Suma kvadrata

Muha, Martina

Sveučilište Josipa Jurja Strossmayera u Osijeku
Fakultet primijenjene matematike i informatike

Sveučilišni prijediplomski studij Matematika

Sume kvadrata

Završni rad

Mentor:
izv. prof. dr. sc. Mirela Jukić Bokun

Student:
Martina Muha

Osijek, 2024.

Sadržaj

1 | Uvod

U ovom radu bavit ćemo se prikazivanjem prirodnih brojeva u obliku sume kvadrata cijelih i prirodnih brojeva. Sumama dva kvadrata bavili su se i antički matematičari; u drugoj knjizi *Artihmeticae* Diofant (III. st. pr. Kr.) je iznio racionalno rješenje jednadžbe $x^2 + y^2 = a^2, a \in \mathbb{Z}$, pomoću konstante $k \neq 0$ kao:

$$x = \frac{2ak}{k^2 + 1},$$
$$y = \frac{a(k^2 - 1)}{k^2 + 1}.$$

Moderni matematičari su se također bavili tim problemom, a najzanimljivije nam je promatrati koji se to cijeli i prirodni brojevi mogu zapisati kao sume dva i četiri kvadrata čime ćemo se u ovom radu baviti. Uz to, proučit ćemo i koji se cijeli brojevi mogu zapisati kao suma tri kvadrata te koji se prirodni brojevi mogu izraziti kao suma više od četiri kvadrata.

2 | Sume dva kvadrata

U ovom ćemo poglavlju pokazati koji se to prirodni brojevi mogu zapisati kao suma kvadrata dva cijela broja. Metode određivanja takvih brojeva iznijeli su, neovisno jedan o drugom, francuski matematičari Albert Girard (1595. - 1632.) i Pierre de Fermat (1601. - 1665.).

2.1 Girandova metoda

Girandov postupak može biti dugotrajan, ali svakako je mjerodavan. Za broj n računamo $n-1^2, n-2^2, n-3^2, \ldots, n-\left\lfloor \frac{\sqrt{n}}{2} \right\rfloor^2$. Ukoliko dobijemo potpun kvadrat u jednom od računa, možemo zaključiti da je n moguće zapisati kao sumu dva kvadrata. Ukoliko ne dobijemo potpun kvadrat, a iskoristili smo sve opcije, zaključujemo da n ne možemo zapisati kao sumu dva kvadrata. U nekim slučajevima, na primjer kada je n relativno velik broj, možemo postupak započeti unatrag tako da prvo utvrdimo najveći cijeli broj koji nije veći od $\sqrt{n}$ i krenemo računati $n-\lfloor\sqrt{n}\rfloor^2, n-(\lfloor\sqrt{n}\rfloor-1)^2, \ldots$ dok ne dođemo do potpunog kvadrata ili dok ne iskoristimo sve opcije.

Primjer 1. *Provjerimo je li broj* 3761 *moguće zapisati kao sumu dva kvadrata.*

Rješenje. Izračunamo da je $\left\lfloor\sqrt{3761}\right\rfloor = 61$ te provodimo postupak kako je gore objašnjeno:

$$\begin{aligned}
3761 - 61^2 &= 40,\\
3761 - 60^2 &= 161,\\
3761 - 59^2 &= 280,\\
3761 - 58^2 &= 397,\\
3761 - 57^2 &= 512,\\
3761 - 56^2 &= 625 = 25^2.
\end{aligned}$$

Dakle, 3761 je moguće zapisati kao sumu dva kvadrata.

2.2 Fermatova metoda

S druge strane, Fermatov način ispitivanja može li se prirodni broj zapisati kao suma dva kvadrata puno je jednostavniji iako ga on sam nije uspio do kraja dokazati. Taj teorem nam je poznat pod nazivom Teorem o dva kvadrata ili Fermatov teorem o dva kvadrata. Prije nego ga iskažemo, iskazat ćemo i dokazati nekoliko propozicija iz kojih će slijediti i dokaz samog Fermatovog teorema.

