

Az úgynevezett pitagoraszai számhármások (azaz olyan a , b , c egész számok, amelyekre $a^2 + b^2 = c^2$ igaz) vizsgálatánál kiderül, hogy mely négyzetszámok állnak elő két négyzetszám összegeként. Megkérdezhető azonban általában is, hogy melyek azok a természetes számok, amelyek felírhatók két négyzetszám összegeként.

Míg a pitagoraszai számhármások vizsgálata egészen elemi oszthatósági tételekkel elvégezhető, itt mélyebb ismeretekre is szükségünk van. Egyelőre – ameddig lehet – csak egészen egyszerű módszerekkel dolgozunk. A későbbiekben is csupán kimondjuk majd azokat a tételeket, amelyeket felhasználunk.

Vizsgáljuk a természetes számoknak azt a $\mathbf{C}$ halmazát, amelynek elemei a két négyzetszám összegeként előállítható számok. Mivel $0 (= 0^2)$ maga is négyzetszám, ezért $\mathbf{C}$ tartalmazza az összes négyzetszámot, és így a 0 -t is.

1. Tétel: $\mathbf{C}$ zárt a szorzásra.

Bizonyítás: Tekintsük $\mathbf{C}$ két elemét: legyenek ezek $a^2 + b^2$ és $c^2 + d^2$. Ezek szorzata

$$(a^2 + b^2) \cdot (c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2,$$

amivel állításunkat bizonyítottuk. (Megjegyezzük, hogy másféle előállítás is lehetséges.)

Mindenekelőtt nézzük meg, nem tartozik-e minden szám e halmazhoz. Azonnal látható, hogy nem. Például 3 sem állítható elő két négyzetszám összegeként. Ennél sokkal többet bizonyíthatunk:

2. Tétel: $4k + 3$ alakú szám nincs $\mathbf{C}$ -ben

Bizonyítás: Feltétel szerint $\mathbf{C}$ minden x eleme $a^2 + b^2$ alakú. Ismeretes, hogy páros szám négyzete osztható 4 -gyel és páratlan szám négyzete 4 -gyel (sőt 8 -cal) osztva 1 -et ad maradékul. Eszerint, ha a és b párosok, akkor $x = a^2 + b^2$ is az (sőt 4 -gyel osztható); ha egyikük páros, másikuk páratlan, akkor x 4 -gyel osztva 1 -et ad maradékul; amennyiben mindkettő páratlan, akkor x ismét páros. A megadott $\mathbf{C}$ -beli x szám tehát soha nem lehet $4k + 3$ alakú.

Ahhoz, hogy megállapítsuk, mely számok tartoznak $\mathbf{C}$ -hez, azt kell megnéznünk, hogy ezek a számok milyen szorzatként épülnek fel. Elképzelhető volna, hogy $\mathbf{C}$ -beli számok minden tényezője is $\mathbf{C}$ -beli. Azonnal látható, hogy ez nem igaz. Hiszen $3 \cdot 3 = 9 \in \mathbf{C}$, míg 3 nincs $\mathbf{C}$ -ben. Ez egy sokkal általánosabb „rossz lehetőséget” mutat: Ha u osztója a és b mindegyikének, akkor osztója $(a^2 + b^2)$ -nek is, noha u -ról semmit sem tudunk. Csak akkor remélhetjük, hogy az $a^2 + b^2$ valamely u osztója is $\mathbf{C}$ -beli, ha u -nak a és b egyikével sincs közös osztója.

3. Tétel: Ha az $a^2 + b^2$ valamely u osztója a és b mindegyikéhez relatív prím, akkor $u \in \mathbf{C}$.

Bizonyítás: Mindenekelőtt megjegyezzük, hogy ezt elegendő prímszámokra bizonyítani. Egyrészt egy a -hoz és b -hez relatív prím osztó bármely osztója is relatív prím a -hoz és b -hez. Másrészt, ha a tételt bebizonyítjuk az u minden prímosztójára, akkor ezek szorzata is $\mathbf{C}$ -beli, az első tétel következtében.

