Prikaz prirodnih brojeva u obliku sume potencija cijelih brojeva

Štengl, Marijana

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni nastavnički studij matematike i informatike

Marijana Štengl

Prikaz prirodnih brojeva u obliku sume potencija cijelih brojeva

Diplomski rad

Osijek, 2019.

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni nastavnički studij matematike i informatike

Marijana Štengl

Prikaz prirodnih brojeva u obliku sume potencija cijelih brojeva

Diplomski rad

Mentor: doc. dr. sc. Ivan Soldo

Osijek, 2019.

Sadržaj

Uvod

Problemom zapisivanja brojeva u obliku sume potencija bavili su se mnogi matematičari kroz povijest. Prvi zapisi u kojima se pojavljuju sume dva kvadrata prirodnih brojeva datiraju iz 2000. godine prije Krista ispisani na glinenim pločicama Babilonaca. Nakon toga, sličan se problem javlja u 3. stoljeću poslije Krista u djelu *„Arithmetica“* Diofanta Aleksandrijskog. Iako bez dokaza, Diofant daje točnu tvrdnju o prikazu brojeva u obliku sume dva kvadrata. Sličnim se pitanjem bavio i francuski matematičar Pierre de Fermat u 17. stoljeću koji iskazuje tvrdnju da svaki prost broj oblika $4k + 1$, $k \in \mathbb{N}$, ima jedinstven prikaz kao zbroj dva kvadrata prirodnih brojeva, ali također bez dokaza. Potpuna karakterizacija brojeva koji se mogu zapisati kao suma kvadrata dva cijela broja pripisuje se Fermatu, iako ju dokazuje švicarski matematičar Leonhard Euler tek nakon više od 100 godina. Osim ovoga, Fermat i Euler doprinijeli su i proučavanju problema prikaza brojeva u obliku sume kvadrata četiri cijela broja za čiju karakterizaciju potpuni dokaz daje matematičar Joseph-Louis Lagrange u 18. stoljeću. U isto vrijeme, pokušavajući generalizirati ovaj problem, engleski matematičar Edward Waring iskazuje tvrdnju, poznatiju pod nazivom *Waringov problem*, da se svaki prirodan broj može zapisati kao suma fiksnog broja nenegativnih k-tih potencija za bilo koji prirodan broj k.

Na početku ovoga rada ponovit ćemo osnovne rezultate teorije brojeva koji će biti potrebni u daljnjim razmatranjima. U drugom ćemo poglavlju okarakterizirati prirodne brojeve koji se mogu zapisati u obliku sume kvadrata dva cijela broja i to počevši s prostim brojevima kojima ćemo posebno posvetiti pažnju. Osim toga, navest ćemo i formule za određivanje broja prikaza u obliku sume kvadrata dva cijela broja. Nadalje, u trećem ćemo poglavlju navesti rezultate vezane za oblike prirodnih brojeva koji se (ne)mogu zapisati kao suma kvadrata tri cijela broja. U četvrtom ćemo se poglavlju najprije baviti prirodnim brojevima koji se mogu zapisati u obliku sume kvadrata četiri cijela broja, a zatim i četiri prirodna broja, te navesti formulu za određivanje broja takvih prikaza, dok ćemo u petom poglavlju iskazati teoreme koji govore koji se brojevi ne mogu zapisati u obliku sume kvadrata pet ili više prirodnih brojeva. U šestom poglavlju prelazimo na razmatranje prikaza u obliku sume kubova cijelih brojeva gdje ćemo navesti koji se prirodni brojevi ne mogu zapisati u navedenom obliku. U posljednjem ćemo poglavlju navesti poopćenje dotad iskazanih važnih teorema, tzv. Waringov problem (teorem). Radi boljeg razumijevanja sve ćemo važnije rezultate potkrijepiti primjerima.

1 Osnovni pojmovi i tvrdnje

Kako bismo pristupili razmatranju problema prikazivanja prirodnih brojeva u obliku sume potencija cijelih brojeva, navest ćemo osnovne definicije, propozicije i teoreme teorije brojeva koji su neophodni za daljnje razumijevanje i praćenje rada. Detalji i dokazi navedenih rezultata mogu se vidjeti primjerice u [6] i [8].

1.1 Djeljivost

Definicija 1. *Neka su $a, b \in \mathbb{Z}$, $a \neq 0$. Kažemo da a dijeli b, i pišemo $a|b$, ako postoji $d \in \mathbb{Z}$ takav da je $b = a \cdot d$. Ako a ne dijeli b, pišemo $a \nmid b$.*

Propozicija 1. (vidjeti [8, Propozicija 1.1.1.]) *Neka su $a, b, c \in \mathbb{Z}$, $a \neq 0$.*

(*i*) *Ako $a|b$ i $b \neq 0$, tada je $|a| \leqslant |b|$.*

(*ii*) *Ako je a djelitelj broja b, tada je a djelitelj i svakog višekratnika od b.*

(*iii*) *Ako je a djelitelj brojeva b i c, tada je djelitelj i brojeva $b + c$, $b - c$ i $b \cdot c$.*

Teorem 1. (vidjeti [6, Teorem 1.1]) *Za proizvoljan prirodan broj a i cijeli broj b postoje jedinstveni cijeli brojevi q i r takvi da je $b = q \cdot a + r$, $0 \leqslant r < a$.*

Korolar 1. *Svaki se cijeli broj za neki $a \in \mathbb{N}$ može prikazati u jednom od oblika aq, $aq + 1$, $aq + 2$, $\ldots$, $aq + (a - 1)$, $q \in \mathbb{Z}$.*

Definicija 2. *Neka su b i c cijeli brojevi. Cijeli broj $a \neq 0$ zovemo zajednički djelitelj od b i c ako $a|b$ i $a|c$. Ako je barem jedan od brojeva b i c različit od nule, onda postoji samo konačno mnogo zajedničkih djelitelja od b i c. Najveći među njima zove se najveći zajednički djelitelj od b i c i označava se s (b, c).*

Za prirodan broj $n > 1$ kažemo da je prost ako nema ni jednog djelitelja d za koji vrijedi $1 < d < n$. Stoga prost broj p ima točno dva pozitivna djelitelja, a to su brojevi 1 i p. Ako broj nije prost, kažemo da je složen, pri čemu za broj 1 kažemo da nije ni prost ni složen. Pojam prostih brojeva jedan je od ključnih pojmova zbog činjenice što se svaki prirodan broj $n > 1$ može zapisati kao produkt prostih faktora što je ključno za dokazivanje nekih važnih teorema u radu.

Definicija 3. *Ako je $(a, b) = 1$ kažemo da su cijeli brojevi a i b relativno prosti.*

Uočimo da je najveći zajednički djelitelj d uvijek prirodan broj te da vrijedi i sljedeće: ako je $(a,b)=d$, onda postoje cijeli brojevi a_1 i b_1 takvi da je $a=da_1$ i $b=db_1$, pri čemu su a_1 i b_1 relativno prosti. Primjerice, $(36,78)=6$, $36=6\cdot 6$, $78=6\cdot 13$ i $(6,13)=1$.

Lema 1. (vidjeti [8, Lema 1.4.1.]) *Neka je p prost broj te neka su a i b prosti brojevi takvi da $p|ab$. Tada $p|a$ ili $p|b$.*

Prethodna se lema može poopćiti na produkt proizvoljno mnogo faktora, tj. ako $p|a_1a_2\cdot\ldots\cdot a_n$, onda $p|a_i$ za neki $i\in\{1,2,\ldots,n\}$.

Teorem 2. (**Osnovni teorem aritmetike**, vidjeti [8, Teorem 1.4.3.]) *Svaki se prirodan broj $n>1$ može na jedinstven način prikazati u obliku produkta potencija prostih faktora, pri čemu je faktorizacija jedinstvena do na poredak faktora.*

Prethodni nam teorem govori da se svaki $n\geqslant 2$, $n\in\mathbb{N}$, može zapisati na sljedeći način:

$$n=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_k^{\alpha_k},$$

pri čemu je $k\in\mathbb{N}$, $p_1,p_2,\ldots,p_k$ različiti prosti brojevi i $\alpha_1,\alpha_2,\ldots,\alpha_k\in\mathbb{N}$. Ovakav se prikaz naziva kanonski rastav broja n na proste faktore, a prikladan je za određivanje djeljivosti.

Propozicija 2. (vidjeti [8, Propozicija 1.4.4.]) *Neka su $a=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_k^{\alpha_k}$ i $b=q_1^{\beta_1}\cdot q_2^{\beta_2}\cdot\ldots\cdot q_l^{\beta_l}$ prirodni brojevi dani svojim kanonskim rastavom na proste faktore. Kažemo da je broj a djeljiv brojem b ako i samo ako za svaki q_j, $j\in\{1,2,\ldots,l\}$, postoji $i\in\{1,2,\ldots,k\}$ tako da je $q_j=p_i$ i $\alpha_i\geqslant\beta_j$.*

Pojam koji će nam biti koristan pri određivanju broja prikaza prirodnog broja u obliku sume kvadrata četiri cijela broja je *suma svih pozitivnih djelitelja prirodnog broja n* koju ćemu označavati sa $\sigma(n)$. Budući da su jedini pozitivni djelitelji prostog broja p broj 1 i on sam, vrijedi sljedeća formula:

$$\sigma(p^k)=1+p+p^2+p^3+\ldots+p^k=\frac{1-p^{k+1}}{1-p}.$$

Primjer 1. $\sigma(13^2)=\frac{1-13^3}{1-13}=183$.

Definicija 4. *Kažemo da je funckija $f\colon\mathbb{N}\to\mathbb{C}$ multiplikativna ako vrijedi:*

(*i*) $f(1)=1$,

(*ii*) $f(m \cdot n) = f(m) \cdot f(n)$, *gdje je* $(m, n) = 1$.

Može se pokazati da je funkcija σ multiplikativna (vidjeti [8, Poglavlje 1, §4]). Nadalje, ako je dan kanonski rastav prirodnog broja n na proste faktore, onda, budući da je σ multiplikativna, vrijedi

$$\sigma(n) = \sigma(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}) = \prod_{j=1}^{k} \frac{1 - p_j^{\alpha_j+1}}{1 - p_j}. \tag{1}$$

Primjer 2. $\sigma(392) = \sigma(2^3 \cdot 7^2) = \frac{1-2^4}{1-2} \cdot \frac{1-7^3}{1-7} = 855.$

1.2 Kongruencije

Definicija 5. *Neka su* $n, a, b \in \mathbb{Z}$, $n \neq 0$. *Ako* $n|a - b$, *kažemo da je* a *kongruentan* b *modulo* n *i pišemo* $a \equiv b \pmod{n}$.

Općenito, modul n iz prethodne definicije može biti cijeli broj različit od nule, ali budući da je razlika $a-b$, $a, b \in \mathbb{Z}$, djeljiva s n i s $-n$ ograničavamo se na prirodne module.

Napomena 1. *Neka je* $n \in \mathbb{N}$, $a \in \mathbb{Z}$. *Ako* $n|a$, *onda* $a \equiv 0 \pmod{n}$.

Propozicija 3. (vidjeti [8, Propozicija 2.1.3.])

(*i*) *Neka su* $a, a', b, b' \in \mathbb{Z}$ *i* $n \in \mathbb{N}$. *Ako je* $a \equiv a' \pmod{n}$ *i* $b \equiv b' \pmod{n}$, *onda je* $a \pm b \equiv a' \pm b' \pmod{n}$ *i* $ab \equiv a'b' \pmod{n}$.

(*ii*) *Neka su* $a, b, c \in \mathbb{Z}$, $n \in \mathbb{N}$ *i* $(a, n) = 1$. *Ako je* $ab \equiv ac \pmod{n}$ *tada je* $b \equiv c \pmod{n}$.

Teorem 3. (**Wilsonov teorem**, vidjeti [8, Teorem 2.3.1.]) *Ako je* p *prost broj onda je*

$$(p-1)! \equiv -1 \pmod{p}. \tag{2}$$

Također vrijedi i obrat Wilsonovog teorema, što nam daje karakterizaciju prostih brojeva. Točnije, ako $n \in \mathbb{N}$ zadovoljava kongruenciju (2) onda je n prost broj.

1.3 Kvadratni ostaci

Definicija 6. *Neka je $n \in \mathbb{N}$, $n > 1$. Skup $S = \{a_1, a_2, \ldots, a_n\}$ naziva se potpuni sustav ostataka modulo n ako za svaki cijeli broj b postoji jedinstveni $a_i \in S$ za koji je $b \equiv a_i \pmod{n}$.*

Za potpuni sustav ostataka najčešće se koristi skup $S = \{1, 2, 3, \ldots, n-1\}$. Općenito ih postoji beskonačno mnogo, ali svi imaju jednak broj elemenata.

Primjer 3. *Potpuni sustav ostataka modulo 8 je skup $S = \{1, 2, 3, 4, 5, 6, 7\}$, ali i skup $S = \{9, 18, 11, 4, 5, 6, -1\}$, i skup $S = \{1, 2, -5, 20, 5, -2, 7\}$.*

Definicija 7. *Neka je $n \in \mathbb{N}$, $n > 1$. Skup $S = \{a_1, a_2, \ldots, a_n\}$ se naziva reducirani sustav ostataka modulo n ako za svaki cijeli broj b koji je relativno prost s n, postoji jedinstveni $a_i \in S$ za koji je $b \equiv a_i \pmod{n}$.*

Reducirani sustav ostataka možemo dobiti tako da iz potpunog sustava ostataka modulo n izbacimo elemente koji nisu relativno prosti s n. Dakle, i njih ima beskonačno mnogo i svaki od njih ima jednak broj elemenata.

