Megoldásvázlatok, megjegyzések

1. Előfordul-e, és ha igen, hányszor, hogy (a) 2; (b) 5; (c) 11; (d) 25 egymást követő négyzetszám összege is négyzetszám?

Megoldás: (a) Az $x^2+(x+1)^2=y^2$ egyenletet 2-vel szorozva és rendezve $(2x+1)^2-2y^2=-1$, azaz $z^2-2y^2=-1$ adódik, ahol z automatikusan páratlan, így ez az eredetivel ekvivalens. Ennél az ún. Pell-típusú egyenletnél érdemes a bal oldalt a valós számok körében szorzattá bontani: $(z-y\sqrt{2})(z+y\sqrt{2})=-1$. Azonnal látszik, hogy $z=y=1$ megoldás, azaz (*) $(1-\sqrt{2})(1+\sqrt{2})=-1$. Ha ezt pl. köbre emeljük, akkor egy újabb megoldást kapunk: $(1-\sqrt{2})^3(1+\sqrt{2})^3=(1-3\sqrt{2}+3\cdot 2-2\sqrt{2})(1+3\sqrt{2}+3\cdot 2+2\sqrt{2})=(7-5\sqrt{2})(7+5\sqrt{2})=-1$, azaz $z=7$, $y=5$, vagyis $x=3$, $y=4$ megoldás (ami persze rögtön is látszik). Az eljárást ismételve (vagy (*)-ot tetszőleges páratlan hatványra emelve) végtelen sok megoldást kapunk.

(b) Nincs megoldás: $(x-2)^2+(x-1)^2+x^2+(x+1)^2+(x+2)^2=y^2$; átalakítva $5(x^2+2)=y^2$, tehát $5\mid x^2+2$, ami nem lehet, mert egy négyzetszám nem adhat 3 maradékot 5-tel osztva.

(c) Végtelen sok megoldás: $(x-5)^2+\ldots+(x+5)^2=y^2$; átalakítva $11(x^2+10)=y^2$, ez pontosan akkor teljesül, ha $x^2+10=11t^2$, azaz $-10=x^2-11t^2=(x-t\sqrt{11})(x+t\sqrt{11})$. Megoldás $x=t=1$, azaz (**) $(1-\sqrt{11})(1+\sqrt{11})=-10$. Hatványozással nem tudunk új megoldásokat kapni, hiszen a -10 nem marad meg. Viszont az $1=x^2-11t^2=(x-t\sqrt{11})(x+t\sqrt{11})$ egyenletnek $x=10$, $t=3$ megoldása, és ebből hatványozással végtelen sok megoldást kapunk, amelyeket $(**)$-gal kombinálva az eredeti feladat végtelen sok megoldását nyerjük, pl. $-10=(-10)\cdot 1=(1-\sqrt{11})(1+\sqrt{11})(10-3\sqrt{11})(10+3\sqrt{11})=(43-13\sqrt{11})(43+13\sqrt{11})=43^2-11\cdot 13^2$, azaz $x=43$, $t=11$, ahonnan $y=11t=143$, tehát $38^2+39^2+\ldots+48^2=143^2$.

(d) Egy megoldás van: $(x-12)^2+\ldots+(x+12)^2=y^2$; átalakítva $25(x^2+52)=y^2$, ez pontosan akkor teljesül, ha $x^2+52=t^2$, azaz $52=t^2-x^2=(t-x)(t+x)$, ahonnan $t=14$, $x=12$, $y=5t=70$; $0^2+1^2+\ldots+24^2=70^2$.

Általánosítások: (A) p egymást követő négyzetszám esetén, ahol $p>3$ prím: $(x-(p-1)/2)^2+\ldots+(x+(p-1)/2)^2=y^2$; az első $(p-1)/2$ négyzetszám összegképlete alapján $p(x^2+(p^2-1)/12)=y^2$, tehát szükséges feltétel: $p\mid x^2+(p^2-1)/12$, azaz 36-tal szorozva $(6x)^2\equiv 3-3p^2\equiv 3 \pmod p$ megoldható. A Legendre-szimbólum tulajdonságai alapján $p=12k\pm 5$ esetén a kongruencia nem oldható meg, tehát ekkor p egymást követő négyzetszám összege nem lehet négyzetszám, sőt semmilyen teljes hatvány sem. Ugyanez a gondolatmenet k egymást követő négyzetszám esetén is érvényes, ha k páratlan és van $p=12k\pm 5$ alakú prímosztója, amelynek a négyzete nem osztója k-nak. A négyzetszámok mod 8 maradékait vizsgálva adódik, hogy pl. $k=8t+4$, $16t+3$ stb. esetén sincs megoldás. Hasonlóan lehet mod 9 stb. vizsgálatával kimutatni, hogy bizonyos k értékekre nincs megoldás.

