

Általános megoldás

Általánosan fogunk keresni egy szükséges és elégséges feltételt a cikkben vizsgált kérdésre; milyen pozitív egész d -kre igaz, hogy ha két $x^2 + dy^2$ alakú szám hányadosa egész, akkor a hányados is felírható ilyen alakban.¹ A cikk első két részében néhány lehetséges d értéket vizsgáltunk. (KöMaL 2000/9. szám, 513–517. oldal és KöMaL 2001/2. szám 77–82. oldal) Az eddigi bizonyítások kevesebbet használtak fel, mint az általános megoldás, és nyújtottak valamiféle képet arról is, hogy mely számok írhatók fel $x^2 + dy^2$ alakban. Most máshonnan fogjuk a problémát megközelíteni.

Már tudjuk, hogy a d -nek négyzetmentesnek kell lennie. Vizsgáljunk egy tetszőleges négyzetmentes d -t. Legyen az $x^2 + dy^2$ alakú számok halmaza az A halmaz, ekkor azt kell megvizsgálnunk, hogy teljesül-e minden a és x pozitív egész számra, hogy

$$(8) \quad ax \in A \quad \text{és} \quad a \in A\text{-ból következik, hogy} \quad x \in A.$$

Nyilván minden négyzetszám eleme A -nak ($a^2 = a^2 + d \cdot 0^2$), így ha egy d -re az állítás igaz, akkor

$$(9) \quad a^2x \in A\text{-ból következik, hogy} \quad x \in A$$

kell, hogy legyen. Ez azonban nemcsak szükséges, hanem elégséges is, ugyanis mivel két A -beli szám szorzata is A -beli, azért

$$ax \in A \quad \text{és} \quad a \in A\text{-ból következik, hogy} \quad a^2x \in A,$$

így a (8) helyett elég a (9)-et vizsgálni. Tehát azt kell megvizsgálnunk, hogy milyen d -kre lehet az A halmazban négyzetszámmal osztani. Nyilván elég a p^2 -tel való osztást vizsgálni.

Definiáljuk a P halmazt a következőképpen: Legyen P azon p prímek halmaza, amelyekre a $-d \equiv x^2 \pmod{p^2}$ kongruenciának nincs megoldása. Vizsgáljuk a P elemeit.

Legyen a P egy tetszőleges eleme p , és vizsgáljunk egy p^2 -tel osztható $x^2 + dy^2$ számot. Ha $(y, p) = 1$ lenne, akkor lenne olyan k egész szám, amelyre $yk \equiv 1 \pmod{p^2}$. Ekkor a $p^2 \mid x^2 + dy^2$ miatt

$$p^2 \mid (xk)^2 + d(yk)^2 \equiv (xk)^2 + d \pmod{p^2},$$

azaz

$$-d \equiv (xk)^2 \pmod{p^2}$$

lenne. De tudjuk, hogy $p \in P$, így ez nem lehetséges. Tehát $(y, p) \neq 1$, azaz $p \mid y$. Ekkor a $p^2 \mid x^2 + dy^2$ miatt $p^2 \mid x^2$, azaz $p \mid x$. Tehát a p^2 -tel osztható $x^2 + dy^2$ számban az x és az y is osztható p -vel, helyükre a p -ed részüket írva az $x^2 + dy^2$ szám p^2 -ed részét kapjuk $x^2 + dy^2$ alakban, így valóban a p^2 -ed része is eleme A -nak. Tehát a $p \in P$ prímekkel mindig lehet osztani (tetszőleges d esetén).

Most vizsgáljuk a $p \notin P$ prímeket. Bebizonyítjuk, hogy akkor és csak akkor teljesül ezekre a p -kre a (9), ha a p^2 felírható $x^2 + dy^2$ alakba, ahol $y \not\equiv 0 \pmod{p}$.

Először bebizonyítjuk, hogy ez a feltétel *elégséges*, tehát $p^2 = x^2 + dy^2$ esetén, ahol $y \not\equiv 0 \pmod{p}$: $p^2 \mid a^2 + db^2$ -ből következik, hogy $\frac{a^2 + db^2}{p^2} \in A$. Vizsgáljuk az $\frac{a^2 + db^2}{p^2}$ számot. Ha $p \mid b$, akkor a fentiekhez hasonló módon $p \mid a$, így valóban $\frac{a^2 + db^2}{p^2} \in A$. Ha viszont $p \nmid b$, akkor, mivel a d négyzetmentes, azért $p^2 \nmid db^2$, így a $p^2 \mid a^2 + db^2$ miatt $p^2 \nmid a^2$,

azaz $p \nmid a$. Tehát az $\frac{a^2 + db^2}{p^2}$ törtet kell vizsgálnunk, ahol $p \nmid a$, $p \nmid b$ és $p^2 = x^2 + dy^2$, ahol $p \nmid y$.