Primjer 4. *Reducirani sustav ostataka modulo 8 je primjerice skup $S = \{1, 3, 5, 7\}$, ali i skup $S = \{-7, 19, -11, 23\}$.*

Definicija 8. *Neka je $a \in \mathbb{Z}$, $n \in \mathbb{N}$ i $(a, n) = 1$. Ako kongruencija $x^2 \equiv a \pmod{n}$ ima rješenja, kažemo da je a kvadratni ostatak modulo n. U suprotnom kažemo da je a kvadratni neostatak modulo n.*

Primjer 5. *Odredimo sve kvadratne ostatke modulo 13.*

Rješenje: Reducirani sustav ostataka modulo 13 je skup $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$.

$$1^2 \equiv 1 \pmod{13}, \qquad 7^2 \equiv 10 \pmod{13},$$
$$2^2 \equiv 4 \pmod{13}, \qquad 8^2 \equiv 12 \pmod{13},$$
$$3^2 \equiv 9 \pmod{13}, \qquad 9^2 \equiv 3 \pmod{13},$$
$$4^2 \equiv 3 \pmod{13}, \qquad 10^2 \equiv 9 \pmod{13},$$
$$5^2 \equiv 12 \pmod{13}, \qquad 11^2 \equiv 4 \pmod{13},$$
$$6^2 \equiv 10 \pmod{13}, \qquad 12^2 \equiv 1 \pmod{13}.$$

Kvadratni ostaci modulo 13 su 1, 3, 4, 9, 10 i 12. Ostali brojevi iz reduciranog sustava ostataka, 2, 5, 6, 7, 8 i 11, kvadratni su neostaci modulo 13. Uočimo da ima točno 6 ($6 = \frac{13-1}{2}$) kvadratnih ostataka, a isto toliko i kvadratnih neostataka modulo 13. To vrijedi i općenito za svaki neparan prost broj, o čemu govori sljedeća propozicija.

Propozicija 4. (vidjeti [6, Teorem 3.1.]) *Neka je p neparan prost broj. Reducirani sustav ostataka modulo p sastoji od $\frac{p-1}{2}$ kvadratnih ostataka i $\frac{p-1}{2}$ kvadratnih neostataka.*

Teorem 4. (**Mali Fermatov teorem**, vidjeti [6, Teorem 2.10]) *Neka je p prost broj. Ako $p \nmid a$ onda je $a^{p-1} \equiv 1 \pmod{p}$.*

2 Suma kvadrata dva cijela broja

U ovome ćemo se poglavlju baviti pitanjem: "koji se prirodni brojevi mogu zapisati u obliku sume kvadrata dva cijela broja?", tj. za koje $n \in \mathbb{N}$ jednadžba

$$n = x^2 + y^2$$

ima rješenja $x, y \in \mathbb{Z}$, te na koliko se načina broj n može zapisati u navedenom obliku. Točnije, najprije ćemo dati karakterizaciju prirodnih brojeva koji se mogu zapisati u obliku sume kvadrata dva cijela odnosno prirodna broja, zatim kao suma dva relativno prosta prirodna broja, a na kraju i formule za određivanje broja prikaza prirodnog broja u obliku sume kvadrata dva cijela broja.

Promotrimo prvih 10 prirodnih brojeva:

$$\begin{aligned} 1 &= 0^2 + (\pm 1)^2, & 6,& \\ 2 &= (\pm 1)^2 + (\pm 1)^2, & 7,& \\ 3,& & 8 &= (\pm 2)^2 + (\pm 2)^2, \\ 4 &= 0^2 + (\pm 2)^2, & 9 &= 0^2 + (\pm 3)^2, \\ 5 &= (\pm 1)^2 + (\pm 2)^2, & 10 &= (\pm 1)^2 + (\pm 3)^2. \end{aligned}$$

Očito se ne mogu svi prirodni brojevi zapisati kao suma kvadrata dva cijela broja, a nas zanima koja svojstva moraju imati da bi mogli. Također, uočimo da se ne mogu svi brojevi koje smo zapisali kao sumu kvadrata dva cijela broja, zapisati i kao suma kvadata dva prirodna broja (npr. broj 4), te da općenito ovakav zapis ne mora biti jedinstven. Upravo navedene činjenice razmatrat ćemo u ovome poglavlju.

2.1 Prikaz prostih brojeva u obliku sume kvadrata dva cijela broja

Radi slijednog uvođenja i dokazivanja važnih teorema, najprije ćemo problem promotriti u skupu prostih brojeva. Stoga, promotrimo prvih nekoliko prostih brojeva koji se mogu zapisati kao suma kvadrata dva cijela broja.

$$2 = 1^2 + 1^2,$$

$$5 = 1^2 + 2^2,$$

$$13 = 2^2 + 3^2,$$

$$17 = 1^2 + 4^2,$$

$$29 = 2^2 + 5^2.$$

"Na prste" možemo provjeriti da se prosti brojevi 3, 7, 11, 19 i 23 ne mogu zapisati u ovome obliku. Nadalje, uočimo da su brojevi 5, 13, 17 i 29 kongruentni 1 modulo 4, tj. mogu se zapisati u obliku $4k+1$, $k \in \mathbb{N}$, dok su brojevi 3, 7, 11, 19 i 23 oblika $4k+3$, $k \in \mathbb{Z}$. Možemo naslutiti da će se neparni prosti brojevi moći zapisati kao suma kvadrata dva cijela broja ako su oblika $4k+1$, $k \in \mathbb{N}$, dok za proste brojeve oblika $4k+3$, $k \in \mathbb{Z}$, to neće vrijediti. Međutim, vrijedi i općenitija tvrdnja:

Propozicija 5. (vidjeti [7, Propozicija 2.]) *Prirodni brojevi oblika $4k+3$, $k \in \mathbb{Z}$, ne mogu se zapisati u obliku sume kvadrata dva cijela broja.*

Dokaz: Neka su x i y cijeli brojevi. Tada vrijedi $x^2, y^2 \equiv 0, 1 \pmod 4$. Stoga je $x^2 + y^2 \equiv 0, 1, 2 \pmod 4$ pa suma kvadrata dva cijela broja ne može biti oblika $4k+3$, $k \in \mathbb{Z}$. □

Kako bismo dokazali karakterizaciju prostih brojeva koji se mogu zapisati kao suma kvadrata dva cijela broja, dokažimo najprije nekoliko pomoćnih tvrdnji.

Propozicija 6. (vidjeti [1, (8.7) Lemma]) *Neka su n_1 i n_2 sume kvadrata dva cijela broja. Tada je i njihov produkt suma kvadrata dva cijela broja.*

Dokaz: Neka je $n_1 = x_1^2 + y_1^2$ i $n_2 = x_2^2 + y_2^2$.

$$\begin{aligned} n_1 \cdot n_2 &= (x_1^2 + y_1^2)(x_2^2 + y_2^2) \\ &= (x_1x_2)^2 + (y_1 + y_2)^2 + (x_1y_2)^2 + (y_1x_2)^2 + 2x_1x_2y_1y_2 - 2x_1x_2y_1y_2 \\ &= (x_1x_2 + y_1y_2)^2 + (x_1y_2 - y_1x_2)^2. \end{aligned}$$

Analogno vrijedi i:

$$n_1 \cdot n_2 = (x_1x_2 - y_1y_2)^2 + (x_1y_2 + y_1x_2)^2.$$

□

Napomena 2. *Prethodna se tvrdnja može poopćiti na produkt konačno mnogo prirodnih brojeva.*

Napomena 3. *Uočimo da je jednakost $n = x^2 + y^2$ povezana s kompleksnim brojevima, točnije s modulom kompleksnog broja:*

$$|x + yi|^2 = x^2 + y^2,$$

te da tvrdnju Propozicije 6 možemo zapisati kao

$$|z_1|^2 \cdot |z_2|^2 = |z_1 \cdot z_2|^2,$$

za $z_1 = x_1 + y_1 i$, $z_2 = x_2 + y_2 i$.

Propozicija 7. (vidjeti [1, Propozicija 2.]) *Neka je p prost broj oblika $4k+3$, $k \in \mathbb{Z}$, i n prirodan broj djeljiv s p.*

(*i*) *Ako $p|x^2 + y^2$, onda $p|x$ i $p|y$.*

(*ii*) *Ako je $n = x^2 + y^2$, onda se p u rastavu broja n na proste faktore pojavljuje s parnim eksponentom.*

Dokaz:

(i) Pretpostavimo suprotno, tj. neka $p|x^2 + y^2$ i $p \nmid x$, $p \nmid y$. Jer $p|x^2 + y^2$, onda je $x^2 \equiv -y^2 \pmod{p}$. Podignemo li prethodnu kongruenciju na $\frac{p-1}{2}$ imamo $x^{p-1} \equiv (-1)^{\frac{p-1}{2}} \cdot y^{p-1} \pmod{p}$. Kako $p \nmid x$ i $p \nmid y$, primjenom Malog Fermatovog teorema slijedi da je $1 \equiv (-1)^{\frac{p-1}{2}} \cdot 1 \pmod{p}$, a kako je p oblika $4k + 3$, $k \in \mathbb{Z}$, to je $\frac{p-1}{2} = \frac{4k+3-1}{2} = \frac{4k+2}{2} = 2k + 1$, te je $(-1)^{2k+1} = -1$ pa dobivamo $1 \equiv -1 \pmod{p}$ što nije moguće. Dakle, $p|x$ i $p|y$.

(ii) Neka je $n = x^2+y^2$. Iz (i) slijedi da $p|x$ i $p|y$, stoga, $p^2|x^2$ i $p^2|y^2$, tj. $p^2|x^2+y^2 = n$. Dakle, n možemo zapisati kao $n = p^2 \cdot n_1$. Podijelimo li jednakost $n = x^2+y^2$ s p^2 imamo $n_1 = \left(\frac{x}{p}\right)^2 + \left(\frac{y}{p}\right)^2$. Ako $p|n_1$, koji je suma kvadrata dva cijela broja, analogno se dobiva da $p^2|n_1$. Nastavljajući ovaj postupak dobijemo da je n djeljiv samo parnim potencijama od p pa slijedi tvrdnja. □

Kako bismo dokazali neke od sljedećih rezultata prisjetimo se Fermatove metode beskonačnog spusta. Ona se bazira na tvrdnji da svaki neprazan podskup skupa prirodnih brojeva ima najmanji element tj. da ne postoji strogo opadajući niz prirodnih brojeva. Stoga, ako želimo pokazati da ne postoji prirodan broj koji zadovoljava neko svojstvo dovoljno je pokazati da iz pretpostavke da neki prirodan

broj to svojstvo zadovoljava, slijedi da postoji i manji prirodan broj s tim istim svojstvom, a takvo beskonačno spuštanje ne dozvoljava struktura skupa prirodnih brojeva. Dakle, koristimo metodu kontradikcije, a možemo reći i da je Fermatova metoda jedan oblik indukcije.

Propozicija 8. (vidjeti [7, Propozicija 3.]) *Ako prost broj p dijeli sumu dva kvadrata cijelih brojeva $x^2 + y^2$, $(x, y) = 1$, onda je p i sam suma kvadrata dva cijela broja.*

Dokaz: Dokaz provedimo primjenom prethodno navedene metode. Neka je $p \cdot k$, $k \in \mathbb{N}$, najmanji višekratnik od p takav da

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

Neka je

$$\begin{aligned} x &\equiv a \pmod{p}, \\ y &\equiv b \pmod{p}, \end{aligned}$$

pri čemu je $|a|,\ |b| \leqslant \frac{p}{2}$. Tada je

$$a^2 + b^2 \equiv x^2 + y^2 \equiv 0 \pmod{p},$$

$a^2,\ b^2 \leqslant \frac{p^2}{4}$, te $a^2 + b^2 \leqslant p \cdot \frac{p}{2}$. Stoga mora vrijediti $1 \leqslant k \leqslant \frac{p}{2}$. Budući da želimo pokazati da je $k = 1$, pretpostavimo suprotno, tj. neka je $k > 1$. Neka je nadalje

$$\begin{aligned} x &\equiv u \pmod{k}, \\ y &\equiv v \pmod{k}, \end{aligned}$$

$|u|,|v| \leqslant \frac{k}{2}$. Analogno je $u^2 + v^2 \equiv 0 \pmod{k}$ i $u^2 + v^2 \leqslant k \cdot \frac{k}{2}$. Neka je npr. $u^2 + v^2 = kl$, $l \in \mathbb{N}$. Tada je $1 \leqslant l \leqslant \frac{k}{2} < k$. Sada imamo dva broja, pk i kl, koji su suma kvadrata dva cijela broja, te po Propoziciji 6 imamo sljedeću jednakost:

$$pk^2 l = (x^2 + y^2)(u^2 + v^2) = (xu + yv)^2 + (xv - yu)^2. \tag{3}$$

Kako je

$$xu + yv \equiv x^2 + y^2 \equiv 0 \pmod{k},$$

postoji x_1 takav da je $xu + yv = x_1 k$. Također, jer je

$$xv - yu \equiv xy - xy \equiv 0 \pmod{k},$$

postoji y_1 takav da je $xv - yu = y_1 k$. Sada iz (3) slijedi

$$pl = \frac{(xu + yv)^2 + (xv - yu)^2}{k^2},$$

a iz prethodnih je jednakosti:

$$pl = x_1^2 + y_1^2.$$

Ako je $(x_1, y_1) = d$, onda je $x_1 = dx_2$, $y_1 = dy_2$, te je

$$p \cdot \frac{l}{d^2} = x_2^2 + y_2^2$$

i $\frac{l}{d^2} \leqslant l < k$, što nije moguće jer smo pretpostavili da je k najmanji takav. Dakle, $k = 1$, te je $p = x^2 + y^2$. □

Propozicija 9. *Ako neparan prost broj p dijeli sumu kvadrata relativno prostih prirodnih brojeva, onda je p oblika $4k + 1$, $k \in \mathbb{N}$.*

Dokaz: Slijedi iz Propozicija 8 i 5. □

Propozicija 10. (vidjeti [7, Propozicija 4.]) *Neka je p prost broj oblika $4k + 1$, $k \in \mathbb{N}$. Tada postoji prirodan broj x takav da $p|x^2 + 1$.*

Dokaz: Kako bismo dokazali ovu tvrdnju iskoristit ćemo Wilsonov teorem. Budući da je $p = 4k + 1$, $k \in \mathbb{N}$, (neparan), onda je

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

Stoga za x možemo uzeti $x = \left(\frac{p-1}{2}\right)!$ pa iz prethodne kongruencije slijedi $p|x^2+1$. □

Radi ilustracije prethodne propozicije, promotrimo sljedeći primjer.