(B) Az (a) feladat átfogalmazható úgy is, hogy hány olyan egész oldalú derékszögű háromszög van, amelyben a két befogó mérőszáma szomszédos. Kérdezhetjük, mi a helyzet, ha a két befogó eltérése k, de az oldalhosszak relatív prímek (ez utóbbi feltétel nélkül könnyen visszavezethetjük a $k=1$ esetre).

2. A számok hány százaléka áll elő két négyzetszám különbségeként? És hány százaléka áll elő három négyzetszám összegeként?

Megoldás: Ezt a következőképpen kell érteni: legyen $f(n)$ az $1, 2, \ldots, n$ egészek közül a megfelelők száma, ekkor a keresett arány (vagy valószínűség) a $\lim_{n\to\infty} f(n)/n$ határérték. Mivel a $k = x^2 - y^2 = (x+y)(x-y)$ diofantikus egyenlet pontosan akkor oldható meg, ha k felírható két azonos paritású osztója szorzataként, azaz ha páratlan vagy osztható 4-gyel, ezért csak a $4t+2$ alakú egészek nem állnak így elő, vagyis a keresett valószínűség $3/4 = 75\%$. A második kérdésnél fel kell használnunk Gauss nevezetes tételét, hogy pontosan a $4^r(8t+7)$ alakú számok nem állnak három négyzetszám összegeként (az, hogy ezek nem állnak elő, r szerinti teljes indukcióval egyszerűen bizonyítható, a tétel nehéz része, hogy más kivétel nincs). Vagyis rosszak a $8t+7$, $32t+28$ stb. egészek, ezek száma n-ig rendre $\lfloor (n+1)/8 \rfloor$, $\lfloor (n+4)/32 \rfloor$, és általában $\lfloor (n+4^r)/(8\cdot 4^r) \rfloor$, vagyis $(n - f(n))/n$ „kb." az $1/8 + 1/32 + \ldots + 1/(8\cdot 4^r) + \ldots$ végtelen mértani sor összege, azaz $1/6$, tehát az előállók aránya $5/6$.

3. Hány egymást követő természetes szám adható meg, amelyek (a) mindegyike felírható; (b) egyike sem írható fel két négyzetszám összegeként?

Megoldás: A két négyzetszám összegeként felírható számok is felismerhetők: pontosan azok állnak így elő, amelyek kanonikus alakjában minden $4t+3$ alakú prím páros kitevővel szerepel. Azonban enélkül is boldogulhatunk. Az első néhány egészt megnézve látjuk, hogy a rosszak a $3, 6, 7, 11, 12, 14, 15, 19, 21, 22, 23, \ldots$, és a gyerekek is könnyen megsejthetik, hogy rosszak pl. (i) a $4t+3$ alakú számok, illetve (ii) a 3 olyan többszörösei, amelyek 9-cel nem oszthatók. Ezek bizonyítása is azonnal adódik mod 4, illetve mod 3 vizsgálatával.

Rátérve (a)-ra, (i)-ből következik, hogy minden negyedik szám biztosan rossz, tehát legfeljebb 3 szomszédos szám írható fel két négyzetszám összegeként. Ennyi létezik is, pl. $8, 9, 10$. Azt sem túl nehéz igazolni, hogy ez végtelen sokszor fordul elő: az 1a feladatban látottak alapján adódik, hogy az $x^2 - 2y^2 = 1$ egyenletnek végtelen sok egész megoldása van, és így $x^2 - 1 = y^2 + y^2$, $x^2 = x^2 + 0^2$, $x^2 + 1 = x^2 + 1^2$ mindegyike két négyzetszám összege.

