A tavalyi pontverseny utolsó feladatai között a májusi számunkban tűztük ki a **B. 3822.** és az **A. 376.** feladatokat. Mindkettő egy számhármasokon definiált különös eljárásra vonatkozott. Ebben a cikkben a feladatok hátterét szeretném bemutatni. Remélem, kiderül, hogy a feladatokban megadott eljárás nagyon is eleven kapcsolatban van a számelmélet egy gazdag fejezetével, a másodfokú diofantikus egyenletek elméletével.

B. 3822. *Az $(a;b;c)$ számhármassal egy lépésben a következőt lehet tenni: tetszőlegesen felcserélhetjük a számokat, vagy lecserélhetjük az $(a;b;2a+2b-c)$ számhármasra. El lehet-e jutni ilyen lépésekkel a $(2;5;13)$ számhármasból az $(1;3;8)$ számhármasba?*

A továbbiakban az $(a;b;c) \rightsquigarrow (x;y;z)$ jelölést használjuk arra, hogy a fenti lépésekkel az $(a;b;c)$ számhármasból el lehet jutni az $(x;y;z)$ számhármasba. Természetesen $(a;b;c) \rightsquigarrow (a;b;c)$, továbbá ha $(a_1;b_1;c_1) \rightsquigarrow (a_2;b_2;c_2)$ és $(a_2;b_2;c_2) \rightsquigarrow (a_3;b_3;c_3)$, akkor $(a_1;b_1;c_1) \rightsquigarrow (a_3;b_3;c_3)$. Vegyük észre, hogy

$$\big(a;b;2a+2b-(2a+2b-c)\big) = (a;b;c);$$

a számok felcserélését és ezen második műveletet is el lehet végezni „visszafelé”. Így ha $(a_1;b_1;c_1) \rightsquigarrow (a_2;b_2;c_2)$, akkor $(a_2;b_2;c_2) \rightsquigarrow (a_1;b_1;c_1)$. A $\rightsquigarrow$ ekvivalenciareláció; ekvivalenciaosztályokra bontja a számhármasokat, a feladat pedig azt kérdezi, hogy az $(1;3;8)$ és a $(2;5;13)$ számhármasok azonos ekvivalenciaosztályokban vannak-e. Az **A. 376.** feladat ugyanezt a kérdést teszi fel az $(1;21;42)$ és $(5;13;42)$ számhármasokról.

Néhány észrevétel

A továbbiakban *invariánsokat* keresünk: olyan jellemzőket, amelyek egy lépés során nem változnak meg. Ha egy ilyen invariáns „értéke” két számhármasra különböző, akkor az egyikből nem lehet eljutni a másikba, különböző ekvivalenciaosztályban vannak. Triviális példa a számhármasok tagjainak egész volta: egy lépés során egészekből álló számhármasból csak egészekből álló számhármast kaphatunk, így például az $(1;2;3)$-ból nem juthatunk el az $\left(\frac{1}{2};\sqrt{2};\pi\right)$ vagy az $\left(\frac{1}{2};1;1\right)$ számhármasba. Ez az invariáns azonban egyik feladatot sem oldja meg, túl gyenge. Ígéretesebbnek tűnhet a számhármas elemeinek a legnagyobb közös osztója. (Gondoljuk meg, hogy – ha eltekintünk az előjelektől – akkor ez valóban invariáns.) A kitűzött feladatokban sajnos ez a legnagyobb közös osztó minden esetben 1, tehát ez az invariáns sem segít. Annyit azért érdemes megjegyeznünk, hogy mivel az adott lépések, illetve a számhármasok tagjainak egy adott egésszel való szorzása felcserélhető, $(a_1;b_1;c_1) \rightsquigarrow (a_2;b_2;c_2)$ akkor és csak akkor teljesül, ha $(ka_1;kb_1;kc_1) \rightsquigarrow (ka_2;kb_2;kc_2)$. Így – ha kényelmes – föltehető, hogy számhármasaink legnagyobb közös osztójaÍ1. Most viszont mutatunk egy ravaszabb invariánst.

