Prikaz prirodnih brojeva kao suma nenegativnih k-tih potencija

Glavačević, Ana

Master's thesis / Diplomski rad

2023

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, School of Applied Mathematics and Informatics / Sveučilište Josipa Jurja Strossmayera u Osijeku, Fakultet primijenjene matematike i informatike**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:126:377446

Sveučilište J.J. Strossmayera u Osijeku
Fakultet primijenjene matematike i informatike
Diplomski studij - Financijska matematika i statistika

Ana Glavačević

Prikaz prirodnih brojeva kao suma nenegativnih k-tih potencija

Diplomski rad

Osijek, 2023.

Sveučilište J.J. Strossmayera u Osijeku
Fakultet primijenjene matematike i informatike
Diplomski studij - Financijska matematika i statistika

Ana Glavačević

Prikaz prirodnih brojeva kao suma nenegativnih k-tih potencija

Diplomski rad

Mentor: prof. dr. sc. Ivan Matić

Osijek, 2023.

Sadržaj

Uvod

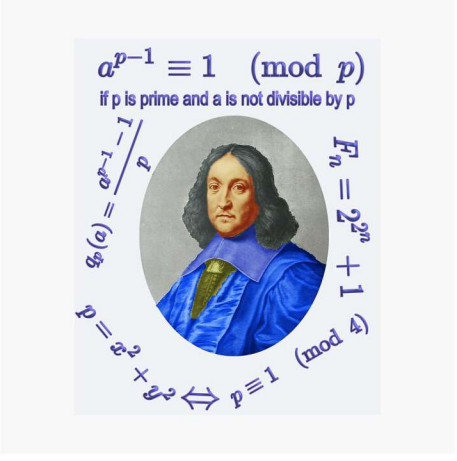
U ovom radu proučavat ćemo prikaz prirodnih brojeva u obliku sume nenegativnih k-tih potencija. Prije nego krenemo u srž samoga problema, reći ćemo nešto o problemu zapisivanja brojeva u obliku sume potencija kroz povijest, a zatim ćemo se prisjetiti osnovnih rezultata teorije brojeva. U trećem poglavlju navest ćemo karakteristike prirodnih brojeva koje možemo prikazati u obliku sume kvadrata dva cijela broja te prosječan broj prikaza danog broja u obliku sume dva kvadrata. U četvrtom ćemo poglavlju okarakterizirati prirodne brojeve koje zapisujemo u obliku sume kvadrata tri cijela broja. U petom poglavlju govorimo o prirodnim brojevima koji imaju prikaz u obliku sume kvadrata četiri cijela broja, ali ćemo najprije početi s prostim brojevima. U zadnjem poglavlju razmatramo reprezentaciju prirodnih brojeva koji se mogu prikazati u obliku sume kvadrata pet ili više prirodnih brojeva. Potkrijepili smo primjerima važne rezultate kako bi bolje i lakše razumjeli prikaz brojeva u obliku sume potencija.

1 Prikaz prirodnih brojeva kroz povijest

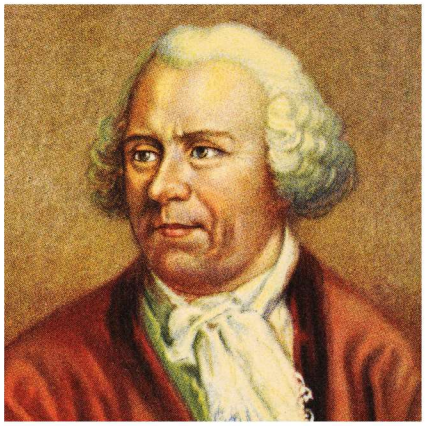
Na temelju nekih povijesnih izvora prvi zapisi prirodnih brojeva u obliku sume dva kvadrata dolaze iz 2000. godine prije Krista, a ispisali su ih Babilonci na glinenim pločama. U 3. stoljeću poslije Krista starogrčki matematičar Diofant iz Aleksandrije u djelu "Arithmetica" napisao je točnu i nedokazanu tvrdnju za prikaz brojeva u obliku sume dva kvadrata.

SLIKA 1. Diofant iz Aleksandrije (3. st.)

U 17. stoljeću poznati francuski matematičar Pierre de Fermat izriče tvrdnju da za svaki prost broj oblika $4k + 1$, $k \in \mathbb{N}$, postoji jedinstven prikaz u obliku sume kvadrata dva prirodna broja. Tu tvrdnju dokazao je švicarski matematičar, fizičar i astronom Leonhard Euler. Navedeni matematičari bavili su se i karakterizacijom prirodnih brojeva koji se mogu reprezentirati u obliku sume kvadrata četiri cijela broja. Njihove rezultate u potpunosti je dokazao matematičar Joseph-Luis Lagrange u 18. stoljeću.



SLIKA 2. Pierre de Fermat (17. st.)



SLIKA 3. Leonhard Euler (18. st.)

Osim njih, matematičari kao Edward Waring, Carl Fridrich Gauss, Edmund Landau, Gordon Pall također su istraživali probleme prikaza broja u obliku sume nenegativnih k-tih potencija i pridonijeli važnim rezultatima kroz povijest.

2 Osnovni pojmovi i tvrdnje

2.1 Djeljivost

Prije prikazivanja brojeva u obliku sume kvadrata nenegativnih k-tih potencija, navesti ćemo osnovne definicije i rezultate iz teorije brojeva.

Definicija 1. (vidjeti [2], Definicija 1.1.) Neka su a i b cijeli brojevi i $a \neq 0$. Kažemo da a dijeli b i pišemo $a \mid b$, ako postoji cijeli broj d takav da b možemo zapisati kao umnožak brojeva a i d, tj. $b = a \cdot d$. Ako a ne dijeli b tada pišemo $a \nmid b$.

Propozicija 1. (vidjeti [3], Propozicija 1.1.1.) Neka su a i b cijeli brojevi i $a \neq 0$.
(i) Ako a dijeli b i $b \neq 0$, tada je $\mid a \mid \leq \mid b \mid$.
(ii) Ako a dijeli b, tada a dijeli i svakog višekratnika broja b.
(iii) Ako a dijeli brojeve b i c, tada a dijeli brojeve $b + c$, $b - c$ i $b \cdot c$.

Teorem 1. (vidjeti [2], Teorem 1.1.) Za proizvoljan $a \in \mathbb{N}$ i $b \in \mathbb{Z}$ postoje jedinstveni $q, r \in \mathbb{Z}$ takvi da je $b = q \cdot a + r$, pri čemu je $0 \leq r < a$.

Definicija 2. (vidjeti [2], Definicija 1.2.) Neka su b i c cijeli brojevi. Za cijeli broj $a \neq 0$ kažemo da je zajednički djelitelj od b i c ako a dijeli b i a dijeli c. Ako je barem jedan od brojeva b i c različit od nule, tada postoji konačno mnogo zajedničkih djelitelja od b i c, a najveći među njima nazivamo najveći zajednički djelitelj od b i c i označavamo ga s (b, c).

Prirodan broj $n > 1$ naziva se prostim brojem ako nema ni jednog djelitelja d za koji vrijedi $1 < d < n$. Dakle, prost broj je djeljiv samo s brojem 1 i sa samim sobom. Ako broj nije prost, kažemo da je složen. Za broj 1 kažemo da nije ni prost ni složen broj. Svaki se prirodan broj $n > 1$ može zapisati kao umnožak prostih faktora što je vrlo bitno u dokazivanju teorema u ovome radu.

Definicija 3. (vidjeti [2], Definicija 1.3.) Ako je najveći zajednički djelitelj od b i c broj 1, kažemo da su brojevi b i c relativno prosti.

Najveći zajednički djelitelj d je uvijek iz skupa prirodnih brojeva. Ako je $(b, c) = d$, onda postoje cijeli brojevi b_1 i c_1 takvi da je $b = db_1$ i $c = dc_1$, pri čemu su b_1 i c_1 relativno prosti. Na primjer $(48, 88) = 8$, $48 = 8 \cdot 6$, $88 = 8 \cdot 11$ i $(8, 11) = 1$.

Lema 1. (vidjeti [3], Lema 1.4.1.) Neka je p prost broj takav da dijeli umnožak brojeva a i b, tj. $p \mid ab$. Tada $p \mid a$ ili $p \mid b$.

Jednako vrijedi i za umnožak proizvoljno mnogo faktora. Ako $p \mid a_1 a_2 \cdots a_n$ onda $p \mid a_j$ za neki $j \in \{1, 2, ..., n\}$.

Teorem 2. (**Osnovni teorem aritmetike**, vidjeti [3], Teorem 1.4.3.) Svaki prirodan broj koji je veći od 1 ima jedinstveni zapis u obliku umnoška potencija prostih faktora, a faktorizacija je jedinstvena do na poredak faktora.

Navedeni teorem kaže da za svaki prirodan broj n veći od 1 vrijedi:

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

pri čemu je $k \in \mathbb{N}$, $p_1, p_2, ..., p_k$ različiti prosti brojevi te $\alpha_1, \alpha_2, ..., \alpha_k \in \mathbb{N}$. Ovakav zapis prirodnog broja n naziva se kanonski rastav broja n na proste faktore i koristi se kod dokazivanja djeljivosti.

Propozicija 2. (vidjeti [3], Propozicija 1.4.4.) Neka su $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ i $b = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdots q_k^{\beta_k}$ prirodni brojevi prikazani u kanonskom rastavu. Broj b je djelitelj broja a ako i samo ako za svaki q_j, $j \in \{1, 2, ..., l\}$ postoji $i \in \{1, 2, ..., k\}$ takav da je $q_j = p_i$ i $\alpha_i \geq \beta_j$.

Lema 2. (vidjeti [5], Chapter V, §5, Exercises 8.) Neka su b i c dva neparna relativno prosta prirodna broja koja se mogu prikazati kao suma kvadrata dva relativno prosta prirodna broja. Tada umnožak bc dopušta barem dva prikaza u obliku sume kvadrata dva relativno prosta broja koji se razlikuju ne samo u redosljedu pribrojnika.

Teorem 3. (vidjeti [5], Chapter IX, §1, Theorem 1.) Postoji beskonačno mnogo prostih brojeva koji su oblika $8k - 1$.

Definicija 4. (vidjeti [4], Poglavlje 1.1) Trokutasti brojevi posebna su klasa figurativnih brojeva koji se dobivaju slaganjem točkica u jednakostraničan trokut. Trokutasti broj t_n dobivamo zbrajanjem prvih n prirodnih brojeva, tj. $t_n = n(n+1)/2$.

2.2 Kongruencije i kvadratni ostaci

Definicija 5. (vidjeti [2], Definicija 2.1.) Kažemo da je a kongruentan b modulo n i pišemo $a \equiv b \pmod{n}$ ako $n \mid a - b$, pri čemu su $n, a, b \in \mathbb{Z}$ i $n \neq 0$.

U prethodnoj definiciji modul n je cijeli broj različit od nule, što znači da je razlika $a - b$ djeljiva sa n i sa $-n$, ali mi ćemo promatrati slučaj samo za module iz skupa prirodnih brojeva. Možemo primjetiti da je a djeljiv s n ako i samo ako je $a \equiv 0 \pmod{n}$.

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

(i) Neka su a, a', b, b' cijeli brojevi i n prirodan broj. Ako je $a \equiv a' \pmod{n}$ i $b \equiv b' \pmod{n}$ tada vrijedi $a \pm b \equiv a' \pm b' \pmod{n}$ i $ab \equiv a'b' \pmod{n}$.

(i) Neka su a, b, c cijeli brojevi, n prirodan broj te a i n relativno prosti brojevi. Ako je $ab \equiv ac \pmod{n}$ tada je $b \equiv c \pmod{n}$.

Teorem 4. (**Wilsonov teorem**, vidjeti [3], Teorem 2.3.1.) Ako je p prost broj onda je

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

Vrijedi i obrat, tj. ako za $p \in \mathbb{N}$ vrijedi $(p-1)! \equiv -1 \pmod{p}$ tada je p prost broj.

Definicija 6. (vidjeti [3], Poglavlje 2.1.1.) Neka je n prirodan broj veći od 1. Ako za svaki cijeli broj b postoji jedinstveni $a_i \in S$ za koji vrijedi da je $b \equiv a_i \pmod{n}$ tada skup $S = \{a_1, a_2, ..., a_n\}$ nazivamo potpuni sustav ostataka modulo n.

Skup $S = \{1, 2, ..., n-1\}$ se najčešće koristi za potpuni sustav ostataka. Generalno, postoji beskonačno mnogo sustava ostataka i svi oni imaju isti broj elemenata.

Definicija 7. (vidjeti [3], Poglavlje 2.1.1.) Neka je n prirodan broj veći od 1. Ako za svaki cijeli broj b za koji vrijedi $(b, n) = 1$ postoji jedinstveni $a_i \in S$ za koji je $b \equiv a_i \pmod{n}$, tada skup $S = \{a_1, a_2, ..., a_n\}$ nazivamo reducirani sustav ostataka modulo n.

Izbacivanjem elemenata iz potpunog sustava ostataka koji nisu relativno prosti s n dobit ćemo reducirani sustav ostataka modulo n.

Definicija 8. (vidjeti [3], Poglavlje 4.1.) Neka je a cijeli broj, n prirodan broj te neka su a i b relativno prosti brojevi. Kažemo da je a kvadratni ostatak modulo n ako kongruencija $x^2 \equiv a \pmod{n}$ ima rješenja. U suprotnome a nazivamo kvadratni neostatak modulo n.

Propozicija 4. (vidjeti [2], Teorem 3.1.) Za neparan prost broj p reducirani sustav ostataka modulo p ima po $\frac{p-1}{2}$ kvadratnih ostataka i kvadratnih neostataka.

Prema navedenoj propoziciji reducirani sustav ostataka modulo 11 ima $\frac{11-1}{2} = 5$ kvadratnih ostataka i neostataka.

