A számelmélet egyik klasszikus eredménye, hogy minden $4k+1$ alakú prím felírható két négyzetszám összegeként. Fermat tisztázta először, hogy általában milyen számokra létezik ilyen felbontás, és a megoldás igazán nehéz része éppen az, hogy a $4k+1$ alakú prímeknek megvan ez a tulajdonsága. Az eltelt 350 évben számos bizonyítás született erre a tételre, kettő például megtalálható *Erdős–Surányi:* Válogatott fejezetek a számelméletből (Polygon Könyvtár – Szeged, 1996) című könyvében.

Az alábbi, valóban meghökkentő bizonyítás még nincs 10 éves, 1990-ben közölte *Don Zagier* amerikai matematikus. A bizonyítás meglehetősen szokatlan környezetbe helyezi az állítást, sokáig nem világos, miért kerül sor az egyes lépésekre, majd a végkifejletben valóban drámai gyorsasággal fény derül a bizonyítás alapeszméjére, és minden a helyére kerül.

Legyen tehát $p = 4k+1$ prím, és tekintsük a következő halmazt:

$$S = \{(x,\ y,\ z) \in \mathbf{N}^3 :\ x^2 + 4yz = p\}.$$

Az S nyilván véges halmaz, egy felület bizonyos egész koordinátájú pontjai alkotják.

A bizonyítás célja annak igazolása, hogy az S halmaz elemszáma *páratlan*; az állítás ebből már következik. Aki akar, töprenghet azon, hogy miért, miközben az S halmaz vizsgálatát követi.

Az első mély észrevétel az, hogy az S halmazt két sík, egyenletük $x = y - z$ és $x = 2y$, három részre osztja. Ez a felbontás valahogy jobban mutatja az S szerkezetét. Ezek a részek:

$$S_1 = \{(x,\ y,\ z) \in S :\ x < y - z\} S_2 = \{(x,\ y,\ z) \in S :\ y - z < x < 2y\} S_3 = \{(x,\ y,\ z) \in S :\ 2y < x\}$$

Ahhoz, hogy valóban az S felbontást kapjuk, szükséges, hogy a síkok ne tartalmazzanak S-beli pontot. Ha $x = y - z$, akkor $p = (y+z)^2$, ha pedig $x = 2y$, akkor $p = 4y(y+z)$ következik, de egyik eset sem lehetséges, hiszen a p prímszám. Az *1. táblázatban* látható az S_1, S_2, S_3 felbontás, ha $p = 41$.

S_1	S_2	S_3
(1, 5, 2)	(1, 1, 10)	(5, 2, 2)
(1, 10, 1)	(1, 2, 5)	(3, 1, 8)
(3, 8, 1)	(3, 2, 4)	(5, 1, 4)
	(3, 4, 2)	
	(5, 4, 1)	

1. táblázat

Ami a példán látszik, általában is igaz: S_1 és S_3 elemszáma egyenlő, S_2 elemszáma pedig páratlan. Ennek igazolásához Zagier egy leképezést ad meg az S halmazon az alábbiak szerint:

$f : S_1 \to S_3 \qquad (x,\ y,\ z) \mapsto (x + 2z,\ z,\ y - x - z) S_2 \to S_2 \qquad (x,\ y,\ z) \mapsto (2y - x,\ y,\ x - y + z) S_3 \to S_1 \qquad (x,\ y,\ z) \mapsto (x - 2$

Könnyű ellenőrizni – ha maga a leképezés már megvan –, hogy az S_1-en és az S_3-on definiált részek kölcsönösen egyértelműek és egymás inverzei, az S_2-n definiált rész pedig ugyancsak kölcsönösen egyértelmű, és egyenlő önmaga inverzével. Így f az S_1-et S_3-ra, az S_3-at S_1-re, az S_2-t pedig önmagára képezi le kölcsönösen egyértelműen.

A *2. táblázatban* ez a leképezés látható a $p = 41$ esetben.