Ugyanakkor akárhány egymást követő egész is megadható, amelyek mindegyike rossz. Ehhez kicsit haladóbb eszközök kellenek: végtelen sok $4t+3$ alakú prímszám van (ez az euklideszi gondolattal simán kijön), a kínai maradéktétel, valamint az, hogy ha egy n szám osztható egy $4t+3$ alakú p prímszámmal, de nem osztható p^2-tel, akkor n nem írható fel két négyzetszám összegeként. Ez utóbbi abból következik, hogy ha $p \mid a^2 + b^2$, azaz $a^2 \equiv -b^2 \pmod{p}$, akkor ezt a kongruenciát $(p-1)/2 = 2t+1$-edik hatványra emelve $a^{p-1} \equiv -b^{p-1} \pmod{p}$ adódik, ami a kis Fermat-tétel miatt csak úgy lehetséges, ha $p \mid a$ és $p \mid b$, de ekkor $p^2 \mid a^2 + b^2 = n$. Legyenek most $p_1, p_2, \ldots, p_r$ tetszőleges (különböző) $4t+3$ alakú prímszámok. Ha $s+i$ osztható p_i-vel, de nem osztható p_i^2-tel, akkor $s+1, \ldots, s+r$ mindegyike rossz. Ilyen s-et pl. az $x + i \equiv p_i \pmod{p_i^2}$, $i = 1, 2, \ldots, r$ szimultán kongruenciarendszer megoldásaként kapunk. Mivel a modulusok páronként relatív prímek, így a kínai maradéktétel szerint van megoldás.

4. Átlagosan hányféleképp áll elő egy szám két négyzetszám összegeként?

Megoldás: Legyen $r(n)$ az $n = x^2 + y^2$ egyenlet $0 \le y \le x$ egész megoldásainak a száma, ekkor a $\lim_{n\to\infty}[r(1)+r(2)+\ldots+r(n)]/n$ határértéket kell kiszámítani. Itt egyáltalán nem segít, ha tudjuk $r(n)$ képletét. Az egész koordinátájú pontok négyzetrácsát érdemes nézni, itt $r(1)+\ldots+r(n)$ az $x^2+y^2 \le n$ megoldásszáma, ami (a $0 \le y \le x$ feltétel mellett) éppen egy origó körüli $\sqrt{n}$ sugarú nyolcadkör rácspontjainak a száma (az origót leszámítva). Ha minden rácspont köré egy egységnégyzetet rajzolunk, amelynek ő a középpontja, akkor ezek az egységnégyzetek nagyjából a nyolcadkört fedik le, azaz a rácspontok száma nagyjából a nyolcadkör területe, vagyis $(\sqrt{n})^2\pi/8$. Így a keresett határérték $\pi/8$, azaz átlagosan ennyiféleképpen írható fel egy pozitív egész két négyzetszám összegeként.

5. Lehet-e (a) 2; (b) 3; (c) 4 egymást követő pozitív egész szorzata négyzetszám?

Megoldás: (a) Nem lehet, hiszen $x^2 < x^2+x < (x+1)^2$. Másképp: ha $x(x+1) = y^2$, akkor $(x, x+1) = 1$ miatt $x = a^2$, $y = b^2$, de két pozitív négyzetszám különbsége nem lehet 1. (A második gondolatmenetből az is adódik, hogy $x(x+1)$ semmilyen teljes hatvány sem lehet.)

(b) Nem lehet: $y^2 = x(x-1)(x+1) = x(x^2-1)$; mivel $(x, x^2-1) = 1$, ezért külön-külön is négyzetszámok, de $x^2 - 1 \ne z^2$.

(c) Ez sem lehet: $y^2 = x(x+1)(x+2)(x+3)$; legyen $u = x(x+3)$, ekkor $y^2 = u(u+2)$. Ha u páratlan, akkor $(u, u+2) = 1$, tehát $u = a^2, u+2 = b^2$, és így $b^2 - a^2 = 2$, ami nem lehet. Ha $u = 2v$, akkor $(y/2)^2 = v(v+1)$, ami az (a) rész alapján lehetetlen.

Megjegyzés: Általában is igaz, hogy egymást követő pozitív egészek szorzata sohasem lehet teljes hatvány, ezt a hosszú ideig megoldatlan sejtést Erdős és Selfridge bizonyították be 1975-ben.

