*[1]Az I. rész a KöMaL 2000/9. számában az 513–517. oldalakon olvasható. Ott az 516. oldal közepén álló egyenőtlenségbe sajtóhiba került. Helyesen:

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

Az első részben elkezdtük vizsgálni, milyen pozitív egész d számokra teljesül, hogy ha két $x^2 + dy^2$ alakú szám hányadosa egész, akkor a hányados is ilyen alakú. A $d = 1$ és a $d = 2$ eset után most vizsgáljuk a $d = 3$ esetet. Legyenek a Q halmaz elemei azok a p prímek, amelyekre $p \mid x^2 + 3y^2$-ből következik, hogy $p \mid x$, $p \mid y$, a P_1 halmaz elemei pedig az $x^2 + 3y^2$ alakú prímek.

Most nem működik a $d = 2$-re adott bizonyítás, ugyanis $2 \notin Q$ (például $2 \mid 1^2 + 3 \cdot 1^2$), és $2 \notin P_1$, hiszen nem írható fel $x^2 + 3y^2$ alakban. Nincs azonban nagy baj, csak kisebb módosításokra van szükség.

Először is megmutatjuk, hogy $2 \mid x^2 + 3y^2$ esetén $4 \mid x^2 + 3y^2$, tehát a 4 bizonyos értelemben prímként viselkedik. Ez könnyen látható, ugyanis

$$x^2 \equiv 0 \quad \text{vagy} \quad 1 \pmod 4 \qquad \text{és} 3y^2 \equiv 0 \quad \text{vagy} \quad 3 \pmod 4, \qquad \text{így} x^2 + 3y^2 \equiv 0 \quad \text{vagy} \quad 1 \quad \text{vagy} \quad 3 \pmod 4.$$

Ha ki tudjuk egészíteni az 1. Tételt azzal, hogy $4 \mid a^2 + 3b^2$ esetén az $\dfrac{a^2 + 3b^2}{4}$ is $x^2 + 3y^2$ alakú, akkor a bizonyítás során a 2 prímszámot a 4-gyel helyettesítve a $d = 2$-re adott bizonyítás már szó szerint működni fog. Ezt a kiegészítést fogjuk most bizonyítani:

Vizsgáljuk az $\dfrac{a^2 + 3b^2}{4}$ törtet. Két lehetőség van: $2 \mid a$ és $2 \mid b$, vagy $2 \not| a$ és $2 \not| b$. Az első estben az állítás nyilvánvaló, a-t és b-t is el kell osztani 2-vel, így az $\dfrac{a^2 + 3b^2}{4}$-et kapjuk $x^2 + 3y^2$ alakban. Ha $2 \not| a$ és $2 \not| b$, akkor az 1. Tételnél leírt bizonyítás szó szerint működik az $x^2 + 3y^2 =$ prím helyett $x^2 + 3y^2 = 4$-re is addig, hogy

$$x^2 + 3y^2 \mid ay - bx \qquad \text{vagy} \qquad x^2 + 3y^2 \mid ay + bx$$

kell, hogy legyen. De most $x = y = 1$, így

$$4 \mid a + b \qquad \text{vagy} \qquad 4 \mid a - b$$

kell, hogy legyen. Mivel a és b páratlan, azért ezek közül az egyik valóban teljesül.

Ezzel az állítást $d = 3$-ra is bebizonyítottuk.[2]Ez volt a decemberben kitűzött **B. 3421.** feladat.

Nagyobb d-kre már ez a bizonyítási módszer nem működik. Például, mint majd később látni fogjuk, $d = 5$-re igaz az állítás, és mégis $2 \notin Q$ (például $2 \mid 1^2 + 5 \cdot 1^2$), $2 \notin P_1$ (nem írható fel $x^2 + 5y^2$ alakban), és az sem igaz, hogy $2 \mid x^2 + 5y^2$ esetén $4 \mid x^2 + 5y^2$ (például $6 = 1^2 + 5 \cdot 1^2$). A bizonyításhoz mindenekelőtt egy, az 1. Tételnél erősebb tételre van szükség:

2. Tétel. *Ha ap és bp is $x^2 + dy^2$ alakú, akkor az ab is $x^2 + dy^2$ alakú.*
(Ennek speciális esete az 1. Tétel: ha az ap és az $1 \cdot p$ is $x^2 + dy^2$ alakú, akkor az $a \cdot 1$ is az).

