Predavanje 13

PREDSTAVLJANJE ZBIROM KVADRATA

Problem *predstavljanja zbirom kvadrata* datog prirodnog broja $n \in \mathbb{N}$ sastoji se u ispitivanju diofantske jednačine

$$x_1^2 + x_2^2 + \cdots + x_k^2 = n,$$

gde je $k \geqslant 2$ broj kvadrata čiji zbir želimo da bude n. Za datu vrednost k, osnovno pitanje je za koje vrednosti paramtera n je prethodna jednačina rešiva. Ispostavlja se da je dovoljno analizirati slučajeve $k = 2, 3, 4$, jer je po Lagranžovoj teoremi o četiri kvadrata gornja jednačina rešiva za sve $n \in \mathbb{N}$ kada je $k = 4$ (pa tako i za sve $k \geqslant 4$). Ovaj rezultat ćemo dokazati u drugom delu ovog predavanja, a prethodno ćemo u potpunosti razmotriti slučaj $k = 2$ i dati karakterizaciju rešivosti gornje jednačine za $k = 3$.

Predstavljanje zbirom dva kvadrata.

U daljem, naš cilj je da ustanovimo za koje brojeve $n \in \mathbb{N}$ je rešiva sledeća diofantska jednačina:

$$x^2 + y^2 = n. \tag{13.1}$$

Neka $S \subseteq \mathbb{N}$ označava skup svih takvih brojeva n. Prva značajna primedba jeste da je skup S zatvoren za množenje.

Lema 13.1. *Ako se brojevi m i ℓ mogu prikazati kao zbirovi dva potpuna kvadrata, onda to važi i za $m\ell$.*

Dokaz. Neka je $m = x^2 + y^2$ i $\ell = u^2 + v^2$ za neke cele x, y, u, v. Tada je

$$m\ell = (x^2 + y^2)(u^2 + v^2) = (xu \pm yv)^2 + (xv \mp yu)^2,$$

pa tvrđenje leme odmah sledi. □

Iz ovog razloga, pitanje predstavljanja *prostih* brojeva zbirom dva kvadrata dolazi u prvi plan. Očito, $2 \in S$, jer je $2 = 1^2 + 1^2$. S druge strane, ako je prost broj p takav da je $p \equiv 3 \pmod 4$ tada $p \notin S$, pošto zbir dva potpuna kvadrata može da daje ostatke $0, 1, 2$ pri deljenju sa 4, ali ne i ostatak 3. Prema tome, preostaje da se vidi šta je sa prostim brojevima oblika $p = 4m + 1$.

Tvrđenje 13.2 (Fermaova teorema o dva kvadrata)**.** *Svaki prost broj p takav da je $p \equiv 1 \pmod 4$ može se predstaviti kao zbir dva kvadrata.*

Dokaz. Po Tvrđenju 9.3 (iii), -1 je kvadratni ostatak po modulu p, pa postoji $a \in \mathbb{Z}$ i $\ell \in \mathbb{Z}^+$ tako da je

$$a^2 + 1 = \ell p.$$

Budući da je $-(p-1)/2, \ldots, -1, -0, -1, \ldots, (p-1)/2$ potpun sistem ostataka po modulu p, možemo pretpostaviti da je $|a| \leqslant (p-1)/2$. Zbog toga možemo pretpostaviti i da je $1 \leqslant \ell < p/4 < p$.

Neka je sada $\ell_0 \geqslant 1$ *najmanji* broj sa osobinom da se $\ell_0 p$ može predstaviti kao zbir dva cela kvadrata; tvrdimo da je $\ell_0 = 1$. Pretpostavimo suprotno. Neka je $\ell_0 p = x^2 + y^2$ za neke $x, y \in \mathbb{Z}$. Odaberimo $u, v \in \mathbb{Z}$ tako da je $u \equiv x \pmod{\ell_0}$, $v \equiv y \pmod{\ell_0}$ i $|u|, |v| \leqslant \ell_0/2$. Kako $\ell_0 \mid x^2 + y^2$, sledi da $\ell_0 \mid u^2 + v^2$, pa je

$$u^2 + v^2 = \ell_0 \ell'$$

za neko $\ell' \in \mathbb{Z}^+$. Kako je $u^2 + v^2 \leqslant \ell_0^2/2$, sledi da je $\ell' \leqslant \ell_0/2$. S druge strane, $\ell' > 0$, jer bi u suprotnom bilo $u = v = 0$, tj. x i y bi bili deljivi sa ℓ_0; tako bismo dobili da $\ell_0^2 \mid x^2 + y^2 = \ell_0 p$ i $\ell_0 \mid p$, što je kontradikcija sa $1 < \ell_0 < p$. Prema tome, $1 \leqslant \ell' \leqslant \ell_0/2 < \ell_0$.