I. megoldás a B. 3822. feladatra. Tekintsük az $a+b$, $a+c$, $b+c$ számokat és legyen $f\big((a;b;c)\big)$ az ezen számok közül a hárommal oszthatók száma. Ha felcseréljük a számokat, akkor f értéke természetesen nem változik. Megmutatjuk, hogy a második művelet esetén sem változik!

$f\big((a;b;2a+2b-c)\big)$ az $a+b$, $3a+2b-c$, $2a+3b-c$ számok közül a 3-mal oszthatók száma, de $3 \mid (3a+2b-c)$ pontosan akkor, ha $3 \mid b+c$, hiszen

$$3a+2b-c \equiv -(b+c) \pmod 3.$$

Tehát f értéke nem változik a lépések során, ugyanakkor $f\big((1;3;8)\big)=1$, míg $f\big((2;5;13)\big)=2$, hiszen az első esetben csak $3 \mid 1+8$ teljesül, míg a második esetben $3 \mid 2+13$ és $3 \mid 5+13$.

A két számhármas tehát különböző ekvivalenciaosztályban van, így a $(2;5;13)$ számhármasból nem lehet eljutni az $(1;3;8)$ számhármasba.

Ez az invariáns sajnos nem oldja meg az **A. 376.** feladatot: $f\big((1;21;42)\big) = f\big((5;13;42)\big) = 1$. Mivel $f\big((1;3;8)\big)=1$, az sem derül ki, hogy $(1;21;42) \rightsquigarrow (1;3;8)$ vagy $(5;13;42) \rightsquigarrow (1;3;8)$ teljesül-e. A következő invariáns segítségével viszont sikerül majd „szétválasztanunk” a **B.** feladat számhármasait az **A.** feladat számhármasaitól.

II. megoldás a B. 3822. feladatra. Tekintsük a következő kifejezést:

$$n(a;b;c) = a^2+b^2+c^2-2ab-2bc-2ca = (a-b)^2 - c(2a+2b-c).$$

Az első alakból látszik, hogy $n(a;b;c)$ invariáns a számok felcserélésére; a másodikból pedig az, hogy a második műveletre is. Mivel $n(2;5;13) = -4$ és $n(1;3;8) = 4$, azért a $(2;5;13)$ számhármasból nem juthatunk el az $(1;3;8)$ számhármasba. Üröm az örömben, hogy az **A. 376.** feladatot még mindig nem sikerült megoldanunk: $n(1;21;42) = n(5;13;42) = 316$. Annyi mindenesetre kiderült, hogy a **B.** feladat számhármasaiból az **A.** feladat egyik számhármasába sem lehet eljutni.

A számhármasok normája

Alakítsuk át a fenti $n(a;b;c)$ kifejezést!

$$n(a;b;c) = a^2 + b^2 + c^2 - 2ab - 2bc - 2ca \equiv$$
$$\equiv a^2 + b^2 + c^2 + 2ab + 2bc + 2ca = (a+b+c)^2 \pmod 4.$$

Tehát $4 \mid n(a;b;c)$ pontosan akkor, ha $2 \mid a+b+c$. Ebben az esetben

$$N(a;b;c) = \frac{1}{4}n(a;b;c) = \frac{1}{4}(a^2 + b^2 + c^2 - 2ab - 2bc - 2ca) = \left(\frac{a+b-c}{2}\right)^2 - ab.$$

Ez azt jelenti, hogy ha $2 \mid a+b+c$, akkor $ab + N(a;b;c)$ négyzetszám. Így például ha $(1;3;8) \rightsquigarrow (a;b;c)$, akkor $ab + N(a;b;c) = ab + N(1;3;8) = ab+1$ négyzetszám (és a szimmetria miatt persze $bc+1$ és $ca+1$ is négyzetszámok). Hasonlóan, ha $(2;5;13) \rightsquigarrow (x;y;z)$, akkor $xy + N(x;y;z) = xy + N(2;5;13) = xy - 1$ (valamint $yx-1$ és $zx-1$) négyzetszám.