Az 1. Tételben $x^2 + dy^2$ alakú prímszámmal osztottunk, most $x^2 + dy^2$ alakú p^2 számmal kell osztanunk. Vizsgáljuk tehát az 1. Tételnél leírt bizonyítást p helyett p^2 -re.

A bizonyítás addig működik, hogy $p^2 \mid ay + bx$ -et vagy $p^2 \mid ay - bx$ -et kell bizonyítani. Az $ay + bx$ és az $ay - bx$ számok összege $2ay$, és tudjuk, hogy $p \nmid a$, $p \nmid y$, így a $p = 2$ esetet kivéve biztos, hogy nem osztható mindkét szám p -vel. Ezért elég a $p^2 \mid (ay + bx)(ay - bx)$ -et bizonyítani. Ezután az 1. Tételnél leírt bizonyítás alkalmazható. Ha pedig $p = 2$, akkor $p^2 = 4 = x^2 + dy^2$, ahol $p \nmid y$, így csak $d = 3$, $x = y = 1$ lehet. Azt már bebizonyítottuk, hogy $d = 3$ esetén lehet osztani 4-gyel.

Ezzel bebizonyítottuk, hogy elégséges feltétel az, hogy minden $p \notin P$ -re a p^2 felírható $x^2 + dy^2$ alakba, ahol $y \not\equiv 0 \pmod{p}$.

Még azt kell bebizonyítani, hogy ez a feltétel *szükséges*, tehát ahhoz, hogy a (9) teljesüljön, szükséges, hogy minden $p \notin P$ -re $p^2 = x^2 + dy^2$ legyen, ahol $y \not\equiv 0 \pmod{p}$. Ezt teljes indukcióval fogjuk bebizonyítani. Először megmutatjuk, hogy a $p = 2$ esetben igaz.

Már megmutattuk, hogy a d -nek, illetve $d > 3$ esetén a $(d + 1)$ -nek is négyzetmentesnek kell lennie. Így $d \not\equiv 0 \pmod{4}$, és $d > 3$ esetén $d \not\equiv 3 \pmod{4}$. De $d \equiv 1$ vagy $d \equiv 2$ esetén $p = 2 \in P$ (mert a -1 és a -2 négyzetes nemmaradék mod 4), így már csak a $d = 3$ eset van hátra. Ekkor valóban $p^2 = x^2 + dy^2$, ahol $y \not\equiv 0 \pmod{2}$, mivel $p^2 = 4 = 1^2 + 3 \cdot 1^2$.

Tegyük fel, hogy a p -nél kisebb prímeke már bebizonyítottuk az állítást, és vizsgáljuk p -re. Két lehetőség van aszerint, hogy

$$\left(\frac{p-1}{2}\right)^2 + d < p^2 \quad \text{vagy} \quad (10) \quad \left(\frac{p-1}{2}\right)^2 + d \geq p^2. (11)$$

Mielőtt rátérnénk ennek a két esetnek a vizsgálatára, bizonyítsuk be az alábbi tételt.

4. Tétel. *Ha van egy $a^2 + db^2$ alakú négyzetszámunk, amely osztható p^2 -tel, és a p^2 -en kívül csak $q^2 = x_1^2 + dy_2^2$ alakú prímnégyzet osztói vannak, akkor $p^2 = x^2 + dy^2$, ahol $p \nmid y$.*

Bizonyítás. Nyilván elég azt bizonyítani, hogy az

$$\frac{a^2 + db^2}{q^2} = \frac{a^2 + db^2}{x_1^2 + dy_2^2}$$

tört $z^2 + dv^2$ alakba írható úgy, hogy $p \nmid v$ legyen. Ekkor ugyanis a q^2 osztókkal rendre leoszthatunk, végül a p^2 -et fogjuk megkapni $x^2 + dy^2$ alakban, ahol $p \nmid y$.

