Bevezetés

Mindannyian tudjuk, hogy két négyzetszám szorzata maga is négyzetszám; ez a szorzás asszociativitásából és kommutativitásából következik. Két pozitív négyzetszám összege azonban nem mindig négyzetszám (és semmiképpen sem a két tag összegének a négyzete!). Pitagorasz tétele nyomán már több, mint kétezer éve ráterelődött a figyelem a két négyzetszám összegeként írható négyzetszámokra. A pitagoraszi számhármasok jellemzése a görög aritmetika egyik látványos eredménye. Jóval később, a XVII. században *Fermat*, aki szisztematikusan vizsgálta ezeket a mennyiségeket, kiderítette, hogy az x^2+y^2 alakú számok sok tekintetben hasonlítanak a négyzetszámokhoz: az utóbbiak prímtényezős felbontásában minden prímszám kitevője páros, ahhoz pedig, hogy egy számot föl lehessen írni két négyzet összegeként, csak a $4k+3$ alakú prímtényezőik kitevőinek kell párosnak lennie. Például a $810 = 2 \cdot 3^4 \cdot 5$ és a $45 = 3^2 \cdot 5$ ilyen számok: prímfelbontásukban a 3 páros kitevőn szerepel (2 és 5 nem $4k+3$ alakú prím). Valóban: $810 = 9^2 + 27^2$ és $45 = 3^2 + 6^2$.

A szerkezeti rokonság viszont hasonló aritmetikai viselkedésben mutatkozik meg: ha összeszorozzuk ezt a két számot, akkor a szorzatban is páros lesz az egyetlen $4k+3$ alakú prímtényező, a 3 kitevője, így az is felírható két négyzetszám összegeként; valóban, némi próbálkozás után[1]

$$810 \cdot 45 = 36\,450 = 189^2 + 27^2.$$

Ez nyilván ugyanígy igaz általában is. Magát a jelenséget úgy szokás fogalmazni, hogy az x^2+y^2 alakú számok halmaza *zárt* a szorzásra nézve.

Négyzetszámok persze el is oszthatók egymással: ha a hányados egész, akkor az maga is négyzetszám. Ebből egyébként az a közismert tény is következik, hogy nem négyzetszámok, például a 2 négyzetgyöke irracionális szám. A prímfelbontás segítségével történő jellemzésből kiderül, hogy a két négyzet összegeként felírható számoknak is megvan ez a tulajdonsága: ha a hányadosuk egész, akkor mivel az osztás megtartja a $4k+3$ alakú prímtényezők kitevőjének a páros voltát, maga is két négyzet összege. A fenti példa számaira $\dfrac{810}{45} = 2 \cdot 3^2 = 3^2 + 3^2$. Az, hogy a szorzatra vonatkozó eredmény simán adódott a Lagrange-azonosságból, arra bátoríthat, hogy most a fordított irányban is kísérletezzünk aritmetikai bizonyítással; így talán, a szorzatéhoz hasonlóan, megkaphatjuk a hányados felbontását is. Ez most az $\dfrac{a^2+b^2}{u^2+v^2} = x^2 + y^2$ átrendezésből adódó

$$a^2 + b^2 = (u^2 + v^2)(x^2 + y^2) = (ux \pm vy)^2 + (vx \mp uy)^2$$

egyenlet, illetve az innen kapott

$$a = ux + vyb = vx - uy\} \qquad\qquad a = ux - vyb = vx + uy\}$$

egyenletrendszerek vizsgátatát jelenti; legalább az egyik esetben egész $(x,\ y)$ értéket kellene kapnunk. A példában $(a = 9,\ b = 27,\ u = 3,\ v = 6)$ sajnos ez nem teljesül. Az első esetben $x = \dfrac{21}{5}$, $y = -\dfrac{3}{5}$, a másodikban pedig az ettől nem sokban különböző $x = \dfrac{21}{5}$, $y = \dfrac{3}{5}$ megoldást kapjuk. Az így nyert felbontásban az egész hányados nem egészek négyzetösszege, ahogy várnánk, pedig tudjuk, hogy létezik ilyen fenbontás is:

$$\frac{9^2 + 27^2}{3^2 + 6^2} = \left(\frac{21}{5}\right)^2 + \left(\frac{3}{5}\right)^2.$$

Ebben a pillanatban meg kell tehát elégednünk az egzisztenciatétel állításával: a felbontás egészek négyzetösszegére létezik.

A probléma egy lehetséges általánosításaként megfogalmazhatunk hasonló kérdéseket az $x^2 + d \cdot y^2$ alakú számok körében is, ahol a d adott egész szám. A Lagrange-azonosság kiterjesztése

$$(u^2 + d \cdot v^2) \cdot (x^2 + d \cdot y^2) = (ux \pm d \cdot vy)^2 + d \cdot (uy \mp vx)^2$$

most is azonnal adja – anélkül, hogy az $x^2 + d \cdot y^2$ alakú számok prímtényezős felbontásának jellemzésével kellene vesződnünk –, hogy az ilyen alakú számok halmaza is zárt a szorzásra nézve. Az eddigiek alapján a hányadosra vonatkozó megfelelő állítás vizsgálata egyáltalán nem látszik könnyűnek; a $d = 0$, illetve 1 esetekben az adott alakú számok prímtényezős felbontásának jellemzéséből kaptuk meg a választ.