Primjer 6. *Neka je dan prost broj 13 koji je za $k = 3$ oblika $4k+1$. Odredimo x iz prethodne tvrdnje.*

Rješenje:

$$\begin{aligned}(13-1)! = 12! &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \\ &\equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot (-6) \cdot (-5) \cdot (-4) \cdot (-3) \cdot (-2) \cdot (-1) \pmod{13} \\ &\equiv (1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6)^2 \pmod{13}.\end{aligned}$$

Dakle, $x = 6! = 720$. Zaista, $720^2 + 1 = 528401$, $528401 \equiv 0 \pmod{13}$.

Teorem 5. (vidjeti [7, Propozicija 5.]) *Prost broj p je suma kvadrata dva cijela broja ako i samo ako je $p = 2$ ili je p oblika $4k + 1$, $k \in \mathbb{N}$.*

Dokaz: Ako je $p = 2$, očito se može zapisati kao suma kvadrata dva cijela broja (npr. $2 = 1^2 + 1^2$). Nadalje, neka je $p \neq 2$ suma kvadrata dva cijela broja. Kako je p neparan prost broj, po Propoziciji 5 ne može biti oblika $4k + 3$, $k \in \mathbb{Z}$, pa p mora biti oblika $4k + 1$, $k \in \mathbb{N}$.
Obratno, neka je p oblika $4k + 1$, $k \in \mathbb{N}$. Tada po Propoziciji 10 postoji x takav da $p|x^2 + 1$, a kako je $(x, 1) = 1$, iz Propozicije 8 slijedi tvrdnja. □

Teorem 6. (vidjeti [7, Lema 2.]) *Prost broj p može se najviše na jedan način prikazati u obliku sume kvadrata dva prirodna broja.*

Dokaz: Pretpostavimo da se prost broj p može prikazati najmanje na dva načina u obliku sume kvadrata dva prirodna broja, tj.

$$p = m^2 + n^2 = k^2 + l^2, \tag{4}$$

gdje su m i k parni, a n i l neparni prirodni brojevi. Neka je $m-k = 2x$, $m+k = 2y$, $l - n = 2z$ i $l + n = 2u$. Sada, uvrštavajući u (4) dobivamo jednadžbu:

$$4xy = 4zu,$$

tj.

$$xy = zu,$$

čija su rješenja $x = ac$, $y = bd$, $z = ad$, $u = bc$, za neke $a, b, c, d \in \mathbb{N}$. Kako je $m = x+y$ i $n = u-z$, imamo $m = ac+bd$ i $n = bc-ad$, odakle je $p = (a^2+b^2)\cdot(c^2+d^2)$, što nije moguće jer je p prost broj. □

2.2 Prikaz prirodnih brojeva u obliku sume kvadrata dva cijela broja

Nakon karakterizacije prostih brojeva koji se mogu zapisati kao suma kvadrata dva cijela broja, poopćimo razmatranje na prirodne brojeve. Sljedeća nam dva teorema daju karakterizaciju prirodnih brojeva koji se mogu zapisati kao suma kvadrata dva cijela i kao suma kvadrata dva prirodna broja.

Teorem 7. (Fermat, Euler, 1749., vidjeti [9, Chapter XI, Theorem 1.]) *Prirodan broj n može se prikazati u obliku sume kvadrata dva cijela broja ako i samo ako se u faktorizaciji broja n na proste faktore svi prosti faktori oblika $4k+3$, $k \in \mathbb{Z}$, pojavljuju s parnim eksponentom.*

Dokaz: Nužnost teorema slijedi iz Propozicije 7.
Nadalje, dokažimo dovoljnost. Bez smanjenja općenitosti pretpostavimo da je $n > 1$ (budući da za 1 imamo $1 = 1^2 + 0^2$). Neka je

$$n = p_1^{\alpha 1} \cdot p_2^{\alpha 2} \cdot \ldots \cdot p_s^{\alpha s}$$

faktorizacija broja n na proste faktore pri čemu se svi prosti faktori oblika $4k+3$, $k \in \mathbb{Z}$, pojavljuju s parnim eksponentom, te m najveći prirodan broj takav da $m^2|n$. Tada postoji l takav da je $n = m^2 l$ pri čemu je $l = 1$ ili je produkt različitih prostih faktora p_i oblika $4k+1$, $k \in \mathbb{N}$ (i eventualno broja 2, $2 = 1^2 + 1^2$). Prema Teoremu 5, svaki je od tih neparnih prostih faktora suma dva kvadrata prirodnih brojeva. Prema Napomeni 2 slijedi da je l, kao produkt faktora koji su sume dva kvadrata cijelih brojeva, također suma kvadrata dva cijela broja, npr. $l = u^2 + v^2$. Sada je

$$n = m^2 l = m^2(u^2 + v^2) = (mu)^2 + (mv)^2$$

pa slijedi tvrdnja. □

Primjer 7. *Ako je moguće prikažimo sljedeće brojeve u obliku sume kvadrata dva cijela broja:*

(*a*) *1805,*

(*b*) *1287,*

(*c*) *2025.*

Rješenje:

(a) Provjerimo najprije može li se broj 1805 zapisati kao suma kvadrata dva cijela broja.

$$1805 = 5 \cdot 19^2.$$

Budući da se u rastavu broja 1805 na proste faktore prost faktor 19 oblika $4k+3$ (za $k = 4$) javlja s parnim eksponentom, prema Teoremu 7 ima traženi prikaz. Slijedi: $m = 19$, $l = 5$,

$$1805 = 19^2 \cdot 5 = 19^2(1^2 + 2^2) = (19 \cdot 1)^2 + (19 \cdot 2)^2 = 19^2 + 38^2.$$

(b) Faktorizirajmo broj 1287 na proste faktore:

$$1287 = 3^2 \cdot 11 \cdot 13.$$

Budući da broj 1287 u faktorizaciji sadrži prost faktor 11, koji je oblika $4k+3$ za $k = 2$, s neparnim eksponentom, prema prethodnom se teoremu ne može zapisati kao suma kvadrata dva cijela broja.

(c) Faktorizirajmo broj 2025 na proste faktore:

$$2025 = 3^4 \cdot 5^2.$$

Prost faktor oblika $4k + 3$ je u ovome slučaju faktor 3 (za $k = 0$), no, on se javlja s parnim eksponentom, te se broj 2025, prema prethodnom teoremu, može zapisati kao suma kvadrata dva cijela broja. Sada je $m = 9$, a $l = 25$:

$$\begin{aligned} 25 &= 3^2 + 4^2, \\ 2025 &= 9^2 \cdot 25 = 9^2(3^2 + 4^2) \\ &= (9 \cdot 3)^2 + (9 \cdot 4)^2 \\ &= 27^2 + 36^2. \end{aligned}$$

Uočimo kako se, primjerice, broj 1 može zapisati kao suma kvadrata dva cijela broja ($1 = 1^2 + 0^2$), međutim, ne može se zapisati kao suma kvadrata dva prirodna broja. Sljedeći teorem daje jaču tvrdnju od prethodnog, a to je koji se prirodni brojevi mogu zapisati kao suma kvadrata dva prirodna broja.

Teorem 8. (vidjeti [9, Chapter XI, Theorem 2.]) *Prirodan broj n je suma kvadrata dva prirodna broja ako i samo ako se svi prosti faktori od n oblika $4k + 3$, $k \in \mathbb{Z}$, pojavljuju s parnim eksponentom te, ili se broj 2 javlja s neparnim eksponentom (u faktorizaciji broja n na proste faktore), ili n ima barem jedan prost faktor oblika $4k + 1$, $k \in \mathbb{N}$.*

Dokaz: Kako bismo dokazali nužnost koristimo metodu beskonačnog spusta. Neka je n prirodan broj koji je zbroj kvadrata dva prirodna broja i koji nije djeljiv prostim brojevima oblika $4k + 1$, $k \in \mathbb{N}$, te u faktorizaciji na proste faktore sadrži prost faktor 2 s parnim eksponentom koji je veći ili jednak 0. Također, neka je n najmanji prirodan broj s navedenim svojstvima. Prema Teoremu 7, svi se prosti faktori, u faktorizaciji od n, oblika $4k+3$, $k \in \mathbb{Z}$, pojavljuju s parnim eksponentom.

Stoga, možemo zapisati $n = 2^{2k}m^2$, pri čemu je m neparan prirodan broj, a $k \geqslant 0$ cijeli broj. Jer je n zbroj dva kvadrata prirodnih brojeva, može se zapisati kao

$$n = x^2 + y^2 = 2^{2k}m^2, \tag{5}$$

gdje su $x, y \in \mathbb{N}$. Ako je $k > 0$, onda je lijeva strana jednakosti (5) djeljiva s 4, pa su stoga x i y parni. Dakle, postoje $x_1, y_1 \in \mathbb{N}$ takvi da je $x = 2x_1$, $y = 2y_1$. Sada imamo:

$$\begin{aligned}(2x_1)^2 + (2y_1)^2 &= 2^{2k}m^2 / : 4\\ 2^{2(k-1)}m^2 &= x_1^2 + y_1^2 < n\end{aligned}$$

što je u kontradikciji s minimalnošću od n. Dakle, $k = 0$, te je stoga

$$n = m^2 = x^2 + y^2 > 1. \tag{6}$$

Uočimo da x i y moraju biti relativno prosti jer bi u suprotnom, za $(x, y) = d > 1$, imali $x = dx_2$, $y = dy_2$, $x_2, y_2 \in \mathbb{N}$, te iz jednakosti (6) da je $m = dm_1$ za neki $m_1 \in \mathbb{N}$ i $m_1 = x_2^2 + y_2^2 < m^2 = n$, što je ponovno u kontradikciji s minimalnošću od n. Budući da je $m > 1$ neparan te ne sadrži faktore oblika $4k + 1$, $k \in \mathbb{N}$, onda sadrži faktor oblika $p = 4k + 3$, $k \in \mathbb{Z}$. No, tada $p|x^2 + y^2$, a po Propoziciji 7 slijedi $p|x$ i $p|y$ što nije moguće jer su x i y relativno prosti. Stoga je dokazano da prirodan broj koji je suma kvadrata dva prirodna broja ima svojstvo da, ili se u faktorizaciji na proste faktore broj 2 javlja na neparan eksponent, ili ima prost faktor oblika $4k + 1$, $k \in \mathbb{N}$. Nadalje, prema Teoremu 7 svi se prosti faktori oblika $4k + 3$, $k \in \mathbb{Z}$, u faktorizaciji od n pojavljuju s parnim eksponentom. Time je nužnost dokazana.

Dokažimo sada dovoljnost. Pretpostavimo da prirodan broj n zadovoljava uvjete teorema. Imamo dva slučaja:

$$\begin{aligned}1^\circ\ & n = 2m^2,\\ 2^\circ\ & n = 2^\alpha m^2 l,\end{aligned}$$

gdje je $\alpha = 0$ ili $\alpha = 1$, $m \in \mathbb{N}$, a l produkt prostih faktora oblika $4k + 1$, $k \in \mathbb{N}$.
1° Ako je $n = 2m^2$, onda je $n = m^2 + m^2$ pa tvrdnja vrijedi.
2° Neka je $n = 2^\alpha m^2 l$. Iz Teorema 5 slijedi da je svaki prost faktor od l suma kvadrata dva prirodna broja (jer su oblika $4k + 1$, $k \in \mathbb{N}$), a prema Napomeni 2 slijedi da je i l suma kvadrata dva prirodna broja, primjerice $l = x^2 + y^2, x, y \in \mathbb{N}$. Odavde je

$$\begin{aligned}m^2 l &= (mx)^2 + (my)^2,\\ n = 2m^2 l &= (mx + my)^2 + (mx - my)^2.\end{aligned} \tag{7}$$

Kako je $l = x^2 + y^2$ neparan, to je $x \neq y$, pa je $mx - my \neq 0$. Dakle, n je suma kvadrata dva prirodna broja. □

Primjer 8. *Ako je moguće prikažimo sljedeće prirodne brojeve u obliku sume kvadrata dva prirodna broja:*

(*a*) *625,*

(*b*) *392,*

(*c*) *304.*

Rješenje: Kako bismo provjerili zadovoljavaju li navedeni brojevi uvjete teorema, najprije ih moramo faktorizirati na proste faktore.

(a) $625 = 5^4$.
Budući da 625 ne sadrži proste faktore oblika $4k + 3$, $k \in \mathbb{Z}$, te je jedini prost faktor oblika $4k + 1$, $k \in \mathbb{N}$, jednak 5, može se zapisati kao suma kvadrata dva prirodna broja. Imamo: $m = 5$, $l = 25$ (slučaj 2° u Teoremu 8).

$$\begin{aligned} 625 &= 2^0 \cdot 5^2 \cdot 25 \\ &= 5^2(3^2 + 4^2) \\ &= (5 \cdot 3)^2 + (5 \cdot 4)^2 \\ &= 15^2 + 20^2. \end{aligned}$$

(b) $392 = 2^3 \cdot 7^2$.
Broj 392 sadrži prost faktor 7 oblika $4k + 3$, za $k = 1$, koji se javlja s parnim eksponentom, dok se faktor 2 javlja s neparnim eksponentom, pa su uvjeti teorema zadovoljeni. Sada imamo slučaj 1° iz prethodnog teorema, tj.

$$\begin{aligned} 392 &= 2 \cdot (2 \cdot 7)^2 \\ &= 2 \cdot 14^2 = 14^2 + 14^2. \end{aligned}$$

(c) $304 = 2^4 \cdot 19$.
U rastavu broja 304 na proste faktore, osim što se faktor 2 javlja na paran eksponent i ne pojavljuju se faktori oblika $4k+1$, $k \in \mathbb{N}$, prost faktor 19 oblika $4k + 3$ ima neparan eksponent. Dakle, broj 304 se ne može zapisati kao suma kvadrata dva prirodna broja.

