Sume kvadrata

Koji se prirodni brojevi mogu prikazati kao zbroj kvadrata dva cijela broja?

Propozicija 1. *Ako su brojevi m i n sume dva kvadrata, onda je i njihov produkt $m \cdot n$ također suma dva kvadrata.*

Dokaz: Iz $m = a^2 + b^2$ i $n = x^2 + y^2$ slijedi

$$mn = (ax + by)^2 + (ay - bx)^2.$$

$\square$

Propozicija 2. *Prost broj p oblika $4k + 3$ nije suma dva kvadrata. Štoviše, ako $p|x^2 + y^2$, onda $p|x$ i $p|y$.*

Dokaz: Pretpostavimo da $p|x^2 + y^2$. Tada je $x^2 \equiv -y^2 \pmod p$. Dignimo ovu kongruenciju na potenciju $\frac{p-1}{2}$, pa dobijemo $x^{p-1} \equiv (-1)^{(p-1)/2} y^{p-1} \pmod p$. Sada iz Malog Fermatovog teorema slijedi da je $1 \equiv -1 \pmod p$. Kontradikcija. (Uočimo da x i y moraju biti relativno prosti sa p ako je $p = x^2 + y^2$.) $\square$

Propozicija 3. *Ako prost broj p dijeli sumu dva kvadrata x^2+y^2, $(x, y) = 1$, onda je p i sam suma dva kvadrata.*

Dokaz: Dokaz provodimo tzv. *metodom spusta.*

Pretpostavimo da je $p \cdot k$ najmanji višekratnik od p koji se može prikazati u obliku

$$pk = x^2 + y^2, \quad (x, y) = 1.$$

Neka je $x \equiv a \pmod p$, $y \equiv b \pmod p$, $|a|, |b| \leq \frac{p}{2}$. Tada je $a^2 + b^2 \equiv x^2 + y^2 \equiv 0 \pmod p$ i $a^2 + b^2 \leq \frac{p^2}{4} + \frac{p^2}{4} = p \cdot \frac{p}{2}$. Zato je $1 \leq k \leq \frac{p}{2}$.

Pretpostavimo da je $k > 1$. Neka je sada $x \equiv u \pmod k$, $y \equiv v \pmod k$, $|u|, |v| \leq \frac{k}{2}$. Tada je $u^2 + v^2 \equiv x^2 + y^2 \equiv 0 \pmod k$, recimo $u^2 + v^2 = kl$. Vrijedi $u^2 + v^2 \leq \frac{k^2}{2}$, pa je $1 \leq l \leq \frac{k}{2} < k$. Promotrimo jednakost

$$pk^2 l = (x^2 + y^2)(u^2 + v^2) = (xu + yv)^2 + (xv - yu)^2.$$

Imamo:

$$xu + yv \equiv x^2 + y^2 \equiv 0 \pmod{k}, \quad \text{recimo } xu + yv = x_0 k;$$

$$xv - yu \equiv xy - xy \equiv 0 \pmod{k}, \quad \text{recimo } xv - yu = y_0 k.$$

Odavde je $pl = x_0^2 + y_0^2$. Ako je $(x_0, y_0) = d$, recimo $x_0 = dx_1$, $y_0 = dy_1$, onda je $p \cdot \frac{l}{d^2} = x_1^2 + y_1^2$. No, $\frac{l}{d^2} \le l < k$, pa smo dobili kontradikciju s minimalnošću od k. Stoga je $k = 1$ (ako je $k = 1$, onda je $l = 0$) i $p = x^2 + y^2$. □

Propozicija 4. *Neka je p prost broj oblika $4k+1$. Tada postoji prirodan broj x takav da $p | x^2 + 1$.*

Dokaz: Koristimo Wilsonov teorem:
Za prost broj p vrijedi $(p-1)! \equiv -1 \pmod{p}$.
Ako je $p = 4k+1$, onda je

$$\begin{aligned}(p-1)! &= 1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2} \cdot \left(p - \frac{p-1}{2}\right) \cdots (p-3)(p-2)(p-1) \\ &\equiv \left(1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2}\right)^2 \pmod{p}.\end{aligned}$$

Dakle, za x možemo uzeti $x = \left(\frac{p-1}{2}\right)!$. □

Propozicija 5. *Prost broj p je suma kvadrata ako i samo ako je $p = 2$ ili $p \equiv 1 \pmod{4}$.*

Dokaz: Direktno iz Propozicija 2, 4 i 3. □

Propozicija 6. *Prikaz prostog broja u obliku sume dva kvadrata je jedinstven (ako postoji).*