Ha $2 \mid a+b+c$, akkor hívjuk az $N(a;b;c)$ mennyiséget az $(a;b;c)$ számhármas *normájának.* Vegyük észre, hogy $2 \mid a+b+c$ invariáns, egy – páros összegű számhármasokból álló – ekvivalenciaosztályon belül tehát nyugodtan beszélhetünk $N(a;b;c)$-ről. Ha például igaz volna a megfordítás, tehát hogy egyenlő normájú számhármasok ekvivalensek is, akkor ebből igenlő válasz következne az **A. 376.** feladatra. A továbbiakban $n(a;b;c)$-vel számolunk majd, de eredményeinket $N(a;b;c)$-re fogalmazzuk meg: így elegánsabb formába írhatók.

Szükségünk lesz arra, hogy c-t kifejezzük a, b, $N(a;b;c)$ segítségével. Nyilván

$$c = a + b \pm 2\sqrt{ab + N(a;b;c)}.$$

A korábbiak szerint a fenti kifejezésben négyzetszám áll a gyökjel alatt. Mint látható, egy számhármas két tagja a normával együtt sem határozza meg egyértelműen a harmadik elemet: két lehetőség adódik.

A következő önmagában is érdekes lemma olyan számhármasokról szól, amelyek normája nulla. Ilyen persze a $(0;0;0)$, amivel nem sokra megyünk, a legegyszerűbb nem triviális példa a $(0;1;1)$.

1. lemma. *$(0;1;1)$-ből csak $\left(x^2;y^2;(x+y)^2\right)$ alakú számhármasokba juthatunk el.*

Bizonyítás. Látszólag kitüntetett szerepe van a harmadik koordinátának, valójában $(x+y)^2 = \left(-(x+y)\right)^2$, így azt is írhatjuk, hogy $(0;1;1)$-ből csak az $(u^2;v^2;w^2)$ alakú számhármasokba lehet eljutni, ahol $u+v+w=0$. Az nyilvánvaló, hogy két elem cseréje nem változtatja meg az alak jellegét, nincs kitüntetett szerepe a harmadik koordinátának.

Mivel $2x^2 + 2y^2 - (x+y)^2 = (x-y)^2$, így a második lépést végrehajtva az $\left(x^2;(-y)^2;(x-y)^2\right)$ számhármast kapjuk, ami láthatóan a kívánt alakú. Mivel a kezdeti $(0;1;1) = (0^2;1^2;1^2)$ is ilyen, azért minden lépés után az $\left(x^2;y^2;(x+y)^2\right)$ alakú számhármasok körében maradunk. $\square$

A látottak szerint nyugodtan végrehajthatjuk az $(a;b;c) \to (a;2a+2c-b;c)$ és az $(a;b;c) \to (2b+2c-a;b;c)$ lépéseket is, hiszen ezek összerakhatók két cseréből és egy második fajta műveletből. A harmadik koordinátának tehát nincsen semmilyen kitüntetett szerepe.

Vegyük észre azt is, hogy transzformációink lineárisak, azaz ha $(a;b;c) = (a_1;b_1;c_1) + (a_2;b_2;c_2)$ akkor

$$(a;b;2a+2b-c) = (a_1;b_1;2a_1+2b_1-c_1) + (a_2;b_2;2a_2+2b_2-c_2),$$

ahol koordinátánként adunk össze. Ugyanígy végezhetjük „tagonként” a koordináták felcserélését is, ügyelve arra, hogy ugyanazokat a cseréket hajtsuk végre a felbontásban szereplő számhármasokban.

Aratás

Tegyünk egy kitérőt és nézzük meg, hogy klasszikus számelméleti eredmények hogyan fogalmazhatók meg ebben a megközelítésben. Egy híres probléma, a két négyzet összegeként felírható számok jellemzésének kulcsa az alábbi

1. tétel. *n^2+1 alakú szám minden pozitív osztója felírható két négyzetszám összegeként.*

Bizonyítás. Ha $u \mid n^2+1$, akkor van olyan v pozitív egész, hogy $uv = n^2+1$. A döntő észrevétel az, hogy mostani jelöléseinkkel ez az egyenlőség azt jelenti, hogy

$$N(u;v;u+v+2n) = -1.$$

Vizsgáljuk meg tehát az $N(a;b;c) = -1$ feltételt kielégítő számhármasokat! Az alábbi lemma azt mondja ki, hogy a -1 értékű norma lényegében egyetlen ekvivalenciaosztályt azonosít.

