

Poglavlje 4

Kvadratne forme

Binarne kvadratne forme su homogeni polinomi u 2 varijable stupnja 2 s cjelobrojnim koeficijentima, odnosno

$$f(x, y) = ax^2 + bxy + cy^2, \quad a, b, c \in \mathbb{Z}.$$

Diskriminanta od f je broj $d = b^2 - 4ac$. Ako je $d < 0$, tada f poprima samo pozitivne ili negativne vrijednosti (ovisno o predznaku a) pa kažemo da je f pozitivno ili negativno definitna. Ako je $d > 0$, tada kažemo da je f indefinitna.

Forma f se matricno može zapisati kao $F = \begin{bmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{bmatrix}$. Kažemo da su dvije kvadratne forme f, g ekvivalentne ako postoji $U \in \text{SL}_2(\mathbb{Z})$ takva da je $G = U^T F U$ i pišemo $f \sim g$. Nije teško provjeriti da je \sim relacija ekvivalencije. Grupa $\text{SL}_2(\mathbb{Z})$ je generirana matricama

$$U = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad V^\pm = \begin{bmatrix} 1 & \pm 1 \\ 1 & 0 \end{bmatrix}$$

pa se svaka transformacija F u G može dobiti uzastopnim konjugiranjem matricama U, V^\pm . Vrijedi

$$U^T F U = \begin{bmatrix} c & \frac{-b}{2} \\ \frac{-b}{2} & a \end{bmatrix}, \quad (V^\pm)^T F V^\pm = \begin{bmatrix} a & \pm a + \frac{b}{2} \\ \pm a + \frac{b}{2} & a \pm b + c \end{bmatrix}.$$

Kažemo da forma f reprezentira neki $n \in \mathbb{Z}$ ako postoje $x, y \in \mathbb{Z}$ takvi da je $f(x, y) = n$. Ako je uz to i $(x, y) = 1$, kažemo da je reprezentacija prava, inače je neprava.

Teorem: *Neka su f, g ekvivalentne kvadratne forme. Tada one imaju istu diskriminantu i za svaki $n \in \mathbb{Z}$ vrijedi*

$$f \text{ (pravo) reprezentira } n \iff g \text{ (pravo) reprezentira } n.$$

Teorem: *Kažemo da je pozitivno definitna kvadratna forma $f = ax^2 + bxy + cy^2$ reducirana ako je $-a < b \leq a < c$ ili $0 \leq b \leq a = c$. Vrijede sljedeće tvrdnje.*

- *Svaka pozitivno definitna kvadratna forma je ekvivalentna nekoj reduciranoj formi.*

- Ako su f, f' reducirane i vrijedi $f \sim f'$, tada je $f = f'$.
- Postoji samo konačno mnogo reduciranih formi s danom diskriminantom d .
- Neka su $d < 0, n > 0$ cijeli brojevi. Tada je n pravo reprezentiran rekombom reduciranom formom s diskriminantom d ako i samo ako kongruencija $x^2 \equiv d \pmod{4n}$ ima rješenja.

Teorem: Prirodan broj n može se prikazati u obliku $n = x^2 + y^2$, $x, y \in \mathbb{Z}$ ako i samo ako se u rastavu broja n na proste faktore svaki $p = 4k + 3$ javlja s parnim eksponentom.

Teorem: Prirodan broj n može se prikazati u obliku $n = x^2 + y^2 + z^2$, $x, y, z \in \mathbb{Z}$ ako i samo ako $n \neq 4^m(8k + 7)$.

Teorem (o četiri kvadrata, Lagrange): Svaki prirodni broj n može se prikazati u obliku $n = x^2 + y^2 + z^2 + w^2$, $x, y, z, w \in \mathbb{Z}$.

Zadatak 4.1. Nađite reduciranu kvadratnu formu ekvivalentnu s $11x^2 + 35xy + 29y^2$.