Az elégségeség bizonyításakor már láttuk, hogy az $\frac{a^2 + db^2}{x_1^2 + dy_1^2}$ tört $z^2 + dv^2$ alakba írható, ahol

$$v = \frac{ay_1 \pm bx_1}{x_1^2 + dy_1^2}.$$

Ahhoz, hogy $p \nmid v$ legyen, így elég a

$$p \nmid (ay_1 + bx_1)(ay_1 - bx_1)$$

tulajdonságot megmutatnunk. Valóban,

$$(ay_1 + bx_1)(ay_1 - bx_1) = (a^2 + db^2)y_1^2 - (x_1^2 + dy_1^2)b^2 = (a^2 + db^2)y_1^2 - q^2b^2,$$

ahol $p \mid a^2 + db^2$, $p \nmid b$, és $p \nmid q$ (mert a q prímszám, és $p \neq q$).

Most vizsgáljuk azokat a p prímeke, amelyekre $\left(\frac{p-1}{2}\right)^2 + d < p^2$ teljesül. Ekkor, mint ahogy azt már sokszor láttuk, van olyan p -vel osztható $x^2 + dy^2$ alakú szám, amelyben $p \nmid y$, és a p -n kívül csak p -nél kisebb prímosztói vannak. Legyen $x^2 + dy^2 = pk$. Ekkor:

$$p^2k^2 = (x^2 + dy^2)(x^2 + dy^2) = (x^2 - dy^2)^2 + d(2xy)^2.$$

Legyen tehát $x^2 - dy^2 = a$ és $2xy = b$, ekkor $p^2k^2 = a^2 + db^2$, és az $a^2 + db^2$ -nek a p^2 -en kívül csak p^2 -nél kisebb prímnégyzet-osztói vannak, amelyekre teljesül az indukciós feltevésünk. Így a 4. Tétel alapján csak azt kell bebizonyítani, hogy $p \nmid b$, azaz $p \nmid 2xy$.

Valóban, $p \nmid 2$ (mert $p > 2$), és azt is tudjuk, hogy $p \nmid y$, így csak a $p \nmid x$ -et kell vizsgálnunk. Mivel $p \nmid d$ (ellenkező esetben $p \in P$ lenne) és $p \mid x^2 + dy^2$, így a $p \nmid dy^2$ miatt valóban $p \nmid x$ kell, hogy legyen.

Most pedig vizsgáljuk azokat a p prímeke, amelyekre $\left(\frac{p-1}{2}\right)^2 + d \geq p^2$ teljesül. Mivel $p \notin P$, azért létezik olyan x , amelyre $p^2 \mid x^2 + d$. Ekkor nyilván létezik olyan x , amelyre $|x| = \frac{p^2 - 1}{2}$, és $p^2 \mid x^2 + d$. Tehát van egy olyan $x^2 + dy^2$ alakú számunk, amely legfeljebb $\left(\frac{p^2 - 1}{2}\right)^2 + d$, osztható p^2 -tel, és $p \nmid y$ (mivel $y = 1$). Bebizonyítjuk, hogy

$$(12) \quad \left(\frac{p^2 - 1}{2}\right)^2 + d < p^2d.$$

Tegyük fel, hogy ez nem igaz, tehát $\left(\frac{p^2 - 1}{2}\right)^2 + d \geq p^2d$. Ebből:

$$\left(\frac{p^2 - 1}{2}\right)^2 \geq (p^2 - 1)d, \frac{p^2 - 1}{4} \geq d.$$

Ugyanakkor tudjuk, hogy teljesül a (11), azaz

$$d \geq p^2 - \left(\frac{p-1}{2}\right)^2.$$

Ezekből:

$$\frac{p^2 - 1}{4} \geq p^2 - \left(\frac{p-1}{2}\right)^2.$$

Ebből rendezés után:

$$0 \geq \frac{p^2 + p}{2},$$

ami nyilván ellentmondás. Tehát valóban teljesül a (12).

Így van egy olyan $x^2 + dy^2 = x^2 + d \cdot 1^2$ alakú számunk, amely osztható p^2 -tel, $p \nmid y$, és kisebb p^2d -nél. Mivel $p^2 \in A$, ezért a p^2 -ed része is A eleme kell legyen. De kisebb p^2d -nél, így a p^2 -ed része kisebb d -nél, tehát csak akkor lehet $x^2 + dy^2$ alakú szám, ha négyzetszám.