3 Suma dva kvadrata

3.1 Prikaz brojeva u obliku sume dva kvadrata

Prije nego što iskažemo teorem koji govori o prikazu prirodnog broja u obliku sume kvadrata dva cijela broja, spomenut ćemo bitne teoreme i lemu.

Teorem 5. (**Fermatov teorem**, vidjeti [3], Teorem 5.3.2.) Neka je p prost broj oblika $4k+1$. Tada se p može prikazati u obliku sume kvadrata dva cijela broja.

Teorem 6. (**Mali Fermatov teorem**, vidjeti [2], Teorem 2.10.) Ako za prost broj p vrijedi da $p \nmid a$ tada je $a^{p-1} \equiv 1 \pmod{p}$.

Lema 3. (vidjeti [5], Chapter XI, §1) Neka je p neparan prost broj. Ako je prost broj p djelitelj sume kvadrata dva relativno prosta cijela broja, tada je p oblika $4k+1$.

Dokaz. Neka su a, b dva relativno prosta cijela broja te neka je p neparan prost broj takav da $p \mid a^2+b^2$.
Tada $a^2 \equiv -b^2 \pmod{p}$ na $(p-1)/2$ potenciju daje $a^{p-1} \equiv -1^{(p-1)/2}\, b^{p-1} \pmod{p}$.
Ali, budući da je $(a,\ b) = 1$, p ne dijeli brojeve a i b pa po Fermatovom teoremu vrijedi: $a^{p-1} \equiv b^{p-1} \equiv 1 \pmod{p}$.
Posljedično, za $p > 2$ $(-1)^{(p-1)/2} \equiv 1 \pmod{p}$ daje $(-1)^{(p-1)/2} = 1$ i dokazuje parnost broja $(p-1)/2$. Stoga p mora biti oblika $4k+1$.

□

Teorem 7. (vidjeti [5], Chapter XI, Theorem 1.) Prirodan broj n može se zapisati kao suma kvadrata dva cijela broja ako i samo ako se u faktorizaciji broja n svi prosti faktori oblika $4k+3, k \in \mathbb{Z}$ pojavljuju s eksponentom koji je paran.

Dokaz. Pretpostavimo da broj n ima prikaz u obliku sume kvadrata dva cijela broja,

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

Neka je

$$n = q_1^{\alpha_1} \cdot q_2^{\alpha_2} \cdots q_s^{\alpha_s},$$

faktorizacija broja n na proste faktore. Neka je prost broj p oblika $4k+3$ djelitelj broja n.
Pišemo $d = (a,b)$, odnosno $a = da_1$ i $b = db_1$ pri čemu je $(a_1, b_1) = 1$.
Kako je $n = a^2 + b^2$, slijedi $d^2 \mid n$ i $n = d^2 n_1$, pri čemu je n_1 prirodan broj.
Pretpostavimo da je eksponent broja p u faktorizaciji $n = q_1^{\alpha_1} \cdot q_2^{\alpha_2} \cdots q_s^{\alpha_s}$ neparan. Kako je $n = d^2 n_1$, dobivamo da $p \mid n_1 = a_1^2 + b_1^2$ što je suprotno Lemi 3. pa smo dokazali da je uvjet teorema nužan.
Kako bismo dokazali da je uvjet teorema dovoljan, bez smanjenja općenitosti možemo pretpostaviti da je n veći od 1 jer za broj 1 vrijedi $1 = 1^2 + 0^2$.
Neka je $n = q_1^{\alpha_1} \cdot q_2^{\alpha_2} \cdots q_s^{\alpha_s}$ faktorizacija broja n na proste faktore. Označimo s m najveći prirodan broj čiji je kvadrat djelitelj broja n. Tada je $n = m^2 k$ pri čemu je k ili broj 1 ili

produkt različitih prostih brojeva pri čemu niti jedan od njih nema oblik $4k+3$.
S obzirom da je $2 = 1^2 + 1^2$, na temelju Fermatovog teorema, svaki od ovih prostih brojeva je suma kvadrata dva prirodna broja. Izraz

$$(a^2 + b^2)(c^2 + d^2) = (ab + cd)^2 + (ad - bc)^2$$

predstavlja produkt dva prirodna broja pri čemu je svaki od njih suma kvadrata dva cijela broja.
Posljedično, k je suma kvadrata dva cijela broja. Kako je $k = u^2 + v^2$, slijedi $n = (mu)^2 + (mv)^2$. Time smo pokazali dovoljnost uvjeta i teorem je dokazan.

□

Korolar 1. (vidjeti [5], Chapter XI, §1) Ako prirodan broj nema prikaz u obliku sume kvadrata dva cijela broja onda nije ni suma kvadrata dva racionalna broja.

Dokaz. Ako prirodan broj n nije suma kvadrata dva cijela broja tada, prema Teoremu 7., postoji prost broj p oblika $4k+3$ koji se u faktorizaciji od n javlja s neparnim eksponentom. Pretpostavimo da je $n = \left(\frac{l}{m}\right)^2 + \left(\frac{l_1}{m_1}\right)^2$ pri čemu su $m, m_1 \in \mathbb{N}$, $l, l_1 \in \mathbb{Z}$. Tada je $(mm_1)^2 n = (lm_1)^2 + (l_1 m)^2$. Ali, p se mora pojaviti s neparnim eksponentom u faktorizaciji na lijevoj strani jednakosti pa prema Teoremu 7. to ne može biti istinito s obzirom na desnu stranu jednakosti. Tako smo pokazali kontradikciju pa je korolar dokazan.

□

Primjer 1. (vidjeti [5], Chapter XI, §1, Exercises 1.) Pronađimo nužan i dovoljan uvjet za racionalan broja $\frac{l}{m}$ kako bi se mogao prikazati kao suma kvadarata dva racionalna broja.
Rješenje:
Takav uvjet je da broj lm bude zbroj kvadrata dva cijela broja. Ako je $\frac{l}{m} = \left(\frac{l_1}{m_1}\right)^2 + \left(\frac{l_2}{m_2}\right)^2$, tada je $lm(m_1 m_2)^2 = (mm_2 l_1)^2 + (mm_1 l_2)^2$ pa lako provjeravamo uvjet. S druge strane, ako je $lm = a^2 + b^2$, tada je $\frac{l}{m} = \left(\frac{a}{m}\right)^2 + \left(\frac{b}{m}\right)^2$.

Iz Primjera 1. i Teorema 7. slijedi da je razlomak $\frac{l}{m}$, pri čemu su l, m prirodni brojevi, suma kvadrata dva racionalna broja ako i samo ako je svaki od brojeva l, m suma kvadrata dva cijela broja.

Primjer 2. (vidjeti [5], Chapter XI, §1, Exercises 3.) Za dani prirodan broj m pronađimo prirodan broj n takav da on ima najmanje m različitih prikaza kao suma kvadrata dva prirodna broja.
Rješenje:
Neka je $n = a^2$ pri čemu je $a = (3^2 + 1)(4^2 + 1) \cdots ((m+2)^2 + 1)$.
Brojevi $\frac{a}{k^2+1}$ su prirodni brojevi za $k = 3, 4, ..., m+2$. Također brojevi

$$a_k = \frac{k^2-1}{k^2+1} a \text{ i } b_k = \frac{2ka}{k^2+1},$$

pri čemu je $k = 3, 4, .., m+2$, su prirodni brojevi. Ali, na temelju izraza

$$a^2 = \left(\frac{k^2-1}{k^2+1} a\right)^2 + \left(\frac{2ka}{k^2+1}\right)^2,$$

ako je $a_k = \frac{k^2-1}{k^2+1}a$, $b_k = \frac{2ka}{k^2+1}$, tada imamo $n = a^2 = a_k^2 + b_k^2$ za $k = 3, 4, ..., m+2$.
Ali, $a_k - b_k = \frac{k^2-2k-1}{k^2+1}a = \frac{(k-1)^2-2}{k^2+1}a > 0$ za $k = 3, 4, ..., m+2$ i $a_k = a - \frac{2a}{k^2+1}$ odakle je $a_3 < a_4 < ... < a_{m+2}$.
Tako uočavamo da su prikazi broja $n = a_k^2 + b_k^2$, za $k = 3, 4, ..., m+2$, različiti i počinju s m. Zbog toga broj n ima potrebna svojstva. U isto smo vrijeme dokazali da za dani prirodan broj m postoji najmanje m nesukladnih Pitagorinih trokuta koji imaju hipotenuzu jednake duljine.

Primjer 3. (vidjeti [5], Chapter XI, §1, Exercises 4.) Neka je dan prikaz broja n kao zbroj kvadrata dva prirodna broja. Pronađimo zapis broja $2n$ kao sume dva kvadrata.
Rješenje: Ako je $n = a^2 + b^2$ tada je $2n = (a+b)^2 + (a-b)^2$.

3.2 Prosječan broj prikaza kao suma dva kvadrata

Sada nam je cilj razmotriti problem kako pronaći sve prikaze danog prirodnog broja u obliku sume dva kvadrata.
Ako je n prikazan kao suma dva kvadrata, tj. ako je

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

tada je $n \geq x^2$ i $n \geq y^2$, odakle vrijedi $\mid x \mid \leq \sqrt{n}$ i $\mid y \mid \leq \sqrt{n}$.
Kako bismo riješili problem, dovoljno je za x uvrstiti cijeli broj čija apsolutna vrijednost nije veća od $\sqrt{n}$ i vidjet ćemo je li broj $n - x^2$ kvadrat ili ne.
Ako je $n - x^2$ kvadrat, tada da je $y = \pm\sqrt{n - x^2}$ te smo dobili prikaz broja n kao sume dva kvadrata.
Ako $n - x^2$ nije kvadrat, takav prikaz se ne može dobiti.
Svoje razmatranje možemo ograničiti na nenegativan x jer predznak od x ne uzrokuje promjenu vrijednosti $n - x^2$.
Vrijedi primjetiti da niz $n, n-1^2, n-2^2, n-3^2, ...$ ima sljedeće svojstvo: razlike uzastopnih brojeva niza su brojevi $1, 3, 5, ...$, tj. čine niz neparnih prirodnih brojeva.

Primjer 4. (vidjeti [5], Chapter XI, §2) Neka je $n = 10$.
Formiramo niz $10, 9, 6, 1$. U danom nizu brojevi 9 i 1 su kvadrati pa možemo uzeti da je $x = \pm 1, y = \pm 3$ ili $x = \pm 3, y = \pm 1$.
Tako dobivamo osam zapisa broja 10:

$$10 = 1^2 + 3^2,\ 10 = 1^2 + (-3)^2,\ 10 = (-1)^2 + 3^2,\ 10 = (-1)^2 + (-3)^2$$
$$10 = 3^2 + 1^2,\ 10 = 3^2 + (-1)^2,\ 10 = (-3)^2 + 1^2,\ 10 = (-3)^2 + (-1)^2.$$

Primjer 5. (vidjeti [5], Chapter XI, §2) Neka je $n = 25$.
Formiramo niz $25, 24, 21, 16, 9, 0$. U danom nizu brojevi $25, 16, 9$ i 0 su kvadrati. Za x, y dobijemo sljedeće vrijednosti:

$$x = 0,\ y = \pm 5; \quad x = \pm 3,\ y = \pm 4; \quad x = \pm 4,\ y = \pm 3; \quad x = \pm 5,\ y = 0.$$

Ako uključimo sve kombinacije predzanka $\pm$, broj 25 ima 12 prikaza kao suma dva kvadrata.

Označimo s $\tau(n)$ broj svih zapisa prirodnog broja n u obliku sume dva kvadrata. Dva prikaza se smatraju različitima i kada se razlikuju samo u redoslijedu pribrojnika. S obzirom na to, vrijedi:

$$\tau(1) = 4,\ \tau(2) = 4,\ \tau(3) = 0,\ \tau(4) = 4,\ \tau(5) = 8,$$

$$\tau(6) = 0,\ \tau(7) = 0,\ \tau(8) = 4,\ \tau(9) = 4,\ \tau(10) = 8.$$

Prema Fermatovom teoremu, svaki prost broj koji ima oblik $4k + 1$ može se zapisati u obliku sume dva kvadrata. Ovo pokazuje da za bilo koji prost broj p oblika $4k + 1$ vrijedi $\tau(p) = 8$. Iz gore navedenih razloga za bilo koji prirodan broj n vrijedi nejednakost $\tau(n) \leq 4\sqrt{n}$.
Sada ćemo izračunati sumu:

$$T(n) = \tau(1) + \tau(2) + ... + \tau(n).$$

Broj $\tau(k)$ je broj rješenja jednadžbe $x^2 + y^2 = k$ za cijele brojeve x, y. Stoga je $T(n)$ broj rješenja nejednadžbe

$$0 < x^2 + y^2 \leq n.$$

Rješenja gornje nejednadžbe dijelimo na klase kada govorimo da dva rješenja pripadaju istoj klasi ako i samo ako su vrijednosti broja x jednake. Pronaći ćemo broj rješenja za svaku klasu.
Ako je $x = 0$, tada zbog gornje nejednadžbe, y može poprimiti cijele vrijednosti takve da je $y^2 \leq n$ odnosno $\mid y \mid \leq \sqrt{n}$. Lako se provjerava da broj takvih y je $2[\sqrt{n}]$. Prisjetimo se da funkcija najveće cijelo od x ili $[x]$ (kraće kažemo "pod" od x) svakom realnom broju x pridružuje najveći cijeli broj koji nije veći od x.
Ako je $x = k \neq 0$, tada zbog gornje nejednakosti dobivamo $k^2 \leq n$ pa je $\mid k \mid \leq \sqrt{n}$ i $y^2 \leq n - k^2$ odakle slijedi $\mid y \mid \leq \sqrt{n - k^2}$. Broj ovakvih y-a je $1 + 2[\sqrt{n - k^2}]$. (Broj 1 je dodan budući da je $y = 0$ uključen).
Budući da k može poprimiti bilo koju vrijednost ± 1, ± 2 ,..., $\pm[\sqrt{n}]$ i predznak $\pm$ nema utjecaj na vrijednost k^2, dobivamo

$$2[\sqrt{n}] + 2\sum_{k=1}^{[\sqrt{n}]}(1 + 2[\sqrt{n - k^2}]) = 4[\sqrt{n}] + 4\sum_{k=1}^{[\sqrt{n}]}[\sqrt{n - k^2}]$$