Rješenje. Ova kvadratna forma reprezentirana je matricom $\begin{bmatrix} 11 & \frac{35}{2} \\ \frac{35}{2} & 29 \end{bmatrix}$. Sada uzastopno primjenjujemo transformacije matricama U, V^\pm . Biramo U ako je $a > c$, a inače V te predznak \pm biramo ovisno o predznaku broja b .

$$\begin{bmatrix} 11 & \frac{35}{2} \\ \frac{35}{2} & 29 \end{bmatrix} \xrightarrow{V^-} \begin{bmatrix} 11 & \frac{13}{2} \\ \frac{13}{2} & 5 \end{bmatrix} \xrightarrow{U} \begin{bmatrix} 5 & \frac{-13}{2} \\ \frac{-13}{2} & 11 \end{bmatrix} \xrightarrow{V^+} \begin{bmatrix} 5 & \frac{-3}{2} \\ \frac{-3}{2} & 3 \end{bmatrix} \xrightarrow{U} \begin{bmatrix} 3 & \frac{3}{2} \\ \frac{3}{2} & 5 \end{bmatrix}$$

Kvadratna forma $3x^2 + 3xy + 5y^2$ je reducirana i ekvivalentna početnoj.

Ako nam je to promaklo i nastavimo proces dalje, dobili bismo

$$\begin{bmatrix} 3 & \frac{3}{2} \\ \frac{3}{2} & 5 \end{bmatrix} \xrightarrow{V^-} \begin{bmatrix} 3 & \frac{-3}{2} \\ \frac{-3}{2} & 5 \end{bmatrix}$$

Nova matrica nema "manje" koeficijente od stare pa nam je to znak da smo došli do kraja procesa.

Zadatak 4.2. Odredite broj reduciranih kvadratnih formi $ax^2 + bxy + cy^2$ s diskriminantom

(a) -32 .

(b) -47 .

Rješenje. (a) Rješavamo jednadžbu $4ac - b^2 = 32$ uz uvjete reduciranosti kvadratne forme. Primijetimo prvo da je b paran. Mora vrijediti $|b| \leq a \leq c$ pa dobivamo $3b^2 \leq 4ac - b^2 = 32 \implies |b| \leq 2$. Sada imamo nekoliko slučaja.

- $b = 0$: $4ac = 32 \implies (a, c) = (1, 8), (2, 4)$.
- $b = 2$: $4ac = 36 \implies (a, c) = (3, 3)$ (par $(1, 9)$ nije rješenje zbog uvjeta reduciranosti).

- $b = -2$: $4ac = 36$, nema rješenja (parovi $(1, 9)$, $(3, 3)$ nisu rješenje zbog uvjeta reduciranosti).

Dakle, $h(-32) = 3$.

(b) Rješavamo jednadžbu $4ac - b^2 = 47$ uz uvjete reduciranosti kvadratne forme. Primijetimo prvo da je b neparan. Mora vrijediti $|b| \leq a \leq c$ pa dobivamo $3b^2 \leq 4ac - b^2 = 47 \implies |b| \leq 3$. Sada imamo nekoliko slučajeva.

- $b = 1$: $4ac = 48 \implies (a, c) = (1, 12), (2, 6), (3, 4)$.
- $b = -1$: $4ac = 48 \implies (a, c) = (2, 6), (3, 4)$ (par $(1, 12)$ nije rješenje zbog uvjeta reduciranosti).
- $b = 3$: $4ac = 56 \implies ac = 14$, nema rješenja zbog $c \geq a \geq 3$.
- $b = -3$: $4ac = 56 \implies ac = 14$, nema rješenja zbog $c \geq a \geq 3$.

Dakle, $h(-47) = 5$.

Zadatak 4.3. Dokažite da od 4 uzastopna prirodna broja barem jedan nije prikaziv kao suma 2 kvadrata cijelih brojeva.

Rješenje. Jedan od ta 4 broja je oblika $4k + 3$ pa se bar jedan njegov prost faktor javlja s neparnim eksponentom.

Zadatak 4.4. Dokažite da za svaki $k \in \mathbb{N}$ jednadžba $x^2 + y^2 = z^k$ ima rješenje u \mathbb{N} .

Rješenje. Ako je $k = 2a$, možemo uzeti $(x, y, z) = (3 \cdot 5^{a-1}, 4 \cdot 5^{a-1}, 5)$. Ako je $k = 2a + 1$, možemo uzeti $(x, y, z) = (5^a, 2 \cdot 5^a, 5)$.

Zadatak 4.5. Riješite jednadžbu $x^4 + 8x^2y^2 - 9y^4 = 1281$ u \mathbb{N} .