2. lemma. *Ha $a > 0$ és $N(a;b;c) = -1$, akkor $(a;b;c) \rightsquigarrow (1;1;2)$, tehát ezek a számhármasok az $(1;1;2)$ ekvivalenciaosztályát alkotják.*

Ilyen például a **B.** feladat $(2;5;13)$ számhármasa és valóban: ha mindig a legnagyobb számot cseréljük ki, akkor két lépésben: $(2;5;\mathbf{13}) \to (2;\mathbf{5};1) \to (2;1;1)$.

A 2. lemma bizonyítása. Ha $N(a;b;c) = -1$, akkor $ab = \left(\frac{a+b-c}{2}\right)^2 + 1 > 0$, vagyis a, b, c egyszerre pozitív vagy negatív. A feltétel szerint $a > 0$, így mindhárom szám pozitív. Megmutatjuk, hogy $(a;b;c) \rightsquigarrow (1;1;2)$. Azt állítjuk, hogy ha a példához hasonlóan minden lépésben a legnagyobb számot cseréljük ki, akkor $a+b+c$ értéke nem nő és csak akkor nem csökken, ha az $(1;1;2)$ egy permutációjával van dolgunk. Mivel számaink pozitívak, az összegük is az; ha pedig ez az összeg lépésenként csökken, előbb-utóbb valóban el kell jutnunk az $(1;1;2)$ számhármashoz.

Az általánosság megszorítása nélkül föltehető, hogy $a \le b \le c$. A fentiek szerint ekkor c-t cseréljük ki $2a+2b-c$-re és azt kell bizonyítanunk, hogy $a+b+c \ge 3a+3b-c$, vagyis $c \ge a+b$.

Ha $ab = 1$, azaz $a = b = 1$, akkor $c = a+b \pm 2\sqrt{ab-1} = a+b = 2$, készen vagyunk. Megmutatjuk, hogy ha $ab > 1$ (és $a \le b$), akkor a c-re adódó két érték kisebbike, $a+b-2\sqrt{ab-1} < b$. Így csak $c = a+b+2\sqrt{ab-1}$ lehetséges, tehát $c > a+b$, amit bizonyítani akartunk.

Állításunk ekvivalens az $a < 2\sqrt{ab-1}$, azaz a négyzetre emeléssel kapott $a^2 < 4ab-4 = ab+(3ab-4)$ egyenlőtlenséggel. Feltevésünk szerint $a^2 \le ab$, továbbá $ab > 1$ miatt $3ab-4 > 0$. Innen pedig már leolvasható a bizonyítandó egyenlőtlenség. □

Ezzel bebizonyítottuk, hogy $N(a;b;c) = -1$, $a > 0$ esetén $(a;b;c) \rightsquigarrow (1;1;2)$. A bizonyításból az is látszik, hogy ha $N(a;b;c) = -1$ és $a < 0$, akkor $(a;b;c) \rightsquigarrow (-1;-1;-2)$.

Térjünk most vissza az 1. tétel bizonyításához. Láttuk, hogy $N(u;v;u+v+2n) = -1$ és így a 2. lemma szerint $(u;v;u+v+2n) \rightsquigarrow (1;1;2)$. Ekkor $(1;1;2) \rightsquigarrow (u;v;u+v+2n)$. Vegyük észre, hogy $(1;1;2)$ két nulla normájú számhármas összegére bontható: $(1;1;2) = (1;0;1) + (0;1;1)$. Az 1. lemma szerint ezekből csak négyzetszámokat tartalmazó számhármasokba juthatunk el, így az $(1;1;2) \rightsquigarrow (u;v;u+v+2n)$ út lépéseit a tagokra végrehajtva az

$$(u;v;u+v+2n) = \left(x_1^2; y_1^2; (x_1+y_1)^2\right) + \left(x_2^2; y_2^2; (x_2+y_2)^2\right)$$

előállítást kapjuk, ahonnan $u = x_1^2 + x_2^2$, és ezt akartuk bizonyítani. □

A 2. lemma algoritmusa elő is állít egy ilyen felbontást. Ha az $(u;v;u+v+2n) \rightsquigarrow (1;1;2) = (1;0;1) + (0;1;1)$ út lépéseit fordított sorrendben hajtjuk végre az $(1;0;1)$ és a $(0;1;1)$ tagokból indulva, akkor megkapjuk az u (és persze a másik két koordináta) felbontását két négyzetszám összegére.