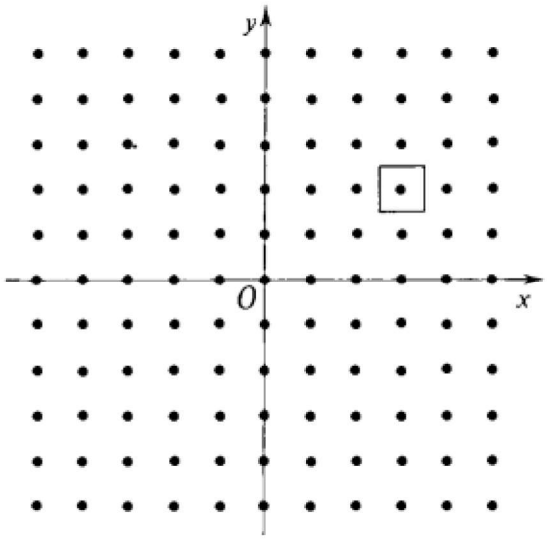
pa je

$$T(n) = 4\sum_{k=0}^{[\sqrt{n}]}[\sqrt{n - k^2}].$$

Na primjer, za $n = 100$ imamo

$$T(100) = 4([\sqrt{100}] + [\sqrt{99}] + [\sqrt{96}] + [\sqrt{91}] + [\sqrt{84}] + [\sqrt{75}] + [\sqrt{64}] + [\sqrt{51}] + [\sqrt{36}] + [\sqrt{19}])$$
$$= 4(10 + 9 + 9 + 9 + 9 + 8 + 8 + 7 + 6 + 4) = 316.$$

Suma $T(n) = \tau(1) + \tau(2) + ... + \tau(n)$ ima geometrijsku interpretaciju. Broj $1 + T(n)$ je broj parova cijelih brojeva koji zadovoljavaju nejednadžbu $x^2 + y^2 \leq n$, ali i broj točaka ravnine s cjelobrojnim koordinatama koje pripadaju krugu K s centrom u ishodištu i radijusom $\sqrt{n}$. Takve točke nazivaju se točke rešetke.
Svakoj točki pridružujemo kvadrat tako da je točka u središtu kvadrata. Kvadrat ima površinu 1, a stranice su mu paralelne sa koordinatnim osima. To možemo uočiti na sljedećoj slici.



SLIKA 1. Točkasta rešetka

Površina P prekrivena kvadratima koji su pridruženi svakoj točki jednaka je broju tih točaka, odnosno jednaka je broju $1 + T(n)$.
Krug K_1 sa središtem u ishodištu i radijusom $\sqrt{n} + \frac{1}{\sqrt{2}}$ sadrži sve točke pokrivene kvadratima koji su pridruženi točkama kruga K. Ovo slijedi iz činjenice da je $1/\sqrt{2}$ najveća moguća udaljenost točke kvadrata površine 1 do središnje točke. Stoga, površina P je manja od površine kruga K_1, odnosno, $P \leq \pi\left(\sqrt{n} + \frac{1}{\sqrt{2}}\right)^2$.
S druge strane, površina kruga K_2 s centrom u ishodištu i radijusom $\sqrt{n} - \frac{1}{\sqrt{2}}$ manja je nego površina P. Dakle, $P > \pi\left(\sqrt{n} - \frac{1}{\sqrt{2}}\right)^2$.
Iz jednadžbe $P = 1 + T(n)$ dobijemo

$$\pi\left(\sqrt{n} - \tfrac{1}{\sqrt{2}}\right)^2 - 1 < T(n) < \pi\left(\sqrt{n} + \tfrac{1}{\sqrt{2}}\right)^2 - 1.$$

Napomenimo da je $\pi\sqrt{2} < 5$ i $0 < \frac{1}{2}\pi - 1 < 1 \leq \sqrt{n}$ za bilo koji prirodan broj n.
Vrijedi:

$$\pi\left(\sqrt{n} + \tfrac{1}{\sqrt{2}}\right)^2 - 1 = \pi n + \pi\sqrt{2}\sqrt{n} + \tfrac{1}{2}\pi - 1 < \pi n + 6\sqrt{n},$$

$$\pi\left(\sqrt{n}-\tfrac{1}{\sqrt{2}}\right)^2-1=\pi n-\pi\sqrt{2}\sqrt{n}+\tfrac{1}{2}\pi-1<\pi n-6\sqrt{n}.$$

Iz ovoga dobijemo da $\pi n-6\sqrt{n}<T(n)<\pi n+6\sqrt{n}$, odakle je $\mid T(n)-\pi n \mid<6\sqrt{n}$ za bilo koji prirodan broj n, odnosno

$$\mid \tfrac{T(n)}{n}-\pi \mid<\tfrac{6}{\sqrt{n}}.$$

Iz $\mid \frac{T(n)}{n}-\pi \mid<\frac{6}{\sqrt{n}}$ i $T(n)=\tau(1)+\tau(2)+...+\tau(n)$ slijedi da je

$$\lim_{n\to\infty}\frac{\tau(1)+\tau(2)+...+\tau(n)}{n}=\pi$$

što znači da je srednja vrijednost funkcije $\tau(n)$ broj π. Također, možemo reći da je prosječno π prikaza prirodnih brojeva u obliku sume dva kvadrata. Kao što smo ustanovili $T(100)=316$, tj. prirodni brojevi manji od 100 imaju prosječno 3.16 dekompozicija u obliku sume dva kvadrata.
Lako možemo provjeriti da je $T(400)=1256$ i $T(1000)=3148$, odakle je $T(400)/400=3.14$ i $T(1000)/1000=3.148$.
Koristeći formulu $T(n)=4\sum_{k=0}^{[\sqrt{n}]}[\sqrt{n-k^2}]$ možemo izračunati $T(n)$ za bilo koji broj n.

3.3 Suma kvadrata dva prirodna broja

Teorem 8. (vidjeti [5], Chapter XI, §3, Theorem 2.) Prirodan broj n ima zapis u obliku sume kvadrata dva prirodna broja ako i samo ako svi prosti faktori koji su oblika $4k+3$ imaju parni eksponent u faktorizaciji broja n te se ili broj 2 javlja s neparnim eksponentom ili n ima barem jedan prost faktor oblika $4k+1, k\in\mathbb{N}$.

Dokaz. Pretpostavimo da postoji prirodan broj koji ima zapis u obliku sume kvadrata dva prirodna broja te zadovoljava sljedeća svojstva: nema prost djelitelj oblika $4k+1$ i u faktorizaciji sadrži prost faktor 2 s eksponentom koji je paran.
Označimo s n najmanji prirodan broj s takvim svojstvima. Prema Teoremu 7. svi prosti faktori oblika $4k+3$ u faktorizaciji broja n sadrže parni eksponent. Stoga, možemo pisati $n=2^{2k}m^2$, pri čemu je m neparan prirodan broj i k nenegativan cijeli broj.
Možemo pisati $n=2^{2k}m^2=a^2+b^2$, pri čemu su a,b prirodni brojevi.
Ako je $k>0$, tada se lijeva strana gornje jednakosti može podijeliti sa 4 pa su brojevi a i b parni, tj. $a=2a_1$, $b=2b_1$.
Slijedi

$$(2a_1)^2+(2b_1)^2=2^{2k}m^2/:4$$
$$2^{2(k-1)}m^2=a_1^2+b_1^2<n$$

što je suprotno od definicije broja n. Slijedi da $k=0$ pa je $n=m^2=a^2+b^2>1$. Brojevi a,b moraju biti relativno prosti jer u slučaju da je $(a,b)=d>1$ imamo $a=da_2$, $b=db_2$, pri čemu su a_2,b_2 prirodni brojevi. Stoga je $m=dm_1$ i $m_1^2=a_2^2+b_2^2<m^2=n$, što je suprotno od definicije broja n pa vrijedi $(a,b)=1$.

Ali, kako je m neparan i veći od 1 (nema prostog faktora koji ima oblik $4k+1$), sadrži prost faktor oblika $p = 4k+3$. Slijedi da $p \mid a^2+b^2$ odakle je $a^2 \equiv -b^2 \pmod{p}$. Ako kongruenciju $a^2 \equiv -b^2 \pmod{p}$ stavimo na potenciju $2k+1$, tada s obzirom na $2(2k+1) = p-1$ i Fermatov teorem, dobijemo $1 \equiv (-1)^{2k+1} \pmod{p}$ što je nemoguće.
Sada smo dokazali da prirodan broj koji ima zapis kao suma kvadrata dva prirodna broja zadovoljava sljedeća svojstva: ili se u faktorizaciji na proste faktore broj 2 pojavljuje s neparnim eksponentom, ili sadrži prost faktor oblika $4k+1$. Prema Teoremu 7., slijedi da svi prosti faktori koji su oblika $4k+3$ imaju paran eksponent. Time smo dokazali nužnost teorema.
Neka prirodan broj n zadovoljava uvjete teorema. Tada je ili $n = 2m^2$ ili $n = 2^\alpha m^2 l$, pri čemu je α jednako 0 ili 1, a l produkt prostih faktora oblika $4k+1$.
Ako je $n = 2m^2$, tada je $n = m^2 + m^2$ i to je suma kvadrata dva prirodna broja.
Pretpostavimo da je $n = 2^\alpha m^2 l$. Prema Fermatovom teoremu, svaki od faktora je suma dva kvadrata. Produkt dva neparna broja, pri čemu je svaki od njih suma dva kvadrata, je opet suma dva kvadrata.
Dakle, ako je $n_1 = a^2+b^2$, $n_2 = c^2+d^2$, pri čemu su n_1, n_2 neparni, tada jedan od brojeva a i b mora biti neparan, a drugi paran. Isto vrijedi i za brojeve c i d.
Tada $n_1 n_2 = (a^2+b^2)(c^2+d^2) = (ad+bc)^2 + (ac-bd)^2$, gdje je $ac-bd \neq 0$ neparan.
Tako vidimo da broj $n_1 n_2$ je suma kvadrata dva prirodna broja. Indukcijom možemo zaključiti da isto vrijedi i za umnožak proizvoljno mnogo faktora oblika $4k+1$.
Zato zaključujemo da je broj l suma kvadrata dva prirodna broja, tj. $l = a^2+b^2$ odakle vrijedi

$$m^2 l = (ma)^2 + (mb)^2$$
$$2m^2 l = (ma+mb)^2 + (ma-mb)^2$$

pri čemu $ma - mb \neq 0$ (a mora biti različit od b s obzirom da je broj $l = a^2+b^2$ neparan). Tako zaključujemo da je za bilo koji α broj n suma kvadrata dva prirodna broja. Dakle, uvjet teorema je dovoljan. Time smo dokazali ovaj teorem.

□

Iz Teorema 8. slijedi: da bi kvadrat n^2 bio suma kvadrata dva prirodna broja nužno je i dovoljno da broj n ima prost djelitelj oblika $4k+1$. Ovo možemo reći i na drugačiji način o čemu govori sljedeći korolar.

Korolar 2. (vidjeti [5], Chapter XI, §3) Prirodan broj n je hipotenuza pravokutnog trokuta ako i samo ako n sadrži barem jedan prost faktor koji ima oblik $4k+1$.

Primjer 6. (vidjeti [5], Chapter XI, §3, Exercises 1.) Dokažimo da se prirodan broj n može zapisati kao suma kvadrata dva različita prirodna broja ako i samo ako:
(i) u faktorizaciji broja n prosti faktori koji su oblika $4k+3$ imaju parne eksponente
(ii) broj n sadrži barem jedan prost faktor oblika $4k+1$.
Rješenje:
Nužnost uvjeta (i) slijedi iz Teorema 7. Pretpostavimo da prirodan broj n ne zadovoljava

uvjet (ii), tj. da nema prost faktor koji je oblika $4k+1$. Ako je $n = a^2+b^2$, tada za $d = (a, b)$ imamo $n = d^2(a_1^2 + b_1^2)$, pri čemu su $a = da_1$, $b = db_1$ i a_1, b_1 su različiti relativno prosti prirodni brojevi.
Broj $a_1^2+b_1^2$ nema prost faktor oblika $4k+1$ i kako je $(a_1, b_1) = 1$, prema obrazloženju u dokazu Teorema 8., broj $a_1^2 + b_1^2$ nema prost faktor oblika $4k + 3$. Stoga, neka je $a_1^2 + b_1^2 = 2^s$, pri čemu je s prirodan broj veći od 1 jer su a_1, b_1 različiti prirodni brojevi. Kao posljedica, broj $a_1^2 + b_1^2$ je djeljiv s brojem 4 odakle slijedi da su brojevi a_1, b_1 parni, ali to je u kontradikciji s činjenicom da $(a_1, b_1) = 1$.
Sada pretpostavimo da prirodan broj n zadovoljava uvjete (i) i (ii). Tada, prema Teoremu 8., imamo $n = a^2 + b^2$, pri čemu su a, b prirodni brojevi.
Ako je $a = b$, tada $n = 2a^2$ i kako n zadovoljava uvjet (ii), broj n ima prost faktor oblika $4k+1$. Kao što smo naveli u Korolaru 2., a je hipotenuza pravokutnog trokuta. To znači da je $a^2 = c^2 + d^2$, pri čemu su c, d prirodni brojevi. Jasno je da je $c \neq d$ jer ako je $c = d$, tada je $a^2 = 2c^2$, što je nemoguće s obzirom da je $\sqrt{2}$ iracionalan broj.
Stoga je $n = 2a^2 = (c+d)^2+(c-d)^2$, pri čemu je $c-d \neq 0$ i $c+d \neq c-d$. Slijedi, n se može prikazati u obliku sume kvadrata dva različita prirodna broja. Time smo dovršili dokaz.