Bizonyítás. Legyen

$$ap = x^2 + dy^2 \qquad \text{és} (3) bp = z^2 + dv^2. (4)$$

Ekkor a $(*)$ azonosság szerint

$$abp^2 = (xz \pm dyv)^2 + d(xv \mp yz)^2.$$

Nyilván elég azt bizonyítani, hogy

$$p \mid xv - yz \qquad \text{vagy} \qquad p \mid xv + yz, \tag{5}$$

mert ekkor $p \mid xz + dyv$, illetve $p \mid xz = dyv$ lesz $(p^2 \mid abp^2 = (xz \pm dyv)^2 + d(xv \mp yz)^2$ miatt), és így

$$ab = \left(\frac{xz \pm dyv}{p}\right) 2 + d\left(\frac{xv \mp yz}{p}\right)^2,$$

ahol az $\dfrac{xz \pm dyv}{p}$ és az $\dfrac{xv \mp yz}{p}$ egész. Ahhoz, hogy az (5) teljesüljön, ismét elég a $p \mid (xv - yz)(xv + yz)$-t, azaz a

$$p \mid x^2v^2 - y^2z^2 \tag{6}$$

oszthatóságot bizonyítani. A (3) és (4) alapján

$$x^2 \equiv -dy^2 \qquad \text{és} \qquad -dv^2 \equiv z^2 \pmod p.$$

---

[1]

[2]*

Ezeket összeszorozva:

$$dx^2v^2 \equiv dy^2z^2, \qquad \text{azaz} d(x^2v^2 - y^2z^2) \equiv 0 \pmod{p}.$$

Így $p \not| d$ esetén a (6) valóban teljesül, ha pedig $p \mid d$, akkor a $p \mid x^2 + dy^2$ és $p \mid z^2 + dv^2$ miatt $p \mid x$ és $p \mid z$, így a (6) ekkor is teljesül.

Most vizsgáljuk a $d = 5$ esetet ($d = 1$, 2, 3-ra már bebizonyítottuk, $d = 4$-re pedig nem igaz, mivel a 4 egy 1-nél nagyobb négyzetszám). Használjuk a szokásos jelöléseket: legyenek a Q halmaz elemei azok a prímek, amelyekre $p \mid x^2 + 5y^2$-ből következik, hogy $p \mid x$ és $p \mid y$, és legyenek a P_1 halmaz elemei azok a prímek, amelyek felírhatók $x^2 + 5y^2$ alakban. Vezessünk be egy P_2 halmazt is: legyenek a P_2 halmaz elemei azok a p prímek, amelyekre a $2p$ felírható $x^2 + 5y^2$ alakban. A 2. tételből, valamint abból, hogy 2 nem írható fel $x^2 + 5y^2$ alakban következik, hogy e három halmaznak nincsen közös eleme.

Be fogjuk bizonyítani, hogy minden p prím eleme Q-nak, P_1-nek vagy P_2-nek. Most is teljes indukcióval fogunk bizonyítani: $p = 2$-re igaz, mert $2 \in P_2$ ($2p = 4 = 2^2 + 5 \cdot 0^2$). Tegyük fel, hogy a p-nél kisebb prímekre már bebizonyítottuk, és vizsgáljuk a p-t.

Tegyük fel, hogy $p \notin Q$. Ekkor a $d = 2$ esethez hasonlóan létezik olyan x, y, amelyre $p \mid x^2 + 5y^2$, ahol $x^2 + 5y^2 \leq \left(\frac{p-1}{2}\right)^2 + 5$. Ez $p \geq 3$ esetén kisebb p^2-nél, tehát a p-n kívül csak p-nél kisebb prímtényezői vannak. Ezek mind elemei Q-nak, P_1-nek vagy P_2-nek az indukciós feltétel alapján. A Q-beli és P_1-beli prímekkel a $d = 2$ esethez hasonlóan leoszthatunk. Így egy olyan $x^2 + 5y^2$ alakú számhoz jutunk, amelynek a prímfelbontásában szerepel egy p tényező, és ezen kívül csak P_2-beli prímtényezők.

Legyen egy ilyen P_2-beli prímtényező q. Legyen $x^2 + 5y^2 = pqa$. Ekkor a pqa $x^2 + 5y^2$ alakú, és mivel a q P_2-beli, azért a $2q$ is az. Így a 2. Tétel alapján a $2pa$ is $x^2 + 5y^2$ alakú. Elvégezve ezt az átalakítást minden 2-nél nagyobb P_2-beli prímtényezővel, végül egy $2^k \cdot p$ számot fogunk kapni $x^2 + 5y^2$ alakban.