6. Adjuk meg pozitív egészek olyan végtelen sorozatát, hogy semelyik két tag (a) összege; (b) különbsége se legyen négyzetszám. Próbáljunk minél sűrűbb ilyen sorozatokat konstruálni.

Megoldás: (a) A $3t + 1$ alakú számok megfelelnek, ezek sűrűsége $1/3$. Sokáig azt hitték, hogy ez a legjobb, de kiderült, hogy a $4t + 1$ alakú számokat, valamint mod 32 a 14, 26 és 30 maradékosztályokat véve egy $11/32$ sűrűségű jó sorozatot kapunk (egy páratlan négyzetszám mod 8 maradéka 1, egy párosé mod 32 pedig 0, 4 vagy 16, és a fenti halmaz két elemét összeadva sohasem kapunk ilyen maradékot). Hosszú évek bizonytalansága után végül Szemerédi Endre igazolta, hogy ennél sűrűbb sorozat már nem létezik.

(b) Itt messze nincs meg a pontos válasz. Először nézzük, mire jutunk a mohó algoritmussal. Ez azt jelenti, hogy minden lépésben a lehető legkisebb számot vesszük hozzá az addig kiválasztottakhoz. Az $1, 2, \ldots, n$ számok közül így $a_1 = 1$, ekkor nem vehető $a_1 + 1 = 2, a_1 + 4 = 5, \ldots$, tehát $a_2 = 3$, így nem vehető $a_2 + 1 = 4, a_2 + 4 = 7, \ldots$, vagyis $a_3 = 6$ stb. Ha $a_1, \ldots, a_r$-et kiválasztottuk, akkor ezek mindegyike az $a_i + h^2$, $h \le \sqrt{n - a_i}$ számokat tiltja le, azaz összesen legfeljebb $r\sqrt{n}$ szám foglalt. Ez azt jelenti, hogy $r < \sqrt{n}$ esetén biztosan találunk újabb, n-nél kisebb szabad elemet, így n-ig mindenképpen ki tudunk választani legalább $\sqrt{n}$ elemet.

Ezt a sűrűséget sokáig csak nagyon nehéz eszközök bevetésével sikerült egy icipicit javítani, míg Ruzsa Imre meg nem találta az alábbi abszolút középiskolás konstrukciót: tekintsük azokat a számokat, amelyek 5-ös számrendszerbeli alakjában a hátulról számított páratlan helyi értékeken csak 0 vagy 2 számjegy állhat. Az n-nél kisebb ilyen számoknak kb. $\log_5 n$ számjegye van (az elején is megengedve 0-kat), ezek fele 5-féle lehet, a másik fele 2-féle, vagyis a számuk kb. $5^{(\log_5 n)/2} \cdot 2^{(\log_5 n)/2} = n^{(1/2)(1+\log_5 2)} = n^{0.71\ldots}$. Meg kell még mutatnunk, hogy ez jó sorozat. Legyen $c = c_0 + 5c_1 + 5^2c_2 + \ldots$ és $d = d_0 + 5d_1 + 5^2d_2 + \ldots$ két ilyen szám, és tegyük fel, hogy $m^2 = c - d = (c_0 - d_0) + 5(c_1 - d_1) + \ldots$ Ezt mod 5 nézve egyrészt $c - d \equiv c_0 - d_0 \equiv 0$, 2 vagy 3, másrészt egy négyzetszám 5-ös maradéka 0, 1 vagy 4. Ezért $c - d \equiv 0 \pmod 5$, tehát $5 \mid c - d = m^2$, innen $25 \mid c - d$, vagyis c és d utolsó két jegye megegyezik. Mindkét számból ezt a részt kivonva és 25-tel osztva $(c - d)/25 = (c_2 - d_2) + 5(c_3 - d_3) + \ldots = (m/5)^2$ adódik. Az előző gondolatmenetet megismételve, majd az eljárást folytatva kapjuk, hogy minden i-re $c_i = d_i$, tehát $c = d$.