Rješenje. Jednadžba je jednaka

$$(x^2 + 9y^2)(x^2 - y^2) = 3 \cdot 7 \cdot 61.$$

Primijetimo da $x^2 + 9y^2$ ne može biti djeljivo s 3 ili 7 pa $x^2 + 9y^2 \mid 61$. Ručnom provjerom dolazimo do jedine mogućnosti $x = 5, y = 2$ što je ujedno i rješenje zadatka.

Zadatak 4.6. Ako se brojevi m, n mogu prikazati kao sume kvadrata 2 prirodna broja, ali mn ne može, dokažite da je mn kvadrat parnog broja.

Rješenje. Neka je $m = a^2 + b^2, n = c^2 + d^2$. Znamo da je

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

Kako mn nije prikaziv kao suma 2 kvadrata prirodnih brojeva, mora biti $ad = bc$ pa je $mn = (ac + bd)^2$. Primijetimo da vrijedi i identitet

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

pa je $ac = bd$. Iz $ad = bc, ac = bd$ možemo zaključiti da je $a = b, c = d$ iz čega slijedi da je $mn = (ac + bd)^2 = (2ac)^2$.

Zadatak 4.7. Neka je $n \in \mathbb{N}$. Dokažite da broj $6 \cdot 4^n$ nije prikaziv kao suma 4 kvadrata prirodnih brojeva.

Rješenje. Pretpostavimo da je $6 \cdot 4^n = x_1^2 + x_2^2 + x_3^2 + x_4^2$. Kako $8 \mid 6 \cdot 4^n$ i $x^2 \equiv 0, 1, 4 \pmod{8}$, zaključujemo da svi brojevi x_i moraju biti parni. Stoga je i broj $6 \cdot 4^{n-1}$ prikaziv kao suma 4 kvadrata prirodnih brojeva. Nakon n ovakvih koraka dolazimo do tvrdnje da je broj 6 prikaziv kao suma 4 kvadrata prirodnih brojeva, što nije istina.

Zadatak 4.8. Pronađite različite brojeve $a, b \in \mathbb{N}$ takve da su a, b prikazivi kao suma kvadrata 3 cijela broja, ali ab nije.

Rješenje. Znamo da su brojevi koji nisu prikazivi kao suma 3 kvadrata točno brojevi oblika $4^n(8k + 7)$. Neka je

$$a = 2 \cdot 4^n(8k + 7) = 4^n(8(2k + 1) + 6), \quad b = 2 = 1^2 + 1^2 + 0^2.$$

Tada su a, b prikazivi kao suma 3 kvadrata, ali $ab = 4^{n+1}(8k + 7)$ nije.

Zadatak 4.9. Odredite sve proste brojeve p prikazive u obliku $p = x^2 + 2y^2$ za $x, y \in \mathbb{Z}$

Rješenje. Diskriminanta ove kvadratne forme je -8 . Znamo da se p može prikazati nekom kvadratnom formom s diskriminantom -8 jest da je $\left(\frac{-8}{p}\right) = 1 \iff p \equiv 1, 3 \pmod{8}$.

Nije teško izračunati da je $h(-8) = 1$ pa je $x^2 + 2y^2$ jedina reducirana kvadratna forma s diskriminantom -8 . Dakle, prosti brojevi prikazivi kao $x^2 + 2y^2$ su točno $p \equiv 1, 3 \pmod{8}$.

Zadatak 4.10. Odredite sve proste brojeve p prikazive u obliku $p = 2x^2 + 3y^2$ za $x, y \in \mathbb{Z}$

Rješenje. Diskriminanta ove kvadratne forme je -24 . Znamo da se p može prikazati nekom kvadratnom formom s diskriminantom -24 jest da je $\left(\frac{-24}{p}\right) = 1 \iff p \equiv 1, 5, 7, 11 \pmod{24}$.

Nije teško izračunati da je $h(-24) = 2$ i da su $x^2 + 6y^2, 2x^2 + 3y^2$ jedine reducirane kvadratne forme s diskriminantom -24 .

Ako je $p = x^2 + 6y^2$, tada je $x^2 \equiv p \pmod{3}$ pa imamo $\left(\frac{p}{3}\right) = 1 \iff p \equiv 1 \pmod{3}$.