S_1	S_3	S_2
(1, 5, 2)	(5, 2, 2)	(1, 1, 10)
(1, 10, 1)	(3, 1, 8)	(1, 2, 5)
(3, 8, 1)	(5, 1, 4)	(3, 2, 4)
		(3, 4, 2)
		(5, 4, 1)

2. táblázat

Az f tehát fölcseréli az S_1 és S_3 elemeit, S_2-t pedig fixen tartja. S_1 és S_3 ezért egyenlő elemszámú, így ahhoz, hogy S-ben páratlan sok elem legyen, S_2-nek kell páratlan elemszámúnak lennie. Ez csak úgy lehetséges, ha az f által létesített párosításban van – mégpedig páratlan sok – egyenlő elemű pár. A *2. táblázatban* ez az (1, 1, 10)–(1, 1, 10), amelyre tehát $f(1,\ 1,\ 10) = (1,\ 1,\ 10)$; az f leképezés *fixpontja*. Vizsgáljuk ezért általában f fixpontjait. Ilyet csak S_2-ben találhatunk, hiszen f fölcseréli S_1 és S_3 elemeit.

Mivel S_2-ben $f(x,\ y,\ z) = (2y - x,\ y,\ x - y + z)$ alakú, $f(x,\ y,\ z) = (x,\ y,\ z)$ pontosan akkor teljesül, ha $x = y$. Az S halmaz pontjain ez a megszorítás azt jelenti, hogy

$$x^2 + 4xz = p,$$

azaz $x(x + 4z) = p$. Innen $x = 1$ – hiszen a p prím – és ezért $z = \dfrac{p-1}{4}$, ami most egész szám, hiszen a $p \quad 4k+1$ alakú. Az f leképezésnek tehát *egyetlen fixpontja* van, az $\left(1,\ 1,\ \dfrac{p-1}{4}\right)$, ebből pedig következik, hogy az S halmaznak páratlan sok eleme van, hiszen f e pont kivételével párokba rendezi az S elemeit.

Nem valószínű, hogy aki eddig követte ezt a lényegében analitikus–kombinatorikus geometriai gondolatmenetet, közelebb érzi a bizonyítandó állítást. Pedig az most már karnyújtásnyira van.

Tekintsük ugyanis ezután a következő, sokkal egyszerűbb leképezést: $g : S \to S$, $g(x,\ y,\ z) = (x,\ z,\ y)$.

A g tehát fölcseréli az S-beli elemek második két koordinátáját. Mivel az S erre a transzformációra szimmetrikus, a g is kölcsönösen egyértelműen képezi le az S halmazt önmagára, és egyenlő a saját inverzével. Mivel pedig S-nek páratlan sok eleme van, a g által létesített párok sem állhatnak valamennyien különböző elemekből,

a g leképezésnek is van fixpontja.

Van tehát olyan S-beli s elem, amelyre $g(s) = s$, azaz

$$(x,\ z,\ y) = (x,\ y,\ z),$$

az s ezért $(x,\ y,\ y)$ alakú.

Minden összeér, hiszen az S definíciója szerint erre az elemre

$$x^2 + 4y^2 = p,$$

éppen az $x^2 + (2y)^2$ alakú felbontás. A *2. táblázatban* ez az S_3-beli $(5,\ 2,\ 2)$, és így kapjuk az $5^2 + 4^2 = 41$ alakot.

A bizonyítás itt véget ér, az Olvasó pedig elmélkedhet a gondolatmenet erején és eleganciáján, de a részleteken is.

A fenti bizonyítás nem konstruktív, nem ad módszert arra, hogy miképpen bontható föl egy prímszám. Látszólag többet is kiad: a fentiekből egészen pontosan annyi következik, hogy a g-nek páratlan sok fixpontja van, azaz a p előállításainak száma páratlan.

Pataki János

Felhasznált irodalom: *Martin Aigner–Günter M. Ziegler:* Proofs from THE BOOK, Springer Verlag.

A következőkben egy bizonyítást közlünk arra, hogy ez az előállítás egyértelmű.