Primjer 7. (vidjeti [5], Chapter XI, §3, Exercises 2.) Dokažimo da se prirodan broj n može zapisati kao suma kvadrata dva relativno prosta prirodna broja ako i samo ako broj n nije djeljiv ni s brojem 4 ni s prirodnim brojem koji je oblika $4k + 3$.
Rješenje:
Pretpostavimo da se prirodan broj n može prikazati u obliku sume kvadrata dva relativno prosta prirodna broja, tj. $n = a^2 + b^2$.
Ako je $n = 4k$, tada su brojevi a, b parni što je suprotno s $(a, b) = 1$.
Ako broj n ima djelitelja oblika $4k + 3$, tada ima prost faktor tog oblika. Prema Teoremu 8., broj n nije djelitelj sume kvadrata dva relativno prosta prirodna broja. Tako uočavamo da je uvjet nužan.
Pretpostavimo da prirodan broj n zadovoljava uvjet. Ako je $n = 2$, tada je $n = 1^2 + 1^2$ i to je suma kvadrata dva relativno prosta prirodna broja. Ako je $n > 2$, tada iz uvjeta slijedi da je n produkt prostih brojeva koji su oblika $4k + 1$ ili produkt broja 2 i prostih brojeva oblika $4k + 1$. U prošlom primjeru n je neparan i svaki prost faktor od n je suma kvadrata dva relativno prosta prirodna broja. Prema Lemi 2., broj n je suma kvadrata dva relativno prosta prirodna broja. Ako je n suma broja 2 i prostog broja oblika $4k + 1$, imamo da je $n = 2(a^2 + b^2)$ gdje su a, b dva relativno prosta prirodna broja. Kako je $a^2 + b^2$ neparan, jedan od brojeva a, b je neparan, a drugi paran. Imamo da je $n = (a^2 + b^2) + (a - b)^2$ gdje su $a + b$ i $a - b$ neparni prirodni brojevi. Osim toga, oni su i relativno prosti brojevi jer ako $d \mid a + b$ i $d \mid a - b$ pri čemu je d prirodan broj, tada $d \mid 2a$ i $d \mid 2b$. Kako je broj d, kao djelitelj neparnog broja $a + b$, neparan vrijedi $d \mid a$ i $d \mid b$ pa s obzirom da je $(a, b) = 1$ iz toga slijedi da je $d = 1$. Stoga vrijedi $(a + b, a - b) = 1$. Pokazali smo da je uvjet dovoljan i dokaz je završen.

4 Suma tri kvadrata

Teorem 9. (**Gaussov teorem**, vidjeti [5], Chapter XI, §4, Theorem 3.) Prirodan broj n oblika $4^l(8k+7)$ nije moguće prikazati u obliku sume tri kvadrata pri čemu su k, l nenegativni cijeli brojevi.

Dokaz. Pretpostavimo da postoji prirodan broj oblika $4^l(8k+7)$, pri čemu su k, l nenegativni cijeli brojevi, koji ima zapis u obliku sume kvadrata tri cijela broja. Neka je n najmanji takav broj. Tada imamo $n = 4^l(8k+7) = a^2 + b^2 + c^2$, gdje su a, b, c cijeli brojevi. Ako među brojevima a, b, c postoji točno jedan neparan broj, tada je zbroj njihovih kvadrata oblika $4t+1$, a to je različito od broja n. Ako su dva broja od a, b, c neparna, tada je suma njihovih kvadrata oblika $4t+2$, a to je različito od broja n. Ako su svi brojevi a, b, c neparni, tada je suma njihovih kvadrata oblika $8t+3$, a to je različito od broja n. Kao posljedica, svaki od brojeva a, b, c mora biti paran.
Neka je $a = 2a_1$, $b = 2b_1$, $c = 2c_1$ pri čemu su a_1, b_1, c_1 cijeli brojevi. Kako je $4^{l-1}(8k+7) = a_1^2 + b_1^2 + c_1^2$, to je suprotno definiciji broja n. Tako smo dokazali da ni jedan prirodan broj oblika $4^l(8k+7)$, gdje su k, l nenegativni cijeli brojevi, ne može biti suma kvadrata tri cijela broja. Time smo dokazali navedeni teorem.

□

Može se pokazati da je uvjet Teorema 9. dovoljan da bi broj n bio suma kvadrata tri cijela broja. Matematičar Carl Friedrich Gauss je među prvima dokazao da je svaki prirodan broj koji nije oblika $4^l(8k+7)$ suma kvadrata tri cijela broja.
Originalni Gaussov dokaz pojednostavili su matematičari Lejeune Dirichlet i Edmund Landau. Nešto kasnije, matematičar Nesmith Cornett Ankeny je dao elementarni dokaz Gaussovog teorema.
Iz Gaussovog teorema zaključujemo da je svaki prirodan broj oblika $8k+3$ suma kvadrata tri cijela broja koji moraju biti neparni. Tako je

$$8k + 3 = (2a+1)^2 + (2b+1)^2 + (2c+1)^2,$$

gdje su a, b, c nenegativni cijeli brojevi. Kako je

$$k = \tfrac{a(a+1)}{2} + \tfrac{b(b+1)}{2} + \tfrac{c(c+1)}{2} = t_a + t_b + t_c,$$

iz Gaussovog teorema slijedi teorem koji tvrdi da je svaki prirodan broj suma tri ili manje trokutasta broja.
Što se tiče brojeva oblika $8k+1$, iz rada matematičara Branta Jonesa i Gordona Palla, proizlazi da su osim brojeva 1 i 25 svi oni suma kvadrata tri prirodna broja.
Među brojevima oblika $8k+5$, koji su manji od $5 \cdot 10^{10}$, samo brojevi $5, 13, 37$ i 85 nisu suma kvadrata tri prirodna broja.
Ne postoji broj oblika $8k+7$ koji je suma kvadrata tri cijela broja, a samim time ni suma kvadrata tri prirodna broja.
Broj oblika $4k$ se može prikazati u obliku sume kvadrata tri prirodna broja ako i samo ako

je sam k suma kvadrata tri prirodna broja. Zapravo, ako je $4k = a^2 + b^2 + c^2$, pri čemu su a, b, c prirodni brojevi, tada brojevi a, b, c moraju biti parni pa je $a = 2a_1$, $b = 2b_1$, $c = 2c_1$, gdje su a_1, b_1, c_1 prirodni brojevi.
Stoga je $k = a_1^2 + b_1^2 + c_1^2$. Kao poslijedica $4k = (2a_1)^2 + (2b_1)^2 + (2c_1)^2$. Iz ovoga lako zaključujemo da ne postoji broj oblika 2^n, $n = 1, 2, ...$, koji je suma kvadrata tri prirodna broja.
Ali, $8 \cdot 3n^2 = (2n)^2 + (2n)^2 + (4n)^2$ pa možemo uočiti kako među brojevima oblika $8k$ postoji beskonačno mnogo prirodnih brojeva koji imaju prikaz u obliku sume kvadrata tri prirodna broja i koji nisu suma kvadrata tri prirodna broja.
Što se tiče brojeva oblika $8k + 2$, matematičar Gordon Pall je rekao: "Pretpostavka je da je svaki broj oblika $2(8n + 1)$ suma kvadrata tri prirodna broja." Matematičar Andrzej Schinzel je dokazao da je ta pretpostavka kriva jer broj $2(8 \cdot 8 + 1) = 130$ nije suma kvadrata tri prirodna broja.
Broj oblika $8k + 4$ je suma kvadrata tri prirodna broja ako i samo ako broj $2k + 1$ ima ovo svojstvo. Kao posljedica, broj oblika $8(4k + 3) + 4 = 4(8k + 7)$ za $k = 0, 1, 2, ...$, nije suma kvadrata tri prirodna broja.
S druge strane, broj oblika $8(4k + 1) + 4 = 4(8k + 3)$ za $k = 0, 1, 2, ...$, je suma kvadrata tri prirodna broja. Bilo koji broj oblika $8k + 6$ je suma kvadrata tri prirodna broja jer je prema Gaussovom teoremu takav broj suma kvadrata tri cijela broja. Međutim, takav broj ne može biti suma kvadrata dva prirodna broja jer $8k + 6 = 2(4k + 3)$.
Označimo s $\tau_3(n)$ broj različitih prikaza broja n kao sume kvadrata tri cijela broja. Za $n \leq 10$ imamo

$$\tau_3(1) = 6, \quad \tau_3(2) = 12, \quad \tau_3(3) = 8, \quad \tau_3(4) = 6, \quad \tau_3(5) = 24$$

$$\tau_3(6) = 24, \quad \tau_3(7) = 0, \quad \tau_3(8) = 12, \quad \tau_3(9) = 30, \quad \tau_3(10) = 24.$$

Iz Teorema 9. slijedi da za beskonačno mnogo brojeva n vrijedi $\tau_3(n) = 0$.
Što se tiče broja $T_3(n) = \tau_3(1) + \tau_3(2) + ... + \tau_3(n)$, geometrijsko značenje je slično kao za sumu kvadrata dva prirodna broja. Racionalne točke ravnine zamjenjujemo točkama trodimenzionalnog prostora čije koordinate su cijeli brojevi, a umjesto krugova i kvadrata imamo kugle i kocke. Vrijedi nejednakost

$$\tfrac{4}{3}\pi\left(\sqrt{n} - \tfrac{\sqrt{3}}{2}\right)^3 - 1 < T_3(n) < \tfrac{4}{3}\pi\left(\sqrt{n} + \tfrac{\sqrt{3}}{2}\right)^3 - 1.$$

Iz ovoga dobivamo da za svaki prirodan broj n vrijedi

$$|T_3(n) - \tfrac{4}{3}\pi n\sqrt{n}| < 10n,$$

odakle slijedi

$$\lim_{n\to\infty} \frac{T_3(n)}{\frac{4}{3}\pi n\sqrt{n}} = 1.$$

Označimo s $f(x)$ broj prirodnih brojeva x koji se mogu prikazati kao suma kvadrata tri prirodna broja. Iz Gaussovog teorema slijedi da je broj $x - f(x)$ broj brojeva koji su manji ili jednaki x i oblika $4^l(8k+7)$, pri čemu su k, l nenegativni cijeli brojevi.
Stoga, za dani nenegativni cijeli broj l imamo $8(k+1)-1 \leq 4^{-l}x$ pa je $k+1 \leq \frac{1}{8}(4^{-l}x+1)$. Dakle, kao neposrednu posljedicu dobivamo

$$x - f(x) = \sum_{l=0}^{[x]} \left[\frac{4^{-l}x+1}{8}\right].$$

Ako je $l > \log x/\log 4$, tada $4^l > x > x/7$, odakle slijedi $(4^{-l}x+1)/8 < 1$. Kao posljedicu dobivamo

$$x - f(x) = \sum_{l=0}^{[\log x/\log 4]} \left[\frac{4^{-l}x+1}{8}\right]$$

pa je

$$x - f(x) = \sum_{l=0}^{[\log x/\log 4]} \frac{4^{-l}x+1}{8} - a\Big(\frac{\log x}{\log 4}+1\Big),$$

gdje je $0 \leq a \leq 1$. Ali,

$$\sum_{l=[\log x/\log 4]+1}^{\infty} 4^{-l} = \frac{4}{3}\cdot 4^{-[\log x \log 4]-1} < \frac{4}{3}\cdot 4^{-\log x/\log 4} = \frac{4}{3x}.$$

Kako je

$$\sum_{l=0}^{\infty} \frac{4^{-l}x}{8} = \frac{x}{6},$$

dobivamo

$$\lim_{x\to+\infty} \frac{x - f(x)}{x} = \frac{1}{6}$$

odakle slijedi

$$\lim_{x\to+\infty} \frac{f(x)}{x} = \frac{5}{6}.$$

Ovu formulu otkrio je matematičar Edmund Landau 1908. godine.

Primjer 8. (vidjeti [5], Chapter XI, §4, Exercises 1.) Dokažimo da broj 130 nema prikaz u obliku sume kvadrata tri prirodna broja.
Rješenje:
Neka je $130 = a^2 + b^2 + c^2$, pri čemu su a, b, c prirodni brojevi. Bez smanjenja općenitosti

pretpostavimo da $a \geq b \geq c$. Tada je $a^2 + 1 + 1 \leq 130 \leq 3a^2$ odakle slijedi $43 < a^2 \leq 128$ i $7 \leq a \leq 11$.
Ali kako je $130 - 7^2 = 81 = 3^4$, $130 - 8^2 = 66 = 2 \cdot 3 \cdot 11$, $130 - 9^2 = 49 = 7^2$, $130 - 10^2 = 30 = 2 \cdot 3 \cdot 5$, $130 - 11^2 = 9 = 3^2$ i gledajući faktorizaciju brojeva $81, 66, 49, 30, 9$ na proste faktore, vidimo da ni jedan od njih ne zadovoljava uvjete Teorema 8. pa se ni jedan od brojeva $81, 66, 49, 30, 9$ ne može prikazati kao suma kvadrata dva prirodna broja. Stoga pretpostavka da je broj 130 suma kvadrata tri prirodna broja dovodi do kontradikcije.
Lako se može dokazati da je 130 najmanji broj oblika $2(8k + 1)$ koji nije suma kvadrata tri prirodna broja.