Példa. $34 \mid 13^2+1$, ugyanis $34 \cdot 5 = 13^2+1$. A megfelelő $(u;v;u+v+2n)$ számhármas $(34;5;34+5+2\cdot 13) = (34;5;65)$. Ekkor

$$\begin{array}{ccccccccccc}
(34; & 5; & \underline{65}) & = & (9; & 1; & 16) & + & (25; & 4; & 49) \\
 & & \downarrow & & & & \uparrow & & & & \uparrow \\
(\underline{34}; & 5; & 13) & = & (9; & 1; & 4) & + & (25; & 4; & 9) \\
\downarrow & & & & \uparrow & & & & \uparrow & & \\
(2; & 5; & \underline{13}) & = & (1; & 1; & 4) & + & (1; & 4; & 9) \\
 & & \downarrow & & & & \uparrow & & & & \uparrow \\
(2; & \underline{5}; & 1) & = & (1; & 1; & 0) & + & (1; & 4; & 1) \\
 & \downarrow & & & & \uparrow & & & & \uparrow & \\
(2; & 1; & 1) & = & (1; & 1; & 0) & + & (1; & 0; & 1).
\end{array}$$

Feladatok. (a) Bizonyítsuk be, hogy egy n^2+2 alakú szám minden osztója a^2+2b^2 alakú. (Segítség: $(1;2;3) = (1;0;1) + 2(0;1;1)$.)

(b) Bizonyítsuk be, hogy $k \mid n^2+5$ esetén k vagy $2k$ a^2+5b^2 alakú. (Segítség: Ekkor két osztály van. $(a;b;c) \rightsquigarrow (1;5;6)$ vagy $(?;?;?)$.)

(c) Legyen $(a;b;c) = 1$ és $N(a;b;c) = 0$. Bizonyítsuk be, hogy ekkor $(a;b;c) \rightsquigarrow (0;1;1)$ vagy $(a;b;c) \rightsquigarrow (0;-1;-1)$.

I. megjegyzés. $65 = 8^2+1^2 = 7^2+4^2$. Hogy melyik felbontást találjuk meg, az $65 \mid n^2+1$ esetén n-től függ: $n = 8$ esetén az elsőt, $n = 18$ esetén pedig a másodikat.

II. megjegyzés. Tételünk egyszerű következményeként adódik az a látszólag erősebb állítás is, hogy ha $(a;b) = 1$, akkor a^2+b^2 minden osztója előáll két négyzetszám összegeként. Két „standard” összefüggésből ugyanis nyomban adódik, hogy ha $(a;b) = 1$, akkor a^2+b^2-nek van n^2+1 alakú többszöröse. Ismeretes, hogy ha $(a;b) = 1$, akkor léteznek olyan s, t egészek, amelyekre $1 = as - bt$. Az *Euler–Lagrange azonosság* szerint ekkor

$$\left(a^2+b^2\right)\left(s^2+t^2\right) = (at+bs)^2 + (as-bt)^2 = (at+bs)^2 + 1.$$

Számhármasok szétbontása

Most a számhármasok szétbontásán alapuló ötletünket fejlesszük tovább: legyen $(a;b;c)=(a_1;b_1;c_1)+(a_2;b_2;c_2)$. Ekkor

$$a^2=a_1^2-(a-a_1)^2+2a(a-a_1)=a_1^2-a_2^2+2aa_2,$$

$$ab=a_1b_1-(a-a_1)(b-b_1)+a(b-b_1)+b(a-a_1)=a_1b_1-a_2b_2+ab_2+ba_2.$$

Tehát

$$(*)\qquad n(a;b;c)=a^2+b^2+c^2-2ab-2bc-2ca=n(a_1;b_1;c_1)-n(a_2;b_2;c_2)-$$
$$-2a(b_2+c_2-a_2)-2b(a_2+c_2-b_2)-2c(a_2+b_2-c_2).$$

Most ezt a kicsit furcsa, de igen hasznos azonosságunkat fogjuk felhasználni a következő tétel bizonyításában.