Primetimo da je sada

$$xu + yv \equiv x^2 + y^2 \pmod{\ell_0}, \quad xv - yu \equiv xy - xy = 0 \pmod{\ell_0},$$

dok je, s druge strane,

$$(xu + yv)^2 + (xv - yu)^2 = (x^2 + y^2)(u^2 + v^2) = \ell_0^2 \ell' p.$$

Prema tome, brojevi

$$\mu = \frac{xu + yv}{\ell_0}, \quad \nu = \frac{xv - yu}{\ell_0}$$

su celi i važi

$$\mu^2 + \nu^2 = \ell' p.$$

Dakle, broj $\ell' p$ se može predstaviti kao zbir dva cela kvadrata; budući da je $1 \leqslant \ell' < \ell_0$, to je kontradikcija sa minimalnošću ℓ_0. Zbog toga mora biti $\ell_0 = 1$, pa je p predstavljiv kao zbir dva kvadrata. □

U prethodnom dokazu ponovo smo primenili Fermaov metod beskonačnog spuštanja.

Kriterijum predstavljivosti broja zbirom dva kvadrata je sledeći.

Teorema 13.3. *Pozitivan ceo broj n se može prikazati kao zbir dva cela kvadrata (tj. jednačina* (13.1) *je rešiva) ako i samo ako se u kanoničkoj faktorizaciji broja n na proste faktore svaki prost faktor oblika $4m+3$ javlja sa parnim eksponentom.*

Dokaz. ($\Leftarrow$): Ako je broj n opisanog oblika, tada se on može napisati u obliku $n = rs^2$, gde je ili $r = 1$, ili su svi prosti faktori od r ili 2, ili oblika $4m + 1$. Uzastopnom primenom Leme 13.1 i Tvrđenja 13.2 dobijamo da postoje $x, y \in \mathbb{Z}$ tako da je $x^2 + y^2 = r$. Ali, tada je $(sx)^2 + (sy)^2 = s^2 r = n$.

($\Rightarrow$): Slučaj $n = 1$ je trivijalan, pa pretpostavimo da je $n \geqslant 2$. Traženo tvrđenje dokazujemo indukcijom, pri čemu pretpostavljamo da su svi brojevi $n' < n$ koji se mogu prikazati putem zbira dva kvadrata baš željenog oblika. Ako n nema proste faktore oblika $4m + 3$, tada nema šta da se dokazuje; stoga, pretpostavimo da je $p \mid n$ jedan takav prost faktor i da je $n = x^2 + y^2$ za neke $x, y \in \mathbb{Z}$. Tvrdimo da tada $p \mid x, y$. Zaista, ako bi, na primer, važilo $p \nmid x$, tada bi postojao ceo broj x' tako da je

$$xx' \equiv 1 \pmod{p}.$$

U tom slučaju bi broj $(x')^2(x^2+y^2) = (xx')^2 + (yx')^2$ bio deljiv sa p, tj. imali bismo

$$(yx')^2 \equiv -(xx')^2 \equiv -1 \pmod{p},$$

što je kontradikcija sa Tvrđenjem 9.3 (iii). Znači, $p^2 \mid x^2+y^2 = n$, pa važi $(x/p)^2 + (y/p)^2 = n/p^2 < n$. Po indukcitvnoj pretpostavci, ili je $n/p^2 = 1$, ili se svi prosti faktori broja n/p^2 oblika $4m+3$ javljaju u njegovoj kanoničkoj faktorizaciji sa parnim eksponentom. No, tada isto važi i za n, što okončava induktivni dokaz. □

Predstavljanje zbirom tri kvadrata.