Propozicija 1 (vidjeti [3, Propozicija 1]). *Ako se prirodni brojevi s i t mogu zapisati kao sume kvadrata dva cijela broja, onda je i $s \cdot t$ suma dva kvadrata.*

Dokaz. Neka su s, t prirodni brojevi koje je moguće zapisati kao sumu dva kvadrata, to jest oblika

$$s = a^2 + b^2,$$
$$t = c^2 + d^2,$$

gdje su $a, b, c, d \in \mathbb{Z}$. Promotrimo umnožak brojeva s i t:

$$st = (a^2 + b^2)(c^2 + d^2) = a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2.$$

Dodamo li i oduzmemo u jednakosti $2abcd$ dobivamo:

$$st = a^2c^2 + 2abcd + b^2d^2 + a^2d^2 - 2abcd + b^2c^2 = (ac + bd)^2 + (ad - bc)^2.$$

Dakle, umnožak dva broja koji se mogu zapisati kao suma kvadrata je također suma dva kvadrata. U ovom koraku došli smo do takozvanog *Diofantovog identiteta* koji ćemo koristiti i kasnije u dokazu:

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2. \tag{2.1}$$

□

Za dokaz jedne tvrdnje vezane uz prikaz prostih brojeva u obliku sume dva kvadrata, bit će nam potreban *Mali Fermatov teorem* pa ga ovdje navodimo:

Teorem 1 (vidjeti [4, Teorem 2.10]). *Neka je p prost broj i a cijeli broj. Ako p ne dijeli a, onda je $a^{p-1} \equiv 1 \pmod{p}$.*

Propozicija 2 (vidjeti [3, Propozicija 2]). *Ukoliko je prost broj p oblika $4k + 3$, njega ne možemo zapisati kao sumu dva kvadrata. Također, ako takav p dijeli $a^2 + b^2$, tada on dijeli i a i b.*

Dokaz. Potpun kvadrat je oblika $4k$ ili $4k + 1$ pa suma dva kvadrata može jedino biti oblika $4k$, $4k + 1$ ili $4k + 2$, stoga ukoliko je prost broj p oblika $4k + 3$, njega ne možemo zapisati kao sumu dva kvadrata i s time smo dokazali prvu tvrdnju teorema.
Nadalje, neka p dijeli $a^2 + b^2$, ali da p ne dijeli a. Iz toga slijedi da p ne dijeli niti b. To možemo zapisati kao $a^2 \equiv -b^2 \pmod{p}$. Ukoliko tu kongruenciju dignemo na potenciju $\frac{p-1}{2}$ dobivamo

$$a^{p-1} \equiv (-1)^{\frac{p-1}{2}} b^{p-1} \pmod{p}.$$

Iz pretpostavke da je p oblika $4k+3$, znamo da je $\frac{p-1}{2}$ neparan. Zbog *Malog Fermatovog teorema* vrijedi $1 \equiv -1 \pmod{p}$. Došli smo do kontradikcije te dokazali drugu tvrdnju.

□

Propozicija 3 (vidjeti [3, Propozicija 3]). *Ako su a i b relativno prosti prirodni brojevi, tada je svakog prostog djelitelja izraza a^2+b^2 moguće zapisati kao sumu dva kvadrata.*

Dokaz. Neka su a i b relativno prosti prirodni brojevi i neka je bez smanjenja općenitosti a^2+b^2 složen broj (kada bi bio prost, tada je jedini faktor u faktorizaciji sam izraz a^2+b^2 pa se ne bi imalo što dokazivati). Neka je p prost djelitelj od a^2+b^2 i neka je $p \cdot k$ najmanji višekratnik od p koji se može prikazati u obliku

$$p \cdot k = a^2 + b^2.$$

Neka su c i d cijeli brojevi čija je apsolutna vrijednost strogo manja od $\frac{p}{2}$ i za koje vrijedi

$$a \equiv c \pmod{p},\ b \equiv d \pmod{p}.$$

Tada vrijedi $p|c^2+d^2$ i

$$c^2 + d^2 < 2\left(\frac{p}{2}\right)^2 = \frac{p}{2}p,$$

što možemo zapisati kao

$$c^2 + d^2 = kp,\ 1 \leq k \leq \frac{p}{2}. \tag{2.2}$$

Bez smanjena općenitosti možemo uvesti pretpostavku da su c i d relativno prosti brojevi. Kada oni to ne bi bili, podijelili bi ih s njihovim najvećim zajedničkim djeliteljem i dobivene brojeve uzeli umjesto njih, a k bi podijelili s kvadratom tog najvećeg zajedničkog djelitelja od c i d. Kada bi k iz (2.2) bio jednak 1, tvrdnja bi bila dokazana jer bi prikazali prost broj p kao sumu dva kvadrata. U drugom slučaju, ako bi k bio strogo veći od 1, primjenjujemo *metodu beskonačnog spusta*. U tom slučaju, definiramo cijele brojeve m i n za koje vrijedi:

$$|m|, |n| \leq \frac{k}{2},$$

$$m \equiv c \pmod{k},\ n \equiv d \pmod{k}.$$

Tada je $m^2+n^2 \equiv c^2+d^2 \equiv 0 \pmod{k}$, što možemo zapisati kao

$$m^2 + n^2 = kr, r \in \mathbb{N}. \tag{2.3}$$

Vrijedi $m^2+n^2 \leq \frac{k^2}{2}$, pa je $1 \leq r \leq \frac{k}{2} \leq k$. Pomnožimo li (2.2) i (2.3) dobivamo:

