**(1976), 565–570.

Négyzet felbontása háromszögekre

57. Tétel. (P. Monsky) *Négyzet csak páros sok egyenlő területű háromszögre bontható.*

Legyen racionális x számok esetén $\|x\|$ a következőképpen definiálva: $\|0\| = 0$ és ha $x = 2^t p/q$ ahol p, q páratlan, t pedig egész, akkor legyen

$$\|x\| = 2^{-t}.$$

Az értékeléselmélet egyik eredménye szerint ez kiterjeszthető az összes valós számra egy olyan $x \mapsto \|x\|$ függvénnyé, amire az alábbi tulajdonságok teljesülnek:

$\|x\| = 0$ akkor és csak akkor, ha $x = 0$;

$\|xy\| = \|x\| \cdot \|y\|$;

$\|-x\| = \|x\|$;

$\|x + y\| \leq \max\big(\|x\|, \|y\|\big)$ és itt egyenlőség áll, ha a jobboldali értékek különbözők.

Színezzük ki a sík pontjait a következőképpen:

(x, y) piros, ha $\|x\|, \|y\| < 1$,

(x, y) kék, ha $\|x\| \geq 1$, $\|x\| \geq \|y\|$,

(x, y) zöld, ha $\|y\| \geq 1$, $\|y\| > \|x\|$.

1. Lemma. *Pont színe nem változik, ha piros színű ponttal (mint vektorral) eltoljuk.*

Bizonyítás. Azt kell tehát bebizonyítani, hogy ha (u, v) piros, akkor (x, y) és $(x + u, y + v)$ színe ugyanaz.

1. Eset. (x, y) *piros.*

Ekkor $\|x + u\| \leq \max\big(\|x\|, \|u\|\big) < 1$ és hasonlóan, $\|y + v\|$, tehát $(x + u, y + v)$ piros.

2. Eset. (x, y) *kék.*

Ekkor $\|x + u\| = \max\big(\|x\|, \|u\|\big) = \|x\| \geq 1$, továbbá, ha $\|y\| < 1$, akkor $\|y + v\| < 1$, ha pedig $\|y\| \geq 1$, akkor $\|y + v\| = \max\big(\|y\|, \|v\|\big) = \|y\|$, azaz $\|x + u\| \geq \|y + v\|$ mindenképpen teljesül, tehát $(x + u, y + v)$ kék.

3. Eset. (x, y) *zöld.*

Ekkor $\|y + v\| = \max\big(\|y\|, \|v\|\big) = \|y\| \geq 1$, és

$$\|y + v\| = \|y\| \geq \max\big(\|x\|, \|u\|\big) \geq \|x + u\|.$$

2. Lemma. *Ha egy háromszög csúcsai különböző színűek, akkor t területére $\|t\| > 1$ teljesül.*

Bizonyítás. Az 1. Lemma szerint a háromszöget visszatolhatjuk a piros színű csúcsával, másszóval, feltehetjük, hogy piros csúcsa az origó. Ha másik két csúcsa a kék (x, y) és a zöld (u, v), akkor t területére $t = \pm\frac{1}{2}(xv - yu)$ teljesül. De erre

$$\|t\| = \left\|\frac{1}{2}\right\| \|xv - yu\| > \|xv - yu\| = \|xv\| \geq 1$$

teljesül, mivel $\|xv\| > \|yu\| = \|-yu\|$ miatt $\|xv - yu\| = \|xv\|$. □

A fenti állítás speciálisan azt is adja, hogy egy egyenesen csak kétféle színű pont lehet.

A 56. Tétel bizonyítása. Legyen tehát az S egységnégyzet felbontva m azonos területű háromszögre. Feltehető, hogy S csúcsai a $(0,0)$, $(1,0)$, $(0,1)$, $(1,1)$ pontok, színeik rendre piros, kék, zöld, zöld.

