A Waring-sejtés bizonyítása

Matematika BSc szakdolgozat

Szerző:
Fazekas Róbert

Témavezető:
Dr. Waldhauser Tamás
Algebra és Számelmélet Tanszék

Szegedi Tudományegyetem Bolyai Intézet

2015

Tartalomjegyzék

Bevezető

A Lagrange-féle négy négyzetszám tétel szerint bármely természetes szám előáll négy négyzetszám összegeként. Természetes módon adódik a kérdés, hogy valamilyen ehhez hasonló tétel igaz-e magasabb hatványokra is. Edward Waring 1770-ben Meditationes Algebraicae című művében azt állította, hogy „minden szám felírható 4 négyzetszám, 9 köbszám, 19 negyedik hatvány stb. összegeként". Ahhoz, hogy a sejtést a modern formalizmusnak és precízségnek megfelelően kimondhassuk, bevezetjük a $g(k,m)$ kétváltozós függvényt.

0.1. Definíció. Legyen k és m két természetes szám. Ekkor $g(k,m)$ jelöli azt a legkisebb természetes számot, ahány darab k-adik hatvány összegeként m előállítható:

$$g(k,m) = \min\{s \in \mathbb{N} : \exists x_1, \dots, x_s \in \mathbb{N}_0, \text{ hogy } m = x_1^k + \dots + x_s^k\}.$$

Waring-sejtés. Tetszőleges rögzített k természetes számra $g(k,m)$ korlátos (mint m függvénye).

Ha a fenti definícióval ellentétben negatív hatványokat is megengedünk az összegként való előállításban, akkor egy lényegesen könnyebben bizonyítható sejtéshez, a könnyű Waring-sejtéshez jutunk. A sejtést precízen kimondani és bizonyítani a második fejezet 2.3. Tételében fogjuk.

0.2. Definíció. Adott k esetén a $g(k,m)$ függvény maximumát $g(k)$ jelöli:

$$g(k) = \max\{g(k,m) \colon m \in \mathbb{N}\}.$$

Waring sejtését csak 1909-ben sikerült David Hilbertnek bizonyítani. Az ő bizonyítását egyszerűsítette többek között François Dress és Kürschák József. Szakdolgozatomban a François Dress által egyszerűsített bizonyítást fogom bemutatni (lásd [1]). A dolgozat alapját a [6] könyv 5. fejezete képzi.

A bizonyítás alapötletét $g(4)$ végességének bizonyításán keresztül mutatjuk be. Ezt az eredményt Joseph Liouville publikálta 1859-ben.

0.3. Tétel. *Bármely természetes szám előáll legfeljebb* 53 *darab negyedik hatvány összegeként, azaz* $g(4) \leq 53$.

Bizonyítás. A hatványozások elvégzésével belátható, hogy bármely $X_1, \dots, X_4 \in \mathbb{Z}$ esetén

$$6(X_1^2 + \dots + X_4^2)^2 = \sum_{i<j} ((X_i + X_j)^4 + (X_i - X_j)^4). \tag{0.1}$$

Itt a jobb oldali összegben 12 darab negyedik hatvány szerepel. A fenti azonosságból Lagrange tétele miatt következik, hogy minden $6X^2$ alakú természetes szám 12 darab negyedik hatvány összege ($X = X_1^2 + \dots + X_4^2$). Lagrange tételének újbóli alkalmazásával kapjuk, hogy bármely $N \in \mathbb{N}$ esetén $6N = 6N_1^2 + \dots + 6N_4^2$, ami az előbbi gondolatmenet alapján 48 negyedik hatvány összege. Mivel bármely természetes szám hattal vett osztási maradéka a $\{0, \dots, 5\}$ halmazból való, ezért a 48 negyedik hatványhoz legfeljebb 5 darab 1^4 hatványt hozzávéve bármely természetes szám előállítható legfeljebb 53 darab negyedik hatvány összegeként. ■

Az általános bizonyítás alapötlete hasonló. Az első fejezetben megmutatjuk, hogy bármely k természetes szám esetén létezik egy (0.1)-hez hasonló alakú azonosság, az ún. Hilbert-Dress azonosság. Ebből a második fejezetben Lagrange négy négyzetszám tételét alkalmazva belátjuk az általános tételt, miszerint $g(k,m)$ korlátos bármely rögzített k természetes számra.

Hilbert eredeti bizonyításának alapja a következő azonosság volt.

0.4. Tétel. *Legyen k természetes szám, és $N = \binom{2k+4}{4}$. Ekkor létezik M pozitív egész, léteznek m_i $(0 \le i \le N)$ nemnegatív egészek, és a_{ij} $(0 \le i \le N, 1 \le j \le 5)$ egész számok, hogy tetszőleges $X_1, \dots, X_5$ valós számokra*

$$M(X_1^2 + \cdots + X_5^2)^k = \sum_{i=0}^{N} m_i(a_{i1}X_1 + \cdots + a_{i5}X_5)^{2k}. \tag{0.2}$$

Ezt az azonosságot konvex geometriai eszközökkel sikerült François Dressnek továbbfejleszteni, ez az ún. Hilbert-Dress azonosság.

0.5. Tétel (Hilbert-Dress azonosság). *Legyen k természetes szám, és $N = \binom{2k+4}{4}$. Ekkor léteznek olyan M, m_{N+1} pozitív egészek, m_i $(0 \le i \le N)$ nemnegatív egészek, és a_{ij} $(0 \le i \le N, 1 \le j \le 5)$ egész számok, hogy tetszőleges $X_1, \dots, X_5$ valós számokra*

$$M(X_1^2 + \cdots + X_5^2)^k = \sum_{i=0}^{N} m_i(a_{i1}X_1 + \cdots + a_{i5}X_5)^{2k} + m_{N+1}X_5^{2k}. \tag{0.3}$$

Látható, hogy a (0.2)-es és a (0.3)-as formulák között egyedül annyi különbség van, hogy Dressnek sikerült egy $m_{N+1}X_5^{2k}$ taggal (m_{N+1} pozitív egész) bővíteni a jobb oldali összeget. Ez az aprónak tűnő módosítás jelentősen leegyszerűsíti a Waring-sejtés bizonyítását. Ezt mutatjuk be a második fejezetben.

A dolgozatban nem adunk konkrét felső becslést $g(k)$-ra, a bizonyítás nem konstruktív. Ellenben éles alsó becslés könnyen adható. A következő eredmény Leonhard Euler fiától, Johann Eulertől (1772) származik.

0.6. Tétel. *Bármely k természetes számra $2^k + \lfloor (\frac{3}{2})^k \rfloor - 2 \le g(k)$.*

Bizonyítás. Mivel $2^k\lfloor (\frac{3}{2})^k \rfloor - 1 < 2^k(\frac{3}{2})^k = 3^k$, ezért a $2^k\lfloor (\frac{3}{2})^k \rfloor - 1$ számot csak 1^k és 2^k hatványok segítségével lehet k-adik hatványok összegeként előállítani. A legkevesebb hatványt akkor használjuk, ha a lehető legtöbb 2^k hatványt, $\lfloor (\frac{3}{2})^k \rfloor - 1$ darabot használunk. A maradék $2^k - 1$ darab 1^k hatvány. Így összesen $2^k + \lfloor (\frac{3}{2})^k \rfloor - 2$ darab k-adik hatványt használtunk fel. ■

Manapság kis bizonytalanságtól eltekintve ismerjük a $g(k)$ értékeket. Pontosabban Kurt Mahlernek sikerült 1957-ben bizonyítani, hogy a fenti alsó korlát legfeljebb véges sok k-tól eltekintve megegyezik $g(k)$-val.

Leonard Eugene Dickson publikálta 1939-ben, hogy a 23 és a 239 kivételével minden természetes szám felírható 8 köbszám összegeként. Yuri Linnik 1943-ban ezt úgy pontosította, hogy minden elegendően nagy szám legfeljebb 7 köbszám összege. Azt sejtik, hogy minden kellően nagy szám már 4 köbszám összegeként is előáll. Vélhetően a 7 373 170 279 850 a legnagyobb természetes szám, amihez 5 köbszám szükséges. Ezen eredmények motiválják a $G(k)$ függvény bevezetését, mellyel itt csak említés szintjén foglalkozunk.

