Hatványokból építkezünk

Hány hatodik hatvány kell? Előállítható-e minden elég nagy pozitív egész hat hatodik hatvány összegeként? Azaz megoldható-e az

$$x_1^6 + x_2^6 + \ldots + x_6^6 = n \tag{1}$$

egyenlet $x_i \geq 0$ egészekben, ha n elég nagy?

A válasz nemleges, ugyanis végtelen sok n nem állítható elő így. Ehhez keresünk egy olyan számot, amivel való osztásnál egy hatodik hatvány maradéka csak 0 vagy 1 lehet. Némi próbálgatás után kiderül, hogy a 7 ilyen:

$$c^6 \equiv \begin{cases} 1 \pmod 7, & \text{ha } 7 \nmid c; \\ 0 \pmod 7, & \text{ha } 7 \mid c. \end{cases} \tag{2}$$

Ez egyébként nem véletlen, hanem a kis Fermat-tétel speciális esete.

Legyen $7 \mid n$, ekkor (1)-et modulo 7 nézve a bal oldal 0, a jobb oldal pedig (2) alapján 0 és 6 közé esik. Egyenlőség tehát csak úgy teljesülhet, ha a jobb oldal 0, ami azt jelenti, hogy mindegyik x_i osztható 7-tel. Ekkor viszont (1) miatt $7^6 \mid n$. Ha tehát $7 \mid n$, de $7^6 \nmid n$, akkor (1) nem állhat fenn.

Vajon hét hatodik hatvány elég-e? Most a modulo 8 maradékokkal konstruálhatunk végtelen sok kivételt, felhasználva, hogy

$$c^6 \equiv \begin{cases} 1 \pmod 8, & \text{ha } 2 \nmid c; \\ 0 \pmod 8, & \text{ha } 2 \mid c. \end{cases}$$

Ebből az előzőekhez hasonlóan adódik, hogy ha n osztható 8-cal, de nem osztható 64-gyel, akkor n nem írható fel hét hatodik hatvány összegeként.

Ugyanígy kapjuk, hogy még nyolc hatodik hatvány sem elég; ekkor modulo 9 kell okoskodnunk:

$$c^6 \equiv \begin{cases} 1 \pmod 9, & \text{ha } 3 \nmid c; \\ 0 \pmod 9, & \text{ha } 3 \mid c. \end{cases}$$

(Ez sem véletlen, mert az Euler–Fermat-tétel speciális esete.) Most biztosan rosszak azok a számok, amelyek oszthatók 9-cel, de nem többszörösei 3^6-nak.

És kilenc hatodik hatványra mi a helyzet? Ez egy régi megoldatlan probléma. Jelenleg csak annyit tudunk, hogy 24 hatodik hatvány összegeként már minden elég nagy pozitív egész előáll.

A következőkben egy kicsit körbejárjuk az általánosabb kérdést.

A 216 éves történet. Waring 1770-ben a következőket írta: Minden szám négy négyzetszám összege, kilenc köbszám összege, tizenkilenc negyedik hatvány összege stb.

Első látásra egyáltalán nem világos, milyen szabályosság szerint folytatódik a számsor. Ennél sokkal nagyobb probléma azonban, hogy egyáltalán folytatható-e a végtelenig, azaz minden k-ra van-e olyan (csak k-tól függő) t darabszám, hogy bármely pozitív egész előáll t darab k-adik hatvány összegeként. (A továbbiakban is k-adik hatványon nem-negatív egészek k-adik hatványát értjük.) Ezt először Hilbert bizonyította be 1909-ben(!). A

minimális ilyen t darabszámot hagyományosan $g(k)$-val jelölik. (Mivel az előállításban 0^k is szerepelhet, ezért feltehetjük, hogy minden szám felírásában pontosan ugyanannyi a tagok száma.)