Nevezzük a felbontás csúcsainak a felbontásban szereplő valamennyi háromszög csúcsait. A háromszögek és S oldalait a felbontás csúcsai szakaszokra bontják. E szakaszokat a végpontok színei szerint piros-kék, stb szakaszoknak nevezzük. S kerületén piros-kék szakasz csak az origó és $(1,0)$ közötti oldalon fordulhat elő és itt páratlan sok van. A felbontás háromszögei közül csak olyan határán lehet páratlan sok piros-kék szakasz, amelyik háromszínű, márpedig minden belső, tehát nem S határán levő szakasz két háromszög határoló szakasza, ezért ha az összes háromszögben összeadjuk a piros-kék szakaszok számát, páratlan számot kapunk. Van tehát háromszínű háromszög, ennek területére a 2. Lemma azt adja, hogy

$$\frac{1}{\|m\|} = \left\|\frac{1}{m}\right\| > 1$$

azaz m páros. □

Nincs szükség a tétel előtt említett mély algebrai eszközökre, ha csak azt az esetet vizsgáljuk, amikor minden kis háromszög csúcsainak koordinátái racionálisok. Ekkor a fenti bizonyítás működik, ehhez csak a racionális számokon értelmezett eredeti $\|\ \|$ függvényt kell használni. Ezt a speciális esetet John Thomas bizonyította, az általánosnál korábban.

Irodalom

[1] P. Monsky: On dividing a square into triangles, *Amer. Math. Monthly*, **77**(1970), 161–164.

[2] J. Thomas: A dissection problem, *Math. Magazine*, **41**(1968), 187–190.

A Kneser-sejtés

Ebben a fejezetben a topológia egyik híres tételét alkalmazzuk egy kombinatorikai problémára.

Borsuk tétele. *Ha (az $\mathbf{R}^{n+1}$ euklideszi térben fekvő) n-dimenziós $\mathbf{S}^n$ egységgömb felszínét $n+1$ zárt halmazzal lefedjük, akkor valamelyik tartalmaz egy átellenes pontpárt.*

Legyen $V = \{v_1, \ldots, v_{2n+k}\}$ egy $2n+k$ elemű halmaz, és tekintsük V n-elemű részhalmazainak $\mathcal{H}(2n+k, n)$ rendszerét. Ezen, mint alaphalmazon definiáljuk a következő $K(2n+k, n)$ gráfot: két $\mathcal{H}(2n+k, n)$-beli halmaz össze van kötve, ha diszjunktak. Erről a gráfról könnyű megmutatni, hogy kromatikus száma legfeljebb $k+2$: fedjük le szögpontjai halmazát a következőképpen:

$$\mathcal{H}(2n+k, n) = \mathcal{H}_1 \cup \mathcal{H}_2 \cup \cdots \cup \mathcal{H}_{k+2}$$

ahol $1 \leq i \leq k+1$-re $\mathcal{H}_i$ be tesszük a v_i-t tartalmazó n-eseket, $\mathcal{H}_{k+2}$ pedig a maradékot tartalmazza, tehát a $\{v_{k+2}, \ldots, v_{2n+k}\}$ halmaz n elemű részhalmazait. Valamennyi halmazrendszer egymást páronként metsző halmazokból áll (az utolsó esetben azért, mert egy $2n-1$ elemű halmaz n elemű részhalmazairól van szó), így adódik, hogy $K(2n+k, n)$ kromatikus száma legfeljebb $k+2$. Kneser nevezetes sejtése az volt, hogy a kromatikus szám itt pontosan $k+2$. Érdekes módon, a helyzet pontosan fordítottja a szokásosnak, mert általában könnyű alulról és nehéz felülről becsülni a kromatikus számot.