2. tétel. *Tegyük fel, hogy $2\mid a+b+c$ és $(a;b;c)\rightsquigarrow(A;B;C)$. Ekkor léteznek u,v egészek, hogy $aA=u^2-N(a;b;c)v^2$.*

Bizonyítás. A bizonyítás a következő felbontáson alapul:

$$\begin{array}{cccc} (a;b;c) & =(a;b-1;c-1)+ & & (0;1;1) \\ \wr & \wr & & \wr \\ (A;B;C)= & (A';B';C') & + & \big(x^2;y^2;(x+y)^2\big). \end{array}$$

Ekkor $n(A;B;C)=n(a;b;c)$, illetve a definíció szerint

$$n(A';B';C')=n(a;b-1;c-1)=(b-c)^2-a\big(2(b-1)+2(c-1)-a\big)=$$
$$=n(a;b;c)+4a.$$

Fennáll továbbá, hogy $n\big(x^2;y^2;(x+y)^2\big)=n(0;1;1)=0$.

Alkalmazzuk a $(*)$ azonosságot az $(A;B;C)=(A';B';C')+\big(x^2;y^2;(x+y)^2\big)$ felbontásra:

$$n(A;B;C)=n(A';B';C')-n\big(x^2;y^2;(x+y)^2\big)-2A\big((x+y)^2+y^2-x^2\big)-$$
$$-2B\big((x+y)^2+y^2-x^2\big)-2C\big(x^2+y^2-(x+y)^2\big).$$

Tehát $n(a;b;c)=n(a;b;c)+4a-2A(2y^2+2xy)-2B(2x^2+2xy)-2C(-2xy)$, vagyis $4\big(Ay^2+(A+B-C)xy+Bx^2-a\big)=0$. Ez y-ra nézve másodfokú egyenlet, amelynek létezik egész megoldása, így a diszkriminánsa négyzetszám:

$$D=(A+B-C)^2x^2-4A(Bx^2-a)=n(A;B;C)x^2+4Aa.$$

Mivel $n(A;B;C)=4N(A;B;C)$, azért $4s^2=D=4\big(N(A;B;C)x^2+Aa\big)$, azaz $Aa=s^2-N(A;B;C)x^2=s^2-N(a;b;c)x^2$.

Ezzel bebizonyítottuk az állítást. $\square$

Végkifejlet

Ha $(1;21;42)\rightsquigarrow(5;13;42)$, akkor a 2. tétel szerint léteznek x, y egészek, hogy $x^2-79y^2=1\cdot5=5$. Megmutatható, hogy ennek a diofantikus egyenletnek nincs x, y egész megoldása és ezzel végre választ kaphatunk az **A. 376.** feladat kérdésére: az $(1;21;42)$ számhármasból nem lehet eljutni az $(5;13;42)$ számhármasba. Ennek részletesebb tárgyalásába nem megyünk bele, később úgy is látunk egy invariánst, amely végleg elintézi ezt a problémát.

Min múlik, hogy az $x^2-79y^2=5$ diofantikus egyenletnek nincs megoldása? Az egyenletet y^2-tel osztva kapjuk, hogy $\dfrac{x^2}{y^2}=79+\dfrac{5}{y^2}\approx79$, vagyis $\dfrac{x}{y}\approx\sqrt{79}$. Az $\dfrac{x}{y}$ racionális szám tehát nagyon jó „hatásfokú", a nevező méretéhez képest kicsiny hibájú közelítése a $\sqrt{79}$ számnak.

Ilyen közelítések sorozata hatékony eljárásokkal állítható elő és ez a sorozat adott szám – mint esetünkben a $\sqrt{79}$ – esetén lényegében egyértelműen meghatározott. A fenti egyenlet megoldása pedig tagja kell legyen ennek a $\sqrt{79}$-hez tartozó sorozatnak. Ennek persze végtelen sok eleme van, de ismeretes, hogy ha az $\dfrac{u}{v}$ elemekhez kiszámoljuk az u^2-79v^2 értékeket, akkor az így előálló számok halmaza már *véges!* Ha pedig ellenőrizzük ezeket az értékeket, kiderül, hogy az 5 nincs közöttük!

A most vázolt eszközök vezetnek el egy az itt leírtaknál finomabb invariánshoz. Erről szól majd a cikk folytatása …