Primjer 9. (vidjeti [5], Chapter XI, §4, Exercises 2.) Koristeći Gaussov teorem dokažimo da prirodan broj ima zapis u obliku sume kvadrata tri racionalna broja ako i samo ako je suma kvadrata tri cijela broja.
Rješenje:
Pretpostavimo da je prirodan broj n suma kvadrata tri racionalna broja. Svodeći sva tri racionalna broja na isti nazivnik možemo pisati $m^2n = a^2 + b^2 + c^2$, gdje su a, b, c cijeli brojevi.
Ako je $n = 4^l(8k+7)$, pri čemu su k, l nenegativni cijeli brojevi, $m = 2^r(2s+1)$, pri čemu su s, r nenegativni cijeli brojevi, dobivamo $m^2n = 4^{k+r}(8t+7)$ gdje su $k+r$ i t nenegativni cijeli brojevi. Na temelju Teorema 9. ovo je nemoguće jer je $m^2n = a^2 + b^2 + c^2$. Kao posljedica, broj n ne može biti oblika $4^l(8k + 7)$ gdje su k, l cijeli brojevi. Prema Gaussovom teoremu, to je suma kvadrata tri cijela broja.

Primjer 10. (vidjeti [5], Chapter XI, §4, Exercises 4.) Koristeći se Gaussovim teoremom dokažimo da je svaki neparan broj oblika $a^2 + b^2 + 2c^2$, pri čemu su a, b, c cijeli brojevi.
Rješenje:
Neka je t proizvoljan nenegativan cijeli broj. Broj $4t + 2$ nije oblika $4^l(8k + 7)$, gdje su k, l nenegativni cijeli brojevi. Stoga, prema Gaussovom teoremu vrijedi $4t + 2 = x^2 + y^2 + z^2$, pri čemu su x, y, z cijeli brojevi. Kako lijeva strana jednakosti nije djeljiva sa 4, nisu svi od brojeva x, y, z parni. Međutim, broj neparnih brojeva među njima mora biti paran. Stoga, neka su x, y neparni, a z paran broj, tj. $z = 2c$. Brojevi $x + y$ i $x - y$ su parni brojevi pa je $x + y = 2a$, $x - y = 2b$ odakle je $x = a + b$, $y = a - b$.
Stoga je $4t + 2 = (a + b)^2 + (a - b)^2 + 4c^2$ odakle je $2t + 1 = a^2 + b^2 + 2c^2$, gdje su a, b, c cijeli brojevi.

Primjer 11. (vidjeti [5], Chapter XI, §4, Exercises 5.) Na temelju Gaussovog teorema pokažimo da je svaki prirodan broj oblika $a^2 + b^2 + c^2$ ili oblika $a^2 + b^2 + 2c^2$, pri čemu su a, b, c cijeli brojevi.
Rješenje:
Ako prirodan broj nije suma kvadrata tri cijela broja, tada je prema Gaussovom teoremu oblika $4^l(8k + 7)$, gdje su k, l nenegativni cijeli brojevi. Prema Primjeru 10. dobivamo $8k+7 = x^2+y^2+2z^2$, gdje su x, y, z cijeli brojevi. Kako je $4^l(8k+7) = (2^l x)^2+(2^l y)^2+(2^l z)^2$, slijedi da je prirodan broj oblika $a^2 + b^2 + 2c^2$, pri čemu su a, b, c cijeli brojevi.

Primjer 12. (vidjeti [5], Chapter XI, §4, Exercises 8.) Pokažimo da postoji beskonačno mnogo prostih brojeva oblika $a^2+b^2+c^2+1$, gdje su a, b, c prirodni brojevi. Za dokaz ćemo koristiti Gaussov teorem.
Rješenje:
Prema Teoremu 3. postoji beskonačno mnogo prostih brojeva oblika $8k+7$. Ako je p prost broj ovog oblika, tada je $p-1=8k+6$. Prema Gaussovom teoremu, svaki broj oblika $8k+6$ je suma kvadrata tri prirodna broja. Tako je $p-1=a^2+b^2+c^2$, gdje su a, b, c prirodni brojevi, pa slijedi da je $p=a^2+b^2+c^2+1$.

Primjer 13. (vidjeti [5], Chapter XI, §4, Exercises 9.) Pronađimo primjer koji pokazuje da umnožak dva broja koji su suma kvadrata tri prirodna broja ne mora biti u obliku sume kvadrata tri prirodna broja.
Rješenje:
Broj $63=3\cdot 21=(1^2+1^2+1^2)(1^2+2^2+4^2)$. Međutim, broj 63 je oblika $8k+7$ pa ne može biti suma kvadrata tri prirodna broja.

5 Suma četiri kvadrata

5.1 Prikaz brojeva u obliku sume četiri kvadrata

Lema 4. (vidjeti [5], Chapter XI, §5, Lemma 1.) Neka neparan prost broj p dijeli sumu kvadrata četiri cijela broja pri čemu barem jedan cijeli broj nije djeljiv sa p. Tada se p može zapisati u obliku sume kvadrata četiri cijela broja.

Dokaz. Pretpostavimo da prost broj p zadovoljava pretpostavku leme. Tada postoji višekratnik broja p koji je suma kvadrata četiri cijela broja pri čemu nisu svi djeljivi s p. Neka je n najmanji takav višekratnik od p. Tada vrijedi $n = mp$, pri čemu je m prirodan broj, i $n = a^2 + b^2 + c^2 + d^2$, pri čemu su a, b, c, d cijeli brojevi pri čemu barem jedan, recimo a, nije djeljiv s p.
Neka su a_0, b_0, c_0, d_0 cijeli brojevi takvi da je

$$a_0 \equiv a \pmod{p}, \qquad b_0 \equiv b \pmod{p}, \qquad c_0 \equiv c \pmod{p}, \qquad d_0 \equiv d \pmod{p}$$

i

$$|a_0| < p/2, \qquad |b_0| < p/2, \qquad |c_0| < p/2, \qquad |d_0| < p/2.$$

Kako bismo pronašli broj a_0, na primjer, dovoljno je pronaći ostatak r pri dijeljenju broja a brojem p i staviti da je $a_0 = r$ ako je $r < p/2$ ili $a_0 = r - p$ ako je $r > p/2$.
Budući da a nije djeljiv sa p pa ni sa a_0, primjenom navedenih jednakosti i kongruencija imamo da je

$$a_0^2 + b_0^2 + c_0^2 + d_0^2 \equiv a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod{p}.$$

Prema definiciji broja n i gornjim nejednakostima dobivamo da je

$$n \leq a_0^2 + b_0^2 + c_0^2 + d_0^2 < 4(p/2)^2.$$

Kao posljedica, $n < p^2$ pa slijedi $mp < p^2$, odakle je $m < p$.
Kako je $n = mp$ i $n = a^2 + b^2 + c^2 + d^2$ preostaje dokazati da je $m = 1$. Neka je $m \neq 1$. Kako je m prirodan broj i $m < p$, vrijedi $1 < m < p$.
Pronašli smo prirodne brojeve a_1, b_1, c_1, d_1 koji zadovoljavaju uvjet

$$a_1 \equiv a \pmod{m}, \qquad b_1 \equiv b \pmod{m}, \qquad c_1 \equiv c \pmod{m}, \qquad d_1 \equiv d \pmod{m}$$

i

$$|a_1| < m/2, \qquad |b_1| < m/2, \qquad |c_1| < m/2, \qquad |d_1| < m/2.$$

Uočimo da $a_1^2 + b_1^2 + c_1^2 + d_1^2 \equiv a^2 + b^2 + c^2 + d^2 \pmod{m}$, odakle slijedi $m \mid a_1^2 + b_1^2 + c_1^2 + d_1^2$. Dakle,

$$a_1^2 + b_1^2 + c_1^2 + d_1^2 = ml, \text{ pri čemu je } l \text{ nenegativan cijeli broj.}$$

Ako je $l = 0$, tada je $a_1 = b_1 = c_1 = d_1 = 0$ pa vrijedi da su svi brojevi a, b, c, d djeljivi s m. Iz $n = a^2 + b^2 + c^2 + d^2$ slijedi da je n djeljiv s m^2 i $m \mid p$ što je u kontradikciji s $1 < m < p$ jer je p prost broj. Kao posljedica, l je prirodan broj.
Pretpostavimo da $|a_1| = |b_1| = |c_1| = |d_1| = m/2$. Ovo je moguće ako je m paran broj, tj. ako je $m = 2k$, pri čemu je k prirodan broj. Iz $a_1 \equiv a \pmod{m}$ dobivamo jednakost $a = a_1 + mt$, gdje je t cijeli broj. S obzirom da je $|a_1| = |b_1| = |c_1| = |d_1| = m/2$ i $m = 2k$, slijedi $a = \pm k + 2kt = (2t \pm 1)k = k_1 k$, gdje je k_1 neparan broj. Na sličan način dobivamo da je

$$a = k_1 k, \qquad b = k_2 k, \qquad c = k_3 k, \qquad d = k_4 k,$$

gdje su k_1, k_2, k_3, k_4 neparni brojevi. S obzirom da je $n = mp$, $m = 2k$ i $n = a^2 + b^2 + c^2 + d^2$, slijedi da je $n = 2kp = k^2(k_1^2 + k_2^2 + k_3^2 + k_4^2)$. Kao posljedica, $2p = k(k_1^2 + k_2^2 + k_3^2 + k_4^2)$. Kako je kvadrat neparnog broja kongruentan 1 modulo 4 zaključujemo da je drugi faktor na desnoj strani zadnje jednakosti djeljiv sa 4 pa vrijedi da $2 \mid p$ što je kontradikcija s pretpostavkom. Time smo pokazali da jednakosti $|a_1| = |b_1| = |c_1| = |d_1| = m/2$ ne vrijede. Kao posljedica, za barem jednu od nejednadžbi $|a_1| \leq m/2$, $|b_1| \leq m/2$, $|c_1| \leq m/2$, $|d_1| \leq m/2$ vrijedi nejednakost. Iz toga slijedi da je $a_1^2 + b_1^2 + c_1^2 + d_1^2 < 4 \cdot \frac{m^2}{4}$, odakle zbog $a_1^2 + b_1^2 + c_1^2 + d_1^2 = ml$ dobivamo $ml < m^2$ pa je $l < m$.
Razmotrimo sada Eulerov identitet

$$(a^2 + b^2 + c^2 + d^2)(a_1^2 + b_1^2 + c_1^2 + d_1^2) =$$
$$(aa_1 + bb_1 + cc_1 + dd_1)^2 + (ab_1 - ba_1 + cd_1 - dc_1)^2 + (ac_1 - ca_1 + db_1 - bd_1)^2 + (ad_1 - da_1 + bc_1 - cb_1)^2.$$

Kako je $n = mp$, $n = a^2 + b^2 + c^2 + d^2$ i $a_1^2 + b_1^2 + c_1^2 + d_1^2 = ml$, lijeva strana jednakosti jednaka je $m^2 lp$.
Iz navedenih kongruencija dobivamo da je

$$a_1 = a + ma_2, \qquad b_1 = b + mb_2, \qquad c_1 = c + mc_2, \qquad d_1 = d + md_2,$$

gdje su a_2, b_2, c_2, d_2 cijeli brojevi. Dobivamo

$$\begin{aligned}
aa_1 + bb_1 + cc_1 + dd_1 &= a^2 + b^2 + c^2 + d^2 + m(aa_2 + bb_2 + cc_2 + dd_2) \\
&= m(p + aa_2 + bb_2 + cc_2 + dd_2) = mt_1, \\
ab_1 - ba_1 + cd_1 - dc_1 &= m(ab_2 - ba_2 + cd_2 - dc_2) = mt_2, \\
ac_1 - ca_1 + db_1 - bd_1 &= m(ac_2 - ca_2 + db_2 - bd_2) = mt_3, \\
ad_1 - da_1 + bc_1 - cb_1 &= m(ad_2 - da_2 + bc_2 - cb_2) = mt_4,
\end{aligned}$$

gdje su t_1, t_2, t_3, t_4 cijeli brojevi. Uvrštavanjem u Eulerov identitet dobivamo
$m^2 lp = m^2(t_1^2 + t_2^2 + t_3^2 + t_4^2)$, odakle slijedi $lp = t_1^2 + t_2^2 + t_3^2 + t_4^2$.
Ako su brojevi t_1, t_2, t_3, t_4 djeljivi s p, tada $p^2 \mid lp$ i $p \mid l$ što je nemoguće jer je l prirodan broj i $l < p$.
Formula $lp = t_1^2 + t_2^2 + t_3^2 + t_4^2$ prikazuje broj lp kao sumu kvadrata četiri cijela broja pri čemu nisu svi djeljivi s p. Iz definicije broja n slijedi $n \leq lp$ i $mp \leq lp$, odakle je $m \leq l$ što

je kontradikcija s $l < m$. Uočavamo da pretpostavka $m \neq 1$ dovodi do kontradikcije. Kao posljedica, mora vrijediti da je $m = 1$ i to je upravo ono što smo trebali dokazati.

□

Lema 5. (vidjeti [5], Chapter XI, §5, Lemma 2.) Svaki prost broj ima zapis u obliku sume kvadrata četiri cijela broja.

Dokaz. Kako je $2 = 1^2 + 1^2 + 0^2 + 0^2$, nema smanjenja općenitosti u pretpostavci da je p neparan prost broj. Prema Lemi 4. dovoljno je pokazati da je p djelitelj sume kvadrata četiri cijela broja pri čemu nisu svi djeljivi s p. Ostaci dobiveni dijeljenjem brojeva

$$1 + 0^2, 1 + 1^2, ..., 1 + \left(\tfrac{p-1}{2}\right)^2$$

brojem p su različiti jer brojevi $0^2, 1^2, ..., \left(\frac{p-1}{2}\right)^2$ pri dijeljenju s brojem p daju različite ostatke. Slično, brojevi

$$-0^2, -1^2, ..., -\left(\tfrac{p-1}{2}\right)^2$$

pri dijeljenju brojem p daju različite ostatke. Pretpostavimo da su ostaci pri dijeljenju brojeva $1 + 0^2, 1 + 1^2, ..., a + \left(\frac{p-1}{2}\right)^2$ brojem p različiti od ostataka pri dijeljenju brojeva $-0^2, -1^2, ..., -\left(\frac{p-1}{2}\right)^2$ brojem p.
Tada je ukupan broj različitih ostataka pri dijeljenju tih brojeva brojem p jednak $2\left(1+\frac{p-1}{2}\right) = p + 1$, što je nemoguće. Kao posljedica, postoji barem jedan član niza $1 + 0^2, 1 + 1^2, ..., a + \left(\frac{p-1}{2}\right)^2$, recimo $1 + x^2$, koji daje isti ostatak kao član niza $-0^2, -1^2, ..., -\left(\frac{p-1}{2}\right)^2$, recimo $-y^2$. Dobivamo da $p \mid 1^2 + x^2 + y^2 + 0^2$ što pokazuje da p dijeli sumu kvadrata četiri cijela broja pri čemu jedan cijeli broj nije djeljiv brojem p. Prema Lemi 4. p je suma kvadrata četiri cijela broja i time smo dokazali ovu lemu.