57. Tétel. (Lovász László) *A $K(2n+k, n)$ gráf kromatikus száma $k+2$.*

Bizonyítás. (Bárány Imre, Joshua Greene) Tegyük fel, hogy

$$F : \mathcal{H}(2n+k, n) \to \{1, \ldots, k+1\}$$

jó színezés. Válasszuk ki az $x_1, \ldots, x_{2n+k}$ független pontokat az $\mathbf{S}^{k+1}$ gömb felszínéről, azaz olyanokat, hogy semelyik $k+2$ nincs egy főkörön (tehát egy legfeljebb k dimenziós altérben). Ezt egymásutáni választással megtehetjük: az első $k+1$-et tetszés szerint választjuk, a következők esetén mindig olyat, ami nincs benne a korábbi pontok $k+1$-esei által meghatározott véges sok főkörön.

Tekintsük az

$$\mathbf{S}^{k+1} = A^0 \cup A^1 \cup \cdots \cup A^{k+1}$$

lefedést, ahol $1 \leq i \leq k+1$-re $x \in A^i$, ha x nyílt félgömbjében vannak $x_{j_1}, \ldots, x_{j_n}$ pontok hogy $F(v_{j_1}, \ldots, v_{j_n}) = i$. Ha x semelyik A^i-ben ($1 \leq$

$i \leq k+1$) sincs benne, legyen $x \in A^0$. Az $A^1, \ldots, A^{k+1}$ halmazok nyíltak, A^0 pedig zárt. Ezért nem alkalmazhatjuk erre a felbontásra közvetlenül a Borsuk-tételt, ehelyett a halmazokat közelítjük zárt halmazokkal.

Legyen $t = 1, 2, \ldots$-re

$$A_t^i = \left\{ x \in A^i : d(x, \overline{A^i}) \geq \frac{1}{t} \right\}$$

és

$$A_t^0 = \left\{ x : d(x, \overline{A^0}) \leq \frac{1}{t} \right\}$$

ahol d a távolságot jelenti, a fölülhúzás pedig a lezártat jelöli.

Az

$$\mathbf{S}^{k+1} = A_t^0 \cup A_t^1 \cup \cdots \cup A_t^{k+1}$$

lefedés már zárt halmazokkal történik, vannak tehát valamelyik részben átellenes pontok. Ha egy t-re valamelyik A_t^i $(1 \leq i \leq k+1)$ tartalmaz átellenes pontokat, akkor készen vagyunk, mert a hozzájuk tartozó nyílt félgömbök diszjunktak és így adódik két diszjunkt, azonos (nevezetesen az i) színnel színezett $\mathcal{H}(2n+k, n)$-beli halmaz, tehát F mégsem jó színezés.

Marad az az eset, amikor minden t-re van átellenes pontpárunk A_t^0-ben, mondjuk, y_t és $-y_t$. $\mathbf{S}^{k+1}$ kompaktsága miatt az $y_1, y_2, \ldots$ sorozatnak van torlódási pontja, mondjuk y. Minden t-re igaz, hogy sem az y_t körüli, sem a $-y_t$ körüli a félgömb $1/t$-vel való rövidítésével kapott gömbsüveg nem tartalmaz az $x_1, \ldots, x_{2n+k}$ pontok közül n-et. Határátmenettel az adódik, hogy az y és $-y$ körüli félgömbökre ez ugyanúgy igaz. Másszóval, az y és $-y$ felező főkörsíkjában a $x_1, \ldots, x_{2n+k}$ pontok közül legalább $2n+k-2(n-1) = k+2$ van, ami ellentmond a pontok kiválasztásának. □

Irodalom

[1] I. Bárány: A short proof of Kneser's conjecture, *Journal of Combinatorial Theory* (A), **25**(1978), 325–326.

[2] J. Greene: A short proof of Kneser's conjecture, *Amer. Math. Monthly.* **109**(2002), 918–920.

[3] L. Lovász: Kneser's conjecture, chromatic number, and homotopy, *Journal of Combinatorial Theory* (A), **25**(1978), 319–324.

[4] J. Matoušek: A combinatorial proof of Kneser's conjecture, *Combinatorica*, **24**(2004), 163–170.

Névmutató

Tartalomjegyzék