Nézzük meg, mire gondolhatott Waring. A $g(k) \geq s$ egyenlőtlenség belátásához elég egyetlenegy olyan n-et találnunk, ami nem írható fel s-nél kevesebb k-adik hatvány összegeként. A 3^k-nál kisebb egészek felírásához csak $(0^k,)\,1^k$ és 2^k használható. Ha $n = r2^k - 1 < 3^k$, akkor n legrövidebb előállításához $r-1$ darab 2^k és 2^k-1 darab 1^k szükséges. Az r legnagyobb értéke $\lfloor (3/2)^k \rfloor$, így $g(k) \geq 2^k + \lfloor (3/2)^k \rfloor - 2$. Ez $k = 2$, 3 és 4 esetén éppen a Waring által felsorolt értékeket adja. Waring tehát minden bizonnyal ezt az alsó becslést találta meg, és úgy gondolta, hogy ez a legrosszabb eset. Ez a sejtése helyesnek bizonyult, azonban $216 (= 6^3)$ és sok nagy matematikus munkája kellett ahhoz, hogy ezt (egy még mindig fennálló apró bizonytalanságtól eltekintve) bizonyítva lássuk. Utolsónak éppen a negyedik hatványok esete, azaz $g(4) = 19$ lett igazolva 1986-ban.

Az apró bizonytalanság abban áll, hogy nincs teljesen kizárva véges sok olyan k létezése (ezek mind csak nagyon nagyok lehetnek), amelyeknél a 4^k alatti egészekre a fentihez hasonló gondolatmenet adja a legrosszabb lehetőséget, azonban ez nagyon valószínűtlen.

Néhány kivételt megengedünk. Láttuk, hogy egyes (viszonylag) kis számok előállításához nagyon sok k-adik hatvány kell. Ezért érdemes vizsgálni, hogy mi az a (minimális) $G(k)$ darabszám, hogy annyi k-adik hatvány összegeként már minden *elég nagy* pozitív egész felírható. Az első részben azt igazoltuk, hogy $G(6) \geq 9$.

Bebizonyították, hogy $G(k)$ sokkal kisebb, mint $g(k)$, tehát tényleg néhány kis szám előállításához kell aránytalanul sok k-adik hatvány. Azonban (a $g(k)$-val ellentétben) $G(k)$ pontos értéke mindössze két esetben ismert: $G(2) = 4$ és $G(4) = 16$. Az első részbeli meggondolásokhoz hasonlóan kaphatók alsó becslések $G(k)$-ra, ha $k = 2^j, 3 \cdot 2^j, p^j(p-1)$ vagy $p^j(p-1)/2$, ahol $p > 2$ prímszám. Tetszőleges $k \geq 2$-re csak a $G(k) \geq k+1$ alsó becslés ismert. A bizonyítás érdekessége, hogy nem explicite ad meg végtelen sok olyan n-et, amelyekhez nem elég k darab k-adik hatvány, hanem egy ügyes leszámlálással azt igazolja, hogy a „legtöbb" szám ilyen. Az alapötlet a következő: M-ig a számok előállításához csak a $\sqrt[k]{M}$-nél nem nagyobb számok k-adik hatványai választhatók, és az ilyenekből képezhető k-tagú összegek száma (az ismétléses kombináció képlete alapján) csak kb. $\left(\sqrt[k]{M}\right)^k / k! = M/k!$, tehát M-ig legfeljebb ennyi szám írható fel k darab k-adik hatvány összegeként.

Előjeles összegek. Legyen $v(k)$ a minimális darabszám, ahány k-adik hatvány *előjeles* összegéből minden egész előáll. Ennek létezése persze következik $g(k)$ vagy $G(k)$ létezéséből, sőt $v(k) \leq G(k)+1$ is rögtön adódik (miért?), azonban $v(k)$ létezését közvetlenül is jóval könnyebben be tudjuk látni, ezt majd alább vázoljuk. Érdekes viszont, hogy $v(k)$ pontos értéke csak $k = 2$-re ismert, $v(2) = 3$, először ezt fogjuk igazolni.