$$k^2pr = (c^2+d^2)(m^2+n^2).$$

Sada upotrebljavamo *Diofantov identitet* (2.1) i dolazimo do:

$$k^2pr = (cm+dn)^2 + (cn-dm)^2. \tag{2.4}$$

Uočimo da k dijeli $cm + dn$ i $cn - dm$, odnosno da vrijedi

$$cm + dn \equiv c^2 + d^2 \equiv 0 \pmod{k},$$
$$cn - dm \equiv mn - nm \equiv 0 \pmod{k},$$

pa (2.4) možemo dijeliti s k^2 pri čemu dobivamo

$$rp = \left(\frac{cm + dn}{k}\right)^2 + \left(\frac{cn - dm}{k}\right)^2,$$

gdje su $\frac{cm+dn}{k}$ i $\frac{cn-dm}{k}$ cijeli brojevi. Ukoliko je njihov najveći zajednički djelitelj recimo x, možemo zapisati $\frac{cm+dn}{k} = xc_1$, $\frac{cn-dm}{k} = xd_1$. Tada je $p \cdot \frac{r}{x^2} = c_1^2 + d_1^2$. Uočimo sada da je $\frac{r}{x^2} \leq r \leq k$ što je kontradikcija s minimalnošću od k. Zato je $k = 1$ (i $r = 0$), a $p = c^2 + d^2$.

□

Prije sljedeće tvrdnje, navest ćemo *Wilsonov teorem* koji će nam biti potreban u dokazu.

Teorem 2 (vidjeti [4, Teorem 2.13]). *Za prost broj p vrijedi $(p-1)! \equiv -1 \pmod{p}$.*

Propozicija 4 (vidjeti [3, Propozicija 4]). *Ukoliko je p prost broj oblika $4k+1$, onda postoji $a \in \mathbb{N}$ takav da p dijeli $a^2 + 1$.*

Dokaz. Ukoliko je p oblika $4k + 1$, tada je

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

Dakle, možemo uzeti $a = (\frac{p-1}{2})!$. □

Sada kada smo postavili temelje za dokaz, možemo iskazati i *Teorem o dva kvadrata*:

Teorem 3 (Teorem o dva kvadrata, vidjeti [3, Propozicija 5]). *Prost broj p može se zapisati kao suma kvadrata dva cijela broja ako i samo ako je $p \equiv 1 \pmod{4}$ ili $p = 2$.*

Dokaz. Dokaz ovog teorema direktno slijedi iz Propozicija 2, 4 i 3 i činjenice da je $2 = 1^2 + 1^2$ suma dva kvadrata. Naime, Prema Propoziciji 2. prost broj oblika $4k + 3$ ne može se zapisati kao suma dva kvadrata. Prema Propoziciji 4 za prost broj p oblika $4k + 1$ postoji cijeli broj x takav da p dijeli $x^2 + 1$, a prema Propoziciji 3 se p onda može prikazati kao suma dva kvadrata. □

Sljedeći teorem koji ćemo iskazati govori nam o jedinstvenosti prikaza prostog broja u obliku sume kvadrata dva prirodna broja.

Teorem 4 (vidjeti [3, Propozicija 6]). *Neka je p prost broj. Prikaz broja p u obliku sume kvadrata dva prirodna broja, ukoliko postoji, je jedinstven do na poredak sumanada.*

Dokaz. Pretpostavimo suprotno, odnosno da se prost broj p može iskazati kao $p = a^2 + b^2$ i kao $p = c^2 + d^2$. Neka su a i c te b i d iste parnosti te neka je $a \neq c$ i $b \neq d$. Sada imamo:

$$\begin{aligned} a^2 + b^2 &= c^2 + d^2, \\ a^2 - c^2 &= d^2 - b^2, \\ (a-c)(a+c) &= (d-b)(d+b), \\ \frac{a-c}{2} \cdot \frac{a+c}{2} &= \frac{d-b}{2} \cdot \frac{d+b}{2}. \end{aligned} \tag{2.5}$$

Označimo s t najveći zajednički djelitelj od $\frac{a-c}{2}$ i $\frac{d-b}{2}$, te neka vrijedi $\frac{a-c}{2} = tu$ i $\frac{d-b}{2} = tv$. Tada (2.5) možemo zapisati kao

$$u \cdot \frac{a+c}{2} = v \cdot \frac{d+b}{2}.$$

Budući da su u i v relativno prosti, imamo $\frac{a+c}{2} = v \cdot z$, $\frac{d+b}{2} = u \cdot z$. Iz toga slijedi da je $a = tu + vz$ i $b = uz - tv$. Sada je po *Diofantovom identitetu* (2.1) $p = a^2 + b^2 = (tu + vz)^2 + (uz - tv)^2 = (t^2 + z^2)(u^2 + v^2)$ što je u kontradikciji s pretpostavkom da je p prost broj. □

Iskažimo još karakterizaciju prirodnih brojeva koji se mogu zapisati kao suma dva kvadrata.