Dokaz: Pretpostavimo da je $p = a^2 + b^2 = c^2 + d^2$. Možemo pretpostaviti da su a i c, te b i d, iste parnosti. Imamo:

$$\frac{a-c}{2} \cdot \frac{a+c}{2} = \frac{d-b}{2} \cdot \frac{d+b}{2}, \quad a \ne c,\ b \ne d.$$

Neka je $(\frac{a-c}{2}, \frac{d-b}{2}) = s$, te neka je $\frac{a-c}{2} = st$, $\frac{d-b}{2} = su$. Imamo: $t \cdot \frac{a+c}{2} = u \cdot \frac{d+b}{2}$. Kako su u i t relativno prosti, to je $\frac{a+c}{2} = uv$, $\frac{d+b}{2} = tv$. Odavde je $a = st + uv$, $b = tv - su$, pa je $p = a^2 + b^2 = (s^2 + v^2)(t^2 + u^2)$, kontradikcija. □

Teorem 1. *Prirodan broj n može se prikazati u obliku sume dva kvadrata ako i samo ako mu se u rastavu na proste faktore svi prosti brojevi oblika $4k+3$ pojavljuju s parnom potencijom.*

Dokaz: Nužnost slijedi iz Propozicije 2. Naime, ako je $p = 4k+3$ i $p|x^2+y^2$, onda $p|x$ i $p|y$. Stoga $p^2|n$, pa isto razmatranje možemo primijeniti na $\frac{n}{p^2}$, te dobivamo da se u rastavu od n prost broj p javlja s parnom potencijom.

Dovoljnost slijedi iz Propozicija 5 i 1. Zaista, n se može zapisati u obliku $n = m^2 \cdot n'$, gdje je n' produkt prostih brojeva oblika $4k+1$ (i možda broja 2). Iz Propozicija 5 i 1, matematičkom indukcijom slijedi da je n' suma dva kvadrata, recimo $n' = x^2+y^2$. No, tada je $n = (mx)^2 + (my)^2$. □

Teorem 2. *Prirodan broj n može se prikazati kao suma kvadrata tri cijela brojeva ako i samo ako n nije oblika $4^m(8k+7)$, $k, m \geq 0$.*

Nužnost se lako pokazuje, dok je dovoljnost znatno teža - u dokazu se koriste rezultati iz teorije ternarnih kvadratnih formi, te Dirichletov teorem o prostim brojevima u aritmetičkom nizu.

Teorem 3. *Svaki prirodan broj može se prikazati u obliku sume kvadrata četiri cijela broja.*

Dokaz: (skica) Koristi se Eulerov identitet:

$$\begin{aligned}
&(x^2+y^2+z^2+w^2)(a^2+b^2+c^2+d^2) \\
&= (ax+by+cz+du)^2 + (ay-bx+dz-cw)^2 \\
&+ (az-cx+bw-dy)^2 + (aw-dx+cy-bz)^2,
\end{aligned}$$

te slijedeće činjenice:
1) Ako p dijeli sumu 4 kvadrata, onda je on i sam suma 4 kvadrata.
2) Za svaki prosti broj p postoje cijeli brojevi x, y takvi da $p|x^2+y^2+1$. □

Primjer 1. *Označimo s $r_2(n)$ broj prikaza broja n u obliku sume kvadrata dva cijela broja. Dokazati da je $r_2(2n) = r_2(n)$ za svaki $n \in \mathbb{N}$.*

Rješenje: Ako je $x^2+y^2 = n$, onda je $(x+y)^2+(x-y)^2 = 2n$. Obratno, ako je $s^2+t^2 = 2n$, onda su s i t iste parnosti, pa je $\left(\frac{s+t}{2}\right)^2 + \left(\frac{s-t}{2}\right)^2 = n$. Prema tome, pridruživanje $(x, y) \mapsto (x+y, x-y)$ je bijekcija među prikazima od n i $2n$. ♢

Primjer 2. *Odrediti sve cijele brojeve koji se mogu prikazati kao razlika kvadrata dva cijela broja.*

Rješenje: To su svi oni cijeli brojevi koji nisu oblika $4k+2$.

Zaista, ako je $n \equiv 2 \pmod 4$ i $n = x^2 - y^2 = (x-y)(x+y)$, onda je jedan od faktora $x-y$, $x+y$ paran. No, onda je i drugi paran, pa $4|n$.