Iz prethodnog teorema možemo zaključiti da je prirodan broj n^2 suma kvadrata dva prirodna broja ako i samo ako n (zbog Napomene 2) ima barem jedan prost faktor oblika $4k+1$, $k \in \mathbb{N}$. Ovu tvrdnju možemo iskazati i na sljedeći način:

Korolar 2. (vidjeti [9, Chapter XI, §3]) *Prirodan broj n je hipotenuza pravokutnog trokuta ako i samo ako n ima barem jedan prost faktor oblika* $4k+1$, $k \in \mathbb{N}$. □

Primjer 9. *Promotrimo sljedeće Pitagorine trojke: (3,4,5), (9,12,15), (10,24,26), (12,35,37), (9,40,41). Uočimo da u svakoj od njih n (treća koordinata uređene trojke) ima prost faktor oblika* $4k+1$, $k \in \mathbb{N}$, *a to su redom: 5, 5, 13, 37 i 41.*

Korolar 3. (vidjeti [9, Chapter XI, Exercises 1.]) *Prirodan broj n je suma kvadrata dva različita prirodna broja ako i samo ako se prosti faktori (u faktorizaciji od n na proste faktore) oblika* $4k+3$, $k \in \mathbb{Z}$, *pojavljuju s parnim eksponentom i n ima barem jedan prost faktor oblika* $4k+1$, $k \in \mathbb{N}$.

Dokaz: Nužnost prvog uvjeta slijedi iz Teorema 7. Pretpostavimo da je n suma dva različita prirodna broja, $n = x^2+y^2$, $x \neq y$, i da nema prost faktor oblika $4k+1$, $k \in \mathbb{N}$. Neka je $(x,y) = d$, tj. $x = dx_1$, $y = dy_1$, $x_1, y_1 \in \mathbb{N}$, $(x_1, y_1) = 1$. Sada je $n = d^2(x_1^2 + y_1^2)$ te kako n nema prostih djelitelja oblika $4k+1$, $k \in \mathbb{N}$, nema ih ni $x_1^2 + y_1^2$, a kako su x_1 i y_1 relativno prosti, iz dokaza Teorema 8 slijedi da $x_1^2 + y_1^2$ nema ni prostog djelitelja oblika $4k+3$, $k \in \mathbb{Z}$. Dakle, $x_1^2 + y_1^2 = 2^s$, $s > 1$ (jer je $x_1 \neq y_1$). Odavde zaključujemo da je $x_1^2 + y_1^2$ djeljiv s 4, pa su stoga x_1, y_1 parni, što nije moguće jer su x_1 i y_1 relativno prosti. Time je nužnost teorema dokazana.

Obratno, neka je n prirodan broj kojemu se prosti faktori oblika $4k+3$, $k \in \mathbb{Z}$, pojavljuju s parnim eksponentom i koji ima barem jedan prost faktor oblika $4k+1$, $k \in \mathbb{N}$. Po Teoremu 8 slijedi da je n suma kvadrata dva prirodna broja, npr, x i y. Ako je $x \neq y$ tvrdnja je dokazana. Stoga, razmotrimo slučaj kada je $x = y$. Tada je $n = 2x^2$ te, budući da n ima prostog djelitelja oblika $4k+1$, $k \in \mathbb{N}$, ima ga i x. Prema Korolaru 3, x je hipotenuza pravokutnog trokuta, tj. $x^2 = a^2 + b^2$, $a, b \in \mathbb{N}$. Uočimo da mora vrijediti da je $a \neq b$ jer bi u suprotnom imali $x^2 = 2a^2$ što nije moguće jer je $\sqrt{2}$ iracionalan. Dakle, $n = 2x^2 = (a+b)^2 + (a-b)^2$ te je tvrdnja dokazana. □

Prisjetimo se sljedećih prikaza brojeva s početka poglavlja:

$$2 = 1^2 + 1^2, \quad 5 = 1^2 + 2^2, \quad 8 = 2^2 + 2^2, \quad 10 = 1^2 + 3^2.$$

Budući da brojevi 2 i 8 nemaju prost faktor oblika $4k+1$, $k \in \mathbb{N}$, ne mogu se zapisati kao suma kvadrata dva različita prirodna broja, dok brojevi 5 i 10 ($10 = 2 \cdot 5$) imaju, pa stoga imaju i navedeni prikaz.

2.2.1 Prikaz prirodnih brojeva u obliku sume kvadrata dva relativno prosta prirodna broja

Radi karakterizacije prirodnih brojeva koji su suma kvadrata dva relativno prosta prirodna broja, dokažimo najprije sljedeću propoziciju.

Propozicija 11. (vidjeti [9, Chapter V, §5, Lemma 2.]) *Ako su m i n dva neparna relativno prosta prirodna broja takva da se svaki od njih može prikazati u obliku sume kvadrata dva relativno prosta prirodna broja, onda njihov produkt mn ima barem dva različita prikaza u obliku sume kvadrata dva relativno prosta prirodna broja koji se ne razlikuju samo po poretku pribrojnika.*

Dokaz: Neka su m i n neparni relativno prosti prirodni brojevi i $a, b, c, d \in \mathbb{N}$ takvi da $(a, b) = (c, d) = 1$, $m = a^2 + b^2$, $n = c^2 + d^2$ i $a \geqslant b$, $c \geqslant d$. Tada je

$$mn = (ac + bd)^2 + (ad - bc)^2 = (ad + bc)^2 + (ac - bd)^2 \tag{8}$$

i

$$(ac + bd)(ad + bc) = cdm + abn. \tag{9}$$

Pokažimo da su prikazi produkta mn u (8) različiti. Mora vrijediti da je $ac + bd \neq ad + bc$ jer bi u suprotnom imali $(a-b)(c-d) = 0$, tj. $a = b$ ili $c = d$, što nije moguće jer bi tada m ili n bio paran. Također, da je $ac + bd = ac - bd$, imali bismo da je $bd = -bd$ što nije moguće jer su b i d prirodni brojevi. Pokažimo još da su ac+bd i ad-bc, te ad+bc i ac-bd relativno prosti. Pretpostavimo da je $(ac + bd, ad - bc) > 1$. Tada $ac + bd$ i $ad - bc$ imaju zajedničkog prostog djelitelja p. Iz (8) slijedi $p|mn$ pa stoga $p|m$ ili $p|n$.
1° Ako $p|m$ onda iz (9) slijedi $p|abn$, a kako su m i n relativno prosti, to $p|ab$. Dakle, $p|a$ ili $p|b$. No, jer smo pretpostavili da $p|m = a^2 + b^2$, onda iz Propozicije 7 slijedi $p|a$ i $p|b$ što nije moguće jer su a i b relativno prosti.
2° Ako $p|n$ onda iz (9) slijedi $p|cdm$, a kako su m i n relativno prosti, to $p|cd$. Analogno kao u prethodnom slučaju dobijemo da $p|c^2 + d^2$ tj. $p|c$ i $p|d$ što nije moguće. □

Napomena 4. *Prethodna se propozicija može poopćiti na produkt konačno mnogo neparnih relativno prostih faktora.*

Koristeći generalizaciju prethodno navedene propozicije (Napomenu 4) dokažimo karakterizaciju prirodnih brojeva koji se mogu zapisati u obliku sume kvadrata dva relativno prosta prirodna broja.

Teorem 9. (vidjeti [9, Chapter XI, Exercises 2.]) *Prirodan broj n može se zapisati u obliku sume kvadrata dva relativno prosta prirodna broja ako i samo ako nije djeljiv s 4, ni s bilo kojim prirodnim brojem oblika $4k+3$, $k \in \mathbb{Z}$.*

Dokaz: Neka je n suma kvadrata dva relativno prosta prirodna broja x i y. U slučaju da je n djeljiv s 4, onda bi x i y bili parni, što nije moguće jer su x i y relativno prosti. Nadalje, pretpostavimo da je n djeljiv prirodnim brojem oblika $4k+3$, $k \in \mathbb{Z}$. Tada n ima i prostog djelitelja toga oblika. Međutim, jer su x i y relativno prosti, a u dokazu Teorema 8 smo pokazali da prost broj oblika $4k+3$, $k \in \mathbb{Z}$, ne dijeli sumu kvadrata dva relativno prosta prirodna broja, dolazimo do kontradikcije.

Obratno, pretpostavimo da n zadovoljava uvjete teorema. Ako je $n = 2$, tvrdnja očito vrijedi jer je $2 = 1^2 + 1^2$. Stoga nadalje pretpostavimo da je $n > 2$. Tada se n, zbog uvjeta teorema, može zapisati u jednom od sljedeća dva oblika:

$$1^\circ\ n = p_1 \cdot p_2 \cdot \ldots \cdot p_s,$$
$$2^\circ\ n = 2 \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_t,$$

pri čemu su svi p_i prosti faktori oblika $4k+1$, $k \in \mathbb{N}$ i $s, t \in \mathbb{N}$.
Ako je n oblika kao u slučaju 1°, onda je neparan i produkt relativno prostih faktora oblika $4k+1$, $k \in \mathbb{N}$, koji se po Teoremu 5 mogu zapisati kao sume dva kvadrata prirodnih brojeva, pa iz Napomene 4 slijedi tvrdnja.
Nadalje, ako je n oblika kao u slučaju 2°, onda se može zapisati u sljedećem obliku:

$$n = 2(x^2 + y^2) = (x+y)^2 + (x-y)^2, \tag{10}$$

pri čemu su x i y relativno prosti prirodni brojevi (što smo dokazali u Teoremu 8). Kako je x^2+y^2 neparan (kao produkt neparnih faktora), to su x i y različite parnosti, pa su $x+y$ i $x-y$ neparni prirodni brojevi. Dokažimo još da su relativno prosti. Pretpostavimo da $(x+y, x-y) = d > 1$. Tada po Propoziciji 1 (*iii*) slijedi $d|2x$ i $d|2y$, no, jer je d neparan, kao djelitelj neparnih brojeva, onda $d|x$ i $d|y$ što nije moguće jer su x i y relativno prosti. □

Navedimo sada bez dokaza rezultat o jedinstvenosti prikaza prirodnih brojeva u obliku sume kvadrata dva relativno prosta prirodna broja.

Teorem 10. (vidjeti [1, Theorem 8.17]) *Prirodan broj $n > 2$ ima jedinstven prikaz u obliku sume kvadrata dva relativno prosta prirodna broja (do na poredak pribrojnika) ako i samo ako je $n = p^m$ ili $n = 2p^m$, gdje je p prost broj oblika $4k + 1$, $k \in \mathbb{N}$, i $m \geqslant 1$.*

Primjer 10. *Ako je moguće prikažimo sljedeće brojeve u obliku sume kvadrata dva relativno prosta prirodna broja:*

(a) *442,*

(b) *286,*

(c) *185.*

Rješenje: Kako bismo provjerili uvjete Teorema 9 faktorizirat ćemo najprije dane brojeve na proste faktore.

(a) $442 = 2 \cdot 13 \cdot 17$. Budući da su 13 i 17 oblika $4k + 1$ (za $k = 3$ i $k = 4$), broj 442 možemo zapisati kao sumu kvadrata dva relativno prosta prirodna broja, a postupamo kao u slučaju 2° Teorema 9 ($221 = 14^2 + 5^2$ iz (6)):

$$442 = 2 \cdot 221 = 2(14^2 + 5^2) = 19^2 + 9^2.$$

Zaista, $(19, 9) = 1$.

(b) $286 = 2 \cdot 11 \cdot 13$. Jer je 11 oblika $4k + 3$ za $k = 2$, broj 286 ne zadovoljava uvjete Teorema 9, pa se ne može zapisati kao suma kvadrata dva relativno prosta prirodna broja.

(c) $185 = 5 \cdot 37$. Oba su faktora oblika $4k + 1$ (za $k = 1$ i $k = 9$) pa broj 185 zadovoljava uvjete Teorema 9. Iz (6) slijedi

$$185 = 4^2 + 13^2.$$

2.3 Broj prikaza prirodnog broja u obliku sume kvadrata dva cijela broja

Nakon što smo okarakterizirali prirodne brojeve koji su suma kvadrata dva cijela broja, intuitivno se nameće pitanje na koliko se različitih načina prirodan broj može prikazati u tome obliku.

Neka je $N(n)$ ukupan broj svih prikaza prirodnog broja n kao sume kvadrata dva cijela broja. Pod izrazom "svih prikaza" podrazumjevat ćemo i slučajeve kada pribrojnici zamjene mjesta (tj. prikaze $n = x^2+y^2$ i $n = y^2+x^2$ smatramo različitima). Na početku ovoga poglavlja prikazali smo brojeve od 1 do 10 u obliku sume kvadrata dva cijela broja. Prisjetimo se primjerice:

$$5 = (\pm 1)^2 + (\pm 2)^2.$$

Uočimo da se broj 5 može na 8 načina prikazati kao suma kvadrata dva cijela broja:

$$\begin{aligned} 5 &= 1^2 + 2^2 = 2^2 + 1^2 = (-1)^2 + 2^2 = 2^2 + (-1)^2 \\ &= 1^2 + (-2)^2 = (-2)^2 + 1^2 = (-1)^2 + (-2)^2 = (-2)^2 + (-1)^2. \end{aligned}$$

Za brojeve od 1 do 10 vrijedi:

$$\begin{gathered} N(1) = 4,\ N(2) = 4,\ N(3) = 0,\ N(4) = 4,\ N(5) = 8, \\ N(6) = 0,\ N(7) = 0,\ N(8) = 4,\ N(9) = 4,\ N(10) = 8. \end{gathered}$$

Napomena 5. *Budući da svaki prost broj p oblika $4k+1$, $k \in \mathbb{N}$, prema Teoremu 6, ima jedinstven prikaz u obliku sume dva kvadrata prirodnih brojeva (ne uzimajući u obzir poredak pribrojnika), vrijedi $N(p) = 8$.*

Sljedeća dva teorema koji daju formule za određivanje broja prikaza prirodnog broja u obliku sume kvadrata dva cijela broja, navest ćemo bez dokaza. Sami dokazi mogu se vidjeti u [1].