0.7. Definíció. Legyen k természetes szám. Ekkor $G(k)$ jelöli azt a legkisebb természetes számot, ahány darab k-adik hatvány összegeként véges sok kivételtől eltekintve minden természetes szám előáll:

$$G(k) = \min\{s \in \mathbb{N} : \exists K \in \mathbb{N}\ \forall m \geq K\ \exists x_1, \ldots, x_s \in \mathbb{N}_0, \text{hogy } m = x_1^k + \cdots + x_s^k\}.$$

Azt, hogy a $G(k)$ számok meghatározása mennyivel nehezebb feladat, mint a $g(k)$ értékeké, jól tükrözi az, hogy csak $G(2)$ és $G(4)$ pontos értéke ismert. Az alábbi táblázatban összefoglaljuk az ismert felső becsléseket (lásd [8]).

k	2	3	4	5	6	7	8	9
$g(k)$	4	9	19	37	73	143	279	548
$G(k)$	4	≤ 7	16	≤ 17	≤ 24	≤ 33	≤ 42	≤ 50

1. táblázat. A $g(k)$ és $G(k)$ értékek ($2 \leq k \leq 9$).

1. A Hilbert-Dress azonosság

A fejezet jórészt konvex geometriai jellegű. Néhány tételt (1.4., 1.5., 1.9., 1.12.) bizonyítás nélkül közlünk. Ezek bizonyítása megtalálható a [4] jegyzetben és az [5], [7] könyvekben. Bevezetjük a gyakran használt jelöléseket, rövidítéseket. Legyen $I := \{(i_1, \dots, i_5) : i_1, \dots, i_5 \in \mathbb{N}_0, i_1 + \dots + i_5 = 2k\}$, és egy tetszőleges elemét jelölje $\mathbf{i} = (i_1, \dots, i_5)$. Legyen V a homogén $2k$-ad fokú $p \in \mathbb{R}[X_1, \dots, X_5]$ polinomok vektortere. Mivel tetszőleges $p \in V$ esetén

$$p = \sum_{\mathbf{i} \in I} c_{\mathbf{i}} \cdot X_1^{i_1} \cdots X_5^{i_5}$$

alakú ($c_{\mathbf{i}} \in \mathbb{R}$), ezért világos, hogy az $X_1^{i_1} \cdots X_5^{i_5}$ monomok egy bázisát alkotják V-nek. Ezen monomok darabszáma megadja V dimenzióját, tehát $\dim(V) = |I| = \binom{2k+4}{4} =: N$. Ezek alapján a fenti $p \in V$ polinomot azonosítani tudjuk a $(c_{\mathbf{i}})_{\mathbf{i} \in I} \in \mathbb{R}^N$ vektorral. A továbbiakban nem teszünk különbséget a $p \in V$ polinom és a neki megfelelő $(c_{\mathbf{i}})_{\mathbf{i} \in I} \in \mathbb{R}^N$ vektor között. Így definiálhatjuk két V-beli polinom (vagy vektor) belső szorzatát. Legyen

$$g = \sum_{\mathbf{i} \in I} a_{\mathbf{i}} \cdot X_1^{i_1} \cdots X_5^{i_5} \text{ és } h = \sum_{\mathbf{i} \in I} b_{\mathbf{i}} \cdot X_1^{i_1} \cdots X_5^{i_5},$$

ekkor $\langle g, h \rangle := \langle (a_{\mathbf{i}})_{\mathbf{i} \in I}, (b_{\mathbf{i}})_{\mathbf{i} \in I} \rangle = \sum_{\mathbf{i} \in I} a_{\mathbf{i}} b_{\mathbf{i}}$. Azaz V-beli polinomok belső szorzatán a velük azonosított $\mathbb{R}^N$-beli vektorok belső szorzatát értjük.

Definiáljuk az

$$f : \mathbb{R}^5 \longrightarrow V \cong \mathbb{R}^N, \mathbf{t} \longmapsto (t_1 X_1 + \dots + t_5 X_5)^{2k} = f(\mathbf{t})$$

leképezést ($\mathbf{t} = (t_1, \dots, t_5) \in \mathbb{R}^5$). A polinomiális tétel alapján

$$f(\mathbf{t}) = \sum_{\mathbf{i} \in I} \binom{2k}{\mathbf{i}} t_1^{i_1} X_1^{i_1} \cdot \ldots \cdot t_5^{i_5} X_5^{i_5} = \sum_{\mathbf{i} \in I} \binom{2k}{\mathbf{i}} t_1^{i_1} \cdots t_5^{i_5} \cdot X_1^{i_1} \cdots X_5^{i_5}, \tag{1.1}$$

ahol $\binom{2k}{\mathbf{i}} := \binom{2k}{i_1, \dots, i_5} = \frac{(2k)!}{i_1! \cdot \ldots \cdot i_5!}$ polinomiális együttható. Világos, hogy f folytonos, és vegyük észre, hogy bármely $\mathbf{t} \in \mathbb{R}^5$ és minden $c \in \mathbb{R}$ esetén

$$f(c\mathbf{t}) = c^{2k} f(\mathbf{t}), \tag{1.2}$$

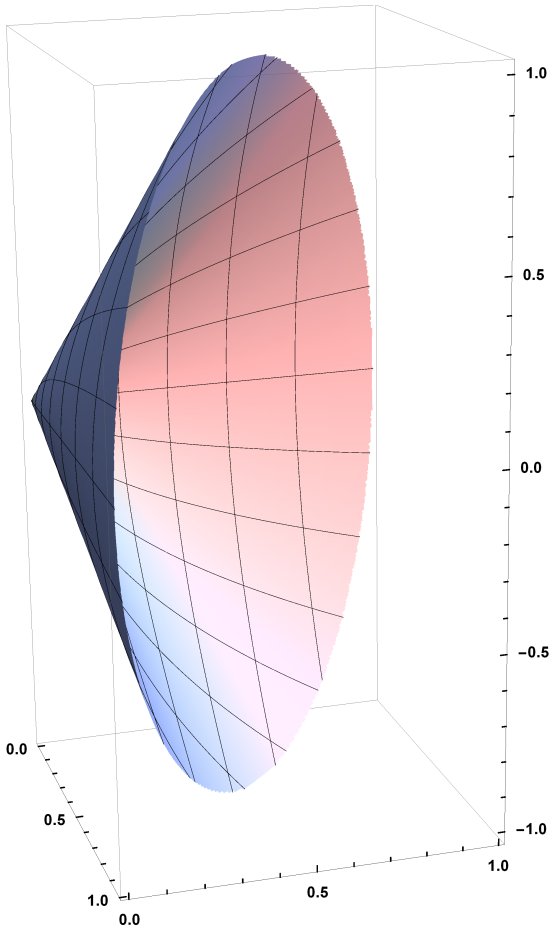
ugyanis $f(c\mathbf{t}) = (ct_1 X_1 + \dots + ct_5 X_5)^{2k} = c^{2k}(t_1 X_1 + \dots + t_5 X_5)^{2k} = c^{2k} f(\mathbf{t})$.

A továbbiakban szükségünk lesz még a $\mathbf{B}$-vel jelölt ötdimenziós zárt egységgömbre, és a $\tilde{\mathbf{B}}$-mal jelölt ötdimenziós racionális egységgömbre, azaz $\mathbf{B} := \{\mathbf{t} \in \mathbb{R}^5 : |\mathbf{t}| \leq 1\}$ és $\tilde{\mathbf{B}} = \{\mathbf{t} \in \mathbb{Q}^5 : |\mathbf{t}| \leq 1\}$. (Itt $|\cdot|$ az euklideszi norma, vagyis $|\mathbf{t}| = \sqrt{t_1^2 + \dots + t_5^2}$.) Az ötdimenziós egységgömb térfogata $\mathrm{vol}(\mathbf{B}) = \frac{8\pi^2}{15}$.

Az $S \subseteq \mathbb{R}^n$ halmaz belsejét $\mathrm{int}(S)$-sel, lezártját $\mathrm{cl}(S)$-sel jelöljük. Ha $\tilde{S} \subseteq S$, és $\mathrm{cl}(\tilde{S}) = S$, akkor azt mondjuk, hogy az $\tilde{S}$ halmaz sűrű S-ben.

1.1. Definíció. Legyen $S \subseteq \mathbb{R}^n$ tetszőleges halmaz. Ekkor S konvex burkának nevezzük azt a $\mathrm{conv}(S)$-sel jelölt legszűkebb konvex halmazt, mely teljes egészében tartalmazza S-et.