De $4 \mid x^2 + 5y^2$ esetén $2 \mid x$ és $2 \mid y$, így $4 \mid x^2 + 5y^2$ esetén x-et és y-t is eloszthatjuk 2-vel. Így a $2^k \cdot p$ számot eloszthatjuk 4-gyel ($k \geq 2$ esetén). Osszuk el 4-gyel annyiszor, ahányszor csak lehet, végül p-t vagy $2p$-t fogunk kapni $x^2 + 5y^2$ alakban. Tehát valóban $p \in P_1$ vagy $p \in P_2$, a megfelelő felbontás most is létezik.

Most azt fogjuk bebizonyítani, hogy ha $p_1 \in P_2$ és $p_2 \in P_2$, valamint a p_1p_2a szám $x^2 + 5y^2$ alakú, akkor az a szám is $x^2 + 5y^2$ alakú. Valóban, ha a p_1p_2a és a $2p_1$ is $x^2 + 5y^2$ alakú, akkor a $2p_2a$ is $x^2 + 5y^2$ alakú, és ha a $2p_2a$ és a $2p_2$ is $x^2 + 5y^2$ alakú, akkor a $2 \cdot 2a$ is $x^2 + 5y^2$ alakú (a 2. Tétel alapján). Azt pedig már bebizonyítottuk, hogy 4-gyel lehet osztani, így valóban az a is $x^2 + 5y^2$ alakú.

Végül bizonyítsuk be, hogy egy $x^2 + 5y^2$ alakú szám mindig néhány Q-beli, néhány P_1-beli és páros sok P_2-beli prím szorzata. Valóban, a Q-beli és P_1-beli prímekkel leoszthatunk, majd párosával leoszthatunk a P_2-beli prímekkel is. Így ha páratlan sok P_2-beli prím lenne, akkor végül egy P_2-beli prímet kapnánk $x^2 + 5y^2$ alakban. Így a p és a $2p$ is $x^2 + 5y^2$ alakú lenne, tehát a 2. Tétel alapján a 2 is, ami ellentmondás.

Ezek után vizsgáljunk egy

$$\frac{x^2 + 5y^2}{z^2 + 5v^2}$$

törtet. Ezt rendre egyszerűsíthetjük a Q-beli, P_1-beli, és párosával a P_2-beli prímekkel, és végül $\frac{x_1^2 + 5y_1^2}{1}$ alakú törtet kapunk, tehát a hányados is ilyen alakú.

Ezzel bebizonyítottuk, hogy $d = 5$-re is igaz az állítás.

Ugyanígy bizonyíthatunk $d = 6$-ra is. Azonban $d = 7$-re már a bizonyítás nem működik, két okból sem: egyrészt nem teljesül $p \geq 3$-ra a

$$\left(\frac{p-1}{2}\right)^2 + d < p^2 \tag{7}$$

(ez lenne a kisebbik probléma, ugyanis $p \geq 5$ esetén már teljesül, a $p = 3$ pedig $d = 7$ esetén Q-beli), másrészt nem lehet 4-gyel osztani. Ez akkora probléma, hogy $d = 7$-re nem is igaz az állítás. Például

$$\frac{1^2 + 7 \cdot 1^2}{2^2 + 7 \cdot 0^2} = 2,$$

ami nem $x^2 + 7y^2$ alakú. Hasonló módon nem igaz $d = 8$-ra sem, ekkor

$$\frac{0^2 + 8 \cdot 2^2}{2^2 + 8 \cdot 0^2} = 2.$$

A $d = 7$ és $d = 8$ esetéből általánosabb tapasztalatot is leszűrhetünk:

3. Tétel. *A d-nek, és $d > 3$ esetén a $(d+1)$-nek is négyzetmentes számnak kell lennie.*

Bizonyítás. Tegyük fel először, hogy a d nem négyzetmentes, tehát a^2b alakba írható, ahol $a \geq 2$. Ekkor

$$\frac{0^2 + d \cdot 1^2}{a^2 + d \cdot 0^2} = b.$$

Mivel $b < d$, ez csak akkor lehetne $x^2 + dy^2$ alakú, ha négyzetszám lenne. De ha a b négyzetszám, akkor a d is az, és azt már tudjuk, hogy a d nem lehet 1-nél nagyobb négyzetszám.