Teorem 11. (vidjeti [1, Theorem 8.11]) *Pretpostavimo da se n može zapisati u obliku sume kvadrata dva cijela broja te neka je $n = 2^a \prod_i p_i^{a_i} \prod_i q_i^{b_i}$, pri čemu su p_i prosti brojevi oblika $4k+1$, $k \in \mathbb{N}$, i q_i prosti brojevi oblika $4k+3$, $k \in \mathbb{Z}$ (b_i parni). Tada vrijedi formula:*

$$N(n) = 4 \prod_i (a_i + 1). \tag{11}$$

Korolar 4. *Za proste brojeve p oblika $4k+1$, $k \in \mathbb{N}$, vrijedi formula:*

$$N(p^m) = 4(m+1).$$

Teorem 12. (**Jacobi**, vidjeti [1, Theorem 8.12]) *Neka je n prirodan broj, D_1 broj pozitivnih djelitelja od n oblika $4k+1$, $k \in \mathbb{N}$, te D_2 broj pozitivnih djelitelja od n oblika $4k+3$, $k \in \mathbb{Z}$. Tada vrijedi:*

$$N(n) = 4(D_1 - D_2).$$

Primjer 11. *Odredimo broj prikaza u obliku sume kvadrata dva cijela broja:*

(*a*) *3185,*

(*b*) *1805,*

(*c*) *625.*

Rješenje:

(a) $3185 = 5 \cdot 7^2 \cdot 13$. Prema Teoremu 7 broj 3185 može se zapisati kao suma kvadrata dva cijela broja. Odredimo sada ukupan broj takvih prikaza. Prosti faktori oblika $4k+1$ su 5 i 13, za $k = 1$ i $k = 3$, pa prema Teoremu 11 imamo:

$$N(3185) = 4(1+1)(1+1) = 16.$$

Iz (7) imamo: $3185 = 7^2 + 56^2$, ($m = 7$, $l = 65 = 1^2 + 8^2$), a ostale prikaze možemo dobiti pomoću Propozicije 6 i formule (7):

$$\begin{aligned} 3185 &= 13 \cdot 245 \\ 245 &= 5 \cdot 7^2 = 7^2(1^2 + 2^2) = 7^2 + 14^2 \\ 3185 &= (2^2 + 3^2)(7^2 + 14^2) = 28^2 + 49^2. \end{aligned}$$

Imamo:

$$\begin{aligned} 3185 &= (\pm 7^2) + (\pm 56^2) = (\pm 56)^2 + (\pm 7)^2 \\ &= (\pm 28^2) + (\pm 49^2) = (\pm 49)^2 + (\pm 28)^2. \end{aligned}$$

(b) U Primjeru 7 smo pokazali da se broj 1805 može prikazati kao suma kvadrata dva cijela broja ($1805 = 19^2 + 38^2$). Nadalje, kako 1805 u faktorizaciji ($1805 = 5 \cdot 19^2$) sadrži samo jedan prost faktor oblika $4k+1$, $k \in \mathbb{N}$, faktor 5, iz Teorema 11 slijedi:

$$N(1805) = 4(1+1) = 8.$$

$$1805 = (\pm 19^2) + (\pm 38^2) = (\pm 38)^2 + (\pm 19)^2.$$

(c) U Primjeru 8 smo pokazali da se 625 može prikazati kao suma kvadrata dva cijela broja ($625 = 15^2 + 20^2$). Promotrimo faktorizaciju: $625 = 5^4$. Jedini se prost faktor 5, oblika $4k+1$, $k = 1$, javlja s eksponentom 4, pa uvrštavajući u formulu imamo:

$$N(625) = 4(4+1) = 20.$$

Koristeći Propoziciju 6 dobivamo i ostale prikaze, pa imamo:

$$\begin{aligned} 625 &= (\pm 15)^2 + (\pm 20)^2 = (\pm 20)^2 + (\pm 15)^2 \\ &= (\pm 7)^2 + (\pm 24)^2 = (\pm 24)^2 + (\pm 7)^2 \\ &= (\pm 25)^2 + 0^2 = 0^2 + (\pm 25)^2. \end{aligned}$$

Sljedeće dvije tvrdnje govore o broju različitih prikaza prirodnih brojeva u obliku sume kvadrata dva cijela broja, ali ako izuzmemo predznake i poredak pribrojnika.

Propozicija 12. (vidjeti [1, Problems and Solutions, 8-45]) *Ako* $8|N(n)$*, onda se* n *može zapisati na točno* $\frac{N(n)}{8}$ *različitih načina u obliku sume kvadrata dva cijela broja.*

Propozicija 13. (vidjeti [1, Problems and Solutions, 8-45]) *Ako* $8 \nmid N(n)$*, onda je* $N(n) = 8k + 4$*,* $k \in \mathbb{Z}$*, i postoji točno* $k + 1$ *različitih prikaza broja* n *u obliku sume kvadrata dva cijela broja.*

U prethodnom smo primjeru imali $N(3185) = 16$, te je broj različitih prikaza broja 3185 u obliku sume kvadrata dva cijela broja jednak $\frac{16}{8} = 2$; $3185 = 7^2 + 56^2 = 28^2 + 49^2$. Slično, $N(1805) = 8$, te je broj različitih prikaza jednak $\frac{8}{8} = 1$, a to je prikaz $1805 = 19^2 + 38^2$. Za broj 625 je $N(625) = 20$, no $8 \nmid 20$ (uvjet prethodne propozicije) i $20 = 8 \cdot 2 + 4$ ($k = 2$), a broj različitih prikaza u obliku sume kvadrata dva cijela broja je $3 = 2 + 1$.

3 Suma kvadrata tri cijela broja

Problem zapisivanja brojeva u obliku sume kvadrata tri cijela broja bitno se razlikuje od problema prikaza u obliku sume kvadrata dva cijela broja. Razlog tome je što za dva prirodna broja koji su suma kvadrata tri cijela broja ne vrijedi analogon Propozicije 6, tj. produkt dva prirodna broja koji su suma kvadrata tri cijela broja, nije i sam suma kvadrata tri cijela broja. Samim time se ovaj problem znantno komplicira te zahtjeva više od osnovnih tvrdnji teorije brojeva pri dokazivanju i argumentiranju.

Sljedeći teorem daje karakterizaciju prirodnih brojeva koji se mogu zapisati u obliku sume kvadrata tri cijela broja, a pripisuje se matematičaru Gaussu koji daje prvi točan i potpun dokaz ove tvrdnje u svome djelu *Disquisitiones Arithmeticae*. Dokazat ćemo samo nužnost ovoga teorema, budući da je dovoljnost znatno kompliciranija, i kao što smo spomenuli, izlazi iz okvira osnovnih tvrdnji teorije brojeva.

Teorem 13. (**Gauss, 1801.**, vidjeti [9, Chapter XI, Theorem 3.]) *Prirodan se broj može zapisati u obliku sume kvadrata tri cijela broja ako i samo ako nije oblika* $4^l(8k+7)$, $k, l \geqslant 0$.

Dokaz: Nužnost dokažimo Fermatovom metodom beskonačnog spusta. Neka je n najmanji prirodan broj oblika $4^l(8k+7)$, $k, l \geqslant 0$, koji se može zapisati u obliku sume kvadrata tri cijela broja. Stoga, postoje $a, b, c \in \mathbb{Z}$ takvi da je

$$n = a^2 + b^2 + c^2. \tag{12}$$

Uočimo da je n oblika $4r+3$, $r \in \mathbb{N}$. Znamo da za parne cijele brojeve a vrijedi $a^2 \equiv 0 \pmod 4$, a za neparne $a^2 \equiv 1 \pmod 4$. Dakle, ako je jedan od brojeva a, b, c neparan onda bi n bio oblika $4r+1 \neq 4r+3$. Ako su dva broja neparna, onda bi n bio oblika $4r+2 \neq 4r+3$, a ako su sva tri broja a, b, c neparna, onda bi n bio oblika $8r+3$, što opet nije moguće. Stoga su svi brojevi a, b, c parni pa postoje a_1, b_1, $c_1 \in \mathbb{Z}$ takvi da je $a = 2a_1$, $b = 2b_1$, $c = 2c_1$. No, sada iz (12) slijedi $4^{l-1}(8k+7) = a_1^2 + b_1^2 + c_1^2$ što je u kontradikciji s minimalnošću od n. □

Intuitivno se može zaključiti da postoji više prirodnih brojeva koji se mogu zapisati kao suma kvadrata tri cijela broja, nego onih koji se mogu zapisati kao suma kvadrata dva cijela broja. Da su brojevi oblika $4^l(8k+7)$, $k, l \geqslant 0$, zapravo jedini brojevi koji se ne mogu zapisati kao suma kvadrata tri cijela broja prvi je uočio matematičar Pierre Fermat još u 17. stoljeću. Neki od tih brojeva su: 7,

15, 23, 28, 60, 92, 112, 240, ... A. M. Legendre 1798. daje nejasan i nepotpun dokaz prethodnog teorema koristeći binarne i ternarne kvadratne forme, a teoriju kvadratnih formi pri dokazivanju koristi i Gauss. Također, Euler 1763. godine pomoću kvadratnih ostataka dokazuje tvrdnju o prikazu prostih brojeva u obliku sume kvadrata tri cijela broja, koja glasi:

Teorem 14. (**Euler**, vidjeti [1, Problems and Solutions 8-90]) *Neka je p prost broj oblika $8k+1$ ili $8k+3$, $k \in \mathbb{Z}$. Tada postoje cijeli brojevi a i b takvi da je*

$$p = 2a^2 + b^2.$$

Posljedično, p je suma kvadrata tri cijela broja.

Primjer 12. *Ako je moguće prikažimo sljedeće brojeve u obliku sume kvadrata tri cijela broja:*

(*a*) *469,*

(*b*) *368,*

(*c*) *131.*

Rješenje: Kako bismo odredili mogu li se navedeni brojevi prikazati kao suma kvadrata tri cijela broja, pogledajmo kojeg su oblika.

(a) $469 \neq 4^l(8k+7)$ pa se može zapisati kao suma kvadrata tri cijela broja. Na primjer:
$$469 = 100 + 144 + 225 = 10^2 + 12^2 + 15^2.$$

(b) $368 = 4^2(8 \cdot 2 + 7)$ pa se, prema Teoremu 13, ne može zapisati kao suma kvadrata tri cijela broja.

(c) $131 = 8 \cdot 16 + 3$ i prost je broj, pa se prema prethodnom teoremu može zapisati kao suma kvadrata tri cijela broja. Kako je:
$$131 = 25 + 25 + 81,$$
slijedi $a = 5$, $b = 9$ pa imamo
$$131 = 5^2 + 5^2 + 9^2.$$

4 Suma kvadrata četiri cijela broja

U prethodnim smo poglavljima vidjeli da se ne mogu svi prirodni brojevi zapisati u obliku sume kvadrata dva cijela broja, ni u obliku sume kvadrata tri cijela broja. No, 1621. godine francuski matematičar C. G. Bachet de Méziriac iskazuje tvrdnju, iako bez dokaza, da se svaki prirodan broj može zapisati kao suma kvadrata najviše četiri cijela broja. Fermat je 1636. godine objavio kako je dokazao ovu tvrdnju koristeći svoju metodu beskonačnog spusta. Ovim se problemom intenzivno bavio i Euler, ali ga ipak ne uspijeva dokazati. Bez obzira na to, njegovi su rezultati znatno doprinijeli konačnom dokazu koji je dao Lagrange 1770. godine na temelju Eulerovih spisa.

U ovome ćemo se poglavlju najprije baviti prikazima prirodnih brojeva u obliku sume kvadrata četiri cijela broja, a zatim okarakterizirati prirodne brojeve koji su suma kvadrata četiri prirodna broja.

4.1 Prikaz prirodnih brojeva u obliku sume kvadrata četiri cijela broja

Dokažimo najprije sljedeću lemu koja predstavlja analogon Propozicije 6, a također se može poopćiti na produkt konačno mnogo faktora.

Lema 2. (**Euler**, vidjeti [1, (8.19) Lemma]) *Ako su m i n sume kvadrata četiri cijela broja, onda je i njihov produkt suma kvadrata četiri cijela broja. Točnije, ako je $m = a^2 + b^2 + c^2 + d^2$ i $n = e^2 + f^2 + g^2 + h^2$ onda je*

$$m \cdot n = x^2 + y^2 + z^2 + v^2, \tag{13}$$

pri čemu je $x = ae + bf + cg + dh$, $y = af - be + ch - dg$, $z = ag - bh - ce + df$, $v = ah + bg - cf - de$.

Dokaz: Raspišimo obje strane jednakosti (13).

$$\begin{aligned} m \cdot n &= (a^2 + b^2 + c^2 + d^2)(e^2 + f^2 + g^2 + h^2) \\ &= (ae)^2 + (af)^2 + (ag)^2 + (ah)^2 + (be)^2 + (bf)^2 + (bg)^2 + (bh)^2 \\ &\quad + (ce)^2 + (cf)^2 + (cg)^2 + (ch)^2 + (de)^2 + (df)^2 + (dg)^2 + (dh)^2. \end{aligned}$$

$$
\begin{aligned}
&x^2+y^2+z^2+v^2\\
&\quad=(ae)^2+(bf)^2+(cg)^2+(dh)^2+2abef+2aceg+2adeh+2bcfg\\
&\qquad+2bdfh+2cdgh+(af)^2+(be)^2+(ch)^2+(dg)^2-2abef\\
&\qquad+2acfh-2adfg-2bceh+2bdeg-2cdgh+(ag)^2+(bh)^2\\
&\qquad+(ce)^2+(df)^2-2abgh-2aceg+2adfg+2bceh-2bdfh\\
&\qquad-2cdef+(ah)^2+(bg)^2+(cf)^2+(de)^2+2abgh-2acfh\\
&\qquad-2adeh-2bcfg-2bdeg+2cdef\\
&\quad=(ae)^2+(bf)^2+(cg)^2+(dh)^2+(af)^2+(be)^2+(ch)^2+(dg)^2\\
&\qquad+(ag)^2+(bh)^2+(ce)^2+(df)^2+(ah)^2+(bg)^2+(cf)^2+(de)^2\\
&\quad=m\cdot n.
\end{aligned}
$$

□

Teorem 15. (**Lagrange; Euler**, vidjeti [5, Theorem 5.8.]) *Svaki se prirodan broj može prikazati u obliku sume kvadrata četiri cijela broja.*