Obrnuto, ako $n \not\equiv 2 \pmod 4$, onda je ili $n = 2k+1$ ili $n = 4k$:

$$2k+1 = (k+1)^2 - k^2,$$

$$4k = (k+1)^2 - (k-1)^2.$$

$\diamondsuit$

Primjer 3. *Odrediti sve prirodne brojeve koji se mogu prikazati kao zbroj kvadrata dva prirodna broja.*

Rješenje: To su oni prirodni brojevi kod kojih u rastavu na proste faktore prosti brojevi oblika $4k+3$ imaju parne eksponente, te prost broj 2 ima neparan eksponent ili imaju barem jedan prosti faktor oblika $4k+1$.

Nužnost: Pretpostavimo da je $n = 2^{2\alpha}m^2 = a^2 + b^2$, gdje su svi faktori od m oblika $4k+3$, te neka je n najmanji prirodan broj s tim svojstvom. Ako je $\alpha > 0$, onda su a i b parni, pa bi i $2^{2(\alpha-1)}m^2 < n$ imao isto svojstvo. Dakle, $\alpha = 0$ i $m^2 = a^2 + b^2$. No, m ima prosti faktor p oblika $4k+3$, pa po Propoziciji 2, $p|a$ i $p|b$, te je $\left(\frac{m}{p}\right)^2 = \left(\frac{a}{p}\right)^2 + \left(\frac{b}{p}\right)^2$, što je opet u suprotnosti s minimalnošću od n.

Dovoljnost: Imamo da je $n = 2m^2$ ili $n = 2^{\alpha}m^2 l$, gdje je $\alpha \in \{0,1\}$, a l je produkt prostih faktora oblika $4k+1$. Ako je $n = 2m^2$, onda je $n = m^2 + m^2$. Broj l je suma kvadrata dva prirodna broja. Zaista, svi njegovi prosti faktori su takvi, a produkt dva neparna broja koji su sume kvadrata dva prirodna broja je i sam takav. Naime, ako je $p_1 = a^2 + b^2$, $p_2 = c^2 + d^2$, te a i c, odnosno b i d, iste parnosti, onda je $p_1 p_2 = (ad+bc)^2 + (ac-bd)^2$ i oba izraza u zagradama su različita od 0. Sada tvrdnja slijedi indukcijom po broju prostih faktora.

Dakle, $l = s^2 + t^2$, $s, t \in \mathbb{N}$, pa je $m^2 l = (ms)^2 + (mt)^2$, dok je $2m^2 l = (ms+mt)^2 + (ms-mt)^2$. Budući da je l neparan, imamo da je $s \neq t$. $\diamondsuit$

Primjer 4. *Neka je $n = 4^m(8k+7)$, $km \geq 0$. Dokazati da se n ne može prikazati u obliku $x^2 + y^2 + z^2$, $x, y, z \in \mathbb{Z}$.*

Rješenje: Pretpostavimo da tvrdnja nije točna, te da je n najmanji prirodan broj za kojeg tvrdnja ne vrijedi. Tada je

$$n = 4^m(8k+7) = x^2 + y^2 + z^2.$$

Kvadrat neparnog broja $(2a+1)^2 = 8\cdot\frac{a(a+1)}{2}+1$ daje ostatak 1 pri dijeljenju s 8. Ako među brojevima x, y, z ima 1, 2 ili 3 neparna broja, onda je $x^2+y^2+z^2$ oblika $4l+1$, $4l+2$ ili $8l+3$. No, n nema niti jedan od ovih oblika. Stogu su x, y, z svi parni: $x = 2x_1$, $y = 2y_1$, $z = 2z_1$. Sada je

$$\frac{n}{4} = x_1^2 + y_1^2 + z_1^2 = 4^{m-1}(8k+7),$$

što je u suprotnosti s minimalnošću od n. $\diamondsuit$

Primjer 5. *Neka je p neparan prost broj. Dokažati da postoje cijeli brojevi x, y takvi da $p|x^2+y^2+1$.*

Rješenje: Promotrimo brojeve

$$0^2,\ 1^2,\ 2^2,\ \ldots,\ (\frac{p-1}{2})^2.$$

Nikoja dva među njima nisu kongruentna modulo p. Isto vrijedi za brojeve

$$-1-0^2,\ -1-1^2,\ -1-2^2,\ \ldots,\ -1-(\frac{p-1}{2})^2.$$

Sve skupa imamo $\frac{p+1}{2}+\frac{p+1}{2} = p+1$ brojeva, pa po Dirichletovom principu dva među njima daju isti ostatakk pri dijeljenju s p. To znači da postoje $x, y \in \{0, 1, \ldots, \frac{p-1}{2}\}$ takvi da je $x^2 \equiv -1-y^2 \pmod{p}$, tj. $p|x^2+y^2+1$. $\diamondsuit$

Primjer 6. *Označimo s $r_4(n)$ broj prikaza broja n u obliku sume kvadrata četiri cijela broja. Dokažati da je $r_4(8n) = r_4(2n)$ za svali $n \in \mathbb{N}$.*

