

Nevezzük jó számnak azokat a számokat, amelyek előállnak $a^2 + 2b^2$ alakban úgy, hogy a és b relatív prímekek és $a, b \geq 0$. Legyen a p prímszám osztója egy jó számnak, és legyen $n = a^2 + 2b^2$ a legkisebb jó szám, amelynek osztója p . Ekkor $n = p \cdot t$ valamely t egészre. Erről a t -ről kell belátnunk, hogy az értéke 1.

Először csak annyit mutatunk meg, hogy $n < p^2$, (azaz $t < p$). Ha $a > \frac{p}{2}$, akkor $|a - p| < a$ és $n_0 = |a - p|^2 + 2b^2$ is osztható p -vel, de kisebb n -nél. Legyen $d = (|a - p|, b)$; ekkor p nem lehet osztója d -nek, hiszen akkor osztója volna b -nek is, $(a - p)$ -nek is, tehát a -nak is, vagyis a és b nem volna relatív prím. Ha viszont p nem osztója d -nek, akkor d^2 -nek sem, így p osztója volna az $\left(\frac{|a - p|}{d}\right)^2 + 2\left(\frac{b}{d}\right)^2 = \frac{n_0}{d^2} < n$ jó számnak is, ami ellentmondana n minimális voltának; tehát $a \leq \frac{p}{2}$. Ugyanígy látható be, hogy $b \leq \frac{p}{2}$, így $n = a^2 + 2b^2 \leq \frac{p^2}{4} + 2\frac{p^2}{4} < p^2$, ahogyan állítottuk.

Tegyük fel ezek után, hogy $t > 1$. Ebből a feltevésből fogunk ellentmondásra jutni. Legyen q egy prímosztója t -nek. Nem oszthatja q a b számot, mert akkor b^2 -nek és $a^2 + 2b^2$ -nek is osztója lévén, osztója lenne a^2 -nek is, prím volta miatt ezért a -nak is. Ez ellentmondana annak, hogy a és b relatív prímekek. Ha viszont q nem osztója b -nek, akkor van olyan $-\frac{q}{2}$ és $\frac{q}{2}$ közötti x szám, amelyre $a - bx$ osztható q -val, tehát $\frac{a - bx}{q}$ egész szám. Megmutatjuk, hogy $x^2 + 2$ is osztható q -val. Nyilván osztható q -val $-(a - bx)(a + bx) + a^2 + 2b^2 = b^2(x^2 + 2)$. Mivel q nem osztója b^2 -nek és prím, ezért osztója az $(x^2 + 2)$ kifejezésnek. Így $ax + 2b$ is osztható q -val, mivel $(a - bx)x + b(x^2 + 2) = ax + 2b$; tehát $(ax + 2b)/q$ is egész szám.

Jelöljük A -val $\frac{|ax + 2b|}{q}$ -t és legyen $B = \frac{|a - bx|}{q}$. Tekintsük az

$$m = A^2 + 2B^2 = \left(\frac{ax + 2b}{q}\right)^2 + 2\left(\frac{a - bx}{q}\right)^2 = \frac{(a^2 + 2b^2)(x^2 + 2)}{q^2} = n \frac{x^2 + 2}{q^2}$$

számot. E szám kisebb n -nél, hiszen $|x| \leq \frac{q}{2}$, ezért $x^2 + 2 \leq \left(\frac{q}{2}\right)^2 + 2 \leq 2$; ($q \geq 2$). Az m nyilván osztható p -vel, hiszen n osztható p -vel, q^2 pedig nem, mivel $q \leq t < p$. Legyen d az A és B legnagyobb közös osztója; ekkor

$$\frac{m}{d^2} = \left(\frac{A}{d}\right)^2 + 2\left(\frac{B}{d}\right)^2 = n \cdot \frac{x^2 + 2}{q^2 d^2}$$

az m -nél (s így n -nél is) kisebb jó szám. Ha osztható p -vel, akkor ellentmondásra jutunk n minimális voltaival. De m osztható p -vel, így $\frac{m}{d^2}$ csak akkor nem lehetne osztható p -vel, ha d^2 , s így d is osztható volna p -vel. Ha viszont d osztható volna p -vel, akkor $d \geq p$, s így $d^2 \geq p^2$ lenne, másrészt $d^2 \leq m < n$, amiből az következne, hogy $n > p^2$. Ez viszont ellentmond a korábban bizonyított $n < p^2$ egyenlőtlenségnek. Mindenképpen ellentmondásra jutottunk tehát a $t > 1$ feltevessel (t -t osztó q prímszám létezésével), így a feladat állítását bebizonyítottuk.

Megjegyzések. 1. A feladat állítása ugyanígy bizonyítható az $a^2 + b^2$ alakú számokra és *majdnem* ugyanígy az $a^2 + 3b^2$ alakú számokra (az $a \leq \frac{p}{2}$, $b \leq \frac{p}{2}$ becslések $p \neq 2$ esetén az $a \leq \frac{p-1}{2}$, $b \leq \frac{p-1}{2}$ becslésekkel helyettesítendőek, de csak a páratlan prímosztókra. Az $a^2 + 4b^2$ alakú számokra már egy helyen módosítani kell a bizonyítást, s most is csak a páratlan prímosztókra igaz az állítás. Az $a^2 + 5b^2$ alakú számokra már csak az igaz, s ez bizonyítható is a fenti módszerrel, hogy minden páratlan prímosztójuk vagy annak kétszerese ugyanilyen alakú. (Igy pl. $1^2 + 5 \cdot 3^2 = 46 = 2 \cdot 23$, de 23 nem áll elő $a^2 + 5b^2$ alakban.)

2. Ha bevezetjük az $a + b\sqrt{2} \cdot i$, alakú „ P -egészeket”, ahol a, b egész, és i a képzetes egység, akkor megmutatható, hogy ezek között is értelmezhető az oszthatóság, elvégezhető a maradékos osztás úgy, hogy a maradék abszolút értéke kisebb legyen az osztóénál, s így e számkörben is egyértelmű a számok prímtényező felbontása (természetesen a P -egészek körében vett prímszámokra).

Végül belátható, hogy minden szám, amely prím a P -egészek között, a konjugáltjával szorozva valódi prímet ad.

Feladatunk állítása – a P -egészek eme tulajdonságainak felhasználásával – a következőképpen igazolható: Bontsuk prímtényezőire az $a + b\sqrt{2} \cdot i$ számot:

$$a + b\sqrt{2} \cdot i = \pi_1 \dots \pi_r,$$

ahol mindegyik π_i P -prím. Ekkor

$$\overline{a + b\sqrt{2} \cdot i} = \bar{\pi}_1 \cdot \bar{\pi}_2 \cdot \dots \cdot \bar{\pi}_r,$$

és

$$a^2 + 2b^2 = (\pi_1 \cdot \bar{\pi}_1) \cdot \dots \cdot (\pi_i \cdot \bar{\pi}_i) \cdot \dots \cdot (\pi_r \cdot \bar{\pi}_r).$$

Itt minden $\pi_i \cdot \bar{\pi}_i$ szorzat prímszám, valamelyik i -re $p = \pi_i \cdot \bar{\pi}_i$, másrészt $\pi_i = x + \sqrt{2}yi$ alakú (x, y egész), tehát $p = \pi_i \cdot \bar{\pi}_i = x^2 + 2y^2$, amit bizonyítani kellett.