□

Teorem 10. (**Lagrangeov teorem**, vidjeti [5], Chapter XI, §5, Theorem 4.) Svaki nenegativan cijeli broj ima prikaz kao suma kvadrata četiri cijela broja.

Dokaz. Prema Eulerovom identitetu, produkt dva broja, pri čemu je svaki od njih suma četiri kvadrata, je također suma četiri kvadrata. Ovo se indukcijom dokazuje za svaki konačni broj faktora. Kako je svaki broj veći od 1 umnožak prostih brojeva, prema Lemi 5. zaključujemo da je sam broj suma četiri kvadrata. Budući da je $0 = 0^2+0^2+0^2+0^2$ i $1 = 1^2+0^2+0^2+0^2$, teorem je dokazan.

□

Spomenut ćemo rezultate istraživanja matematičara Derricka Henrya Lehmera koji je rekao da među prirodnim brojevima samo brojevi $1, 2, 5, 7, 11, 15, 23$ i brojevi oblika $4^h m$, pri čemu je $h = 0, 1, 2, ...$, $m = 2, 6$ ili 14, su takvi da je prikaz bilo kojeg od njih kao suma četiri kvadrata jedinstven osim redoslijeda pribrojnika.
Indijski matematičar Srinivasa Ramanujan je istraživao sustave prirodnih brojeva a, b, c, d takve da se svaki prirodan broj n može prikazati u obliku $ax^2 + by^2 + cz^2 + dt^2$, pri čemu su

x, y, z, t cijeli brojevi. Dokazao je da za fiksni redosljed brojeva a, b, c, d, recimo $a \leq b \leq c \leq d$, postoji 54 takva sustava, naime

$$1, 1, 1, d \text{ gdje je } d = 1, ..., 7;$$
$$1, 1, 2, d \text{ gdje je } d = 2, ..., 14;$$
$$1, 1, 3, d \text{ gdje je } d = 3, ..., 6;$$
$$1, 2, 2, d \text{ gdje je } d = 2, ..., 7;$$
$$1, 2, 3, d \text{ gdje je } d = 3, ..., 10;$$
$$1, 2, 4, d \text{ gdje je } d = 4, ..., 14;$$
$$1, 2, 5, d \text{ gdje je } d = 6, ..., 10.$$

Teorem 11. (**Jacobijev teorem**, vidjeti [5], Chapter XI, §5) Svaki prirodan broj je oblika $x^2 + 2y^2 + 3z^2 + 6t^2$, pri čemu su x, y, z, t cijeli brojevi.

Dokaz. Neka je n prirodan broj. Prema Teoremu 10. postoje cijeli brojevi a, b, c, d takvi da je

$$n = a^2 + b^2 + c^2 + d^2.$$

Dokazat ćemo da nakon odgovarajuće promjene zapisa i predznaka od a, b, c, d vrijedi da $3 \mid a+b+c$. Ovo vrijedi ako su barem tri od brojeva a, b, c, d djeljiva sa 3. Pretpostavimo da su samo dva broja, recimo c i d, djeljiva sa 3. Tada je $a \equiv \pm 1 \pmod 3$ i $b \equiv \pm 1 \pmod 3$, odakle za prikladan izbor predznaka imamo $3 \mid a \pm b$ pa $3 \mid a \pm b + c$. Konačno, ako barem tri od brojeva a, b, c, d, recimo a, b, c, nisu djeljiva sa 3, tada za prikladan izbor predznaka $\pm$ imamo $3 \mid a \pm b \pm c$.
Stoga bez smanjenja općenitosti možemo pretpostaviti da

$$a + b + c = 3z,$$

pri čemu je z cijeli broj. Ali, između tri cijela broja barem su dva iste parnosti. Dakle, dodatno možemo pretpostaviti da $a \equiv b \pmod 2$), odakle slijedi $a + b = 2k$, pri čemu je k cijeli broj pa je $a - b = 2(k - b) = 2y$, pri čemu je y cijeli broj. Lako možemo provjeriti da vrijedi sljedeća jednakost

$$3(a^2 + b^2 + c^2) = (a + b + c)^2 + 2\left(\tfrac{a+b}{2} - c\right)^2 + 6\left(\tfrac{a-b}{2}\right)^2,$$

odakle slijedi

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

pa zbog $a + b + c = 3z$ vrijedi da $3 \mid k - c$ pa je $k - c = 3t$, pri čemu je t cijeli broj. Kako je $a + b + c = 3z$ i $n = a^2 + b^2 + c^2 + d^2$ vrijedi da $a^2 + b^2 + c^2 = 3z^2 + 6t^2 + 2y^2$ i $n = d^2 + 2y^2 + 3z^2 + 6t^2$ i time smo došli do kraja dokaza ovog teorema.

□

Primjer 14. (vidjeti [5], Chapter XI, §6, Exercises 1.) Na temelju Teorema 10. dokažimo da se svaki prirodan broj koji je djeljiv brojem 8 može prikazati kao suma kvadrata osam neparnih cijelih brojeva.
Rješenje:
Ako je n prirodan broj, tada prema Teoremu 10. postoje četiri cijela broja a, b, c, d takva da

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

odakle je

$$8n = (2a-1)^2 + (2a+1)^2 + (2b-1)^2 + (2b+1)^2 + (2c-1)^2 + (2c+1)^2 + (2d-1)^2 + (2d+1)^2.$$

Primjer 15. (vidjeti [5], Chapter XI, §6, Exercises 2.) Dokažimo da ne postoji prirodan broj djeljiv s 8 koji je suma kvadrata manje od osam neparnih cijelih brojeva.
Rješenje:
Suma kvadrata od s neparnih brojeva je oblika $8k + s$, pri čemu je k nenegativan cijeli broj. Ako je suma djeljiva brojem 8, tada $8 \mid s$ i $s \geq 8$.

5.2 Suma kvadrata četiri prirodna broja

Na temelju Teorema 10. možemo zaključiti da se svaki prirodan broj može prikazati kao suma kvadrata četiri ili manje prirodnih brojeva. Koristeći Gaussov teorem dokazat ćemo sljedeći teorem.

Teorem 12. (vidjeti [5], Chapter XI, §6, Theorem 5.) Prirodan broj n ima prikaz u obliku sume kvadrata četiri prirodna broja ako i samo ako ne pripada nizu brojeva $1, 3, 5, 9, 11, 17, 29, 41, 4^h \cdot 2, 4^h \cdot 6, 4^h \cdot 14$, pri čemu je $h = 0, 1, 2, ...$

Dokaz. Reći ćemo da je prirodan broj S_m ako je suma kvadrata m prirodnih brojeva. Direktno se može vidjeti da niti jedan od brojeva $1, 3, 5, 9, 11, 29, 41$ nije S_4. Na primjer, dokazat ćemo da broj 41 nije S_4. Pretpostavimo suprotno, tj. da je 41 S_4. Tada imamo $41 = a^2 + b^2 + c^2 + d^2$, pri čemu su a, b, c, d prirodni brojevi i $a \geq b \geq c \geq d$. Stoga je $a^2 < 41 \leq 4a^2$ i $4 \leq a \leq 6$. Ako je $a = 6$, tada je $5 = b^2 + c^2 + d^2$, što je nemoguće. Ako je $a = 5$, tada je $16 = b^2 + c^2 + d^2$, što je također nemoguće jer 16 nije S_3. Ako je $a = 4$, tada je $25 = b^2 + c^2 + d^2$, što je nemoguće jer 25 nije S_3. Prema tome, 41 ne može biti S_4.
Neka broj m označava bilo koji od brojeva $2, 6, 14$. Tada je m oblika $4k + 2$. Pretpostavimo da postoji nenegativni cijeli broj h takav da je $4^h m$ S_4. Neka h označava najmanji takav cijeli broj. Budući da $2, 6, 14$ nisu S_4 vrijedi da je $h \geq 1$. Tada imamo $4^h m = a^2 + b^2 + c^2 + d^2$, pri čemu su a, b, c, d prirodni brojevi. Lijeva strana jednakosti je djeljiva brojem 8 jer je $h \geq 1$ i $m = 2(2k + 1)$. Iz ovoga možemo zaključiti da svaki od brojeva a, b, c, d mora biti paran. Neka je $a = 2a_1$, $b = 2b_1$, $c = 2c_1$, $d = 2d_1$, pri čemu su a_1, b_1, c_1, d_1 prirodni brojevi. Stoga je $4^{h-1} m = a_1^2 + b_1^2 + c_1^2 + d_1^2$, a to znači da je $4^{h-1} m$ S_4 što je kontradikcija s definicijom broja h. Time smo dokazali da broj $4^h m$, pri čemu je $m = 2, 6, 14$, nije S_4 za nenegativne cijele brojeve h. Time smo pokazali nužnost uvjeta Teorema 12.

Sada označimo s n neparan prirodan broj koji zadovoljava uvjet Teorema 12. Kao posljedica, $n \neq 1, 3, 5, 9, 11, 17, 29, 41$. Kako je n neparan, on mora biti u jednom od oblika $8k+1$, $8k+3$, $8k+5$, $8k+7$.

Pretpostavimo da je $n = 8k+1$. Razmotrit ćemo četiri slučaja: $k = 4t$, $k = 4t+1$, $k = 4t+2$, $k = 4t+3$. Ako je $k = 4t$, tada je $n = 32t+1$. Kako je $n \neq 1$ mora vrijediti da je $t \geq 1$ i $t = u+1$, pri čemu je u nenegativan cijeli broj. Stoga je $n = 32(u+1)+1 = 4(8u+6)+9$. Prema Gaussovom teoremu broj $8u+6$ je suma kvadrata tri cijela broja. Budući da $8u+6 = 2(4u+3)$ ne može biti suma kvadrata dva cijela broja, uočavamo da je $8u+6$ S_3, odakle slijedi da je broj $n = 2^2(8u+6)+3^2$ S_4.

Ako je $k = 4t+1$, tada je $n = 32t+9$. Kako je $n \neq 9$ i $n \neq 41$ vrijedi da je $t \geq 2$ pa je $t = u+2$, pri čemu je u nenegativan cijeli broj. Stoga je $n = 32(u+2)+9 = 2^2(8u+6)+7^2$ pa zaključujemo da je n S_4.

Ako je $k = 4t+2$, tada je $n = 32t+17$ i s obzirom da je $n \neq 17$ vrijedi da je $t \geq 1$ pa je $t = u+1$, pri čemu je u nenegativan cijeli broj. Stoga je $n = 32(u+1)+17 = 2^2(8u+6)+5^2$ pa vrijedi da je n S_4.

Ako je $k = 4t+3$, tada je $n = 32t+25 = 2^2(8t+6)+1^2$ i vrijedi da je n S_4. Stoga vidimo da je uvjet Teorema 12. dovoljan pod uvjetom da je $n = 8k+1$.

Sada pretpostavimo da je $n = 8k+3$. Kako je $n \neq 3$ i $n \neq 11$, vrijedi da je $k \geq 2$ pa je $k = t+2$, pri čemu je t nenegativan cijeli broj. Tada je $n = 8(t+2)+3 = 8t+3+4^2$. Dakle, na temelju Gaussovog teorema koji implicira da je broj $8t+3$ suma kvadrata tri neparna broja, možemo zaključiti da je n S_4. Vidimo da je uvjet Teorema 12. dovoljan pod uvjetom da je $n = 8k+3$.

Nadalje, pretpostavimo da je $n = 8k+5$. Razmotrit ćemo četiri slučaja: $k = 4t$, $k = 4t+1$, $k = 4t+2$, $k = 4t+3$. Ako je $k = 4t$, tada je $n = 32t+5$. Kako je $n \neq 5$ imamo da je $t > 0$ pa je $t = u+1$, pri čemu je u nenegativan cijeli broj. Stoga je $n = 32(u+1)+5 = 2^2(8u+3)+5^2$, odakle možemo zaključiti da je n S_4.

Ako je $k = 4t+1$, tada je $n = 32t+13 = 2^2(8t+3)+1^2$ pa možemo zaključiti da je n S_4.

Ako je $k = 4t+2$, tada je $n = 32t+21 = 2^2(8t+3)+3^2$ pa zaključujemo da je n S_4.

Ako je $k = 4t+3$, tada je $n = 32t+29$. S obzirom da je $n \neq 29$ vrijedi da je $t > 0$ pa je $t = u+1$, pri čemu je u nenegativan cijeli broj. Dobivamo da je $n = 32(u+1)+29 = 2^2(8u+3)+7^2$ odakle možemo uočiti da je n S_4. Uvjet Teorema 12. je dovoljan pod uvjetom da je $n = 8k+5$.

Konačno, pretpostavimo da je $n = 8k+7$. Tada, prema Teoremu 10., postoje cijeli brojevi a, b, c, d takvi da je $n = a^2+b^2+c^2+d^2$. S druge strane, prema Teoremu 9., kako je $n = 8k+7$ niti jedan od brojeva a, b, c, d ne može biti jednak nuli. Stoga vrijedi da je n S_4.