1.2. Definíció. Az $S \subseteq \mathbb{R}^n$ konvex halmazt konvex testnek nevezzük, ha kompakt és belseje nem üres.



1. ábra. A $\varphi(\mathbf{B_2}) \subseteq \mathbb{R}^3$ halmaz egy ellipszis alapú egyenes kúp palástja.

1.3. Megjegyzés. A fejezet bevezetőjében lévő konstrukció megértését megkönnyítendő bemutatjuk annak egy alacsonyabb dimenziós analogonját. Legyen W a homogén másodfokú $p \in \mathbb{R}[X_1, X_2]$ polinomok vektortere:

$$W = \{aX_1^2 + bX_1X_2 + cX_2^2 : a, b, c \in \mathbb{R}\}.$$

Világos, hogy minden $p \in W$ polinom azonosítható az $(a, b, c) \in \mathbb{R}^3$ együtthatóvektorával, tehát $W \cong \mathbb{R}^3$. Most definiáljuk a

$$\varphi : \mathbb{R}^2 \longrightarrow W, (t_1, t_2) \longmapsto (t_1X_1 + t_2X_2)^2$$

leképezést. A definícióból látható, hogy

$$\varphi(t_1, t_2) = t_1^2X_1^2 + 2t_1t_2X_1X_2 + t_2^2X_2^2.$$

Mivel minden $\varphi(t_1, t_2) \in W$ polinomot azonosítottunk a $(t_1^2, 2t_1t_2, t_2^2) \in \mathbb{R}^3$ együtthatóvektorával, ezért jogosan merül fel a kérdés, hogy hogyan néz ki a $(t_1^2, 2t_1t_2, t_2^2)$ alakú pontok halmaza $\mathbb{R}^3$-ban. Valójában a későbbieket figyelembe véve a legfontosabb a $\varphi(\mathbf{B_2}) \subseteq \mathbb{R}^3$ halmaz ismerete. Itt $\mathbf{B_2}$ jelöli a síkbeli zárt egységkörlapot: $\mathbf{B_2} = \{(t_1, t_2) \in \mathbb{R}^2 : t_1^2 + t_2^2 \leq 1\}$. Az 1. ábra mutatja, de számítással is ellenőrizhető, hogy a $\varphi(\mathbf{B_2})$ halmaz egy ellipszis alapú egyenes kúp palástja, tehát $\mathrm{conv}(\varphi(\mathbf{B_2}))$ egy tömör kúp.

Tehát nem tévedünk nagyot, ha a későbbiekben tárgyalandó $\mathrm{conv}(f(\mathbf{B})) \subseteq V \cong \mathbb{R}^N$ halmazra is, mint egy N-dimenziós kúpra gondolunk. Ebből precízen csak annyit fogunk bizonyítani, hogy a $\mathrm{conv}(f(\mathbf{B}))$ halmaz konvex test.

1.4. Lemma. *Legyen $S \subseteq \mathbb{R}^n$ tetszőleges halmaz, ekkor* $\mathrm{conv}(\mathrm{cl}(S)) \subseteq \mathrm{cl}(\mathrm{conv}(S))$. *Ha S korlátos, akkor* $\mathrm{conv}(\mathrm{cl}(S)) = \mathrm{cl}(\mathrm{conv}(S))$, *következésképp kompakt halmaz konvex burka is kompakt.*

1.5. Lemma. *Ha $K \subseteq \mathbb{R}^n$ konvex, akkor* $\mathrm{int}(K) = \mathrm{int}(\mathrm{cl}(K))$.

1.6. Lemma. *A* $\mathrm{conv}(f(\mathbf{B})) \subseteq V$ *halmaz konvex test.*

Bizonyítás. Először megmutatjuk, hogy $f(\mathbf{B})$ kifeszíti V-t. Indirekt tegyük fel, hogy ez nem igaz. Ekkor létezik olyan $\mathbf{n} \in V\backslash\{\mathbf{0}\}$, hogy bármely $\mathbf{u} \in \mathbf{B}$ esetén $f(\mathbf{u}) \perp \mathbf{n}$, azaz $\langle f(\mathbf{u}), \mathbf{n}\rangle = 0$. Legyen $\mathbf{t} \in \mathbb{R}^5$ tetszőleges, ekkor $\mathbf{t} = |\mathbf{t}|\cdot \mathbf{t}^*$, ahol $|\mathbf{t}^*| = 1$. Az (1.2)-es egyenlőség és a belső szorzat homogenitása miatt világos, hogy

$$\langle f(\mathbf{t}), \mathbf{n}\rangle = \langle f(|\mathbf{t}|\cdot \mathbf{t}^*), \mathbf{n}\rangle = \langle |\mathbf{t}|^{2k} f(\mathbf{t}^*), \mathbf{n}\rangle = |\mathbf{t}|^{2k}\langle f(\mathbf{t}^*), \mathbf{n}\rangle = 0.$$

(Itt kihasználtuk, hogy $f(\mathbf{t}^*) \perp \mathbf{n}$, mert $\mathbf{t}^* \in \mathbf{B}$.) A most kapott eredmény és (1.1) alapján

$$\langle f(\mathbf{t}), \mathbf{n}\rangle = \sum_{\mathbf{i}\in I} \binom{2k}{\mathbf{i}} n_{\mathbf{i}}\cdot t_1^{i_1}\cdots t_5^{i_5} = 0$$

minden $\mathbf{t} \in \mathbb{R}^5$-re. A fenti összeg polinomfüggvénye a $t_1, \ldots, t_5$ változóknak. Végtelen test fölött egy polinomfüggvény csak akkor lehet konstans 0, ha minden együtthatója 0, tehát $n_{\mathbf{i}} = 0$ bármely $\mathbf{i} \in I$-re. Ekkor viszont $\mathbf{n} = \mathbf{0}$, ami ellentmondás.

Mivel $f(\mathbf{B})$ kifeszíti V-t, ezért létezik $\mathbf{v}_1, \ldots, \mathbf{v}_N \in f(\mathbf{B})$ lineárisan független vektorrendszer. Tudjuk, hogy $\mathbf{0} \in f(\mathbf{B})$, ugyanis $f(\mathbf{0}) = \mathbf{0}$. A $\mathrm{conv}(\mathbf{0}, \mathbf{v}_1, \ldots, \mathbf{v}_N)$ halmaz egy N-dimenziós szimplex, melynek belseje nyilván nem üres, és részhalmaza $\mathrm{conv}(f(\mathbf{B}))$-nek. Így $\mathrm{conv}(f(\mathbf{B}))$ belseje sem üres.

Azt tudjuk, hogy $\mathbf{B}$ kompakt, és, hogy kompakt halmaz folytonos képe is az. Az 1.4. Lemma alapján kompakt halmaz konvex burka is kompakt, ezért $\mathrm{conv}(f(\mathbf{B}))$ kompakt. ■

1.7. Lemma. *Létezik olyan c pozitív valós szám, melyre*

$$\mathbf{S} := \frac{1}{\mathrm{vol}(\mathbf{B})}\int_{\mathbf{B}} f(\mathbf{t})d\mathbf{t} = c(X_1^2 + \cdots + X_5^2)^k.$$

Bizonyítás. Mivel $f(\mathbf{t}) \in V$, ezért $\mathbf{S}$ is az $X_1, \ldots, X_5$ határozatlanok polinomja. Elég belátni, hogy létezik olyan c pozitív valós szám, hogy minden $x_1, \ldots, x_5 \in \mathbb{R}$ esetén $\mathbf{S}(x_1, \ldots, x_5) = c(x_1^2+\cdots+x_5^2)^k$. Legyen $\mathbf{x} = (x_1, \ldots, x_5) \in \mathbb{R}^5$, és $\mathbf{x} = |\mathbf{x}|\cdot \mathbf{x}^*$, ahol $|\mathbf{x}^*| = 1$. Világos, hogy

$$\mathbf{S}(x_1, \ldots, x_5) = \frac{1}{\mathrm{vol}(\mathbf{B})}\int_{\mathbf{B}} (t_1x_1 + \cdots + t_5x_5)^{2k} d\mathbf{t} =$$

$$\frac{1}{\mathrm{vol}(\mathbf{B})}\int_{\mathbf{B}} \langle \mathbf{t}, \mathbf{x}\rangle^{2k} d\mathbf{t} = \frac{|\mathbf{x}|^{2k}}{\mathrm{vol}(\mathbf{B})}\int_{\mathbf{B}} \langle \mathbf{t}, \mathbf{x}^*\rangle^{2k} d\mathbf{t}.$$

Az utolsó integrál értéke nem függ $\mathbf{x}^*$-tól. Ugyanis ha $\mathbf{y}^* \in \mathbb{R}^5$ egy másik egységvektor, és az utolsó integrálban $\mathbf{x}^*$ helyébe $\mathbf{y}^*$-ot írunk, akkor a gömböt megfelelően forgatva az eredeti integrált kapjuk vissza. Tudjuk, hogy a forgatás mátrixa ortogonális és determinánsa 1. Így helyettesítéses integrálással számolva a Jacobi-determináns értéke 1 lesz, és az integrálási tartomány is változatlan marad.