Teorem 5 (vidjeti [1, Theorem 8.6])**.** *Broj $n \in \mathbb{N}$ se može zapisati kao $n = a^2 + b^2$, za $a, b \in \mathbb{Z}$, onda i samo onda kada se svaki prosti faktor p od n oblika $p = 4k + 3$, u rastavu broja n na proste faktore, pojavljuje na parnu potenciju.*

Dokaz. Ukoliko je $n = a^2 + b^2$, a p njegov prost djelitelj oblika $4k + 3$, tada po Propoziciji 2 p^2 dijeli n. Ukoliko $n = a^2 + b^2$ podijelimo s p^2, dobivamo

$$\frac{n}{p^2} = \left(\frac{a}{p}\right)^2 + \left(\frac{b}{p}\right)^2.$$

Neka je $n = p^2 n_1$. Ukoliko p dijeli n_1, onda opet po Propoziciji 2 vrijedi $p^2 | n_1$. Nastavimo li s ovim postupkom, primjećujemo da n mora biti djeljiv upravo s parnim brojem faktora p.
Pretpostavimo sada da se svaki prosti faktor od n oblika $4k + 3$ pojavljuje na parnu potenciju. Tada možemo zapisati $n = p_1 p_2 \dots p_m n_1^2$ pri čemu su p_i međusobno različiti prosti brojevi te pri čemu samo jedan može biti jednak 2 dok su ostali oblika $p_i = 4k + 1$. Sada iz Teorema 3 slijedi da se svaki p_i može zapisati kao suma dva kvadrata cijelih brojeva, a iz *Diofantovog identiteta* (2.1) pak slijedi da se n može zapisati kao $n = a^2 + b^2$, za $a, b \in \mathbb{Z}$. □

2.3 Broj prikaza prirodnog broja u obliku sume dva kvadrata

Sada kada znamo koji se to prirodni brojevi mogu zapisati kao suma dva kvadrata cijelih brojeva, možemo se zapitati koji je ukupni broj različitih prikaza pojedinog

broja u tom obliku. Označimo s $N_2(n)$ funkciju koja će nam za prirodan broj n dati broj različitih prikaza broja n kao sume kvadrata dva cijela broja. Pogledajmo na primjer broj 9:

$$9 = 0^2 + 3^2 = 3^2 + 0^2 = 0^2 + (-3)^2 = (-3)^2 + 0^2.$$

Dakle, njega možemo na četiri različita načina prikazati kao sumu dva kvadrata pa je stoga $N_2(9) = 4$. Iskažimo sada formalno kako se računa $N_2(n)$.

Teorem 6 (vidjeti [1, Theorem 8.11]). *Neka je n moguće zapisati kao sumu kvadrata dva cijela broja te neka su p_i i q_i prosti brojevi za koje vrijedi $p_i \equiv 1 \pmod 4$ i $q_i \equiv 3 \pmod 4$ i za koje je $n = 2^a \prod_i p_i^{a_i} \prod_i q_i^{b_i}$, pri čemu si b_i parni. Tada je*

$$N_2(n) = 4 \prod_i (a_i + 1).$$

Još jednu zanimljivu karakterizaciju prirodnog broja u obliku sume dva kvadrata iznio je Carl Gustav Jacobi (1804.-1851.).

Teorem 7 (vidjeti [1, Theorem 8.12]). *Ako je n prirodan broj i ako su D_1 i D_3 redom brojevi njegovih djelitelja oblika $4k+1$ i $4k+3$, tada je*

$$N_2(n) = 4(D_1 - D_3).$$

3 | Sume tri kvadata

U ovom poglavlju bavimo se prikazivanjem cijelih brojeva kao sume tri kvadrata cijelih brojeva. Značajnu ulogu u istraživanju takvih brojeva imao je francuski matematičar i astronom Adrien-Marie Legendre (1752.-1833.) koji je zaključio da ako je neki broj moguće zapisati kao sumu tri kvadrata, isti sigurno nije oblika $4^x(8y+7)$. Iako su prije njega postojale ideje koji se to brojevi mogu zapisati kao suma tri kvadrata, on je prvi postavio klasifikaciju tih brojeva na početku 19. stoljeća. Pedesetak godina kasnije, dokaz je iznio Dirichlet (1805. - 1859.). No osim toga, danas je poznato da vrijedi i obrat što ćemo samo iskazati sljedećim teoremom, a dokaz izostaviti.