⋆

[1] A két négyzetszám összegeként felírható számok aritmetikájában alapvető szerepe van az ún. Lagrange-azonosság idevonatkozó speciális esetének:

$$(u^2 + v^2)(x^2 + y^2) = (ux + vy)^2 + (vx - uy)^2 = (ux - vy)^2 + (vx + uy)^2.$$

Ezzel a négyzetszámok összegeként felírható számok szorzatára vonatkozó állítás aritmetikai magyarázatát kapjuk, az azonosság ténylegesen előállítja a szorzatot két négyzetszám összegeként.

Csörnyei Marianna, a University College of London ösztöndíjas kutatója ezt a cikket még a Fazekas M. Fővárosi Gyakorló Gimnázium másodikos diákjaként írta egy órán fölvetett kérdés megválaszolásaként. A cikkben megfigyelhető, hogy a kétfajta megközelítés, az aritmetikai és a szerkezeti, hogyan működik együtt és vezet el a probléma megoldásához.

JSP

⋆

A cikkben azt fogjuk megvizsgálni, hogy a $d = 1$-en kívül még milyen pozitív, 1-nél nagyobb d-kre teljesül, hogy ha két $x^2 + dy^2$ alakú szám hányadosa egész, akkor a hányados is ilyen alakú.

Könnyen belátható, hogy a d nem lehet 1-nél nagyobb négyzetszám. Ugyanis $d = d_1^2$ esetén $\dfrac{d_1^2 + d \cdot 1^2}{d_1^2 + d \cdot 0^2} = 2$, és ez $d \geq 4$ esetén nem írható fel $x^2 + dy^2$ alakba. Tehát az állításunk biztosan nem fog minden d-re teljesülni.

Mielőtt továbbmennénk, bizonyítsuk be az alábbi tételt:

1. Tétel. *Ha két $x^2 + dy^2$ alakú szám hányadosa egész, és az osztó prím, akkor a hányados is $x^2 + dy^2$ alakú.*[**0]

Bizonyítás. Két $x^2 + dy^2$ alakú szám szorzata is ilyen alakú:

$$(*) \qquad (x^2 + dy^2)(z^2 + dv^2) = (xz \pm dyv)^2 + d(xv \mp yz)^2.$$

Vizsgáljuk most az $\dfrac{a^2 + db^2}{x^2 + dy^2}$ törtet, ahol $x^2 + dy^2$ prím, és $x^2 + dy^2 \mid a^2 + db^2$. A $(*)$ azonosság alapján elég azt megmutatni, hogy a és b felírható

$$a = xz \pm dyv (1) b = xv \mp yz (2)$$

alakba, ahol z és v egész (mert ekkor a hányados $z^2 + dv^2$ lesz). Az (1) és (2) egyenletekből kifejezve v-t:

$$v = \pm \frac{ay \pm bx}{x^2 + dy^2},$$

így ahhoz, hogy a v egész legyen, arra van szükség, hogy

$$x^2 + dy^2 \mid ay + bx \qquad \text{vagy} \qquad x^2 + dy^2 \mid ay - bx$$

teljesüljön. Mivel az $x^2 + dy^2$ prím, azért ehhez elég az

$$x^2 + dy^2 \mid (ay + bx)(ay - bx)$$

oszthatóságot megmutatnunk:

$$(ay + bx)(ay - bx) = a^2y^2 - b^2x^2 = a^2y^2 + db^2y^2 - db^2y^2 - b^2x^2 == (a^2 + db^2)y^2 - (x^2 + dy^2)b^2.$$

Mivel $x^2 + dy^2 \mid a^2 + db^2$, azért így valóban

$$x^2 + dy^2 \mid (ay + bx)(ay - bx),$$

tehát a két eset $(\pm)$ közül az egyikben a v egész lesz. Az (1) és (2) egyenletekből könnyen látható, hogy a z racionális. Azt is tudjuk, hogy a $z^2 + dv^2$ egész, így ha a v egész, akkor a z is biztosan egész.

A $d = 2$ eset

Be fogjuk bizonyítani, hogy $d = 2$ esetén az állításunk igaz, tehát ha két $x^2 + 2y^2$ alakú szám hányadosa egész, akkor a hányados is ilyen alakú.

Legyenek a Q halmaz elemei azok a p prímek, amelyekre $p \mid x^2 + 2y^2$-ből következik, hogy $p \mid x$ és $p \mid y$, és legyenek a P_1 halmaz elemei azok a prímek, amelyek felírhatók $x^2 + 2y^2$ alakba. Bebizonyítjuk, hogy ekkor minden prím eleme P_1-nek vagy Q-nak. A prímeknek ez a felbontása nyilván közös elem nélküli, hiszen $p = x^2 + 2y^2$ esetén $0 < |x| < p$ és $0 < |y| < p$, tehát p nem oszthatja x-et és y-t. Magát az állítást teljes indukcióval fogjuk bizonyítani.