Teorema 13.4. *Pozitivan ceo broj n se može prikazati kao zbir tri cela kvadrata ako i samo ako n* nije *oblika $4^\ell(8m+7)$, $\ell, m \geqslant 0$.*

Nije teško videti da se nijedan broj oblika $4^\ell(8m+7)$ ne može predstaviti kao zbir tri kvadrata. Naime, ako je $x^2+y^2+z^2$ deljivo sa 4, tada svaki od brojeva x, y, z mora biti paran. Otuda sledi da se broj n može predstaviti kao zbir tri kvadrata ako i samo ako to isto važi i za $4n$. Prema tome, dovoljno je uvideti da se nijedan broj oblika $8m+7$ ne može prikazati kao zbir tri kvadrata; međutim, ovo lako sledi iz činjenice da potpun kvadrat može da daje ostatke $0, 1, 4$ po modulu 8.

Znatno teži deo dokaza (koji ovde ne navodimo) se sastoji u tome da se pokaže da svaki broj koji *nije* navedenog oblika zaista jeste zbir tri kvadrata. Teškoće na koje se nailazi u tom dokazu delimično potiču i od činjenice da skup brojeva koji se mogu predstaviti kao zbir tri kvadrata nije zatvoren za množenje: $3 = 1^2+1^2+1^2$ i $5 = 2^2+1^2+0^1$ imaju to svojstvo, ali to ne važi i za $15 = 8\cdot 1+7$.

Lagražova teorema o četiri kvadrata.

U ovom delu, naš cilj je da se dokaže sledeći rezultat.

Teorema 13.5 (Lagranž)**.** *Svaki pozitivan ceo broj se može prikazati kao zbir četiri cela kvadrata.*

Najpre, važi svojstvo slično slučaju zbirova dva kvadrata, tj. analogon Leme 13.1: skup brojeva predstavljivih zbirom četiri kvadrata zatvoren je za množenje.

Lema 13.6. *Ako se celi brojevi $m, \ell \in \mathbb{Z}^+$ mogu prikazati kao zbirovi četiri cela kvadrata, onda to važi i za $m\ell$.*

Dokaz. Slično kao i u dokazu Leme 13.1, traženo tvrđenje sledi iz identiteta:

$$\begin{aligned}(a^2+b^2+c^2+d^2)(A^2+B^2+C^2+D^2) = \\ = (-aA+bB+cC+dD)^2 + (aC-bD+cA+dB)^2 + \\ + (aD+bC-cB+dA)^2 + (aB+bA+cD-dC)^2.\end{aligned}$$

□

Prethodni identitet, kao ni identitiet iz Leme 13.1, nije rezultat slučajnosti, niti je dobijen nasumičnim računanjem. Na primer, identitet iz dokaza Leme 13.1 rezultat je uvođenja pojma *norme* $|\cdot| : \mathbb{C} \to \mathbb{R}_0^+$ u polje kompleksnih brojeva, funkcije koja je definisana sa

$$|a+bi|^2 = (a+bi)(a-bi) = a^2+b^2.$$

(U pitanju je zapravo rastojanje kompleksnog broja $a+bi$ od koordinatnog početka kompleksne ravni.) Norma je multiplikativna funkcija, tj. za sve $\alpha, \beta \in \mathbb{C}$ važi $|\alpha\beta| = |\alpha| \cdot |\beta|$ i pomenuti identitet iz Leme 13.1 izražava upravo ovu činjenicu. Slično se u tzv. Hamiltonovoj 4-dimenzionalnoj $\mathbb{R}$-algebri *kvaterniona*, koja se sastoji od elemenata oblika $z = a+bi+cj+dk$, gde je $i^2 = j^2 = k^2 = -1$, $ij = k = -ji$, $jk = i = -kj$, $ki = j = -ik$ može definisati norma

$$(\mathbf{N}(a+bi+cj+dk))^2 = (a+bi+cj+dk)(a-bi-cj-dk) = a^2+b^2+c^2+d^2,$$

i identitet iz prethodne leme je zapravo samo drugi oblik kojim se izražava multiplikativnost ove funkcije.

U dokazu Lagranžove teoreme će nam biti potrebno i sledeće pomoćno tvrđenje.

Lema 13.7. *Neka je $p > 2$ prost broj. Tada kongruencija*

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

ima rešenja u skupu celih brojeva.