Dokaz: Ako je $n=1$, onda tvrdnja vrijedi jer je $1=1^2+0^2+0^2+0^2$.
Nadalje, pretpostavimo da je $n>1$. Tada se n može zapisati kao produkt prostih faktora pa je zbog Leme 2 dovoljno pokazati da se svaki prost broj p može prikazati u obliku sume kvadrata četiri cijela broja. Razmotrit ćemo tri slučaja: kada je $p=2$, kada je p oblika $4k+1$, $k\in\mathbb{N}$, i kada je oblika $4k+3$, $k\in\mathbb{Z}$. Budući da su svi prosti brojevi različiti od 2 neparni, ne moramo razmatrati slučaj $4k+2$.
1° Za $p=2$ imamo $2=1^2+1^2+0^2+0^2$.
2° Ako je $p=4k+1$, $k\in\mathbb{N}$, prema Teoremu 5 p se može zapisati u obliku sume kvadrata dva cijela broja x i y, $p=x^2+y^2$, pa stoga i kao suma kvadrata četiri cijela broja:

$$p=x^2+y^2+0^2+0^2.$$

3° Neka je $p=4k+3$, $k\in\mathbb{Z}$, i $(a+1)$ najmanji kvadratni neostatak modulo p. Budući da je i -1 kvadratni neostatak modulo p, onda su a i $-(a+1)$ kvadratni ostaci modulo p. Dakle, postoje $x,y\in\{-\frac{p-1}{2},\ldots,-1,0,1,\ldots,\frac{p-1}{2}\}$ takvi da je $x^2\equiv a \pmod p$ i $y^2\equiv -(a+1) \pmod p$ pa je

$$x^2+y^2+0^2+1^2\equiv 0 \pmod p \tag{14}$$

i

$$p\leqslant x^2+y^2+1<2\left(\frac{p}{2}\right)^2+1<p^2.$$

Posebno, zbog prethodne nejednakosti, postoji $m \in \mathbb{N}$, $1 \leqslant m < p$, najmanji takav da se mp može zapisati u obliku sume kvadrata četiri cijela broja. Nadalje, želimo pokazati da je $m = 1$.
Pretpostavimo stoga da je $1 < m < p$ i

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2, \quad x_1, x_2, x_3, x_4 \in \mathbb{Z}, \tag{15}$$

Pokažimo da m mora biti neparan. Ako je m paran onda i desna strana jednakosti (15) mora biti parna, što znači da paran broj pribrojnika mora biti paran. Bez spanjenja općenitosti pretpostavimo da je $x_1 \equiv x_2 \pmod 2$, $x_3 \equiv x_4 \pmod 2$. Sada imamo:

$$\frac{m}{2}p = \left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2$$

što nije moguće jer je m najmanji takav. Dakle, m mora biti neparan.
Neka su $y_i \in \mathbb{Z}$ takvi da je

$$-\frac{m}{2} < y_i < \frac{m}{2} \quad i \quad y_i \equiv x_i \pmod m, i = 1, 2, 3, 4. \tag{16}$$

Iz (15) i (16) imamo

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod m$$

pa postoji $m_0 \in \mathbb{Z}$ takav da je

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = mm_0. \tag{17}$$

Kombinirajući (16) i (17) imamo

$$mm_0 < 4\left(\frac{m}{2}\right)^2 = m^2,$$

pa je $m_0 < m$.
S druge strane, m_0 mora biti različit od 0 jer bi u suprotnom $y_i = 0$ za svaki $i = 1, 2, 3, 4$, pa bi za sve x_i moralo vrijediti $x_i \equiv 0 \pmod m$. Nadalje bi m^2 dijelio sumu $x_1^2 + x_2^2 + x_3^2 + x_4^2$, a onda bi i $m|p$ što nije moguće jer je $1 < m < p$ po pretpostavci. Dakle, $1 \leqslant m_0 < m$. Sada, kombinirajući (13), (15) i (17) slijedi

$$\begin{aligned} m_0 p m^2 =& (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_1 + x_2y_4 - x_4y_3)^2 \\ &+ (x_1y_3 + x_3y_1 - x_2y_4 + x_4y_2)^2 + (x_1y_4 - x_4y_1 - x_3y_2 + x_2y_3)^2. \end{aligned} \tag{18}$$

Iz (15) i (16) imamo

$$x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod{m},$$

a svaki je od izraza

$$x_1y_2 - x_2y_1 + x_2y_4 - x_4y_3,$$
$$x_1y_3 + x_3y_1 - x_2y_4 + x_4y_2,$$
$$x_1y_4 - x_4y_1 - x_3y_2 + x_2y_3,$$

kongruentan 0 modulo p. No, sada je svaki pribrojnik iz (18) djeljiv s m^2, pa iz (18) dijeljenjem s m^2 slijedi da je m_0p suma kvadrata četiri cijela broja. Ali kako je $m_0 < m$ dolazimo do kontradikcije s minimalnošću od m. □

Primjer 13. *Primijenimo postupak prikaza brojeva u obliku sume kvadrata četiri cijela broja iz dokaza prethodnog teorema na sljedećim brojevima:*

(*a*) *11,*

(*b*) *7.*

Rješenje:

(a) Uočimo da je broj 11 oblika $4k+3$ za $k = 2$ pa postupamo kao u slučaju 3° iz dokaza Teorema 15. Odredimo najprije kvadratne ostatke modulo 11:

$$1^2 \equiv 1 \pmod{11}, \qquad 6^2 \equiv 3 \pmod{11},$$
$$2^2 \equiv 4 \pmod{11}, \qquad 7^2 \equiv 5 \pmod{11},$$
$$3^2 \equiv 9 \pmod{11}, \qquad 8^2 \equiv 9 \pmod{11},$$
$$4^2 \equiv 5 \pmod{11}, \qquad 9^2 \equiv 4 \pmod{11},$$
$$5^2 \equiv 3 \pmod{11}, \qquad 10^2 \equiv 1 \pmod{11}.$$

Najmanji kvadrani neostatak je 2 pa je $a = 1$, $x = 1$ jer je $1^2 \equiv a \pmod{11}$ i $y = 3$ jer je $3^2 \equiv -(a+1) \pmod{11}$. Sada iz (14) slijedi

$$x^2 + y^2 + 0^2 + 1^2 = 1^2 + 3^2 + 0^2 + 1^2 = 11$$

pa postupak staje. Odnosno, odredili smo traženi prikaz.

(b) Broj 7 je također oblika $4k+3$ za $k = 1$ pa provodimo analogan postupak.

$$1^2 \equiv 1 \pmod 7, \qquad 4^2 \equiv 2 \pmod 7,$$
$$2^2 \equiv 4 \pmod 7, \qquad 5^2 \equiv 4 \pmod 7,$$
$$3^2 \equiv 2 \pmod 7, \qquad 6^2 \equiv 1 \pmod 7.$$

Najmanji kvadratni neostatak je 3, pa je $a = 2$. Sada je $x = 3^2 \equiv 2 \pmod 7$ i $y = 2^2 \equiv -3 \pmod 7$. Nadalje, iz (14) je

$$x^2 + y^2 + 0^2 + 1^2 = 3^2 + 2^2 + 0^2 + 1^2 = 14 = 2 \cdot 7.$$

Budući da nismo dobili prikaz broja 7 ($m = 2$) u obliku sume kvadrata četiri cijela broja, nastavljamo postupak tako da na prethodni izraz djelujemo modulo 2. Dobivamo:

$$1^2 + 0^2 + 0^2 + 1^2 = 2 = 1 \cdot 2$$

pa je $m_0 = 1$. Sada primjenom (18) imamo

$$1 \cdot 7 \cdot 2^2 = 4^2 + 2^2 + 2^2 + 2^2,$$

a dijeljenjem s 2^2 slijedi konačan zapis:

$$7 = 2^2 + 1^2 + 1^2 + 1^2.$$

Primjer 14. *Dokažimo da je svaki prirodan broj djeljiv s 8 suma kvadrata osam neparnih cijelih brojeva.*

Rješenje: Neka je $n \in \mathbb{N}$ djeljiv s 8. Tada postoji $m \in \mathbb{N}$ takav da je $n = 8m$. Prema prethodnom se teoremu $m > 1$ može zapisati kao suma kvadrata četiri cijela broja, tj. postoje a, b, c, $d \in \mathbb{Z}$ takvi da je

$$m - 1 = a^2 + b^2 + c^2 + d^2,$$

(za $m = 1$ je $m - 1 = 0 = 0^2 + 0^2 + 0^2 + 0^2$), pa je

$$\begin{aligned} n = 8m &= 8(m-1) + 8 \\ &= (2a-1)^2 + (2a+1)^2 + (2b-1)^2 + (2b+1)^2 + (2c-1)^2 + (2c+1)^2 \\ &\quad + (2d-1)^2 + (2d+1)^2. \end{aligned}$$

Spomenimo i rezultat američkog matematičara D. H. Lehmera koji je pokazao da se od svih prirodnih brojeva jedino brojevi 1, 2, 5, 7, 11, 15, 23 i brojevi oblika

$4^k m$, $k = 0, 1, 2, \ldots$, $m = 2, 3, 14$, mogu na jedinstven način prikazati u obliku sume kvadrata četiri cijela broja, ne uzimajući u obzir poredak pribrojnika. Matematičari su se također bavili problemom zapisivanja prirodnog broja u obliku sume četiri različita kvadrata pa navedimo neke od tih rezultata.

Teorem 16. (**G. Pall**, vidjeti [9, Chapter XI, §6]) *Jedini prirodni brojevi koji se ne mogu prikazati u obliku sume kvadrata četiri različita nenegativna cijela broja su brojevi oblika $4^k a$, gdje je $k = 0, 1, 2, \ldots$, $a = 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 23, 25, 27, 31, 33, 37, 43, 47, 55, 67, 73, 97, 103, 2, 6, 10, 18, 22, 34, 58, 82$.*

Primjer 15. *Provjerimo mogu li se sljedeći brojevi prikazati u obliku sume kvadrata četiri različita cijela broja, a ako mogu odredimo jedan od tih prikaza:*

(*a*) *226,*

(*b*) *421,*

(*c*) *304.*

Rješenje:

(a) Budući da broj 226 nije oblika $4^k a$, za k i a kao u prethodnom teoremu, ima traženi prikaz. Primjerice:

$$226 = 225 + 1 = 144 + 81 + 1 + 0 = 12^2 + 9^2 + 1^2 + 0^2.$$

(b) Analogno kao u (a) broj 421 ima traženi prikaz:

$$421 = 400 + 16 + 4 + 1 = 20^2 + 4^2 + 2^2 + 1^2.$$

(c) Budući da je $394 = 4^2 \cdot 19$, prema prethodnom se teoremu ne može prikazi kao suma kvadrata četiri različita cijela broja.

Kao i kod sume kvadrata dva cijela broja, navedimo rezultat vezan za ukupan broj prikaza prirodnog broja u obliku sume kvadrata četiri cijela broja.

Teorem 17. (**Jacobi**, vidjeti [1, Theorem 8.24]) *Neka je $M(n)$ ukupan broj prikaza prirodnog broja n u obliku sume kvadrata četiri cijela broja (uključujući različite predznake i poretke pribrojnika). Onda je $M(n) = 8k$, gdje je k suma svih pozitivnih djelitelja od n koji nisu djeljivi s 4.*

Primjer 16. *Odredimo ukupan broj prikaza broja 1725 u obliku sume kvadrata četiri cijela broja te odredimo neke od njih.*

Rješenje: Kako bismo odredili sumu svih pozitivnih djelitelja broja 1725 najprije ga faktorizirajmo na proste faktore:

$$1725 = 3 \cdot 5^2 \cdot 23.$$

Uočimo najprije da ni jedan faktor nije djeljiv s 4. Sada, primjenom formule (1) imamo:

$$\begin{aligned}\sigma(1725) &= \frac{1-3^{1+1}}{1-3} \cdot \frac{1-5^{2+1}}{1-5} \cdot \frac{1-23^{1+1}}{1-23} = \frac{1-3^2}{1-3} \cdot \frac{1-5^3}{1-5} \cdot \frac{1-23^2}{1-23} \\ &= \frac{-8}{-2} \cdot \frac{-124}{-4} \cdot \frac{-528}{-22} = 2976.\end{aligned}$$

Ukupan broj različitih prikaza jednak je $M(1725) = 8 \cdot 2976 = 23\,808$. Odredimo sada pomoću (13) neke od njih:

$$3 = 1^2 + 1^2 + 1^2 + 0^2,$$

$$23 = 3^2 + 3^2 + 2^2 + 1^2,$$

$$\begin{aligned}3 \cdot 23 &= (3+3+2+0)^2 + (3-3+1-0)^2 + (2-1-3+0)^2 + (1+2-3-0)^2 \\ &= 8^2 + 1^2 + 2^2 + 0^2\end{aligned}$$

Sada množenjem s 5^2 imamo:

$$1725 = 40^2 + 5^2 + 10^2 + 0^2.$$

Budući da $5^2 = 25$ možemo zapisati kao $25 = 3^2 + 4^2$ imamo još jedan zapis:

$$1725 = 40^2 + 3^2 + 4^2 + 10^2,$$

ili npr. $10^2 = 100 = 36 + 64 = 6^2 + 8^2$ pa imamo:

$$1725 = 40^2 + 5^2 + 6^2 + 8^2.$$

4.2 Prikaz prirodnih brojeva u obliku sume kvadrata četiri prirodna broja

Nakon što smo dokazali da se svaki prirodan broj može zapisati u obliku sume kvadrata četiri cijela broja, možemo se pitati, slično kao kod sume kvadrata dva

cijela broja, mogu li se svi prirodni brojevi zapisati kao suma kvadrata četiri prirodna broja. Očito to neće vrijediti budući da, primjerice za brojeve 1 i 5, imamo: $1 = 1^2 + 0^2 + 0^2 + 0^2$, $5 = 1^2 + 2^2 + 0^2 + 0^2$. Sljedeći nam rezultati govore koji će se prirodni brojevi moći prikazati u navedenom obliku.