Mivel $(c+1)^2 - c^2 = 2c+1$ és $(c+2)^2 - c^2 = 4(c+1)$, ezért a páratlan és a 4-gyel osztható számok előállnak $x_1^2 - x_2^2$ alakban. A kimaradó $4k+2$ alakú számok viszont nem, mert egy négyzetszám 4-es maradéka 0 vagy 1 lehet, így két négyzetszám különbségének 4-es maradéka nem lehet 2. Ha $n = 4k+2$, akkor viszont $n = 1+(4k+1) = 1+(2k+1)^2-(2k)^2$, tehát $v(k) \leq 3$. Itt egyenlőség áll, mert a $8k+6$ alakú számok nem írhatók fel (nemcsak két négyzetszám különbségeként, hanem) két négyzetszám összegeként sem.

Nézzük a köbszámokat. A négyzetszámok mintájára induljunk ki az

$$f_1(c) = (c+1)^3 - c^3 = 3c^2 + 3c + 1$$

egyenlőségből. A harmadfokú tag kiküszöböléséhez hasonlóan ezután a másodfokú tagot is ki tudjuk ejteni:

$$f_2(c) = f_1(c+1) - f_1(c) = (c+2)^3 - 2(c+1)^3 + c^3 = 6(c+1).$$

Azaz a 6 többszörösei előállnak négy köbszám előjeles összegeként. Egy tetszőleges egész pedig felírható $n = 6u + h$ alakban, ahol $|h| \leq 3$, tehát a h-t legfeljebb három $\pm 1^3$ összegeként előállítva kapjuk, hogy $v(3) \leq 7$. Ez a $6 \mid h^3 - h$ észrevétel alapján tovább javítható:

$$n = 6u + h = 6u + (h - h^3) + h^3 = 6h' + h^3,$$

és $6h'$ előáll négy köbszám előjeles összegeként, tehát $v(3) \leq 5$. Ez a jelenlegi legjobb felső becslés. Alsó becslésként $v(3) \geq 4$ adódik, ugyanis egy köbszám 9-es maradéka csak 0 és ± 1 lehet, ezért a $9q \pm 4$ alakú számok nem írhatók fel 4-nél kevesebb köbszám összegeként.

A négyzetszámoknál és köbszámoknál látott módszer általánosítható tetszőleges k-adik hatványokra. Legyen rekurzíve $f_1(c) = (c+1)^k - c^k$ és $f_j(c) = f_{j-1}(c+1) - f_{j-1}(c)$, ha $2 \leq j \leq k-1$. Ekkor teljes indukcióval adódik, hogy f_j egy $k-j$-edfokú egész együtthatós polinom, amelynek főegyütthatója $k(k-1)\dots(k-j+1)$ és amely 2^j darab k-adik hatvány előjeles összege (ezek akár explicite, képlettel is megadhatók). Így $j = k-1$ esetén $f_{k-1}(c) = k!c + d_k$, ahol d_k csak a k-tól függő konstans, továbbá f_{k-1} felírható 2^{k-1} darab k-adik hatvány előjeles összegeként. Tetszőleges n-re legyen $n - d_k = k!u + h$, ahol $|h| \leq k!/2$. Ekkor $n = (k!u + d_k) + h$, és itt $k!u + d_k = f_{k-1}(u)$ előáll 2^{k-1} darab k-adik hatvány előjeles összegeként, h pedig $k!/2$ darab 1^k és 0^k előjeles összege. Tehát minden egész szám felírható $2^{k-1} + k!/2$ darab k-adik hatvány előjeles összegeként. Ezzel beláttuk, hogy $v(k)$ valóban létezik és $v(k) \leq 2^{k-1} + k!/2$. Természetesen, mélyebb módszerek felhasználásával ennél sokkal jobb felső becslés is adható.