Mivel $|\mathbf{x}|^{2k} = (x_1^2 + \cdots + x_5^2)^k$, ezért a $c = \frac{1}{\mathrm{vol}(\mathbf{B})} \int_{\mathbf{B}} \langle \mathbf{t}, \mathbf{x}^* \rangle^{2k} d\mathbf{t}$ választás megfelelő. ■

1.8. Megjegyzés. Az $\mathbf{S}$ polinom nem más, mint az f függvény $\mathbf{B}$-n vett integrálközepe, ezért szemléletesen világos, hogy $\mathbf{S} \in \mathrm{conv}(f(\mathbf{B}))$. Ezt be is fogjuk bizonyítani az 1.9. Lemma segítségével, ami a konvex halmazokra vonatkozó klasszikus szeparációs tételek egy változata.

1.9. Lemma. *Legyen $S \subseteq \mathbb{R}^n$ konvex test, és $\mathbf{v} \in \mathbb{R}^n$ vektor. Ha $\mathbf{v} \notin \mathrm{int}(S)$, akkor létezik olyan H hipersík, hogy $\mathbf{v} \in H$ és S teljes egészében benne van a H által meghatározott egyik zárt féltérben.*

1.10. Lemma. *Az $\mathbf{S} \in V$ integrálközép a $\mathrm{conv}(f(\mathbf{B}))$ halmaz belsejében van.*

Bizonyítás. Indirekt tegyük fel, hogy $\mathbf{S} \notin \mathrm{int}(\mathrm{conv}(f(\mathbf{B})))$. Ekkor az 1.9. Lemma alapján létezik olyan H hipersík, hogy $\mathbf{S} \in H$ és $\mathrm{conv}(f(\mathbf{B}))$ az egyik H által meghatározott zárt féltérben van. Legyen $\mathbf{n} \in H^\perp$, azaz $\mathbf{n}$ a H egy normálvektora. Definiáljuk az

$$L : V \longrightarrow \mathbb{R}, \mathbf{x} \longmapsto \langle \mathbf{x}, \mathbf{n} \rangle = L(\mathbf{x})$$

lineáris funkcionált. Mivel $\mathbf{S} \in H$, ezért H egyenlete $L(\mathbf{x}) = L(\mathbf{S})$. A H által meghatározott két zárt féltér pedig a $T_1 = \{\mathbf{x} \in V : L(\mathbf{x}) \leq L(\mathbf{S})\}$ és a $T_2 = \{\mathbf{x} \in V : L(\mathbf{x}) \geq L(\mathbf{S})\}$ halmaz.

Az általánosság megszorítása nélkül feltehetjük, hogy $\mathrm{conv}(f(\mathbf{B}))$ a T_1 féltérbe esik. A belső szorzat homogenitása miatt

$$L(\mathbf{S}) = L\left(\frac{1}{\mathrm{vol}(\mathbf{B})} \int_{\mathbf{B}} f(\mathbf{t}) d\mathbf{t}\right) = \frac{1}{\mathrm{vol}(\mathbf{B})} \int_{\mathbf{B}} L(f(\mathbf{t})) d\mathbf{t}.$$

Mivel itt $f(\mathbf{t}) \in f(\mathbf{B}) \subseteq \mathrm{conv}(f(\mathbf{B}))$ a T_1 féltérbe esik, ezért $L(f(\mathbf{t})) \leq L(\mathbf{S})$, és így

$$\frac{1}{\mathrm{vol}(\mathbf{B})} \int_{\mathbf{B}} L(f(\mathbf{t})) d\mathbf{t} \leq \frac{1}{\mathrm{vol}(\mathbf{B})} \int_{\mathbf{B}} L(\mathbf{S}) d\mathbf{t} = \frac{L(\mathbf{S})}{\mathrm{vol}(\mathbf{B})} \int_{\mathbf{B}} d\mathbf{t} = L(\mathbf{S}).$$

Tehát azt kaptuk, hogy

$$L(\mathbf{S}) = \frac{1}{\mathrm{vol}(\mathbf{B})} \int_{\mathbf{B}} L(f(\mathbf{t})) d\mathbf{t} \leq \frac{1}{\mathrm{vol}(\mathbf{B})} \int_{\mathbf{B}} L(\mathbf{S}) d\mathbf{t} = L(\mathbf{S}),$$

azaz az $L(f(\mathbf{t}))$ és $L(\mathbf{S})$ függvények integrálja megegyezik. Mivel mindkét függvény folytonos és $L(f(\mathbf{t})) \leq L(\mathbf{S})$ minden $\mathbf{t} \in \mathbf{B}$ esetén, ezért a két függvény megegyezik a $\mathbf{B}$ halmazon. Vagyis bármely $\mathbf{t} \in \mathbf{B}$-re $f(\mathbf{t}) \in H$, azaz $f(\mathbf{B}) \subseteq H$, és így $\mathrm{conv}(f(\mathbf{B})) \subseteq H$, ami ellentmond az 1.6. Lemmának, hiszen a most kapott eredmény szerint $\mathrm{conv}(f(\mathbf{B}))$ „legfeljebb $(N-1)$-dimenziós” és így belseje üres. ■

1.11. Lemma. *A $\mathrm{conv}(f(\mathbf{B}))$ halmaz belseje megegyezik a $\mathrm{conv}(f(\tilde{\mathbf{B}}))$ halmaz belsejével.*

Bizonyítás. Tudjuk, hogy $\tilde{\mathbf{B}}$ sűrű $\mathbf{B}$-ben, így f folytonossága miatt $f(\tilde{\mathbf{B}})$ sűrű $f(\mathbf{B})$-ben, azaz $\mathrm{cl}(f(\tilde{\mathbf{B}})) = f(\mathbf{B})$. Mivel $f(\tilde{\mathbf{B}})$ korlátos, ezért az 1.4. Lemma alapján $\mathrm{conv}(f(\mathbf{B})) = \mathrm{conv}(\mathrm{cl}(f(\tilde{\mathbf{B}}))) = \mathrm{cl}(\mathrm{conv}(f(\tilde{\mathbf{B}})))$. Vagyis $\mathrm{int}(\mathrm{conv}(f(\mathbf{B}))) = \mathrm{int}(\mathrm{cl}(\mathrm{conv}(f(\tilde{\mathbf{B}})))) = \mathrm{int}(\mathrm{conv}(f(\tilde{\mathbf{B}})))$. Itt az utolsó egyenlőség az 1.5. Lemma alapján teljesül. ■

1.12. Tétel (Carathéodory-tétel). *Legyen $S \subseteq \mathbb{R}^n$ tetszőleges halmaz. Ekkor bármely $\mathbf{v} \in \mathrm{conv}(S)$ esetén $\mathbf{v}$ előáll legfeljebb $n+1$ darab S-beli vektor konvex lineáris kombinációjaként. Azaz minden $\mathbf{v} \in \mathrm{conv}(S)$-re léteznek olyan $\lambda_0, \ldots, \lambda_n$ nemnegatív valós számok, és $\mathbf{v}_0, \ldots, \mathbf{v}_n \in S$ vektorok, hogy $\mathbf{v} = \sum_{i=0}^{n} \lambda_i \mathbf{v}_i$, és $\sum_{i=0}^{n} \lambda_i = 1$.*

1.13. Következmény. *Ha a Carathéodory-tételben szereplő $\mathbf{v}, \mathbf{v}_0, \ldots, \mathbf{v}_n$ vektorok mindegyike racionális koordinátájú, akkor léteznek olyan $\lambda_0, \ldots, \lambda_n$ nemnegatív racionális számok, melyekre $\mathbf{v} = \sum_{i=0}^{n} \lambda_i \mathbf{v}_i$, és $\sum_{i=0}^{n} \lambda_i = 1$.*

