Tudjuk, hogy minden $4k+1$ alakú prímszám felbontható két négyzetszám összegére. Most – geometriai módszerekkel – bebizonyítjuk, hogy ez a felbontás lényegében egyértelmű. A bizonyítás során először azt igazoljuk, hogy ha egy $p = 4k + 1$ alakú természetes szám kétféleképpen is felbontható két négyzetszám összegére, akkor található olyan „ferde helyzetű" téglalap, amelynek mind a négy csúcsa rácspont, és átlója $\sqrt{p}$; majd megmutatjuk, hogy ezen téglalap segítségével fel tudjuk írni az eredeti p számnak két valódi osztóját. Ez nem lehetséges, így a felbontás valóban egyértelmű.

Legyen tehát $p = 4k + 1 = a^2 + b^2 = c^2 + d^2$, és a, b, c, d páronként különböző pozitív egészek.

Látható, hogy a és b, illetve c és d egyike páros, másika páratlan, feltehető, hogy

(1) $$a \text{ és } c \text{ páros} b \text{ és } d \text{ páratlan.}$$

Vegyük a síkot az egységoldalú négyzetráccsal; az origóból mind a $P_1(a, b)$, mind a $P_2(c, d)$ pontba mutató vektor hossza $\sqrt{p}$.

Ekkor az OP_1P_2 háromszög csúcsai rácspontok, (1) miatt a P_1P_2 szakasz F felezőpontja, $\left(\frac{a+c}{2}, \frac{b+d}{2}\right)$ is rácspont, és mivel az OP_1P_2 háromszög egyenlőszárú, ezért $OF \perp P_1P_2$. Tehát az OP_1F háromszög derékszögű, így azt átfogójának felezőpontjára tükrözve téglalapot kapunk, melynek mind a négy csúcsa rácspont, és átlója $\sqrt{p}$ hosszúságú.

Ismeretes, hogy ha egy négyzetrácsban két rácspontot összekötünk, akkor az így kapott szakasz egyik végpontjában rá merőlegest húzva, a vele azonos hosszúságú szakasz másik végpontja is rácspont. Ebből következik, hogy ha két, közös végpontú szakasz mindegyikének mindkét végpontja rácspont és egymásra merőlegesek, akkor mindkét szakasz hossza egész számszorosa a közös végponttól számított első rácspont és a közös végpont távolságának. Ha ez a távolság f, akkor a két említett szakasz, OF és FP_1 hossza kf, illetve hf (k és h pozitív egészek). Ekkor a Pitagorasz-tétel miatt

$$\sqrt{p} = \sqrt{(hf)^2 + (kf)^2}.$$

azaz $p = (hf)^2 + (kf)^2 = (h^2 + k^2)f^2$. Mivel f rácspontokat összekötő szakasz, f^2 biztosan egész; mivel h és k egészek, azért $h^2 + k^2$ is egész; így $p = (h^2 + k^2)f^2$ szerint p-t két pozitív egész szám szorzatára bontottuk. Ezek csak akkor nem valódi osztók, ha $h^2 + k^2 = 1$, vagy ha $f^2 = 1$. f egy egész befogójú derékszögű háromszög átfogója, így értéke legalább $\sqrt{2}$, ezért $f^2 > 1$. $h^2 + k^2 = 1$ pedig csak úgy lehetséges, ha h és k valamelyike 0, ekkor azonban a két szakasz valamelyike 0 hosszúságú volna. Így p-t a két különböző felbontás felhasználásával két 1-nél nagyobb egész szám szorzatára bontottuk, tehát p nem lehet prímszám.

Szabó István
programtervező matematikus

Irodalom: *Erdős Pál–Surányi János:* Válogatott fejezetek a számelméletből (2. kiadás), Polygon Könyvtár, JATE Bolyai Intézet, Szeged, 1996.