Teorem 8 (vidjeti [12, Theorem 5.6]). *Cijeli broj n je oblika $n = a^2 + b^2 + c^2$, $a, b, c \in \mathbb{Z}$ ako i samo ako vrijedi $n \neq 4^x(8y+7)$, gdje su $x \in \mathbb{N}$, $y \in \mathbb{Z}$.*

Dokaz. Dokazat ćemo da ukoliko je $n \in \mathbb{Z}$ oblika $n = 4^x(8y+7)$, n nije suma tri kvadrata. Pretpostavimo da je

$$n = 4^x(8y+7) = a^2 + b^2 + c^2,\ n, y, a, b, c \in \mathbb{Z},\ x \in \mathbb{N}. \tag{3.1}$$

Neka je $x = x_0$ najmanji mogući takav da n bude najmanji prirodni broj za kojeg će (3.1) vrijediti. Promotrimo sljedeće:

Neka je $p \in \mathbb{Z}$. Znamo da je potpuni sustav ostataka modulo 8 skup $\{0, 1, 2, 3, 4, 5, 6, 7\}$. Promotrimo što se događa sa potpunim sustavom ostataka modulo 8 ukoliko gledamo kvadrate:

- Ako je $p \equiv 0 \pmod 8$, onda je $p^2 \equiv 0 \pmod 8$.
- Ako je $p \equiv 1 \pmod 8$, onda je $p^2 \equiv 1 \pmod 8$.
- Ako je $p \equiv 2 \pmod 8$, onda je $p^2 \equiv 4 \pmod 8$.
- Ako je $p \equiv 3 \pmod 8$, onda je $p^2 \equiv 1 \pmod 8$.
- Ako je $p \equiv 4 \pmod 8$, onda je $p^2 \equiv 0 \pmod 8$.
- Ako je $p \equiv 5 \pmod 8$, onda je $p^2 \equiv 1 \pmod 8$.
- Ako je $p \equiv 6 \pmod 8$, onda je $p^2 \equiv 4 \pmod 8$.
- Ako je $p \equiv 7 \pmod 8$, onda je $p^2 \equiv 1 \pmod 8$.

Promotrimo sada što se dogodi sa ostatcima ako gledamo sumu tri kvadrata. Ispitat ćemo sve mogućnosti:

$$\begin{aligned}
0+0+0 &= 0 \equiv 0 \pmod 8,\\
0+0+1 &= 1 \equiv 1 \pmod 8,\\
0+0+4 &= 4 \equiv 4 \pmod 8,\\
0+1+1 &= 2 \equiv 2 \pmod 8,\\
0+1+4 &= 5 \equiv 5 \pmod 8,\\
0+4+4 &= 8 \equiv 0 \pmod 8,\\
1+1+1 &= 3 \equiv 3 \pmod 8,\\
1+1+4 &= 6 \equiv 6 \pmod 8,\\
1+4+4 &= 9 \equiv 1 \pmod 8,\\
4+4+4 &= 12 \equiv 4 \pmod 8.
\end{aligned}$$

Imajući na umu da je zbrajanje komutativno, iz ovoga se da zaključiti sljedeće:

$$a^2+b^2+c^2 \equiv \begin{cases} 0 \text{ ili } 4 & \text{ako su } a,b,c \text{ parni.}\\ 1 \text{ ili } 5 & \text{ako su } a,b \text{ parni, } c \text{ neparan.}\\ 2 \text{ ili } 6 & \text{ako su } b,c \text{ neparni, } a \text{ paran .}\\ 3 & \text{ako su } a,b,c \text{ neparni.}\end{cases} \tag{3.2}$$

Kako je n definiran kao $n = 4^{x_0}(8y+7)$, znamo da je on sigurno paran i djeljiv s 4. To znači da je n kongruentan 0 ili 4 modulo 8 pa iz (3.2) slijedi da su a,b,c parni brojevi. To znači da $n = 4^{x_0}(8y+7) = a^2+b^2+c^2$ možemo podijeliti s 4 pri čemu dobivamo:

$$N = 4^{x_0-1}(8y+7) = x^2+y^2+z^2, \tag{3.3}$$

gdje su $x,y,z \in \mathbb{Z}$. Kako smo x_0 postavili na minimalnu vrijednost za koju je n najmanji prirodni broj za koji vrijedi tvrdnja, došli smo do kontradikcije jer smo u (3.3) pokazali da je N dobro definiran i ako uzmemo $x_0 - 1$. Dakle, ne postoji broj koji je oblika $n = 4^x(8y+7)$ koji se može zapisati kao suma tri kvadrata. □

Drugi smjer dokaza nije elementaran nego se temelji na *ternarnim kvadratnim formama*. Upravo taj smjer dokaza je iznio Dirichlet 1850. godine, a isti se može vidjeti u [10]. Pogledajmo za kraj ovoga poglavlja jedan primjer.