Bizonyítás. Ha a $\mathbf{v} = \sum_{i=0}^{n} \lambda_i \mathbf{v}_i$ egyenletet koordinátánként kiírjuk, akkor egy $n+1$ ismeretlenes egyenletrendszert kapunk, melyben az ismeretlenek a λ_i együtthatók ($i \in \{0, \ldots, n\}$). Egészítsük ki ezt az egyenletrendszert a $\sum_{i=0}^{n} \lambda_i = 1$ egyenlettel. Ennek az új egyenletrendszernek a Carathéodory-tétel miatt létezik nemnegatív valós megoldása. Ez Gauss-eliminációval meghatározható. Mivel $\mathbf{v}, \mathbf{v}_0, \ldots, \mathbf{v}_n$ mindegyike racionális koordinátájú és az elimináció során csak a négy alapművelet fordul elő, így ha csak egy megoldás van, akkor a $\lambda_0, \ldots, \lambda_n$ együtthatók is szükségszerűen racionálisak lesznek. Ha több megoldás is létezik, akkor a függő változók a szabad változókból racionális együtthatókkal fejezhetőek ki, tehát a szabad változóknak racionális értékeket adva minden változó racionális lesz. Ilyen racionális megoldással tetszőlegesen megközelíthetjük a Carathéodory-tétel által biztosított nemnegatív valós megoldást, ezért nemnegatív racionális megoldás is létezik. ■

1.14. Tétel (Hilbert-Dress azonosság). *Legyen k természetes szám, és $N = \binom{2k+4}{4}$. Ekkor léteznek olyan M, m_{N+1} pozitív egészek, m_i $(0 \le i \le N)$ nemnegatív egészek, és a_{ij} $(0 \le i \le N, 1 \le j \le 5)$ egész számok, hogy tetszőleges $X_1, \ldots, X_5$ valós számokra*

$$M(X_1^2 + \cdots + X_5^2)^k = \sum_{i=0}^{N} m_i (a_{i1}X_1 + \cdots + a_{i5}X_5)^{2k} + m_{N+1}X_5^{2k}. \tag{1.3}$$

Bizonyítás. Az 1.7., 1.10. és 1.11. Lemmák miatt

$$\mathbf{S} = c(X_1^2 + \cdots + X_5^2)^k \in \mathrm{int}(\mathrm{conv}(f(\mathbf{B}))) = \mathrm{int}(\mathrm{conv}(f(\tilde{\mathbf{B}}))),$$

ezért létezik olyan $\varepsilon > 0$, hogy az $\mathbf{S}$ integrálközép ε sugarú környezete teljes egészében benne van a $\mathrm{conv}(f(\tilde{\mathbf{B}}))$ halmazban. Ekkor tetszőleges $0 < \mu < \varepsilon$ esetén $\mathbf{S} - \mu X_5^{2k} \in \mathrm{conv}(f(\tilde{\mathbf{B}}))$ (lásd a 2. ábrát). Az origót az $\mathbf{S} - \mu X_5^{2k}$ ponttal összekötő szakasz pontjai felírhatók $\lambda(\mathbf{S} - \mu X_5^{2k})$ alakban, ahol $0 \le \lambda \le 1$. Ezek a pontok mind $\mathrm{conv}(f(\tilde{\mathbf{B}}))$-ban vannak, mert $\mathbf{0} = f(0,0,0,0,0) \in \mathrm{conv}(f(\tilde{\mathbf{B}}))$, tehát

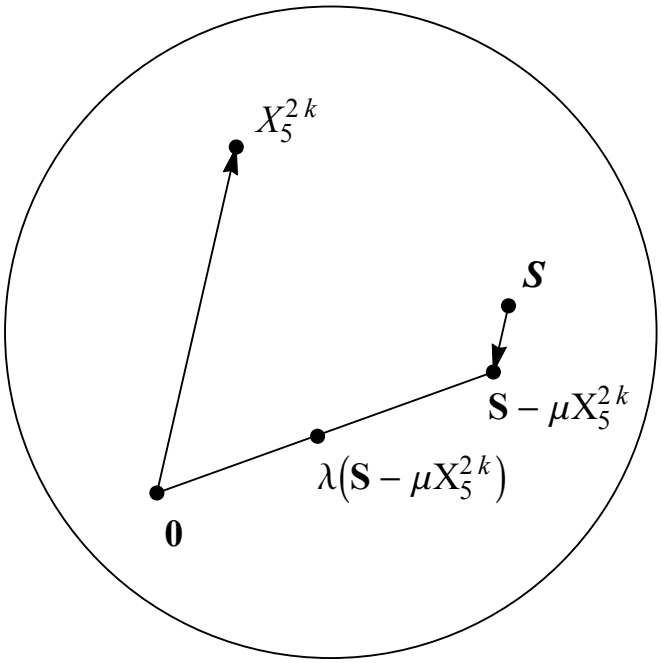
$$\lambda c(X_1^2 + \cdots + X_5^2)^k - \lambda\mu X_5^{2k} \in \mathrm{conv}(f(\tilde{\mathbf{B}})). \tag{1.4}$$

Létezik olyan 0 és 1 közé eső λ, melyre λc pozitív racionális szám, és ehhez a λ-hoz választható olyan elég kicsi μ, melyre $\lambda\mu$ is pozitív racionális szám. Tehát λ és μ megfelelő választásával az (1.4)-ben szereplő vektor racionális koordinátájú lesz.

Azt tudjuk, hogy az $f(\tilde{\mathbf{B}})$ halmaz $(a_1X_1 + \cdots + a_5X_5)^{2k}$ alakú polinomokból áll $(a_1, \ldots, a_5 \in \mathbb{Q})$, és ezek (1.1) miatt racionális koordinátájúak, ezért a Carathéodory-tétel következménye miatt léteznek olyan r_i nemnegatív racionális számok, hogy $\sum_{i=0}^{N} r_i = 1$, és

$$\lambda c(X_1^2 + \cdots + X_5^2)^k - \lambda\mu X_5^{2k} = \sum_{i=0}^{N} r_i(a_{i1}X_1 + \cdots + a_{i5}X_5)^{2k}.$$

Ezt a $\lambda c, \lambda\mu, r_i, a_{ij}^{2k}$ $(0 \le i \le N, 1 \le j \le 5)$ racionális számok nevezőinek legkisebb közös többszörösével megszorozva megkapjuk a kívánt egyenlőséget. ■



2. ábra. A Hilbert-Dress azonosság bizonyítása. (A kör a $\mathrm{conv}(f(\tilde{\mathbf{B}}))$ halmazt jelöli.)

2. A Waring-sejtés bizonyítása

2.1. Lemma. *Tetszőleges k természetes szám és x valós szám esetén érvényes a következő azonosság:*

$$\sum_{j=0}^{k-1}(-1)^{k-1-j}\binom{k-1}{j}(x+j)^k = k!\cdot x + \frac{k!(k-1)}{2}. \tag{2.1}$$

Bizonyítás. Az egyenlőséget elég csak $x \in \mathbb{N}$ esetén bizonyítani, ugyanis ekkor a formulát nullára rendezve azt kapjuk, hogy egy legfeljebb k-ad fokú polinomnak végtelen sok zérushelye van, ez pedig csak úgy lehetséges, ha az a konstans 0 polinom volt.

Tehát a bizonyítás $x \in \mathbb{N}$ esetén: Találjunk ki egy kombinatorika feladatot, melynek a megoldása éppen a bal oldali formula. Ha ez sikerült, rá fogunk jönni, hogy van egy sokkal egyszerűbb megoldás is, ez adja a jobb oldali képletet. A feladat a következő: Számoljuk meg az összes olyan $f : [k] \longrightarrow [k-1]\cup X$ leképezést, melyre $[k-1]$ minden elemének van őse, ahol X egy x-elemű halmaz ami diszjunkt a $[k-1]$ halmaztól. (Itt $[n] := \{1,\dots,n\}$.)