Dokaz. Posmatrajmo sledeće skupove klasa ostataka po modulu p:

$$X = \{(x^2)_p : \ 0 \leqslant x < p\}, \quad Y = \{(-1-y^2)_p : \ 0 \leqslant y < p\}.$$

Prema Posledici 9.2 (primenjenoj na slučaj $k = 2$) oba ova skupa imaju tačno po $(p+1)/2$ elemenata (pošto uključuju, respektivno, i klase $(0)_p$, odnosno $(-1)_p$). Pošto je $|X| + |Y| = p+1$, dok je $|X \cup Y| \leqslant p$, sledi da ovi skupovi imaju neprazan presek; drugim rečima, za neke $0 \leqslant x, y < p$ važi $(x^2)_p = (-1-y^2)_p$, što je ekvivalentno tvrđenju leme. □

Dokaz Teoreme 13.5. Dokaz u velikoj meri imitira dokaz Fermaove teoreme o dva kvadrata. Naime, imajući u vidu Lemu 13.6, dovoljno je dokazati teoremu (tj. razloživost na zbir četiri kvadrata) samo za proste brojeve p. Jasno, $2 = 1^2+1^2+0^2+0^2$, pa možemo pretpostaviti da je p neparan, tj. $p > 2$.

Na osnovu prethodne leme zaključujemo da p ima umnožak koji se može prikazati kao zbir četiri kvadrata, budući da postoje $x, y \in \mathbb{Z}$ takvi da je

$$x^2 + y^2 + 1^2 + 0^2 = mp$$

za neko $m \geqslant 1$. Štaviše, iz dokaza prethodne leme je jasno da možemo odabrati x, y tako da je $|x|, |y| \leqslant (p-1)/2$, tako da možemo pretpostaviti da je $m < p$. Neka je sada m_0 najmanji broj sa osobinom da se $m_0 p$ može prikazati kao zbir četiri kvadrata. Tvrdimo da je $m_0 = 1$, što, kao što smo primetili, okončava dokaz teoreme.

Pretpostavimo suprotno. Neka je $m_0 p = a^2 + b^2 + c^2 + d^2$. Sada možemo odabrati cele brojeve A, B, C, D koji su po apsolutnoj vrednosti ne veći od $m_0/2$ tako da važe kongruencije

$$\begin{aligned} A &\equiv -a \pmod{m_0}, \\ B &\equiv b \pmod{m_0}, \\ C &\equiv c \pmod{m_0}, \\ D &\equiv d \pmod{m_0}. \end{aligned}$$

Sada je $A^2 + B^2 + C^2 + D^2 \leqslant m_0^2$. Ukoliko bi važila jednakost, tada bi svaki od A, B, C, D bio jednak $m_0/2$ ili $-m_0/2$ (i pri tome bi m_0 bio paran broj), pa bi svaki od a, b, c, d davao ostatak $m_0/2$ po modulu m_0. U tom slučaju bi $a^2+b^2+c^2+d^2 = m_0 p$ bilo deljivo sa m_0^2, tj. imali bismo $m_0 \mid p$, što je nemoguće, jer je, po učinjenim pretpostavkama, $1 < m_0 < p$. Iz sličnog razloga mora biti $A^2 + B^2 + C^2 + D^2 > 0$. Zbog toga je $A^2 + B^2 + C^2 + D^2 = m_0 m'$ za neko $1 \leqslant m' < m_0$. Otuda je

$$\begin{aligned} m_0^2 m' p &= (a^2 + b^2 + c^2 + d^2)(A^2 + B^2 + C^2 + D^2) \\ &= (-aA + bB + cC + dD)^2 + (aC - bD + cA + dB)^2 + \\ &\quad + (aD + bC - cB + dA)^2 + (aB + bA + cD - dC)^2. \end{aligned}$$

Direktnim uvrštavanjem se proverava da su sva četiri broja u osnovama kvadrata sa desne strane gornje jednakosti deljivi sa m_0. Ako sada definišemo

$$\begin{aligned} \alpha &= \tfrac{1}{m_0}(-aA + bB + cC + dD), \\ \beta &= \tfrac{1}{m_0}(aC - bD + cA + dB), \\ \gamma &= \tfrac{1}{m_0}(aD + bC - cB + dA), \\ \delta &= \tfrac{1}{m_0}(aB + bA + cD - dC), \end{aligned}$$

dobijamo da su $\alpha, \beta, \gamma, \delta$ celi brojevi za koje važi

$$\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = m' p.$$

Ovo je kontradikcija sa minimalnošću m_0; zato mora biti $m_0 = 1$, tj. p je predstavljiv zbirom četiri kvadrata. □