Primjer 2. *Pogledajmo brojeve* $36, 37, 38, 39$*:*

$$\begin{aligned}
36 &= 4\cdot 8+4,\\
37 &= 4\cdot 8+5,\\
38 &= 4\cdot 8+6,\\
39 &= 4\cdot 8+7.
\end{aligned}$$

Po prethodnom teoremu, 39 *ne možemo zapisati kao sumu tri kvadrata, dok ostale možemo:*

$$\begin{aligned}
36 &= 6^2+0^2+0^2,\\
37 &= 6^2+1^2+0^2,\\
38 &= 6^2+1^2+1^2.
\end{aligned}$$

4 | Sume četiri kvadrata

U ovom poglavlju pozabavit ćemo se sumom četiri kvadrata. Da se svi prirodni brojevi mogu zapisati kao suma četiri kvadrata prvi je naslutio Fermat, ali s dokazom su se mučili mnogi matematičari. Euler je na tom dokazu radio preko 40 godina, ali nije bio uspješan. Lagrange je u tom pothvatu uspio i zato danas idući teorem nazivamo po njemu.

Za dokaz tog teorema bit će nam potrebna sljedeća tvrdnja koju navodimo bez dokaza.

Teorem 9 (vidjeti [4, Teorem 3.2]). *Neka je p neparan prost broj. Reducirani sustav ostataka modulo p sastoji se od $\frac{p-1}{2}$ kvadratnih ostataka i isto toliko kvadratnih neostataka.*

Teorem 10 (Lagrangeov teorem o četiri kvadrata, vidjeti [4, Teorem 4.9]). *Svaki prirodan broj n može se zapisati kao suma kvadrata četiri cijela broja.*

Dokaz. Promotrimo sljedeći identitet:

$$\begin{aligned}(a^2+b^2+c^2+d^2)(x^2+y^2+z^2+w^2) &= (ax+by+cz+dw)^2 \\ &+ (ay-bx-cw+dz)^2 + (az+bw-cx-dy)^2 + (aw-bz+cy-dx)^2.\end{aligned} \tag{4.1}$$

Dakle, dovoljno je provjeriti da tvrdnja teorema vrijedi za proste prirodne brojeve. Očito je $2 = 1^1 + 1^1 + 0^2 + 0^2$. Pretpostavimo zato da je p neparan prost broj. Ako pogledamo brojeve

$$0^2, 1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2, \tag{4.2}$$

zbog tvrdnje iz Teorema 9, zaključujemo da nikoja dva broja nisu kongruentna modulo p. To također vrijedi i za brojeve

$$-1-0^2, -1-1^2, -1-2^2, \ldots, -1-\left(\frac{p-1}{2}\right)^2. \tag{4.3}$$

U (4.2) i (4.3) imamo ukupno $p+1$ bojeva. Pozivajući se na *Dirichletov princip*, dva broja među gore navedenima daju isti ostatak pri dijeljenju s p. Dakle, postoje cijeli brojevi a, b takvi da je $a^2 \equiv -1 - b^2 \pmod{p}$ te vrijedi $a^2 + b^2 + 1 < 1 + 2 \cdot \left(\frac{p}{2}\right)^2 < p^2$. Iz toga slijedi da je $mp = a^2 + b^2 + 1^2$ za neki cijeli broj m za koji vrijedi $0 < m < p$.

Uzmimo sada najmanji prirodan broj l takav da je $lp = a^2 + b^2 + c^2 + d^2$ za cijele brojeve a, b, c, d. Tada je $l \leq m < p$. Ako je l paran, među brojevima a, b, c, d bi postojao paran broj neparnih brojeva, što bi značilo da su $a + b$, $a - b$, $c + d$, $c - d$ parni. Ako promotrimo sljedeću jednakost

$$\frac{1}{2}lp = \left(\frac{a+b}{2}\right)^2 + \left(\frac{a-b}{2}\right)^2 + \left(\frac{c+d}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2,$$

uočavamo da l ne zadovoljava uvjet minimalnosti te da trebamo uzimati u obzir samo neparne brojeve l.
Dokažemo li da je $l = 1$, dokazali smo i tvrdnju teorema. Iz tog razloga, pretpostavimo suprotno, odnosno da je $l > 1$.
Neka su a', b', c', d' apsolutne vrijednosti najmanjih ostataka pri dijeljenju brojeva a, b, c, d, redom s l. Neka je nadalje