A bal oldal esetén a szita formulát használjuk. Legyen

$$S = \{f : [k] \longrightarrow [k-1]\cup X\} \text{ és } A_i = \{f \in S : i \notin f([k])\}, \text{ ahol } i \in [k-1].$$

Ekkor $|S| = (k-1+x)^k$ és a kérdéses leképezések száma $|S\setminus\bigcup_{i=1}^{k-1} A_i|$. Legyen $L \subseteq [k-1]$, és $A_L := \bigcap_{i\in L} A_i$. Ha $|L| = \ell$, akkor világos, hogy $|A_L| = (k-1+x-\ell)^k$. Ezek után a szita formulát (lásd [3]) alkalmazva adódik, hogy

$$\left|S\setminus\bigcup_{i=1}^{k-1} A_i\right| = \sum_{L\subseteq[k-1]}(-1)^{|L|}|A_L| = \sum_{\ell=0}^{k-1}(-1)^{\ell}\binom{k-1}{\ell}(k-1+x-\ell)^k.$$

Áttérve a $j = k-1-\ell$ futóindexre, megkapjuk (2.1) bal oldalát.

Most számoljuk meg ezeket a leképezéseket másként. A feladat feltételei szerint $f([k]) \supseteq [k-1]$. Tehát vagy $f([k]) = [k-1]$ vagy $f([k]) = [k-1]\cup\{h\}$, ahol $h \in X$. Az első esetben pontosan két elem képe lesz ugyanaz. Válasszuk ki ezeket az $i,j \in [k]$ elemeket, és a közös $f(i) = f(j) = c \in [k-1]$ képüket. Erre $\binom{k}{2}(k-1)$ lehetőségünk van. Világos, hogy $f|_{[k]\setminus\{i,j\}} \longrightarrow [k-1]\setminus\{c\}$ bijekció, ezért a maradék $k-2$ elem képének megválasztására $(k-2)!$ lehetőségünk van. Látható, hogy ez összesen $\binom{k}{2}(k-1)(k-2)! = \frac{k!(k-1)}{2}$ lehetőség. A második esetben először kiválasztjuk $[k]$-ból azt a g elemet, melynek a képe X-ből való, és kiválasztjuk a képét, h-t $(h \in X)$. Erre $k\cdot x$ lehetőségünk van. Az első esethez hasonlóan $f|_{[k]\setminus\{g\}} \longrightarrow [k-1]$ bijekció, így a maradék $k-1$ elem képét $(k-1)$!-féleképpen választhatjuk meg. Ez összesen $k\cdot x\cdot(k-1)! = k!\cdot x$ lehetőség. A két eset együttesen adja (2.1) jobb oldalát. ■

2.2. Következmény. *Tetszőleges k természetes számhoz léteznek olyan csak k-tól függő R, A, B természetes számok és $a_1,\dots,a_R,a'_1,\dots,a'_R$ egészek, hogy bármely x valós számra igaz a következő:*

$$\sum_{i=1}^{R}(x+a_i)^{2k} - \sum_{j=1}^{R}(x+a'_j)^{2k} = Ax + B. \tag{2.2}$$

Bizonyítás. Helyettesítsünk (2.1)-be k helyére $2k$-t és bontsuk két részre a bal oldali összeget aszerint, hogy a benne szereplő binomiális együttható nevezője páros vagy páratlan. Ekkor azt kapjuk, hogy

$$\sum_{m=1}^{k}\binom{2k-1}{2m-1}(x+2m-1)^{2k}-\sum_{n=1}^{k}\binom{2k-1}{2n-2}(x+2n-2)^{2k}=$$
$$=(2k)!\cdot x+\frac{(2k)!(2k-1)}{2}. \quad (2.3)$$

Kombinatorikából tudjuk, hogy $\sum_{j=0}^{\ell}\binom{\ell}{j}=2^{\ell}$ valamint $\sum_{j=0}^{\ell}(-1)^j\binom{\ell}{j}=0$. Az utóbbi egyenlőség úgy értelmezhető, hogy egy ℓ elemű halmaznak ugyanannyi páros elemszámú részhalmaza van, mint ahány páratlan elemszámú. Ezek után mivel

$$\sum_{m=1}^{k}\binom{2k-1}{2m-1}+\sum_{n=1}^{k}\binom{2k-1}{2n-2}=\sum_{j=0}^{2k-1}\binom{2k-1}{j}=2^{2k-1},$$

világos, hogy

$$\sum_{m=1}^{k}\binom{2k-1}{2m-1}=\sum_{n=1}^{k}\binom{2k-1}{2n-2}=2^{2k-2}.$$

Ha a (2.3) bal oldalán álló első szummában lévő binomiális együtthatókat, mint 1-esek összegét fogjuk fel, azt kapjuk, hogy a szumma egyenlő 2^{2k-2} darab $(x+a_i)^{2k}$ alakú kifejezés összegével, ahol a_i egész minden $i\in\{1,2,\dots,2^{2k-2}\}$-re. Hasonló igaz a második szummára is. Így (2.3)-at az említett módon átírva és átindexezve megkapjuk a kívánt formulát. Ezek alapján az állításban szereplő konstansok értékei is meghatározhatók: $R=2^{2k-2}$, $A=(2k)!$, $B=\frac{(2k)!(2k-1)}{2}$. ■

2.3. Tétel (könnyű Waring-sejtés). *Bármely egész szám előáll legfeljebb $2^{k-1}+k!$ darab k-adik hatvány előjeles összegeként.*

Bizonyítás. Ha a (2.1) bal oldalán álló binomiális együtthatókat mint 1-esek összegét fogjuk fel, akkor azt kapjuk, hogy bármely $k!\cdot x+\frac{k!(k-1)}{2}$ alakú egész szám felírható, mint $\sum_{j=0}^{k-1}\binom{k-1}{j}=2^{k-1}$ darab k-adik hatvány előjeles összege. (Itt x természetesen csak egész szám lehet.) Ezek után elég belátni, hogy bármely $n\in\mathbb{Z}$ egész szám előáll

$$n=k!\cdot x+\frac{k!(k-1)}{2}+1^k+\dots+1^k \quad (2.4)$$

alakban, ahol az 1-esek számát tudjuk egy csak k-tól függő korláttal felülről becsülni. Ez x megfelelő választásán múlik. Legyen

$$x=\left\lfloor\frac{n-\frac{k!(k-1)}{2}}{k!}\right\rfloor=\left\lfloor\frac{n}{k!}-\frac{k-1}{2}\right\rfloor.$$

(Itt $\lfloor.\rfloor$ az egészrészt jelöli.) Nyilvánvaló, hogy

$$\frac{n}{k!}-\frac{k-1}{2}-1<x\le\frac{n}{k!}-\frac{k-1}{2}.$$

Az egyenlőtlenséget átalakítva kapjuk, hogy

$$n-k!<k!\cdot x+\frac{k!(k-1)}{2}\le n,$$

azaz n és $k!\cdot x+\frac{k!(k-1)}{2}$ különbsége legfeljebb $k!$. Tehát (2.4)-ben legfeljebb $k!$ darab 1^k lép fel. Így a 2.1. Lemma alapján n előáll legfeljebb $2^{k-1}+k!$ darab k-adik hatvány előjeles összegeként. ■

2.4. Lemma. *Legyen k természetes szám és $\kappa=1-1/k$. Ekkor tetszőleges $x\geq 0$ valós szám esetén $0\leq x-\lfloor\sqrt[k]{x}\rfloor^k\leq kx^\kappa$.*

Bizonyítás. Az első egyenlőtlenség egyszerű átrendezésből adódik. A második egyenlőtlenséghez alkalmazzuk a Lagrange-féle középértéktételt az $f(x)=x^k$ függvényre az $(\lfloor\sqrt[k]{x}\rfloor;\sqrt[k]{x})$ intervallumon. A tétel szerint létezik egy olyan c eleme az említett intervallumnak, melyre

$$(\sqrt[k]{x}-\lfloor\sqrt[k]{x}\rfloor)f'(c)=x-\lfloor\sqrt[k]{x}\rfloor^k.$$

Mivel $f'(x)=kx^{k-1}$ ezen az intervallumon monoton növő, ezért a $c=\sqrt[k]{x}$ helyettesítéssel kapjuk, hogy

$$x-\lfloor\sqrt[k]{x}\rfloor^k\leq(\sqrt[k]{x}-\lfloor\sqrt[k]{x}\rfloor)f'(\sqrt[k]{x})=(\sqrt[k]{x}-\lfloor\sqrt[k]{x}\rfloor)kx^\kappa.$$

Mivel $\sqrt[k]{x}-\lfloor\sqrt[k]{x}\rfloor\leq 1$, ezért ezt elhagyva felülről becsüljük a kifejezést, így megkapjuk a kívánt egyenlőtlenséget. ■

2.5. Lemma. *Legyen k természetes szám és $\kappa=1-1/k$. Tetszőleges $x\geq 0$ valós szám és t természetes szám esetén x előállítható $x=z_1^k+\cdots+z_t^k+r_t$ alakban, ahol $z_1,\ldots,z_t\in\mathbb{N}_0$ és $0\leq r_t\leq k^k x^{\kappa^t}$.*

Bizonyítás. Megmutatjuk, hogy a fenti előállítás létezik akkor is, ha r_t-re erősebb egyenlőtlenséget követelünk meg:

$$0\leq r_t\leq k^{\sum_{i=0}^{t-1}\kappa^i}x^{\kappa^t}. \tag{2.5}$$

Ez valóban erősebb egyenlőtlenség, mert a k kitevőjében szereplő szummát felülről becsülhetjük a $\sum_{i=0}^{\infty}\kappa^i$ mértani sorral, melynek összege $\frac{1}{1-\kappa}=k$. (A sor konvergens lesz, mert $\kappa<1$ bármely k-ra.) Tehát elég az erősebb állítást bizonyítani, ez pedig t szerinti teljes indukcióval történik.