Az állítás $p = 2$ esetén igaz, mivel $2 = 0^2 + 2 \cdot 1^2$, tehát $2 \in P_1$. Legyen a $p > 2$ prím, és tegyük fel, hogy az összes p-nél kisebb prímről már bebizonyítottuk, hogy eleme P_1-nek vagy Q-nak. Tegyük fel, hogy $p \notin Q$, és bizonyítsuk be, hogy ekkor $p \in P_1$.

Mivel $p \notin Q$, azért létezik olyan x és y, amelyre $p \mid x^2 + 2y^2$ és $p \not| y$. Szorozzuk meg az x-et és az y-t egy olyan k számmal, hogy $yk \equiv 1 \pmod{p}$ legyen. Nyilván $p \mid (xk)^2 + 2(yk)^2$, és mivel $yk \equiv 1 \pmod{p}$, így $p \mid (xk)^2 + 2 \cdot 1^2$. Biztos, hogy létezik olyan x_1, amelyre $x_1 \equiv xk \pmod{p}$ és $|x_1| \leq \dfrac{p-1}{2}$. Így $p \mid x_1^2 + 2 \cdot 1^2$, ahol

$$x_1^2 + 2 \cdot 1^2 \leq \left(\frac{p-1}{2}\right)^2 < p^2.$$

[0] A tételt feladatként tűztük ki a KöMaL 2000/7. számában. A feladat száma helyesen: **B. 3400.**

Tehát találtunk egy olyan $x^2 + 2y^2$ alakú számot, amely osztható p-vel és kisebb p^2-nél. Így a prímtényezős felbontásában szerepel egy p tényező, és ezen kívül csak p-nél kisebb prímtényezői vannak, amelyekre teljesül az indukciós feltevésünk. Ha vannak Q-beli prímosztói, akkor osszuk el ezekkel az x-et és az y-t. Így egy olyan $x^2 + 2y^2$ alakú számot kapunk, amely osztható p-vel, és ezen kívül csak P_1-beli, azaz $x^2 + 2y^2$ alakú prímosztói vannak. Ezekkel az 1. Tétel alapján sorra leoszthatunk, végül p marad, és ezt a p-t $x^2 + 2y^2$ alakban fogjuk megkapni. Így valóban $p \in P_1$.

Ezzel bebizonyítottuk, hogy minden prím eleme P_1-nek vagy Q-nak. Most vizsgáljuk az

$$\frac{x^2 + 2y^2}{z^2 + 2v^2}$$

törtet. Ha a $(z^2 + 2v^2)$-nek van Q-beli prímosztója, akkor azzal eloszthatjuk az x, y, z, v számokat. Így egy olyan

$$\frac{x_1^2 + 2y_1^2}{z_1^2 + 2v_1^2}$$

törtet kapunk, ahol a $z_1^2 + 2v_1^2$ csupa P_1-beli, azaz $x^2 + 2y^2$ alakú prím szorzata. Az 1. Tétel alapján ezekkel lehet egyszerűsíteni, így velük sorra egyszerűsítve végül egy $x^2 + 2y^2$ alakú számot fogunk kapni.

Ezzel az állításunkat $d = 2$-re bebizonyítottuk.

Megjegyzés. Hasonlóan bizonyíthatunk $d = 1$ esetén is. Legyenek most a Q halmaz elemei azon p prímek, amelyekre $p \mid x^2 + y^2$-ből következik, hogy $p \mid x$, $p \mid y$, és legyenek a P_1 halmaz elemei az $x^2 + y^2$ alakú prímek. A fentiekhez hasonlóan bizonyíthatjuk, hogy minden prímszám eleme P_1-nek vagy Q-nak, majd hogy ha két $x^2 + y^2$ alakú szám hányadosa egész, akkor az is $x^2 + y^2$ alakú.

A bizonyítás alapján azt is könnyen megmondhatjuk, hogy mely számok írhatóak fel $x^2 + y^2$ alakba: azok és csak azok a számok, amelyek prímfelbontásában a Q-beli prímek páros kitevőn szerepelnek. A Q-beli prímek pedig azok, amelyekre a -1 négyzetes nemmaradék modulo p, vagyis a $4k + 3$ alakú prímek.

Így egy elemi és nem túl bonyolult bizonyítást kaptunk arra, hogy azok és csak azok a számok írhatóak fel két négyzetszám összegeként, amelyek prímtényezős felbontásában a $4k + 3$ alakú prímek páros kitevőn szerepelnek.

Ha ugyanezt kérdezzük a most vizsgált számokról, akkor a $d = 1$ esethez hasonlóan itt is annyit mondhatunk, hogy azok a számok írhatók x^2+2y^2 alakba, amelyek prímtényezős felbontásában a Q-beli prímek páros kitevőn szerepelnek. A Q-beli prímek: 5, 7, 13, 23, 29, 31, ... szerkezete azonban egyáltalán nem olyan egyszerű, mint a $d = 1$ esetben.

Csörnyei Marianna