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

Zaključujemo da je $n \equiv 0 \pmod{l}$ i $n > 0$, jer bi u suprotnom l dijelio p. Također, vrijedi i $n < 4\left(\frac{l}{2}\right)^2 = l$ pa je $n = k \cdot l$ za $k \in \mathbb{Z}$ takav da je $0 < k < l$. Iz identiteta (4.1) s početka dokaza proizlazi da je $(kl)(lp)$ moguće zapisati kao sumu kvadrata četiri cijela broja te vrijedi da je svaki od tih kvadrata djeljiv s l^2. Iz ovoga pak slijedi kontradikcija s minimlanošću od l zato što je broj kp moguće zapisati kao sumu četiri kvadrata cijelih brojeva. □

Navedimo još jednu tvrdnju vezanu za prikaz prirodnog broja u obliku sume četiri kvadrata.

Teorem 11 (vidjeti [9, Chapter XI, Theorem 5]). *Prirodan broj n se može prikazati kao suma kvadrata četiri prirodna broja onda i samo onda kada n ne pripada nizu brojeva* $1, 3, 5, 9, 11, 17, 29, 41, 4^x \cdot 2, 4^x \cdot 6, 4^x \cdot 14$, *za* $x = 0, 1, 2, \ldots$

4.1 Broj prikaza prirodnog broja u obliku sume četiri kvadrata

Kao što smo i u prikazu prirodnog broja u obliku sume dva kvadrata gledali koliko je ukupno takvih prikaza, tako možemo tražiti i ukupan broj prikaza prirodnog broja u obliku sume četiri kvadrata. Označimo s $N_4(n)$ funkciju koja će nam opisivati ukupan broj prikaza broja n u obliku sume kvadrata četiri cijela broja, a da pri tome ne uzimamo u obzir poredak sumanada.

Teorem 12 (vidjeti [1, Theorem 8.24]). *Neka je d suma svih pozitivnih djelitelja broja n koji nisu djeljivi sa 4. Tada je $N_4(n) = 8 \cdot d$.*

Primjer 3. *Pogledajmo na primjer broj* 240. *Njegovi djelitelji su* $1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 16, 20, 24, 30, 40, 48, 60, 80, 120$ *i* 240. *Suma svih njegovih djelitelja koji nisu djeljivi s* 4 *iznosi* 72, *pa po prethodnom teoremu zaključujemo da postoji* 576 *različitih prikaza broja* 240 *u obliku sume kvadrata četiri cijela broja.*

5 | Sume više kvadrata

U posljednjem poglavlju pogledat ćemo rezultate za prikaz prirodnih brojeva u obliku suma više od četiri kvadrata. Naime, ako pogledamo Teorem 11, bilo koji neparni broj veći od 41 možemo zapisati kao sumu kvadrata četiri prirodna broja. Tada, ukoliko tom broju dodamo 1^2 ili 2^2, možemo zaključiti da sve parne brojeve koji su veći od 42 i sve neparne brojeve koji su veći od 45, možemo zapisati kao sumu pet kvadrata prirodnih brojeva. Ostalo je za provjeriti koji se brojevi manji ili jednaki 45 mogu zapisati kao suma pet kvadrata prirodnih brojeva. Rezultat je dan u sljedećem teoremu.

Teorem 13 (vidjeti [9, Chapter XI, Theorem 8]). *Jedini prirodni brojevi koji se ne mogu zapisati kao suma kvadrata pet prirodnih brojeva su* $1, 2, 3, 4, 6, 7, 9, 10, 12, 15, 18$ *i* 33.

Iskažimo tvrdnju koja nam daje informaciju koji se to cijeli brojevi mogu zapisati kao suma šest ili više kvadrata prirodnih brrojeva.

Teorem 14 (vidjeti [9, Chapter XI, Theorem 9]). *Neka je* $n \in \mathbb{N}$, $n \geq 6$. *Jedini pozitivni cijeli brojevi koji se ne mogu zapisati kao suma kvadrata n prirodnih brojeva su brojevi* $1, 2, 3, \ldots, n-1, n+1, n+2, n+4, n+5, n+7, n+10, n+13$.