A $t=1$ esetben legyen $z_1=\lfloor\sqrt[k]{x}\rfloor$ és $r_1=x-\lfloor\sqrt[k]{x}\rfloor^k$. Ekkor megkapjuk a kívánt előállítást, hiszen $x=z_1^k+r_1$, és a 2.4. Lemma alapján r_1 is eleget tesz (2.5)-nek.

Ezek után az indukciós feltevésünk az, hogy t-re létezik a fenti előállítás, azaz $x=z_1^k+\cdots+z_t^k+r_t$, ahol $z_1,\ldots,z_t\in\mathbb{N}_0$ és r_t eleget tesz (2.5)-nek. A $t=1$ eset gondolatmenetét alkalmazzuk r_t-re, tehát legyen $z_{t+1}=\lfloor\sqrt[k]{r_t}\rfloor$ és $r_{t+1}=r_t-\lfloor\sqrt[k]{r_t}\rfloor^k$. Így $x=z_1^k+\cdots z_t^k+z_{t+1}^k+r_{t+1}$ és r_{t+1}-re a kívánt egyenlőtlenség teljesül, mert

$$r_{t+1}=r_t-\lfloor\sqrt[k]{r_t}\rfloor^k\leq kr_t^\kappa\leq k(k^{\sum_{i=0}^{t-1}\kappa^i}x^{\kappa^t})^\kappa=k^{\sum_{i=0}^{t}\kappa^i}x^{\kappa^{t+1}}.$$

Az első egyenlőtlenség a 2.4. Lemma alapján, a második az indukciós feltevés miatt teljesül. Így az állítást $t+1$-re is beláttuk. ■

2.6. Lemma. *Rögzítsünk egy k természetes számot, és tekintsük az (1.3)-beli M együtthatót. Ekkor létezik olyan Q természetes szám, hogy bármely $\ell\in\mathbb{N}$ és $x\in\mathbb{Z}$ esetén, ha $|x|\leq\sqrt{\ell}$, akkor léteznek olyan $u_1,u_2,\ldots,u_Q$ egész számok, melyekre*

$$M\ell^k=x^{2k}+\sum_{h=1}^{Q}u_h^{2k}.$$

Bizonyítás. Ha $|x| \leq \sqrt{\ell}$, akkor $\ell - x^2$ nemnegatív egész, ezért a Lagrange-féle négy négyzetszám tétel szerint léteznek olyan $x_1, \ldots, x_4$ egészek, hogy $\ell - x^2 = x_1^2 + x_2^2 + x_3^2 + x_4^2$. Azaz $\ell = x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2$, ahol $x_5 = x$. Így (1.3) alapján

$$M\ell^k = x^{2k} + \overbrace{x^{2k} + \cdots + x^{2k}}^{m_{N+1}-1} + \sum_{i=0}^{N} \overbrace{(a_{i1}x_1 + \cdots + a_{i5}x_5)^{2k} + \cdots + (a_{i1}x_1 + \cdots + a_{i5}x_5)^{2k}}^{m_i}.$$

Tehát $M\ell^k$ előáll, mint $x_5^{2k} = x^{2k}$ és $Q = m_{N+1} - 1 + \sum_{i=0}^{N} m_i$ darab $2k$-adik hatvány összege. Ezzel az állítást bebizonyítottuk. ■

2.7. Tétel. *Bármely rögzített k természetes számra $g(k, m)$ korlátos.*

Bizonyítás. Rögzítsünk egy k természetes számot. Világos, hogy $g(k, m) \leq m$, ugyanis m mindig felírható $m = 1^k + \cdots + 1^k$ alakban. Ezt a korlátot szeretnénk javítani úgy, hogy az csak k-tól függjön. Tegyük fel, hogy létezik olyan m_0 küszöb és K csak k-tól függő korlát, hogy bármely $m \geq m_0$ esetén $g(k, m) \leq K$. Ekkor minden m-re $g(k, m) \leq \max\{K, g(k, 1), \ldots, g(k, m_0)\} \leq \max\{K, m_0\}$, ezért a kérdést elég csak nagy m-ekre vizsgálni.

Tekintsük az (1.3)-beli M és (2.2)-beli R számokat (ezek nyilván csak k-tól függnek), és legyen m a k-adik hatványok összegeként előállítani kívánt természetes szám. Legyen $x = \frac{m}{RM}$ és $\ell = \lfloor \sqrt[k]{x} \rfloor$. Ekkor világos, hogy ℓ^k a legnagyobb k-adik hatvány, ami nem nagyobb, mint $\frac{m}{RM}$. Így ℓ választása miatt $\ell^k \leq \frac{m}{RM} \leq (\ell+1)^k$. Ha $m \geq RM$, akkor $\ell \geq 1$ és így $\ell + 1 \leq 2\ell$. Tehát, ha $m \geq RM$, akkor $\ell^k \leq \frac{m}{RM} \leq (2\ell)^k$. Ebből következik, hogy $\frac{1}{2}(\frac{m}{RM})^{1/k} \leq \ell \leq (\frac{m}{RM})^{1/k}$.

Ezek után alkalmazzuk x-re a 2.4. Lemmát: $0 \leq \frac{m}{RM} - \ell^k \leq k(\frac{m}{RM})^{\kappa}$. Az egyenlőtlenséget RM-mel szorozva és bevezetve az $r_0 = m - RM\ell^k$ jelölést, azt kapjuk, hogy $m = RM\ell^k + r_0$, és

$$0 \leq r_0 \leq kRM \left(\frac{m}{RM}\right)^{\kappa}. \tag{2.6}$$

Mivel $\kappa = 1 - 1/k < 1$, ezért $\kappa^t \longrightarrow 0$, ha $t \longrightarrow \infty$, így létezik olyan t, hogy $\kappa^{t+1} < \frac{1}{3k}$. Tekintsük ezen t-k közül a legkisebbet, és alkalmazzuk a 2.5. Lemmát r_0-ra. Így

$$0 \leq r_0 = z_1^k + \cdots + z_t^k + r_t,$$

ahol $z_i \in \mathbb{N}_0$ minden $i \in \{1, \ldots, t\}$ esetén és $0 \leq r_t \leq k^k r_0^{\kappa^t}$. Most (2.6) alapján tovább becsüljük r_t-t:

$$0 \leq r_t \leq k^k r_0^{\kappa^t} \leq k^k \left(kRM \left(\frac{m}{RM}\right)^{\kappa}\right)^{\kappa^t} = k^k (kRM)^{\kappa^t} \frac{1}{(RM)^{\kappa^{t+1}}} (m^{\kappa})^{\kappa^t} = C_k m^{\kappa^{t+1}},$$

ahol C_k csak k-tól függő konstans. Ez tovább becsülhető, ugyanis t választása miatt $C_k m^{\kappa^{t+1}} \leq C_k m^{1/(3k)}$. Jelenleg ott tartunk, hogy m-et sikerült előállítani

$$m = RM\ell^k + z_1^k + \cdots + z_t^k + r_t$$

alakban, ahol $r_t \leq C_k m^{1/(3k)}$.