Rješenje: Ako je $8n = x_1^2+x_2^2+x_3^2+x_4^2$, onda su svi x_i parni. Zaista, ako su svi neparni, onda je $x_1^2+x_2^2+x_3^2+x_4^2 \equiv 4 \pmod{8}$, a ako su dva parna i dva neparna, onda je $x_1^2+x_2^2+x_3^2+x_4^2 \equiv 2 \pmod{4}$. Stoga je $2n = (\frac{x_1}{2})^2+(\frac{x_2}{2})^2+(\frac{x_3}{2})^2+(\frac{x_4}{2})^2$. Obratno, ako je $2n = y_1^2+y_2^2+y_3^2++y_4^2$, onda je $8n = (2y_1)^2+(2y_2)^2+(2y_3)^2+(2y_4)^2$. $\diamondsuit$

Primjer 7. *Dokazati da se broj 2^{2k+1}, $k \in \mathbb{N}$, ne može prikazati kao suma kvadrata četiri prirodna broja.*

Rješenje: Jedini prikaz broja 2 kao sume četiri kvadrata je $2 = 1^2+1^2+0^2+0^2$. Kao je $r_4(2^{2k+1}) = r_4(2^{2k-1}) = \cdots r_4(2^1)$, to je jedini prikaz broja 2^{2k+1} kao sume četiri kvadrata

$$2^{2k+1} = (2^k)^2+(2^k)^2+0^2+0^2.$$

$\diamondsuit$

Primjer 8. *Dokazati da se svaki prirodan broj $n > 169$ može prikazati kao suma kvadrata pet prirodnih brojeva.*

Rješenje: Zapišimo prirodan broj $n-169$ kao sumu kvadrata četiri cijela broja:

$$n - 169 = x_1^2 + x_2^2 + x_3^2 + x_4^2, \quad x_1 \geq x_2 \geq x_3 \geq x_4 \geq 0.$$

Ako su svi $x_i > 0$, onda zapišimo $169 = 13^2$. Ako je $x_4 = 0$ i $x_3 > 0$, onda zapišimo $169 = 12^2 + 5^2$, pa je $n = x_1^2 + x_2^2 + x_3^2 + 12^2 + 5^2$. Ako je $x_3 = x_4 = 0$ i $x_2 > 0$, onda zapišimo $169 = 12^2 + 4^2 + 3^2$. Konačno, ako je $x_2 = x_3 = x_4 = 0$, onda zapišimo $169 = 10^2 + 8^2 + 2^2 + 1^2$. $\diamondsuit$

Primjer 9. *Dokazati da se svaki cijeli broj n može na beskonačno mnogo načina prikazati u obliku $n = x^2 + y^2 - z^2$.*

Rješenje:

$$(2k-1) = (2l^2 - k)^2 + (2l)^2 - (2l^2 - k + 1)^2,$$

$$2k = (2l^2 + 2l - k)^2 + (2l+1)^2 - (2l^2 + 2l - k + 1)^2.$$

$\diamondsuit$

Primjer 10. *Dokazati da se svaki prirodan broj n može prikazati u obliku $x^2 + 2y^2 + 3z^2 + 6t^2$, gdje su $x, y, z, t \in \mathbb{Z}$.*

Rješenje: Znamo da se n može prikazati u obliku $n = a^2 + b^2 + c^2 + d^2$. Možemo pretpostaviti da je pritom $a + b + c \equiv 3 \pmod 3$ i $a \equiv b \pmod 2$. Stavimo: $a + b + c+ = 3z$, $a + b = 2k$, $a - b = 2y$, pa imamo

$$3(a^2 + b^2 + c^2) = (a + b + c)^2 + 2(k - c)^2 + 6y^2.$$

Odavde slijedi da $3|k - c$, tj. $k - c = 3t$, pa dobivamo

$$a^2 + b^2 + c^2 = 3z^2 + 6t^2 + 2y^2.$$

$\diamondsuit$

Primjer 11. *Ako prirodan broj n nije suma kvadrata dva cijela broja, onda n nije niti suma kvadrata dva racionalna broja.*

Rješenje: Ako n nije suma dva kvadrata, onda n ima prosti faktor oblika $4k + 3$ koji ga dijeli s neparnom potencijom. Pretpostavimo da je $n = (\frac{a}{b})^2 + (\frac{c}{d})^2$. Tada je $n(bd)^2 = (ad)^2 + (bc)^2$. No, p se pojavljuje s neparnom potencijom na lijevoj strani jednakosti, pa smo dobili kontradikciju. $\diamondsuit$