Tehát van egy olyan $x^2 + dy^2 = x^2 + d \cdot 1^2$ alakú négyzetszámunk, amely osztható p^2 -tel, $p \nmid y$ és kisebb p^2d -nél. Ha kisebb p^4 -nél is, akkor csak p^2 -nél kisebb prímnégyzet-osztói vannak, amelyekre teljesül az indukciós feltevésünk, így ekkor a 4. Tétel alapján készen vagyunk. Ezért elég azt az esetet vizsgálni, amikor az $x^2 + dy^2$ legalább p^4 .

Most legyen egy olyan $x^2 + dy^2 = x^2 + d \cdot 1^2$ alakú négyzetszámunk, amely osztható p^2 -tel, $p \nmid y$, kisebb p^2d -nél és legalább p^4 . Ekkor nyilván $p^4 < p^2d$, azaz $p^2 < d$. Ezen kívül $p^2 \mid x^2 + d$ esetén $p^2 \mid (p^2 - x)^2 + d$. Bebizonyítjuk, hogy ez a $(p^2 - x)^2 + d$ szám is kisebb p^2d -nél.

Tegyük fel, hogy ez nem igaz, azaz

$$(p^2 - x)^2 + d \geq p^2d.$$

Ebből:

$$(p^2 - 1)^2 \geq p^2d(p^2 - 1)^2 \geq (p^2 - 1)dp^2 - 1 \geq dp^2 > d,$$

viszont tudjuk, hogy $p^2 < d$. Így valóban a $(p^2 - x)^2 + d$ szám is kisebb p^2d -nél. Ekkor az $x^2 + d$ -hez hasonlóan a $(p^2 - x)^2 + d$ is négyzetszám.

De a p^2 páratlan, így az x és a $p^2 - x$ különböző maradékot ad 2-vel osztva, tehát az x^2 és a $(p^2 - x)^2$ közül az egyik 0-t, a másik 1-et ad 4-gyel osztva maradékul. Az $x^2 + d$ és a $(p^2 - x)^2 + d$ is négyzetszám, és egy négyzetszám csak 0-t vagy 1-et adhat 4-gyel osztva maradékul, így csak $d \equiv 0 \pmod{4}$ lehet. Azt pedig már beláttuk, hogy a d négyzetmentes kell legyen, így ez nem lehetséges.

Következmények: Bebizonyítottuk, hogy szükséges és elégséges feltétel az, hogy minden $p \notin P$ -re $p^2 = x^2 + dy^2$ legyen, ahol $p \nmid y$. A bizonyításból az is kitűnt, hogy elég azokat a $p \notin P$ prímekeket vizsgálni, amelyekre teljesül (11), ha ezekre az állításunk teljesül, akkor teljesül a többi $p \notin P$ prímre is. És ez minden d -re csak véges sok eset.

Vizsgáljuk a (11) egyenlőtlenséget. Átalakítva:

$$d \geq p^2 - \left(\frac{p-1}{2}\right)^2 = \frac{3p^2 + 2p - 1}{4} > \frac{p^2}{4}.$$

Így $4d > p^2$. Ugyanakkor $p^2 = x^2 + dy^2$, így csak $2 > y$ lehet, azaz $y = 0$ vagy $y = 1$. De azt is tudjuk, hogy $p \nmid y$, így csak $y = 1$ lehet. Ekkor $p^2 = x^2 + dy^2 = x^2 + d$, vagyis a $p^2 - d$ négyzetszám.

Összefoglalva: szükséges és elégséges feltétel, hogy minden p prímre, amelyre $\left(\frac{p-1}{2}\right)^2 + d \geq p^2$ és $p \notin P$, a $p^2 - d$ egy négyzetszám legyen.

Megjegyzés. Ez egy nagyon erős feltétel; minél nagyobb a d , annál erősebb. A 95 milliónál kisebb d számok, amelyek kielégítik ezt a feltételt:

1, 2, 3, 5, 6, 10, 13, 21, 22, 30, 33, 37, 42, 57, 58, 70, 78, 85, 93, 102, 105, 130, 133, 165, 177, 190, 210, 253, 273, 330, 345, 357, 385, 462, 1365.

Kárpáti Attila számítógépes programja alapján 95 millióig több ilyen szám nincs.

Csörnyei Marianna