Most R-szer fogjuk alkalmazni a 2.6. Lemmát. Legyenek $x_1, \dots, x_R$ olyan egészek, melyek abszolút értéke $\sqrt{\ell}$-nél nem nagyobb (ezek értékét később fogjuk pontosan megválasztani). A lemma alapján

$$\begin{aligned} M\ell^k &= x_1^{2k} + \sum_{h=1}^{Q} u_h^{2k}, \\ M\ell^k &= x_2^{2k} + \sum_{h=Q+1}^{2Q} u_h^{2k}, \\ &\dots \\ M\ell^k &= x_R^{2k} + \sum_{h=(R-1)Q+1}^{RQ} u_h^{2k}, \end{aligned}$$

ahol $u_1, \dots, u_{RQ}$ egészek. A kapott R egyenlőséget összeadva adódik, hogy

$$RM\ell^k = \sum_{j=1}^{R} x_j^{2k} + \sum_{h=1}^{RQ} u_h^{2k}.$$

Összegezve az eddigieket, m felírható

$$m = \sum_{j=1}^{R} x_j^{2k} + \sum_{h=1}^{RQ} u_h^{2k} + z_1^k + \dots + z_t^k + r_t \tag{2.7}$$

alakban, azaz sikerült előállítani $R + RQ + t$ darab k-adik hatvány és egy r_t maradéktag összegeként, ahol $r_t \le C_k m^{1/(3k)}$.

Az x_j egészek megválasztására van bizonyos szabadsági fokunk ($|x_j| \le \sqrt{\ell}$, $j \in \{1, \dots, R\}$). Tekintsük a (2.2)-ben szereplő a_i, a'_j egész számokat, és írjunk fel minden x_j-t $x_j = x + a'_j$ alakban ($x \in \mathbb{Z}$), valamint vezessük be az $y_i = x + a_i$ változókat. Az itt használt x egész számot később fogjuk megválasztani (nem egyezik a korábban definiált $x = \frac{m}{RM}$-mel). Ezek után a (2.2) formulát átrendezve és élve az y_i-kre és x_j-kre bevezetett jelölésekkel adódik, hogy

$$\sum_{j=1}^{R} x_j^{2k} = \sum_{i=1}^{R} y_i^{2k} - (Ax + B),$$

amit behelyettesítünk (2.7)-be és így azt kapjuk, hogy

$$m = \sum_{i=1}^{R} y_i^{2k} + \sum_{h=1}^{RQ} u_h^{2k} + z_1^k + \dots + z_t^k + r_t - (Ax + B). \tag{2.8}$$

Azt szeretnénk, hogy $r_t - (Ax + B)$ kicsi legyen, azaz egy k-tól függő korlát alatt maradjon. Most fogjuk kihasználni az x_j-k megválasztására vonatkozó szabadságunkat. Válasszuk x-et a könnyű Waring-sejtésnél látotthoz hasonló módon $x = \lfloor \frac{r_t - B}{A} \rfloor$-nek. Világos, hogy

$$\frac{r_t - B}{A} - 1 < x \le \frac{r_t - B}{A}.$$

Átalakítás után látható, hogy $0 \leq r_t - (Ax + B) < A$, és mivel A csak k-tól függ, így sikerült az $r_t - (Ax + B)$ kifejezést egy csak k-tól függő korlát alatt tartani.

Egy kérdés marad csak, hogy $|x_j| = |x + a'_j| \leq \sqrt{\ell}$ igaz-e, máskülönben ugyanis nem teljesül a 2.6. Lemma ezen feltétele. Ehhez egy ennél jóval erősebb állítást fogunk bizonyítani: $\frac{|x_j|}{\sqrt{\ell}} \longrightarrow 0$, ha $m \longrightarrow \infty$. Becsüljük $|x_j|$-t felülről:

$$|x_j| = |x+a'_j| \leq |x|+|a'_j| = \left|\left\lfloor \frac{r_t - B}{A} \right\rfloor\right| + |a'_j| \leq \left|\frac{r_t - B}{A}\right| + 1 + |a'_j| \leq \frac{r_t}{A} + \frac{B}{A} + 1 + |a'_j|.$$

Itt használtuk a háromszög-egyenlőtlenséget, azt, hogy bármely $v \in \mathbb{R}$ esetén $||\lfloor v \rfloor|| \leq |v| + 1$, valamint hogy A, B és r_t nemnegatívok. Most tekintsük az

$$\frac{\frac{r_t}{A} + \frac{B}{A} + 1 + |a'_j|}{\sqrt{\ell}} \geq \frac{|x_j|}{\sqrt{\ell}}$$

hányadost, amint m tart a végtelenhez. Tudjuk, hogy $m \geq RM$ esetén $\ell \geq \frac{1}{2}(\frac{m}{RM})^{1/k}$, ezért ℓ is végtelenbe tart. Mivel $\frac{B}{A} + 1 + |a'_j|$ egy k-tól függő konstans, így ez $\sqrt{\ell}$-lel osztva 0-hoz tart. A megmaradt $\frac{r_t}{A\sqrt{\ell}}$ kifejezésben az A konstans szintén nincs befolyással a határértékre, így elég az $\frac{r_t}{\sqrt{\ell}}$ hányados határértékét vizsgálni. Az eddigiek alapján tudjuk, hogy $r_t \leq C_k m^{1/(3k)}$ és $\sqrt{\ell} \geq \sqrt{\frac{1}{2}(\frac{m}{RM})^{1/k}}$, ha $m \geq RM$. Így a vizsgált hányados felülről becsülhető:

$$\frac{r_t}{\sqrt{\ell}} \leq \frac{C_k m^{1/(3k)}}{\sqrt{\frac{1}{2}(\frac{m}{RM})^{1/k}}} = \frac{C_k}{\sqrt{\frac{1}{2}(\frac{1}{RM})^{1/k}}} \frac{1}{m^{1/(6k)}}.$$

Az utolsó formulában az $\frac{1}{m^{1/(6k)}}$ kifejezés csak egy konstanssal van szorozva, így világos, hogy 0-hoz tart. Tehát $\frac{r_t}{\sqrt{\ell}} \longrightarrow 0$, ha $m \longrightarrow \infty$. Azaz beláttuk, hogy $\frac{|x_j|}{\sqrt{\ell}} \longrightarrow 0$, ha $m \longrightarrow \infty$. Tehát sikerült bebizonyítani, hogy elég nagy m esetén $|x_j| \leq \sqrt{\ell}$ minden $j \in \{1, \ldots, R\}$-re.

A (2.8)-ban szereplő $r_t - (Ax + B)$ kifejezés egy egész szám (hiszen az összes többi tag is egész), és láttuk, hogy $0 \leq r_t - (Ax + B) < A$, tehát felírható A-nál kevesebb 1^k összegeként. Így $g(k, m) \leq R + RQ + t + A - 1$ egy csak k-tól függő alkalmas felső korlát. Ezzel tételünket bebizonyítottuk. ■

Hivatkozások

[1] F. Dress, *Théorie additive des nombres, problème de Waring et théorème de Hilbert,* Enseignement Math. (2) **18** (1972), 175–190.

[2] Freud Róbert, Gyarmati Edit, *Számelmélet,* Nemzeti Tankönyvkiadó, Budapest, 2000.

[3] Hajnal Péter, *Összeszámlálási problémák,* Polygon jegyzettár, Szeged, 1997.

[4] Kovács Zoltán, *Konvexitás,* előadásvázlat, Nyíregyházi Főiskola, 2004. http://zeus.nyf.hu/∼kovacsz/konvex.pdf

[5] S. R. Lay, *Convex sets and their applications,* John Wiley & Sons, New York, 1982.

[6] P. Pollack, *Not always buried deep: A second course in elementary number theory,* American Mathematical Society, Providence, RI, 2009.

[7] Szabó László, *Konvex geometria,* egyetemi jegyzet, ELTE TTK, Budapest, 1996.

[8] R. C. Vaughan, T. D. Wooley, *Waring's problem: a survey*, Number theory for the millennium, III (Urbana, IL, 2000), pp. 301–340, A K Peters, Natick, MA, 2002.

Nyilatkozat

Alulírott Fazekas Róbert kijelentem, hogy a szakdolgozatban foglaltak saját munkám eredményei, és csak a hivatkozott forrásokat (szakirodalom, eszközök, stb.) használtam fel. Tudomásul veszem, hogy szakdolgozatomat a Szegedi Tudományegyetem könyvtárában a kölcsönözhető könyvek között helyezik el, és az interneten is nyilvánosságra hozhatják.

Szeged, 2015. december 2. .....

aláírás