Time smo dokazali sljedeće: da bi neparan prirodni broj bio suma kvadrata četiri prirodna broja potrebno je i dovoljno da ne bude niti jedan od brojeva $1, 3, 5, 9, 11, 17, 29, 41$. Iz ovoga slijedi da je bilo koji neparan prirodan broj veći od 41 suma kvadrata četiri prirodna broja.

Označimo s n paran prirodan broj različit od $4^h \cdot 2$, $4^h \cdot 6$, $4^h \cdot 14$ pri čemu je $h = 0, 1, 2, ...$ Označimo s 4^h najveću potenciju broja 4 koja dijeli broj n. Imamo $n = 4^h m$, pri čemu m nije djeljiv brojem 4. Kao posljedica, $m = 4k+1$, $m = 4k+2$ ili $m = 4k+3$.

Ako je $m = 4k+1$ takav da je k paran, tj. $k = 2t$, tada je $m = 8t+1$ S_4 ako je $m \neq 1, 9, 17, 41$. Također, tada je $n = 4^h m$ S_4. Ali, s obzirom da je n paran i m nije djeljiv sa 4 mora vrijediti da $h > 0$. Jasno je da je broj 4 S_4. Nadalje, $4 \cdot 17 = 68 = 1^2 + 3^2 + 3^2 + 7^2$ i $4 \cdot 41 = 164 = 1^2 + 1^2 + 9^2 + 9^2$, odakle vrijedi da su $4^h \cdot 1 = 4(2^{h-1})^2$, $4^h \cdot 9 = 4(2^{h-1} \cdot 3)^2$, $4^h \cdot 17 = 4 \cdot 17(2^{h-1})^2$, $4^h \cdot 41 = 4 \cdot 41(2^{h-1})^2$ S_4.
Tako uočavamo da ako je $m = 4k + 1$ i k paran, tada je $n = 4^h m$ S_4. Ako je $m = 4k + 1$ i k neparan, tj. $k = 2t + 1$, tada je $m = 8t + 5$ S_4 pod uvjetom da je $m \neq 5$ i $m \neq 29$. Ali, $4 \cdot 5 = 20 = 1^2 + 1^2 + 3^2 + 3^2$ i $4 \cdot 29 = 116 = 1^2 + 3^2 + 5^2 + 9^2$, pa s obzirom da je m neparan, n paran i h prirodan broj zaključujemo da su oba broja S_4. Time smo dokazali da ako je $m = 4k + 1$, tada je $n = 4^h m$ S_4.
Pretpostavimo da je $m = 4k + 2$. Ako je $k = 2t$, tada imamo $m = 8t + 2$. S obzirom da je $n \neq 4^h \cdot 2$ i $n = 4^h m$, imamo da je $m \neq 2$ pa je $t > 0$, tj. $t = u + 1$, pri čemu je u nenegativan cijeli broj. Tada je $m = 8(u + 1) + 2 = 8u + 6 + 2^2$. S obzirom da smo prethodno pokazali da je $8u + 6$ S_3, možemo zaključiti da je m S_4, a kao posljedica je i $n = 4^h m$ S_4.
Ako je $k = 2t + 1$, tada je $m = 8t + 6$. Kako je $n \neq 4^h \cdot 6$ i $n \neq 4^h \cdot 14$ vrijedi da je $t \geq 2$ pa je $t = u + 2$ pri čemu je u nenegativan cijeli broj. Tada je $m = 8(u + 2) + 6 = 8u + 6 + 4^2$. S obzirom na činjenicu da je $8u + 6$ S_3, vrijedi da je m S_4 pa slijedi da je $n = 4^h m$ također S_4. Time smo dokazali da ako je $m = 4k + 2$, tada je $n = 4^h m$ S_4.
Konačno, ako je $m = 4k + 3$, tada u slučaju $k = 2t$ imamo da je $m = 8t + 3$. Kao što smo pokazali ranije, za $m \neq 3$ i $m \neq 11$ broj $m = 8t + 3$ je S_4. Ako je $m = 4k + 3$, tada je broj $n = 4^h m$ S_4 pod uvjetom da $n \neq 4^h \cdot 3$ i $n \neq 4^h \cdot 11$. Ali vrijedi, $4 \cdot 3 = 12 = 1^2 + 1^2 + 1^2 + 3^2$ i $4 \cdot 11 = 44 = 1^2 + 3^2 + 3^2 + 5^2$. Tada je $n = 4^h m$, pri čemu je $h > 0$, S_4 jer je n paran i m neparan broj.
U slučaju $k = 2t + 1$ dobivamo da $m = 8t + 7$ pa vrijedi da je m S_4, a iz toga slijedi da je $n = 4^h m$ također S_4. Time smo dokazali da ako je $m = 4k + 3$, tada je $n = 4^h m$ S_4.
Rezultate koje smo upravo dokazali sažimamo u sljedećoj izjavi: ako je n paran broj različit od $4^h \cdot 2$, $4^h \cdot 6$, $4^h \cdot 14$, pri čemu je $h = 0, 1, 2, ...$, tada vrijedi da je n S_4. Također smo dokazali da je paran broj n u obliku sume kvadrata četiri prirodna broja ako i samo ako n nije niti jedan od brojeva $4^h \cdot 2$, $4^h \cdot 6$, $4^h \cdot 14$, pri čemu je $h = 0, 1, 2, ...$
Time smo, u kombinaciji s rezultatima dobivenim za neparne brojeve, dovršili dokaz Teorema 12.

□

Iz Teorema 12. slijedi korolar.

Korolar 3. (vidjeti [5], Chapter XI, §6, Corollary) Kvadrat bilo kojeg prirodnog broja većeg od 1, s iznimkom 3^2, je suma kvadrata četiri prirodna broja.

Primjer 16. (vidjeti [5], Chapter XI, §6, Exercise) Bez korištenja Gaussovog teorema, dokažimo da je svaki pozitivan racionalan broj suma kvadrata četiri pozitivna racionalna broja.
Rješenje:
Neka je r pozitivan racionalan broj, tj. $r = l/m$ pri čemu su l i m prirodni brojevi. Prema Teoremu 10. vrijedi da je svaki prirodan broj suma kvadrata četiri ili manje prirodnih

brojeva. Ako je $lm = a^2 + b^2 + c^2 + d^2$, pri čemu su a, b, c, d prirodni brojevi, tada je $r = l/m = (a/m)^2 + (b/m)^2 + (c/m)^2 + (d/m)^2$ pa možemo uočiti da je r suma kvadrata četiri prirodna broja. Ako je $lm = a^2 + b^2 + c^2$, pri čemu su a, b, c prirodni brojevi, tada je $r = l/m = (a/m)^2 + (b/m)^2 + (3c/5m)^2 + (4c/5m)^2$. Ako je $lm = a^2 + b^2$, pri čemu su a, b prirodni brojevi, tada je $r = l/m = (a/m)^2 + (b/3m)^2 + (2b/3m)^2 + (2b/3m)^2$. Konačno, ako je $lm = a^2$, pri čemu je a prirodan broj, tada je $r = l/m = 4(a/2m)^2$. Dakle, u svakom slučaju r je suma kvadrata četiri pozitivna racionalna broja.

Kao što smo dokazali, brojevi oblika 2^n, pri čemu $n = 1, 2, ...$, i brojevi oblika $4^h \cdot 2$, pri čemu je $h = 0, 1, 2, ...$, nisu S_3. S druge strane, za $h = 0, 1, 2, ...$ vrijedi

$$\begin{aligned} 3 &= 1^2 + 1^2 + 1^2, \\ 9 &= 1^2 + 2^2 + 2^2, \\ 11 &= 1^2 + 1^2 + 3^2, \\ 17 &= 2^2 + 2^2 + 3^2, \\ 29 &= 2^2 + 3^2 + 4^2, \\ 41 &= 1^2 + 2^2 + 6^2, \\ 4^h \cdot 6 &= (2^h)^2 + (2^h)^2 + (2^{h+1})^2, \\ 4^h \cdot 14 &= (2^h)^2 + (2^{h+1})^2 + (2^h \cdot 3)^2. \end{aligned}$$

Iz Teorema 12. dobivamo novi teorem.

Teorem 13. (vidjeti [5], Chapter XI, §6, Theorem 6.) Prirodan broj n se može zapisati u obliku sume kvadrata tri ili četiri prirodna broja ako i samo ako broj n nije niti jedan od brojeva $1, 5, 4^h \cdot 2$, pri čemu je $h = 0, 1, 2, ...$

Ovaj teorem, kao posljedicu, daje sljedeći korolar.

Korolar 4. (vidjeti [5], Chapter XI, §6, Corollary) Neparan prirodan broj n ima prikaz u obliku sume kvadrata tri ili četiri prirodna broja ako i samo ako je različit od 1 i 5.

Na ovome korolaru temelji se dokaz sljedećeg teorema.

Teorem 14. (vidjeti [5], Chapter XI, §6, Theorem 7.) Jedini prirodni brojevi n za koje n^2 nije suma kvadrata tri prirodna broja su brojevi $n = 2^h$ i $n = 2^h \cdot 5$, pri čemu je $h = 0, 1, 2, ...$

Dokaz. Dokazali smo da, ako k nije S_3, tada broj $4k$ nije S_3. Kako brojevi 1 i 5^2 nisu S_3, brojevi 4^h i $4^h \cdot 5^2$, za $h = 0, 1, 2, ...$, nisu S_3. Time nam ostaje dokazati da, ako je n prirodan broj različit od 2^h i $2^h \cdot 5$, pri čemu je $h = 0, 1, 2, ...$, tada je n^2 S_3.
Pretpostavimo da je n prirodan broj takav da $n \neq 2^h$ i $n \neq 2^h \cdot 5$, pri čemu je $h = 0, 1, 2, ...$ Neka je s najveći eksponent za koji 2^s dijeli n. Imamo $n = 2^s m$, pri čemu je m neparan. Na temelju uvjeta za broj n, broj m mora biti različit od 1 i 5. Iz Korolara 4. slijedi da je

m suma kvadrata tri ili četiri prirodna broja, tj. $m = a^2 + b^2 + c^2 + d^2$, pri čemu su a, b, c prirodni brojevi i d nenegativan cijeli broj. Stoga je

$$\begin{aligned} m^2 &= (a^2 + b^2 + c^2 + d^2)^2 \\ &= (a^2 + b^2 - c^2 - d^2)^2 + (2(ac + bd))^2 + (2(ad - bc))^2 \\ &= (a^2 + b^2 - c^2 - d^2)^2 + (2(ad + bc))^2 + (2(ac - bd))^2. \end{aligned}$$

S obzirom da je m neparan broj, iz jednadžbe $m = a^2 + b^2 + c^2 + d^2$ slijedi da su među brojevima a, b, c, d jedan ili tri broja neparni, a ostali parni brojevi. Stoga je broj $a^2+b^2-c^2-d^2$ neparan i različit od nule. Kako su a, b, c prirodni brojevi, $ac+bd$ i $ad+bc$ su također prirodni brojevi. Dokazat ćemo da je barem jedan od brojeva $ad-bc, ac-bd$ različit od nule. Pretpostavimo da je $ad = bc$ i $ac = bd$. Tada je $adc = bc^2$ i $acd = bd^2$, odakle je $bc^2 = bd^2$. Kako je $b > 0$, vrijedi da $c^2 = d^2$. S obzirom da $c > 0$ vrijedi da $a = b$, odakle je $m = 2(a^2 + c^2)$, a to je nemoguće jer je m neparan broj. Dakle, barem je jedan od brojeva $ad - bc$ i $ac - bd$ različit od nule. Stoga barem jedna od gore navedenih suma daje prikaz broja m^2 u obliku sume kvadrata tri prirodna broja. Tako dobivamo da $m^2 = x^2+y^2+z^2$, pri čemu su x, y, z prirodni brojevi. Vrijedi da $n^2 = (2^s x)^2 + (2^s y)^2 + (2^s z)^2$, a time je pokazano da je n^2 S_3 i teorem je dokazan.

□

Iz Teorema 14. slijedi da za svaki neparan prirodan broj t različit od 1 i 5 postoje prirodni brojevi x, y, z takvi da je $t^2 = x^2 + y^2 + z^2$. Postavlja se pitanje postoje li za svaki neparan prirodni broj t različit od 1 i 5 prirodni brojevi x, y, z takvi da je njihov najveći zajednički djelitelj jednak broju 1 i $x^2 + y^2 + z^2 = t^2$. Poljski matematičar Andrzej Schnitzel je rekao da postoje takvi brojevi. On je dao nužne i dovoljne uvjete za prikaz prirodnog broja n u obliku $x^2 + y^2 + z^2$, pri čemu su x, y, z prirodni brojevi takvi da $(x, y, z) = 1$.
Problem prikaza prirodnog broja u obliku sume kvadrata četiri različita cijela broja je također razmatran. O tome nam govori sljedeći teorem, a dao ga je matematičar Gordon Pall.