Teorem 18. (vidjeti [9, Chapter XI, Theorem 5]) *Prirodan broj n je suma kvadrata četiri prirodna broja ako i samo ako ne pripada nizu brojeva 1, 3, 5, 9, 11, 17, 29, 41, $2 \cdot 4^k$, $6 \cdot 4^k$, $14 \cdot 4^k$, $k = 0, 1, 2, \ldots$*

Korolar 5. (vidjeti [9, Chapter XI, §6, Corollary]) *Kvadrat svakog prirodnog broja većeg od 1, osim 3^2, je suma kvadrata četiri prirodna broja.*

Primjer 17. *Odredimo mogu li se sljedeći brojevi prikazati u obliku sume kvadrata četiri prirodna broja te ako mogu odredimo jedan od prikaza:*

(a) *896,*

(b) *300,*

(c) *484.*

Rješenje:

(a) Budući da je $896 = 14 \cdot 4^3$ prema prethodnom se teoremu ne može zapisati kao suma kvadrata četiri prirodna broja.

(b) Broj 300 ne pripada nizu iz prethodnog teorema pa se može zapisati u traženom obliku. Primjenom (13) imamo

$$\begin{aligned} 300 &= 30 \cdot 10 = (1^2 + 2^2 + 3^2 + 4^2) \cdot (1^2 + 1^2 + 2^2 + 2^2) \\ &= 17^2 + 3^2 + 1^2 + 1^2. \end{aligned}$$

(c) Jer je $484 = 22^2$ prema prethodnom se korolaru može zapisati kao suma kvadrata četiri prirodna broja. Ponovno iz (13) slijedi

$$\begin{aligned} 484 &= 22 \cdot 22 = (1^2 + 1^2 + 2^2 + 4^2) \cdot (0^2 + 2^2 + 3^2 + 3^2) \\ &= 20^2 + 4^2 + 8^2 + 2^2. \end{aligned}$$

Teorem 19. (vidjeti [9, Chapter XI, Theorem 6.]) *Prirodan broj n je suma kvadrata tri ili četiri prirodna broja ako i samo ako n nije jedan od brojeva 1, 5 i $2 \cdot 4^k$, $k = 0, 1, 2, \ldots$*

Uočimo da je niz brojeva iz prethodnog teorema podskup niza brojeva iz Teorema 18 budući da se odnosi i na prikaze u obliku sume kvadrata tri prirodna broja. Direktna posljedica Teorema 19 je sljedeći korolar:

Korolar 6. (vidjeti [9, Chapter XI, §6, Corollary]) *Neparan prirodan broj je suma kvadrata tri ili četiri prirodna broja ako i samo ako je $n \neq 1, 5$.*

Napomena 6. *Kao što je prikaz prirodnog broja u obliku sume kvadrata dva cijela broja povezan s modulom kompleksnog broja, identitet sa sumom kvadrata četiri cijela broja povezan je s modulom na isti način, ali s drugim brojevnim sustavom - kvaternionima. Kvaternioni su brojevi koji čine četverodimenzionalan vektorski prostor, a oblika su*

$$a + bi + cj + dk,$$

gdje su $a, b, c, d \in \mathbb{R}$, a za i, j, k vrijedi:

$$i^2 = j^2 = k^2,$$

i

$$ij = -ji = k, \quad jk = -kl = i, \quad ki = -ik = j.$$

Modul kvaterniona analogan je modulu kompleksnog broja:

$$|z|^2 = a^2 + b^2 + c^2 + d^2,$$

za $z = a + bi + cj + dk$, a analogno vrijedi i

$$|z_1|^2 \cdot |z_2|^2 = |z_1 z_2|^2.$$

5 Suma kvadrata barem pet prirodnih brojeva

U ovome ćemo se poglavlju baviti prikazima brojeva u obliku sume pet ili više kvadrata prirodnih brojeva. Točnije, navest ćemo rezultate koji govore kojeg su oblika brojevi koji se ne mogu zapisati u navedenom obliku. Nažalost, kako su dokazi egzistencijalnog tipa, nemamo konkretan postupak za određivanje takvih prikaza.

Teorem 20. (vidjeti [9, Chapter XI, Theorem 8]) *Jedini prirodni brojevi koji se ne mogu zapisati u obliku sume kvadrata pet prirodnih brojeva su 1, 2, 3, 4, 6, 7, 9, 10, 12, 15, 18 i 33.*

Dokaz: Prema Teoremu 18 svaki se neparan prirodan broj veći od 41 može zapisati u obliku sume kvadrata četiri prirodna broja. Dakle, ako bilo kojem od tih brojeva dodamo 1^2 ili 2^2 slijedi da se svaki paran prirodan broj veći od 42 i svaki neparan prirodan broj veći od 45 može zapisati u obliku sume kvadrata pet prirodnih brojeva. Stoga tvrdnju moramo dokazati za brojeve $n \leqslant 45$. Po Teoremu 18 se brojevi 4, 7, 10, 12, 15, 16, 18, 19, 20, 21, 22, 23, 25, 26, 27, 28, 30, 31, 33, 34, 35, 36, 37, 38, 39, 40, 42, 43 i 44 mogu zapisati kao suma kvadrata četiri cijela broja, pa dodavanjem brojeva 1 i 4 toj sumi dobivamo prikaz u obliku sume kvadrata pet prirodnih brojeva. Tako nam još ostaju brojevi 1, 2, 3, 4, 6, 7, 9, 10, 12, 15, 19 i 33. Naime, ni jedan se od njih ne može zapisati u obliku sume kvadrata pet prirodnih brojeva. Dokažimo to za broj 33. Pretpostavimo da je $33 = a^2 + b^2 + c^2 + d^2 + e^2$, gdje su $a, b, c, d, e \in \mathbb{N}$ takvi da je $a \geqslant b \geqslant c \geqslant d \geqslant e$. Onda je $a^2 + 4 \leqslant 33 \leqslant 5a^2$, te je $6 < a^2 \leqslant 29$, zbog čega je $3 \leqslant a \leqslant 5$. Ako je $a = 3$ onda se broj $33 - a^2 = 24 = 4 \cdot 6$ može zapisati kao suma kvadrata četiri cijela broja, što nije moguće po Teoremu 18. Za $a = 4$ imamo da se broj 17, a za $a = 5$ da se broj 8 može zapisati kao suma kvadrata četiri cijela broja, što opet po Teoremu 18 nije moguće jer su oblika $4k$. Slično se pokaže i za ostale brojeve. □

Teorem 21. (**Pall**, vidjeti [9, Chapter XI, Theorem 9]) *Ako je m prirodan broj, $m \geqslant 6$, onda su jedini prirodni brojevi koji se ne mogu prikazati u obliku sume kvadrata m prirodnih brojeva brojevi 1, 2, 3, ..., $m-1$, $m+1$, $m+2$, $m+4$, $m+5$, $m+7$, $m+10$ i $m+13$.*

Dokaz: Neka je $m \geqslant 6$ prirodan broj. Pronađimo $n \leqslant m + 13$ koji se mogu zapisati u obliku sume kvadrata m prirodnih brojeva. Neka n ima to svojstvo. Tada postoje brojevi $a_1, a_2, \ldots, a_m$ takvi da je $a_1 \geqslant a_2 \geqslant \ldots \geqslant a_m$ i $n = a_1^2 + a_2^2 + \ldots + a_m^2$. Onda je $a_1^2 + (m-1) \leqslant n \leqslant m + 13$, iz čega slijedi $a_1^2 \leqslant 14$ pa je $a_1 \leqslant 3$.

Ako je $a_1 = 1$, onda su svi $a_i = 1$ te je $m = n$. Nadalje neka je $a_1 = 2$. Ako su najmanje četiri broja od brojeva $a_2, a_3, \ldots, a_m$ jednaki 2, onda je $n \geqslant 5 \cdot 4 + (m-5)$, što je u kontradikciji s $n \leqslant m + 13$. Dakle, najviše tri broja a_i, $i \in \{2, 3, \ldots, m\}$ mogu biti jednaki 2. Imamo četiri slučaja:
1° ni jedan od brojeva $a_2, a_3, \ldots, a_m$ nije jednak 2: tada je $n = 4 + (m-1) = m+3$;
2° jedan od brojeva $a_2, a_3, \ldots, a_m$ jednak je 2: tada je $n = 2 \cdot 4 + (m-2) = m+6$;
3° dva su broja $a_2, a_3, \ldots, a_m$ jednaka 2: tada je $n = 3 \cdot 4 + (m-3) = m+9$;
4° tri su broja $a_2, a_3, \ldots, a_m$ jednaka 2: tada je $n = 4 \cdot 4 + (m-4) = m+12$.

Sada još ostaje za razmotriti kada je $a_1 = 3$. Za $a_1 = 3$ imamo $n - 9 = a_2^2 + a_3^2 + \ldots + a_m^2$. Ako je $a_2 = 3$, onda je $n \geqslant 18 + (m-2)$ što je u kontradikciji s $n \leqslant m + 13$. Stoga je $a_2 \leqslant 2$. Ako je $a_2 = 1$, onda su $a_3 = a_4 = \ldots = a_m = 1$ te je $n = 3^2 + m - 1 = m + 8$. Ako je $a_2 = 2$ i ako među brojevima $a_2, a_3, \ldots, a_m$ postoje dva ili više broja koja su jednaka 2, onda je $n \geqslant 3^2 + 2^2 + 2^2 + (m-3) = m + 14$, što je ponovno u kontradikciji s $n \leqslant m + 13$. Dakle, $a_3 = a_4 = \ldots = a_m = 1$ pa je $m = 3^2 + 2^2 + (m-2) = m + 11$.

Pokazali smo da se među prirodnim brojevima koji su manji ili jednaki od $m+13$ jedino brojevi m, $m+3$, $m+6$, $m+8$, $m+9$, $m+11$ i $m+12$ mogu zapisati u obliku sume kvadrata m prirodnih brojeva. Nadalje, neka je $n > m + 13$. Ako je $n = m + 28$, onda je $n = m + 28 = 2 \cdot 3^2 + 4 \cdot 2^2 + (m-6) \cdot 1^2$, budući da je $m \geqslant 6$. Tj. n se može zapisati u obliku sume m kvadrata. Ako je $n \neq m + 28$, onda je $n - (m-5) > 18$ (jer je $n > m + 13$) i $n - (m-5) \neq 33$. Sada iz prethodnog teorema slijedi da se broj $n - (m-5)$ može zapisati kao suma pet kvadrata te se broj $n = n - (m-5) + (m-5) \cdot 1^2$ može zapisati u obliku sume m kvadrata. □

Primjer 18. *Odredimo mogu li se sljedeći brojevi prikazati u obliku sume kvadrata sedam prirodnih brojeva, a ako mogu odredimo jedan od tih prikaza.*

(*a*) *16,*

(*b*) *20,*

(*c*) *21.*

Rješenje:

(a) Budući da broj 16 nije element niza iz prethodnog teorema, može se zapisati u obliku sume kvadrata sedam prirodnih brojeva.

$$16 = 1^2 + 1^2 + 1^2 + 1^2 + 2^2 + 2^2 + 2^2.$$

(b) Jer je $20 = 7 + 13$ prema prethodnom se teoremu ne može zapisati u traženom obliku.

(c) Broj 21 također nije jedan od brojeva niza iz prethodnog teorema te se može zapisati u navedenom obliku.

$$21 = 1^2 + 1^2 + 1^2 + 1^2 + 2^2 + 2^2 + 3^2.$$

Iz Teorema 20 i 21 zaključujemo da se bilo koji dovoljno velik prirodan broj može zapisati u obliku sume kvadrata $m \geqslant 5$ prirodnih brojeva. Naravno, kao što smo u ranijim poglavljima pokazali, ovo ne vrijedi za $m = 1, 2, 3, 4$ jer postoji beskonačno mnogo prirodnih brojeva koji nisu: kvadrat prirodnog broja (npr. $n^2 + 1$), suma kvadrata dva cijela broja (npr. brojevi oblika $4k+3$, $k = 0, 1, 2, \ldots$), suma kvadrata tri cijela broja (npr. brojevi oblika $8k+7$, $k = 0, 1, 2, \ldots$), suma kvadrata četiri cijela broja (npr. brojevi oblika $4^k \cdot 2$, $k = 0, 1, 2, \ldots$). Isto tako, postoji beskonačno mnogo prirodnih brojeva koji nisu suma kvadrata tri ili više prirodnih brojeva, primjerice brojevi oblika $8k + 7$, $k = 1, 2, \ldots$, a po Lagrangeovom se teoremu svaki prirodan broj može zapisati u obliku sume kvadrata četiri ili više prirodnih brojeva.

6 Suma kubova cijelih brojeva

Nakon što smo razmotrili prikaze brojeva u obliku sume kvadrata cijelih brojeva, pogledajmo prikaze u obliku sume kubova cijelih brojeva. Budući da je ovaj problem nešto složeniji, nema određenog algoritma kako prirodan broj zapisati u obliku sume kubova cijelih brojeva kao što smo imali kod nekih prikaza u obliku sume kvadrata cijelih brojeva. Također, nije poznato ni kojeg su točno oblika brojevi koji imaju traženi prikaz, stoga ćemo navest rezultat koji govori koji cijeli brojevi nemaju navedeni prikaz.

Propozicija 14. (vidjeti [9, Chapter XI, §9]) *Cijeli broj oblika* $9k \pm 4$, $k \in \mathbb{Z}$, *ne može se zapisati u obliku sume tri ili manje kubova.*

Dokaz: Promotrimo ostatke kubova cijelih brojeva pri dijeljenju s 9:

$$\begin{aligned} 0^3 &\equiv 0 \pmod 9, & 5^3 &\equiv 8 \pmod 9,\\ 1^3 &\equiv 1 \pmod 9, & 6^3 &\equiv 0 \pmod 9,\\ 2^3 &\equiv 8 \pmod 9, & 7^3 &\equiv 1 \pmod 9,\\ 3^3 &\equiv 0 \pmod 9, & 8^3 &\equiv 8 \pmod 9,\\ 4^3 &\equiv 1 \pmod 9, & 9^3 &\equiv 0 \pmod 9. \end{aligned}$$

Budući da su kubovi cijelih brojeva kongruentni 0, 1, 8 modulo 9, zbroj dva kuba cijelih brojeva može biti kongruentan 0, 1, 2, 7, 8 modulo 9, a zbroj tri kuba cijelih brojeva može biti kongruentan 0, 1, 2, 3, 6, 7, 8 modulo 9. Dakle, za $k \in \mathbb{Z}$ zbroj tri kuba cijelih brojeva ne može biti oblika $9k + 4$, ni $9k + 5$, tj. oblika $9k \pm 4$. □

Iz prethodne propozicije zaključujemo da postoji beskonačno mnogo cijelih brojeva koji se ne mogu zapisati u obliku sume dva ili tri kuba cijelih brojeva i da su oni oblika $9k \pm 4$, $k \in \mathbb{Z}$. Međutim, ne znamo ima li svaki cijeli broj koji nije toga oblika prikaz u obliku sume dva kuba cijelih brojeva.