Feltétel szerint létezik olyan v pozitív egész szám, amelyre $a^2 + b^2 = v \cdot u$. Tekintsük az olyan v pozitív egészeket, amelyekre $v \cdot u = a'^2 + b'^2$, valamilyen a' és b' egész számokkal. Tegyük fel, hogy úgy választottuk meg a v -t, hogy az a lehető legkisebb legyen. Azt fogjuk belátni, hogy ekkor v biztosan 1 , ami éppen u -nak a kívánt alakban való előállítását adja.

Osszuk el a' -t is és b' -t is u -val; mégpedig ne úgy, hogy a legkisebb pozitív maradékot kapjuk, hanem úgy, hogy a legkisebb abszolút értékű maradék adódjék. (Ha például 8 -at osztjuk 5 -tel, akkor ne azt a felírást vegyük, hogy $8 = 1 \cdot 5 + 3$, hanem azt, hogy $8 = 2 \cdot 5 + (-2)$.) Legyen $a' = r \cdot u + c$ és $b' = s \cdot u + d$, ahol c és d megfelelően a legkisebb abszolút értékű maradék. Ez azt jelenti, hogy $|c|, |d| \leq u/2$. Ebből azt kapjuk, hogy

$$\begin{aligned} c^2 + d^2 &= (a' - r \cdot u)^2 + (b' - s \cdot u)^2 = \\ &= a'^2 + b'^2 - u \cdot (2a'r - r^2u + 2b's - s^2u). \end{aligned}$$

Itt – feltétel szerint – az első tag is osztható u -val, ezért $c^2 + d^2$ is többszöröse u -nak, mondjuk w -szerese. Mivel $|c|, |d| \leq u/2$, ezért $c^2 + d^2 \leq 2 \cdot (u/2)^2 = u^2/2$.

$c^2 + d^2$ helyébe $w \cdot u$ -t írva $w \cdot u \leq u \cdot u/2$, azaz $w \leq u/2$ adódik. Ebből $w < u$ következik, mert u pozitív egész.

Mivel az u prímszám sem a' -nek sem b' -nek nem osztója, ezért nem osztója $c = (a' - ru)$ -nak és $d = (b' - su)$ -nak sem; így v minimalitása folytán $v < u$ is igaz.

Tegyük fel, hogy $v > 1$, és végezzük most el az előbbi eljárást u helyett v -vel. Legyen tehát

$$a' = p \cdot v + f, \quad b' = q \cdot v + g, \quad |f|, |g| \leq v/2.$$

Az előbbihez hasonlóan most azt kapjuk, hogy $f^2 + g^2 = y \cdot v$, ahol $y < v$.

Mivel u prím és $v < u$, ezért u nem osztója v -nek. Ebből az is következik, hogy v nem lehet osztója a' és b' mindegyikének; ellenkező esetben ugyanis $(a'/v)^2 + (b'/v)^2$ is osztható volna u -val, ami a $v \neq 1$ esetben ellentmond a választott $a'^2 + b'^2$ felírás minimalitásának. Ezért nem lehet f és g mindegyike 0 , vagyis y is pozitív.

Legyen

$$(1) \quad i = a'f + b'g \quad \text{és} \quad j = a'g - b'f.$$

Ekkor

$$i = a'(a' - pv) + b'(b' - qv) = u \cdot v - (a'p + b'q)v;$$

$$\text{és } j = a'(b' - qv) - b'(a' - pv) = (b'p - a'q)v.$$

Eszerint i és j mindegyike osztható v -vel, és ezért

$$(2) \quad (i/v)^2 + (j/v)^2 = (i^2 + j^2)/v^2$$

egész szám. A (2) alatti összeget (1) felhasználásával átírjuk:

$$(i^2 + j^2)/v^2 = ((a'f + b'g)^2 + (a'g - b'f)^2)/v^2 =$$

$$= ((a'^2 + b'^2)(f^2 + g^2))/v^2 = (v \cdot u) \cdot (y \cdot v)/v^2 = y \cdot u.$$

Mivel $y < u$ és u prím, ezért i/v és j/v egyike sem lehet u -val osztható. Eszerint $y \cdot u$ is két olyan négyzet összege volna, amelyek egyike sem osztható u -val. Ez pedig $0 < y < v$ és v minimalitása miatt nem lehet, tehát csak $v = 1$ lehetséges, mint ahogy bizonyítani akartuk.