Prema prethodna dva teorema možemo zaključiti da, ako je n prirodan broj koji je ≥ 5, tada je bilo koji dovoljno velik prirodni broj zbroj kvadrata n prirodnih brojeva. Kao što smo u prethodnim poglavljima vidjeli, to ne vrijedi za $n = 1, 2, 3, 4$, jer postoji beskonačno mnogo prirodnih brojeva koji:

1. nisu kvadrati prirodnih brojeva (npr. brojevi $x^2 + 1$, gdje je $x = 1, 2, 3, \ldots$),
2. se ne mogu zapisati kao suma kvadrata dva prirodna broja (npr. brojevi oblika $4k + 3$, gdje je $k = 0, 1, 2, \ldots$),
3. se ne mogu zapisati kao suma kvadrata tri prirodna broja (npr. brojevi oblika $8k + 7$, gdje je $k = 0, 1, 2, \ldots$),
4. se ne mogu zapisati kao suma kvadrata četiri prirodna broja (npr. brojevi oblika $4^m \cdot 2$, gdje je $m = 0, 1, 2, \ldots$).

Literatura

[1] A. Adler, J. E. Coury, *The Theory of Numbers: A Text and Source Book of Problems*, The University of British Columbia, 1995.

[2] J. Cafuk, *O nekim Eulerovim doprinosima u teoriji brojeva*, PMF-MO, Sveučilište u Zagrebu, Diplomski rad, 2018., dostupno na `https://urn.nsk.hr/urn:nbn:hr:217:863766`

[3] A. Dujella, *Suma kvadrata*, Matematički odsjek, Prirodoslovno-matematički fakultet, Sveučilište u Zagrebu, dostupno na `https://web.math.pmf.unizg.hr/~duje/utb/sumekvadrata2.pdf`

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

[5] L. Euler, *Proofs of Fermat's theorem on sums of two squares*, dostupno na `\http://eulerarchive.maa.org//correspondence/letters/OOO852.pdf`

[6] L. Euler, *De numerus qui sunt aggregata duorum quadratorum.* (*Novi commentarii academiae scientiarum Petropolitanae 4* (*1752/3*), *1758, 3-40*), dostupno na `http://eulerarchive.maa.org//docs/originals/E228.pdf`

[7] L. Euler, *Demonstratio theorematis FERMATIANI omnem numerum primum formae 4n+1 esse summam duorum quadratorum.* (*Novi commentarii academiae scientiarum Petropolitanae 5* (*1754/5*), *1760, 3-13*), dostupno na `http://eulerarchive.maa.org//docs/originals/E241.pdf`

[8] G. A. Jones, J. M. Jones, *Elementary Number Theory*, Springer-Verlag, London, 2004.

[9] W. Sierpinski, *Elementary Theory of Numbers*, North-Holland Mathematical Library, Volume 31., Warszawa, 1988

[10] Z.-W. Sun, *The Three-square theorem and its applications*, dostupno na `http://maths.nju.edu.cn/~zwsun/Three-Square-Theorem.pdf`

[11] J.J. Tattersall, *Elementary Number Theory in Nine Chapters*, Cambridge University Press, Cambridge, 1999.

[12] M. Wong, *Representing integers as sums of squares*, dostupno na: `http://www.math.uchicago.edu/~may/VIGRE/VIGRE2009/REUPapers/Wong.pdf`

[13] *Proofs of Fermat's theorem on sums of two squares*, dostupno na `https://en.wikipedia.org/wiki/Proofs_of_Fermat%27s_theorem_on_sums_of_two_squares`

Sažetak

U ovom radu obrađena je tema prikazivanja prirodnih brojeva u obliku sume kvadrata cijelih i prirodnih brojeva. Predstavljeni su teoremi i metode za određivanje koji se brojevi mogu izraziti kao suma dva, tri, četiri i više kvadrata. Posebna pozornost posvećena je Teoremu o dva kvadrata te Lagrangeovom teoremu o četiri kvadrata. Također, razmatra se broj različitih načina prikazivanja brojeva kao sume kvadrata.

Ključne riječi

sume kvadrata, Fermatov teorem o dva kvadrata, Lagrangeov teorem o četiri kvadrata, Diofantov identitet

Sum of squares

Summary

In this paper, the topic of representing natural numbers as the sum of squares of integers and natural numbers is addressed. Theorems and methods for determining which numbers can be expressed as the sum of two, three, four, or more squares are presented. Special attention is given to the Sum of two squares theorem and Lagrange's four-square theorem. Additionally, the number of different ways to represent numbers as the sum of squares is considered.

Keywords

sum of squares, sum of two squares theorem, Lagrange's four-square theorem, Diophantus' identity

Životopis

Moje ime je Martina Muha i rođena sam 04. srpnja 1997. godine u Osijeku. U razdoblju od 2004./2005. do 2011./2012. pohađala sam Osnovnu školu Retfala, nakon koje sam upisala III. gimnaziju Osijek u kojoj sam maturirala 2016. godine. Iste godine upisujem tadašnji Odjel za matematiku, smjer Preddiplomski studij matematike.