Kao i u prethodnom poglavlju, možemo se pitati koji se prosti brojevi mogu zapisati u obliku sume kubova dva cijela broja. Neka je stoga p prost broj takav da je $p = x^3 + y^3$, $x, y \in \mathbb{N}$. Tada je

$$p = (x + y)(x^2 - xy + y^2) = (x + y)((x - y)^2 + xy).$$

Jer je $x + y \geqslant 2$ i p prost broj, mora vrijediti $p = x + y$, $(x - y)^2 + xy = 1$, odakle je $x = y$, $xy = 1$, tj. $x = y = 1$, pa je $p = 2$. Dakle, jedini prost broj koji se može zapisati u obliku sume kubova dva prirodna broja je broj 2 ($2 = 1^3 + 1^3$). Uočimo da je to i jedini prikaz broja 2 toga oblika. Općenito, vrijedi sljedeće:

Propozicija 15. (vidjeti [9, Chapter XI, §9]) *Svaki prirodan broj koji se može prikazati u obliku sume kubova dva cijela broja ima konačan broj takvih prikaza.*

Dokaz: Neka je $n = x^3 + y^3$, pri čemu je $x > 0$ i $y < 0$. Tada je

$$n = (x + y)(x^2 - xy + y^2).$$

No, kako je $x + y > 0$, to je $x + y \geqslant 1$ pa imamo

$$x^2 - xy + y^2 \leqslant n,$$

a iz $-xy > 0$ slijedi

$$x < \sqrt{n}$$

i

$$0 < -y < \sqrt{n}.$$

Dakle, postoji konačano mnogo brojeva x, y s navedenim svojstvom. □

Nadalje, navedimo neke rezultate vezane za prikazivanje brojeva u obliku sume kubova tri cijela broja. Matematičari V. L. Gardiner, R. B. Lazarus i P. R. Stein pronašli su rješenja jednadžbe

$$x^3 + y^3 - z^3 = \epsilon k,$$

za $0 < k < 1000$ u cijelim brojevima koji zadovoljavaju nejednakost $0 \leqslant x \leqslant y \leqslant 2^{16}$, $\epsilon = \pm 1$. Pokazali su da nema rješenja za $k = 30, 33, 39, 42, 52, 74, 75, 84$, a da za $k = 12$ i $\epsilon = 1$ postoji točno jedno rješenje: $x = 7$, $y = 10$, $z = 11$, tj. da je $12 = 7^3 + 10^3 - 11^3$.

Za neke je cijele brojeve k moguće pokazati da postoji beskonačno mnogo prikaza u obliku sume kubova tri cijela broja. Navest ćemo primjere za brojeve 1, 2 i 3.

$$1 = (9n^4)^3 + (1 - 9n^3)^3 + (3n - 9n^4)^3,\ n = 0, \pm 1, \pm 2, \ldots$$

Postoje i drugi prikazi osim ovoga, primjerice $1 = 94^3 + 64^3 + (-103)^3$, a D. H. Lehmer je pokazao da postoji beskonačno mnogo takvih prikaza. No, za broj 2 za sada nije poznat ni jedan drugi oblik prikaza u obliku sume tri kuba osim sljedećeg:

$$2 = (1 + 6n^3)^3 + (1 - 6n^3)^3 + (-6n^2)^3,\ n = 0, \pm 1, \pm 2, \ldots$$

Za broj 3 su poznata samo dva različita prikaza:

$$3 = 1^3 + 1^3 + 1^3 = 4^3 + 4^3 + (-5)^3.$$

U 20. stoljeću matematičar Wacław F. Sierpiński iskazuje sljedeću tvrdnju: *"Svaki se cijeli broj n može na beskonačno mnogo načina prikazati u obliku*

$$n = x^3 + y^3 - z^3 - t^3,$$

gdje su x, y, z, t prirodni brojevi", a dokazuje ju matematičar Dam'yanenko za cijele brojeve $-1000 \leqslant n \leqslant 1000$ i za sve $n \neq 9k \pm 4$, $k \in \mathbb{Z}$ (detaljnije opisano u [9, Chapter XI, §12]).

7 Waringov problem

Iste godine kada Lagrange objavljuje svoj teorem o sumi kvadrata četiri cijela broja (1770.g.), britanski matematičar Edward Waring iskazuje puno općenitiju tvrdnju, tj. da se svaki prirodan broj može zapisati kao suma četiri kvadrata, devet kubova, 19 četvrtih potencija cijelih brojeva i općenito u obliku sume fiksnog broja k-tih potencija za svaki pozitivan broj k, no, bez dokaza.

Teorem 22. (**Waringov problem**, vidjeti [1, (8.26) Waring's Problem.]) *Za svaki $k \geqslant 2$ postoji pozitivan cijeli broj s (koji ovisi samo o k) takav da se svaki pozitivan cijeli broj može zapisati u obliku sume od s nenegativnih k-tih potencija.*

Pred kraj 19. stoljeća dokazano je da za svaki $k \leqslant 8$ postoji cijeli broj s s navedenim svojstvom. Potpuni je dokaz za postojanje broja s dao David Hilbert 1909. godine. Međutim, dokaz je egzistencijalni i ne daje postupak kojim se može odrediti prikaz broja u obliku sume od s nenegativnih k-tih potencija.

Uočimo da za $k = 1$ Teorem 22 očito vrijedi ako stavimo $s = 1$ ($n = n^1, \forall n \in \mathbb{N}$). Neka je $g(k)$ najmanji broj s takav da se svaki pozitivan cijeli broj može prikazati u obliku sume od s nenegativnih k-tih potencija. Johannes Euler, sin Leonharda Eulera, daje procjenu za $g(k)$:

$$g(k) \geqslant 2^k + \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 2, \forall k \geqslant 2. \tag{19}$$

Dokaz se može vidjeti u [9, Chapter XI, §15]. Za $k = 2$ imamo

$$g(2) \geqslant 2^2 + \left\lfloor \left(\frac{3}{2}\right)^2 \right\rfloor - 2 = 4,$$

a iz Lagrangeovog teorema slijedi $g(2) = 4$. Za $k > 2$ problem se znatno komplicira što potvrđuje činjenica da u 100 godina nakon objave Teorema 22 nije bilo gotovo nikakvog napretka u pokušajima dokaza. Osim za $k = 2, 3$ u dokazima se koriste analitičke tehnike i teorija funkcija kompleksne varijable. Za $k = 3$ iz (19) slijedi

$$g(3) \geqslant 2^3 + \left\lfloor \left(\frac{3}{2}\right)^3 \right\rfloor - 2 = 9,$$

a A. Wieferich 1909. dokazuje da je svaki prirodan broj suma devet pozitivnih kubova. Za $k = 4$ imamo

$$g(4) \geqslant 2^4 + \left\lfloor \left(\frac{3}{2}\right)^4 \right\rfloor - 2 = 19,$$

a 1986. matematičari Balasubramanian, Dress i Deshonilles dokazuju da je $g(4) = 19$. Iz (19) je $g(5) \geqslant 37$, a 1964. J. R. Chen dokazuje da je $g(5) = 37$. L.E. Dickson dokazuje formulu (19) za $6 \leqslant k \leqslant 400$, K. Mahler za sve dovoljno velike brojeve k i R. M. Stemmler za $400 < k \leqslant 200\,000$.

Literatura

[1] A. Adler, J. Coury, *The Theory of Numbers*, Jones and Bartlett Publishers, London, 1995.

[2] F. M. Brückler, *Povijest matematike II*, Odjel za matematiku Sveučilišta J. J. Strossmayera u Osijeku, Osijek, 2010.

[3] F. M. Brückler, *Povijest matematike I*, Odjel za matematiku Sveučilišta J. J. Strossmayera u Osijeku, Osijek, 2014.

[4] P. Cameron, *A Course on Number Theory*, Lecture notes, University of London, London, 2009.

[5] W. Chen, *Elementary Number Theory*, Lecture notes at Imperial College, University of London, London, 1981.-1990.

[6] A. Dujella, *Uvod u teoriju brojeva*, Matematički odsjek, Prirodoslovno-matematički fakultet, Sveučilište u Zagrebu, Zagreb, 2002.

[7] A. Dujella, *Sume kvadrata*, Matematički odsjek, Prirodoslovno-matematički fakultet, Sveučilište u Zagrebu, Zagreb, pisani materijali.

[8] I. Matić, *Uvod u teoriju brojeva*, Odjel za matematiku Sveučilišta J. J. Strossmayera u Osijeku, Osijek, 2013.

[9] W. F. Sierpiński, *Elementary Theory of Numbers*, North Holland, Amsterdam, 1988.

Sažetak

Zapisivanjem prirodnih brojeva u obliku sume nenegativnih potencija bavili su se mnogi matematičari, a neki iskazani rezultati nisu u potpunosti dokazani ni danas.

U sklopu razmatranja koji se prirodni brojevi mogu zapisati u obliku sume kvadrata dva cijela broja okarakterizirani su prosti brojevi s navedenim prikazom. Točnije, prost broj će biti suma kvadrata dva cijela broja ako i samo ako je jednak broju 2 ili ako je oblika $4k+1$, $k \in \mathbb{N}$. Generalizirajući prethodnu tvrdnju na prirodne brojeve dolazimo do Fermat-Eulerovog teorema koji govori da se jedino prirodni brojevi koji sadrže proste faktore oblika $4k+3$, $k \in \mathbb{Z}$, s parnim eksponentom mogu zapisati kao suma kvadrata dva cijela broja. Dana je i formula za određivanje broja takvih prikaza. Razmatrani su i problemi zapisivanja prirodnih brojeva u obliku sume kvadrata dva prirodna broja, te dva relativno prosta prirodna broja. Zatim je naveden Gaussov rezultat vezan za prirodne brojeve koji se mogu prikazati u obliku sume kvadrata tri cijela broja, tj. brojeve koji nisu oblika $4^l(8k+7)$, $k, l \geqslant 0$. Zanimljiva tvrdnja koja se pripisuje Lagrangeu i Euleru govori da se svaki prirodan broj može zapisati u obliku sume kvadrata četiri cijela broja, a navedeno je i koji se prirodni brojevi mogu prikazati kao suma kvadrata četiri prirodna broja. Iako ne postoji postupak za određivanje prikaza prirodnih brojeva u obliku sume kvadrata pet ili više prirodnih brojeva, navedeni su rezultati koji govore koji se brojevi ne mogu zapisati u tome obliku. Zatim se fokus prebacuje na prikaze u obliku sume kubova cijelih brojeva, a na kraju na završno poopćenje, tj. Waringov problem.

Ključne riječi

Suma kvadrata cijelih brojeva, suma kubova cijelih brojeva, Waringov problem

Representation of positive integers as a sum of powers of integers

Summary

Many mathematicians considered the problem of representation of positive integers as a sum of non-negative powers and still some of the results have not been proved.

By observing positive integers that can be represented in the form of two squares of integers, we characterized primes in the such form. More precisely, prime number is a sum of two squares of positive integers if and only if it is equal two or it has the form of $4k + 1$, $k \in \mathbb{N}$. Generalizing the previous statement to positive integers, we have Fermat-Euler's theorem which states that only positive integers which contain primes of the form $4k+3$, $k \in \mathbb{Z}$, with the even exponent are the sum of two squares of integers. We also gave the formula for the number of such representations. Moreover, we considered the problem of representation of positive integers as the sum of squares of two positive integers and two coprime positive integers. Furthermore, we stated the result of Gauss concerning the representation of positive integers as the sum of three squares of integers, i.e. numbers which are not of the form $4l(8k + 7)$, $k, l \geqslant 0$. The interesting statement attributed to Lagrange and Euler states that every positive integer can be written as the sum of four squares of integers. Also, we expressed the positive integers that can be represented as the sum of four squares of positive integers. While there is no algorithm for the representation of positive integers as the sum of five or more squares of positive integers, we mentioned the results concerning to numbers that cannot be represented in that form. Finally, we focused on representation of positive integers as the sum of cubes of integers and considered the generalization known as Waring's problem.

Keywords

Sum of sqaures of integers, sum of cubes of integers, Waring's problem

Životopis

Rođena sam 7. ožujka 1996. godine u Slavonskom Brodu. Živim u Sikirevcima gdje sam pohađala Osnovnu školu "Sikirevci", nakon čega 2010. godine upisujem opću gimnaziju u Gimnaziji Antuna Gustava Matoša u Đakovu koju završavam 2014. godine. Nakon toga upisujem Sveučilišni nastavnički studij matematike i informatike na Odjelu za matematiku u Osijeku.

U travnju 2016. godine sudjelovala sam na Festivalu znanosti na Odjelu za matematiku. Sudjelovala sam i na regionalnom natjecanju *Primatijada* koje se održalo u svibnju 2018. godine u Budvi. Tamo sam zajedno s kolegicama s Odjela za matematiku za rad "Analiza terorističke mreže 9/11" osvojila treće mjesto. U travnju 2019. godine sudjelovala sam na 9. geometrijskoj školi Stanka Bilinskog u Našicama, a u svibnju 2019. godine na Međunarodnoj znanstvenoj konferenciji "Didaktički izazovi III" na Fakultetu za odgojne i obrazovne znanosti u Osijeku. Od 2017. godine članica sam Studentskog zbora i Etičkog povjerenstva Odjela za matematiku te predstavnica studenata u Vijeću Odjela za matematiku. Od veljače 2018. do lipnja 2019. godine volontirala sam u Dokkici ("Dječja osječka kreativna kućica") kao voditeljica poduka u sklopu programa "Razvoj alternativnih inovativnih usluga - alternativni centri podrške za djecu i roditelje". Trenutno sam zaposlena u Osnovnoj školi "Sikirevci" u Sikirevcima i Gimnaziji Antuna Gustava Matoša u Đakovu kao nastavnica informatike.