7. Van-e végtelen sok olyan háromtagú számtani sorozat, amelynek az elemei relatív prím négyzetszámok?

Megoldás: Van, sőt olyan is, ahol az első tag 1: az $1 + v^2 = 2u^2$ Pell-egyenletről az 1a feladatban megmutattuk, hogy végtelen sok megoldása van. Az összes számhármast a következőképpen kaphatjuk meg: $r^2 + s^2 = 2t^2 \iff [(r + s)/2]^2 + [(r - s)/2]^2 = t^2$, amivel a feladatot a pitagoraszi számhármasokra vezettük vissza, amelyeknek jól ismert a paraméteres előállítása.

8. Mely számrendszerekben lesz az (a) 3; (b) 5; (c) 33 darab 1-esből álló szám négyzetszám?

Megoldás: (a) Nincs ilyen: $x^2 < x^2 + x + 1 < (x + 1)^2$.

(b) Itt is megpróbáljuk $f(x) = x^4 + x^3 + x^2 + x + 1$-et két négyzetszám közé beszorítani: $z^2 = (x^2 + x/2 + 3/8)^2 = f(x) - 5x/8 - 55/64 < f(x)$ és $(z + 1/8)^2 = (x^2 + x/2 + 4/8)^2 = f(x) + x^2/4 - x/2 - 3/4 > f(x)$, ha $x > 3$. Ha $f(x)$ négyzetszám, akkor egyben egy 8 nevezőjű törtnek a négyzete, viszont $x > 3$ esetén két egymást követő ilyen tört négyzete közé esik. Ezért csak $x = 2$ vagy 3 jöhet szóba, amelyek közül $x = 3$ valóban megfelel: $1+3+9+27+81 = 11^2$. (Dolgozhatunk végig egészekkel is; ehhez az egyenletet $64 = 8^2$-tel be kell szorozni.)

(c) $t^2 = 1 + x + \ldots + x^{32} = (1 + x + x^2)(1 + x^3 + x^6 + \ldots + x^{30})$. Megmutatjuk, hogy a két tényező relatív prím; ebből következik, hogy külön-külön is négyzetszámok, de 8a-ban beláttuk, hogy az első tényező nem lehet az, vagyis nincs megoldás. Tegyük fel, hogy a két tényezőnek p közös prímosztója. Ekkor $p \mid x^2 + x + 1 \mid x^3 - 1$, azaz $x^3 \equiv 1 \pmod p$, és így a második tényező 11 maradékot ad p-vel osztva, tehát csak $p = 11$ lehet. Azonban az $x^2 + x + 1 \equiv 0 \pmod{11}$ kongruencia nem oldható meg, ezt pl. a $0, 1, \ldots, 10$ értékek végigpróbálásával vagy pedig a 4-gyel való beszorzás után kapott $(2x + 1)^2 \equiv -3 \pmod{11}$ megoldhatatlanságával igazolhatjuk.

9. Adott 11 (különböző) pozitív egész, amelyek egyikének sincs 30-nál nagyobb prímosztója. Bizonyítsuk be, hogy a számok közül kiválasztható néhány (lehet, hogy csak egy, lehet, hogy az összes), amelyek szorzata négyzetszám.

Megoldás: Tekintsük a számokból képezhető $2^{11} - 1$ szorzat kanonikus alakját, ezekben a 30-nál kisebb 10 prímszám hatványai szerepelnek. A négyzetszámok szempontjából csak a kitevők paritása számít, így ezekre 2^{10} különböző lehetőség van. A skatulyaelv miatt lesz két olyan szorzat, amelyben a prímek kitevőinek paritása páronként egyforma, pl. $a_1a_2a_3$

és a_2a_4. Ezt a két szorzatot összeszorozva négyzetszámot kapunk, és ha elhagyjuk a duplán előforduló tényezőket, akkor a megmaradó csupa különböző tényező szorzata továbbra is négyzetszám marad (a példánkban ez $a_1a_2a_3a_2a_4/(a_2)^2 = a_1a_3a_4$).