Most vizsgáljuk azt, amikor a $d+1$ nem négyzetmentes, tehát $d+1 = a^2b$, ahol $a \geq 2$. Ekkor

$$\frac{1^2 + d \cdot 1^2}{a^2 + d \cdot 0^2} = b,$$

ami a fentiekhez hasonló módon csak akkor lehet x^2+dy^2 alakú, ha a $d+1$ négyzetszám. Így $d+1 \equiv 0$ vagy $1 \pmod 4$, azaz $d \equiv -1$ vagy $0 \pmod 4$. Ha $d \equiv 0 \pmod 4$, akkor a d nem négyzetmentes, így a fentiek alapján nem igaz rá az állításunk. Ha pedig $d \equiv -1 \pmod 4$, akkor az

$$\frac{1^2 + d \cdot 1^2}{2^2 + d \cdot 1^2} = \frac{d+1}{4} \qquad \frac{3^2 + d \cdot 1^2}{2^2 + d \cdot 1^2} = \frac{d+9}{4}$$

törtek egészek. De $d > 3$ esetén a törtek kisebbek d-nél, igy csak akkor lehetnek $x^2 + dy^2$ alakúak, ha négyzetszámok. De a két tört különbsége 2, és két négyzetszám különbsége nem lehet 2.

Vizsgáljuk tovább a d lehetséges értékeit. Láttuk, hogy a $d = 7$-re és $d = 8$-ra nem igaz az állításunk. Nyilván $d = 9$-re sem igaz, mert a 9 négyzetszám. Azonban $d = 10$-re igaz, itt működik a $d = 5$-re adott bizonyítás: ekkor $2 \in Q$, 4-gyel lehet osztani, $3 \in Q$, és $p > 3$-ra teljesül a (7) egyenlőtlenség, így innentől működik a teljes indukció. A $d = 11$ és $d = 12$ esetben nem igaz az állítás, mert ekkor a $d+1$, illetve a d nem négyzetmentes. A $d = 13$ esetben megint csak működik a $d = 5$-re adott bizonyítás ($2 \in Q$, 4-gyel lehet osztani, $3 \in Q$, $p > 3$-ra teljesül a (7) egyenlőtlenség). A $d = 14$ esetben sem a $(d+1)$-nek, sem a d-nek nincs 1-nél nagyobb négyzetszám osztója, az állítás mégsem igaz:

$$\frac{2^2 + 14 \cdot 1}{3^2 + 14 \cdot 0} = 2.$$

A $d = 15, 16, \ldots, 20$ esetben a d vagy a $d+1$ nem négyzetmentes.

Most vizsgáljuk a $d = 21$ esetet. A már ismert Q, P_1, P_2 halmazokon kívül vezessük be a P_3 és P_6 halmazokat, a P_3 elemei legyenek azok a p prímek, amelyekre a $3p$ felírható $x^2 + 21y^2$ alakban, a P_6 elemei pedig azok, amelyekre a $6p$ felírható $x^2 + 21y^2$ alakban.

Ekkor $2 \in P_2$, $3 \in P_3$, $5 \in P_6$ (mert $2p = 4 = 2^2 + 21 \cdot 0^2$, $3p = 9 = 3^2 + 21^0$, illetve $6p = 30 = 3^2 + 21 \cdot 1^2$), $p > 5$-re pedig teljesül a (7) egyenlőtlenség. Ezen kívül 2^2-nel és 3^2-nel lehet osztani, így a $d = 5$ esethez hasonlóan be lehet bizonyítani, hogy minden prím eleme Q-nak, P_1-nek, P_2-nek, P_3-nak vagy P_6-nak.

A $d = 5$ esethez hasonlóan be lehet bizonyítani, hogy egy szám akkor és csak akkor írható fel $x^2 + 21y^2$ alakban, ha P_2-beli és P_6-beli prím összesen páros sok van benne, valamint P_3-beli és P_6-beli prím összesen páros sok van benne: le lehet osztani a Q-beli és P_1-beli prímekkel, párosával le lehet osztani a P_2-beli, P_3-beli, valamint a P_6-beli prímekkel, továbbá le lehet osztani egy P_2-beli, egy P_3-beli és egy P_6-beli prímmel egyszerre. Ezek után a bizonyítás folytatható.

Csörnyei Marianna