Nézzük most a $\mathbf{C}$ egy $a^2 + b^2$ elemét. Legyen a és b legnagyobb közös osztója e . Mint ismeretes, ekkor $a = ce$ és $b = de$, ahol c és d relatív prímek. Az $a^2 + b^2$ összeg e^2 és $c^2 + d^2$ szorzata, és természetesen e tényezőik mindegyike $\mathbf{C}$ -beli. Mivel $\mathbf{C}$ zárt a szorzásra és tartalmazza a négyzetszámokat, ezért elég $\mathbf{C}$ -nek azokat a $c^2 + d^2$ alakú elemeit megvizsgálni, amelyekben c és d relatív prímek. Ezeknek minden u prímosztója olyan, hogy c és d egyikének sem osztója, hiszen egyébként mindkettőnek osztója volna, ami ellentmond annak, hogy e számok relatív prímek. A harmadik tétel szerint e számok maguk is $\mathbf{C}$ -beliek. Ezzel a következőt láttuk be:

4. Tétel: *Ha egy szám felírható két négyzetszám összegeként, akkor ez úgy bontható fel prímszámok hatványainak a szorzatára, hogy minden olyan prímszám, amely páratlan kitevőn szerepel, maga is két négyzetszám összegeként írható fel. Ezért a páratlan kitevőn szereplő prímszámok nem lehetnek $4k + 3$ alakúak.*

Kérdés, hogy a nem $4k + 3$ alakú prímek felírhatóak-e két négyzetszám összegeként? Ha a prím páros ($p = 2$), akkor ilyen felírás triviálisan létezik: $2 = 1 + 1$.

Nehezebb annak a belátása, hogy a $4k + 1$ alakú prímekre létezik ilyen felírás. A – talán legegyszerűbb – bizonyításhoz fel kell használni az úgynevezett Wilson tételt, amely így szól:

Ha p prímszám, és az 1-től $(p - 1)$ -ig terjedő számok szorzatához 1-et adunk, akkor p -vel osztható számot kapunk.

Legyen $q = (p - 1)/2$, és írjuk fel a fenti szorzat tényezőit a következőképpen:

$$1, 2, \dots, q - 1, q, p - q, p - (q - 1), \dots, p - 2, p - 1.$$

A „ q ” utáni számokat kéttagú összegeknek tekintjük, amelyek első tagja p . A szorzást ennek megfelelően elvégezve, lesznek olyan tagok, amelyekben p fellép tényezőként, ezeket összeadva egy $p \cdot N$ alakú számot kapunk. Egyetlen olyan szorzat lesz, amely kimaradt, ez az

$$1 \cdot 2 \cdot \dots \cdot q \cdot (-q) \cdot \dots \cdot (-2) \cdot (-1)$$

szorzat. Legyen most $Q = 1 \cdot 2 \cdot \dots \cdot q$, ekkor a Wilson tétel szerint $(-1)^q \cdot Q^2 + 1$ osztható p -vel. Ha most $p = 4k + 1$ alakú, akkor $q = 2k$, azaz $(-1)^q = +1$. Eszerint $Q^2 + 1$ osztható p -vel. $1 = 1^2$ miatt ez két négyzet összege. Mivel p nem osztója 1-nek, ezért alkalmazhatjuk a harmadik tételt, amiből következik, hogy p maga is két négyzet összege. Végeredményben tehát beláttuk a következőt:

Tétel: *Egy természetes szám pontosan akkor áll elő két négyzetszám összegeként, ha prímtényezői felbontásában $4k + 3$ alakú prímszám csak páros kitevőn szerepel.*