Egy másik megoldás a következő. Mindegyik a_i számnak feleltessük meg a benne szereplő prímek kitevőinek 10 elemű $A_i = (k_{i,1}, \ldots, k_{i,10})$ paritásvektorát, ahol k_{ij} aszerint 0 vagy 1, hogy a_i-ben a j-edik prím kitevője páros vagy páratlan. Egy szorzat pontosan akkor négyzetszám, ha a megfelelő vektorok összege a nullvektor. Ha a vektorokat a modulo 2 test feletti 10-dimenziós vektortér elemeinek tekintjük, akkor a 11 vektor biztosan lineárisan összefüggő, azaz (mivel a skaláregyütthatók csak 0 és 1 lehetnek) néhány vektor összege a nullvektor.

Megjegyzés: A második bizonyítás fölösleges nagyágyúnak tűnik, azonban jelentős előnye, hogy a kérdést egy homogén lineáris egyenletrendszer megoldására visszavezetve gyors algoritmust ad megfelelő szorzat megtalálására, míg az első bizonyítás csak azt adja, hogy a rengeteg eset végigpróbálásával biztosan célhoz érünk. A feladat (10/11 helyett nagyobb számokra) fontos szerepet játszik (viszonylag hatékony) prímfelbontási algoritmusok konstruálásában. A probléma magasabb kitevőjű hatványokra történő általánosítása csak részben megoldott és másfajta matematikai eszközöket igényel. (Mindezekről részletesebben lásd pl. a Freud Lineáris algebra könyv 9.3 pontját.)

10. Milyen n-ekre igaz, hogy n darab alkalmas (nem feltétlenül egybevágó) négyzetből, mindegyiket felhasználva, hézagtalanul kirakható egy (nagyobb) négyzet? És mi a helyzet a térben, ha ugyanezt kockákra kérdezzük?

Megoldás: Érdemesebb fordítva okoskodni, hogy egy nagy négyzetet hány kis négyzetre vághatunk szét. Ha k részre ez megoldható, akkor az egyik négyzetet négyfelé vágva $k+3$-ra is kapunk egy jó felbontást, így $n = 1, 4, 7, \ldots$ biztosan elérhető. Ha a négyzetet t^2 egybevágó kis négyzetre vágjuk, és $(t-1)^2$ kis négyzetet egyesítünk egy (közepes) négyzetté, akkor az eredeti négyzetünk $t^2 - (t-1)^2 + 1 = 2t$ négyzet egyesítése, azaz $n = 6, 8, 10, \ldots$ is jó. Ezeket 3-mal növelve kapjuk, hogy minden $n \neq 2, 3, 5$ megfelel. A 2 és a 3 nyilván nem jó, mert az eredeti négyzet mind a 4 sarkába kell egy négyzet, és könnyen belátható az is, hogy az 5 sem jó.

Rátérve a kockákra, itt minden él felezésével azt kapjuk, hogy ha k jó, akkor $k+7$ is, a harmadolással pedig azt, hogy $k+26$ is. Így biztosan jó minden $n = 1 + 7r + 26s$ alakú szám, ahol r és s nemnegatív egészek. Mivel $(7, 26) = 1$, ezért $0 \cdot 26, 1 \cdot 26, 2 \cdot 26, \ldots, 6 \cdot 26$ mind különböző maradékot adnak 7-tel osztva, így $n-1 \geq 6 \cdot 26 - 6 = 150$ esetén n biztosan előáll ilyen alakban. A fenti módszer persze finomítható, például ha az élek harmadolása után keletkező 27 kis kockából 8-at összeragasztunk, akkor 26 helyett 19 a növekedés, vagy az élnegyedelés után a 64 kis kockából 27-et egyesítve 37 a növekmény stb. Ilyen trükkökkel megmutatható, hogy minden $n > 47$ megfelel, azonban megoldatlan, hogy pl. 47-re mi a helyzet.

Megjegyzés: Ha $a_1, \ldots, a_k$ pozitív, relatív prím egészek, akkor az $a_1x_1 + \ldots + a_kx_k = n$ diofantikus egyenletnek minden, az a_i-ktől függően elég nagy n esetén létezik $x_i \geq 0$ megoldása, azonban $k > 2$-re nem ismert a küszöbértékre általános használható képlet. Ezt az ún. Frobenius-problémát sokat és intenzíven vizsgálták (köztük Erdős is), a témáról Kiss Géza írt feladatokat is tartalmazó nagyon jó áttekintő cikket (Teaching Mathematics and Computer Science 1/2 (2003), 203–218).