Teorem 15. (vidjeti [5], Chapter XI, §6) Jedini prirodni brojevi koji nemaju prikaz u obliku sume kvadrata četiri različita nenegativna cijela broja su brojevi oblika $4^h a$, pri čemu je $a = 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 23, 25, 27, 31, 33, 37, 43, 47, 55, 67, 73, 97, 103, 2, 6, 10, 18, 22, 34, 58, 82$ i $h = 0, 1, 2, ...$

6 Suma pet ili više kvadrata

Prema Teoremu 12. svaki je neparan prirodan broj veći od 41 S_4. Stoga, ako bilo kojem takvom broju dodamo 1^2 ili 2^2, vidimo da je svaki paran broj veći od 42 i svaki neparan broj veći od 45 također S_5. Ostaje nam razmotriti brojeve koji su manji ili jednaki od 45. Prema Teoremu 12. brojevi $4, 7, 10, 12, 15, 16, 18, 19, 20, 21, 22, 23, 25, 26, 27, 28, 30, 31, 33, 34, 35, 36, 37, 38, 39, 40, 42, 43, 44$ su S_4. Ako bilo kojem od navedenih brojeva dodamo 1 ili 4 dobivamo brojeve koji su S_5. Postoje još brojevi $1, 2, 3, 4, 6, 7, 9, 10, 12, 15, 18, 33$ koje treba razmotriti. Lako se može pokazati kako niti jedan od njih nije S_5. Pokazat ćemo da broj 33 nije S_5. Pretpostavimo da je 33 S_5, tj. da je $33 = a^2+b^2+c^2+d^2+e^2$, pri čemu su a, b, c, d, e prirodni brojevi takvi da je $a \geq b \geq c \geq d \geq e$. Stoga vrijedi je $a^2 + 4 \leq 33 \leq 5a^2$ pa je $6 < a^2 \leq 29$. Tada je $3 \leq a \leq 5$, odakle slijedi da je $a = 3$ ili $a = 4$ ili $a = 5$. U slučaju da je $a = 3$, broj $33 - a^2 = 24 = 4 \cdot 6$ je S_4 što je kontradikcija s Teoremom 12. Ako je $a = 4$, tada je broj $33 - a^2 = 17$ S_4 što je također kontradikcija s Teoremom 12. Za $a = 5$ dobivamo $33 - a^2 = 8 = 4 \cdot 2$ što je isto nemoguće jer $4 \cdot 2$ nije S_4.

Teorem 16. (vidjeti [5], Chapter XI, §7, Theorem 8.) Jedini prirodni brojevi koji nemaju zapis kao suma kvadrata pet prirodnih brojeva su brojevi $1, 2, 3, 4, 6, 7, 9, 10, 12, 15, 18, 33$.

Neka je m prirodan broj koji je veći ili jednak od 6. Pronaći ćemo prirodan broj koji je S_m i manji ili jednak $m + 13$. Pretpostavimo da je n takav broj. Tada postoje prirodni brojevi $a_1, a_2, ..., a_m$ takvi da $a_1 \geq a_2 \geq ... \geq a_m$ i $n = a_1^2 + a_2^2 + ... + a_m^2$. Budući da je $a_1^2 + (m - 1) \leq n \leq m + 13$, slijedi da je $a_1^2 \leq 14$ pa je $a_1 \leq 3$. Stoga vrijedi da je $a_1 = 1$ ili $a_1 = 2$ ili $a_1 = 3$. U slučaju $a_1 = 1$, imamo $a_1 = a_2 = ... = a_m = 1$ pa je $m = n$. Pretpostavimo da je $a_1 = 2$. Ako su najmanje četiri broja od brojeva $a_1, a_2, ..., a_m$ jednaka broju 2, tada je $n \geq 5 \cdot 4 + (m - 5) = m + 15$ što je u kontradikciji s pretpostavkom da je $n \leq m + 13$. Kao posljedica, najviše tri broja od brojeva $a_1, a_2, ..., a_m$ mogu biti jednaka broju 2. Stoga, postoje četiri mogućnosti:
1. niti jedan od brojeva nije jednak broju 2, tada je $n = 4 + (m - 1) = m + 3$;
2. jedan od brojeva je jednak broju 2, tada $n = 2 \cdot 4 + (m - 2) = m + 6$;
3. dva su broja jednaka broju 2, tada je $n = 3 \cdot 4 + (m - 3) = m + 9$;
4. tri su broja jednaka broju 2, tada je $n = 4 \cdot 4 + (m - 4) = m + 12$.

Dakle, sve što ostaje za razmotriti je slučaj kada je $a_1 = 3$. Tada je $n-9 = a_2^2+a_3^2+\cdots+a_m^2$. Ako je $a_2 = 3$, tada je $n \geq 18+(m-2)$ što je kontradikcija s pretpostavkom da je $n \leq m+13$. Slijedi da je $a_2 \leq 2$. Ako je $a_2 = 1$, tada je $a_3 = a_4 = ... = a_m = 1$ pa je $n = 3^2+m-1 = m+8$. Ako je $a_2 = 2$ i ako među brojevim $a_2, a_3, ..., a_m$ postoje dva ili više brojeva koji su jednaki broju 2, tada je $n \geq 3^2+2^2+2^2+(m-3) = m+14$ što je kontradikcija s pretpostavkom da je $n \leq m+13$. Dakle, $a_3 = a_4 = ... = a_m = 1$ odakle vrijedi da je $m = 3^2+2^2+(m-2) = m+11$. Time smo dokazali da su među brojevima manjim ili jednakim $m+13$ samo brojevi m, $m+3$, $m + 6$, $m + 8$, $m + 9$, $m + 11$, $m + 12$ S_m.
Sada pretpostavimo da je n prirodan broj veći od $m+13$. Ako je $n = m+28$, tada s obzirom da je $m \geq 6$ vrijedi da $n = m + 28 = 2 \cdot 3^2 + 4 \cdot 2^2 + (m - 6) \cdot 1^2$. Time smo pokazali da je n

S_m. Pretpostavimo da je $n \neq m+28$. Tada prema Teoremu 16. slijedi da je broj $n-(m-5)$ S_5 pa je broj $n = n-(m-5)+(m-5)\cdot 1^2$ S_m. Iz dobivenih rezultata slijedi idući teorem.

Teorem 17. (vidjeti [5], Chapter XI, §7, Theorem 9.) Za prirodan broj m veći od 5 brojevi 1, 2, 3,...,$m-1$, $m+1$, $m+2$, $m+4$, $m+5$, $m+7$, $m+10$, $m+13$ su jedini prirodni brojevi koji se ne mogu prikazati kao suma kvadrata m prirodnih brojeva.

Prema Teoremu 16. i Teoremu 17. možemo zaključiti da, ako je m prirodan broj koji je veći ili jednak broju 5, tada je bilo koji dovoljno veliki prirodan broj suma kvadrata m prirodnih brojeva. Ovo ne vrijedi za $m = 1, 2, 3, 4$ zato što postoji beskonačno mnogo prirodnih brojeva:
1) koji nisu kvadrati prirodnih brojeva kao npr. brojevi oblika n^2+1, pri čemu je $n = 1, 2, ...$
2) koji nisu S_2 kao npr. brojevi oblika $4k+3$, pri čemu je $k = 0, 1, 2, ...$
3) koji nisu S_3 kao npr. brojevi oblika $8k+7$, pri čemu je $k = 0, 1, 2, ...$
4) koji nisu S_4 kao npr. brojevi oblika $4^h \cdot 2$, pri čemu je $h = 0, 1, 2, ...$
Jednako tako postoji beskonačno mnogo prirodnih brojeva koji nisu suma kvadrata tri ili više prirodnih brojeva kao npr. brojevi oblika $8k+7$, pri čemu je $k = 0, 1, 2, ...$
Međutim, prema Lagrangeovom teoremu, svaki prirodan broj je suma kvadrata četiri ili više prirodnih brojeva.

Primjer 17. (vidjeti [5], Chapter XI, §7, Exercises 1.) Dokažimo da za svaki prirodan broj m postoji beskonačno mnogo prirodnih brojeva koji su S_i, za $i = 1, 2, ..., m$.
Rješenje:
Pokazali smo da za svaki broj veći od $m+13$ i oblika $(13k)^2$ ima ovo svojstvo. Zapravo, vrijedi da je $n = (13k)^2 = (5k)^2 + (12k)^2 = (3k)^2 + (4k)^2 + (12k)^2 = (2k)^2 + (4k)^2 + (7k)^2 + (10k)^2$ pa je n S_1, S_2, S_3 i S_4. Ako je $i > 4$ i $i \leq m$, tada vrijedi da je $n = (13k)^2 > 33$ i $n > m+13$ pa je $n > i+13$. Prema Teoremu 16. i Teoremu 17. vidimo da je n S_i.

Napomena 1. (vidjeti [5], Chapter XI, §7) Može se dokazati da je 169 najmanji broj koji je S_1, S_2 i S_3. Broj 169 je S_i za svaki $i \leq 155$ i za $i = 157, 158, 160, 161, 163, 166, 169$. Dokaz da je 169 S_{100} slijedi, na primjer, iz jednakosti $169 = 23 \cdot 2^2 + 77 \cdot 1^2$ ili iz jednakosti $169 = 8^2 + 2 \cdot 2^2 + 97 \cdot 1^2$.

Primjer 18. (vidjeti [5], Chapter XI, §7, Exercises 2.) Pronađimo najmanji prirodan broj n koji je S_i za svaki $i \leq 1000$.
Rješenje:
Kako je n S_i, slijedi da je $n = k^2$, pri čemu je k prirodan broj. Kako je n S_{1000}, dobivamo da $k^2 \geq 1000$ i $k \geq 32$. Ali, prema Teoremu 8., brojevi $32^2 = 2^{10}$ i $33^2 = (3 \cdot 11)^2$ ne mogu biti S_2. Međutim, $34^2 = 16^2 + 30^2 = 2^2 + 24^2 + 24^2$, odakle zaključujemo da je 34^2 S_1, S_2, S_3. Prema Teoremu 12. vidimo da je 34^2 S_4, a prema Teoremu 16. da je 34^2 S_5. Primjenom Teorema 17. uočavamo da je 34^2 S_i pod uvjetom da $34^2 > i+13$ te $i \geq 6$. Stoga je 34^2 S_i za svaki $i \leq 1142$. Primjer prikaza broja 34^2 kao sume tisuću kvadrata je $34^2 = 2 \cdot 8^2 + 2 \cdot 4^2 + 996 \cdot 1^2$.

7 Sažetak

Na početku diplomskog rada govorimo o povijesnom razvoju zapisa prirodnih brojeva u obliku sume nenegativnih k-tih potencija. Mnogi matematičari proučavali su različite zapise prirodnih brojeva, a neki rezultati njihovog rada nisu ni danas dokazani. U diplomskom radu naveli smo da prost broj oblika $4k + 1$ ima prikaz u obliku sume kvadrata dva cijela broja. Također, iskazali smo teorem koji govori da se jedino prirodni brojevi koji u faktorizaciji sadrže proste faktore oblika $4k + 3$, $k \in \mathbb{Z}$, s parnim eksponentom mogu zapisati kao suma kvadrata dva cijela broja. Osim toga, izveli smo i formulu za određivanje broja takvih prikaza i objasnili geometrijsku interpretaciju. Naveli smo i teorem koji govori o karakterizaciji prirodnih brojeva koji se mogu zapisati kao suma kvadrata dva prirodna broja. U četvrtom poglavlju naveden je i dokazan Gaussov teorem vezan za prirodne brojeve koji se mogu zapisati kao suma kvadrata tri cijela broja. U petom dijelu kroz Lagrangeov teorem govorimo o prikazu prirodnih brojeva u obliku sume kvadrata četiri cijela broja. U zadnjem dijelu proučavamo prikaz prirodnog broja u obliku sume kvadrata pet ili više prirodnih brojeva i navodimo rezultate koji govore o brojevima koji se mogu zapisati u tome obliku.

Ključne riječi: Povijesni pregled, Prikaz prirodnih brojeva, Suma nenegativnih potencija, Suma dva kvadrata, Prosječan broj prikaza, Suma tri kvadrata, Suma četiri kvadrata, Suma $m \geq 5$ kvadrata.

8 Abstract

At the beginning of the thesis, we talk about the historical development of the notation of natural numbers in the form of the sum of non-negative k powers. Many mathematicians studied different notations of natural numbers, and some results of their work have not been proven even today. In the thesis, we stated that a prime number of the form $4k + 1$ has a representation in the form of the sum of the squares of two integers. Also, we have stated a theorem that says that only natural numbers that in the factorization contain simple factors of the form $4k + 3$, $k \in \mathbb{Z}$, with an even exponent can be written as the sum of the squares of two integers. In addition, we derived the formula for determining the number of such representations and explained the geometric interpretation. We also stated a theorem that describes the characterization of natural numbers that can be written as the sum of the squares of two natural numbers. In the fourth chapter, the Gauss's theorem related to natural numbers that can be written as the sum of the squares of three integers is stated and proved. In the fifth part, through Lagrange's theorem, we talk about the representation of natural numbers in the form of the sum of the squares of four whole numbers. In the last part, we study the representation of a natural number in the form of the sum of the squares of five or more natural numbers and list the results that speak about the numbers that can be written in this form.

Keywords: Historical overview, Representations of natural numbers, Sums of non-negative powers, Sums of two squares, The average number of representations, Sums of three squares, Sums of four squares, Sums of $m \geq 5$ squares.

Životopis

Moje ime je Ana Glavačević i rođena sam 30. kolovoza 1993. u Slavonskome Brodu. Osnovnu školu Augusta Šenoe upisala sam 2000. godine, a završila 2008. godine. Srednješkolsko obrazovanje nastavila u općoj gimnaziji Matije Mesića u Slavonskom Brodu. 2012. godine upisala sam Preddiplomski studij matematike Odjela za matematiku na Sveučilištu J.J.Strossmayera u Osijeku, a 2018. godine stekla sam akademski naziv sveučilišna prvostupnica matematike. Upisala sam program pedagoško-psihološko-didaktičko-metodičkih kompetencija za nastavni rad u osnovnoškolskim i srednjoškolskim ustanovama jer volim prenositi svoje znanje, poticati i motivirati osobe da savladaju matematičke probleme, a najviše od svega pratiti njihov napredak tokom procesa podučavanja. Trenutno sam zaposlena kao nastavnica matematike i fizike u Osnovnoj školi "Bogoslav Šulek" u Slavonskom Brodu.

Literatura

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

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

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

[4] M. Pavlović, *Trokutasti brojevi*, Matematički odsjek, Prirodoslovno-matematički fakultet, Sveučilište u Zagrebu, Zagreb, 2021.

[5] W. F. Sierpinski, *Elementary Theory of Numbers*, North Holland, Amsterdam, 1988.