Ako je $p = 2x^2 + 3y^2$, tada je $2x^2 \equiv p \pmod{3}$ pa imamo $\left(\frac{2p}{3}\right) = 1 \iff p \equiv -1 \pmod{3}$.

Dakle, prosti brojevi prikazivi kao $2x^2 + 3y^2$ su točno $p \equiv 5, 11 \pmod{24}$.

Zadatak 4.11. Ako je n trokutast broj, dokažite da su brojevi $8n^2, 8n^2 + 1, 8n^2 + 2$ prikazivi kao suma dva kvadrata cijelih brojeva.

Rješenje. Vrijedi

$$8n^2 = 4n^2 + 4n^2, \quad 8n^2 + 2 = (1 + 1)(4n^2 + 1) = (2n + 1)^2 + (2n - 1)^2.$$

Ovdje zapravo nismo koristili da je n trokutast, ali ta pretpostavka će nam trebati za preostali broj.

Kako je n trokutast, postoji $k \in \mathbb{N}$ takav da je $n = \frac{k(k+1)}{2}$. Tada je

$$\begin{aligned} 8n^2 + 1 &= 2k^2(k+1)^2 + 1 = 2k^4 + 4k^3 + 2k^2 + 1 = \\ &= k^4 + 4k^3 + 4k^2 + k^4 - 2k^2 + 1 = (k^2 + 2k)^2 + (k^2 - 1)^2. \end{aligned}$$

Zadatak 4.12. Ako je p prost broj oblika $8k+7$, dokažite da ne postoje $x, y, z \in \mathbb{N}$ takvi da je $x^2 + y^2 + z^4 = p^2$.

Rješenje. Jednadžba je jednaka

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

Kako je $1 \leq z < p$, vrijedi $(p - z^2, p + z^2) = (p + z^2, 2p) = (p + z^2, 2) \mid 2$.

Ako $2 \mid z$, tada je $p - z^2$ oblika $4k+3$ pa vrijedi $p - z^2 \nmid x^2 + y^2$. Ako $2 \nmid z$, tada je $p - z^2$ oblika $8k+6 = 2 \cdot (4k+3)$ pa opet vrijedi $p - z^2 \nmid x^2 + y^2$.

Zadatak 4.13. Dokažite da se svaki neparni prirodni broj može prikazati u obliku $x^2 + y^2 + 2z^2$, $x, y, z \in \mathbb{Z}$.

Rješenje. Osnovna ideja je

$$n = x^2 + y^2 + 2z^2 \iff 2n = (x+y)^2 + (x-y)^2 + 4z^2.$$

Neka je $n = 2k+1$. Tada znamo da se $4k+2$ može prikazati kao suma 3 kvadrata. Gledajući mod 4, možemo BSO pretpostaviti da je $4k+2 = a^2 + b^2 + 4c^2$, $2 \nmid a, b$. Tada je

$$n = 2k+1 = \left(\frac{a+b}{2}\right)^2 + \left(\frac{a-b}{2}\right)^2 + 2c^2.$$

Zadatak 4.14. Dokažite da se svaki neparni prirodni broj može prikazati kao suma kvadrata četiriju cijelih brojeva od kojih su dva susjedni brojevi.

Rješenje. Osnovna ideja je slična,

$$n = x^2 + y^2 + z^2 + (z+1)^2 \iff 2n-1 = (x+y)^2 + (x-y)^2 + (2z+1)^2.$$

Neka je $n = 2k+1$. Tada znamo da se $2n-1 = 4k+1$ može prikazati kao suma 3 kvadrata. Gledajući mod 4, možemo BSO pretpostaviti da je $4k+1 = a^2 + b^2 + (2c+1)^2$, gdje su a, b iste parnosti. Tada je

$$n = 2k+1 = \left(\frac{a+b}{2}\right)^2 + \left(\frac{a-b}{2}\right)^2 + c^2 + (c+1)^2.$$

Zadatak 4.15. Prikažite broj $2^{2025} + 6$ kao sumu 3 kvadrata cijelih brojeva.

Rješenje. Primijetimo da je $2^{2025} = 2x^2$ pa imamo

$$2x^2 + 6 = 2(x^2 + 1) + 4 = (x-1)^2 + (x+1)^2 + 2^2.$$

Zadatak 4.16. Dokažite da se svaki prirodni broj $n > 169$ može prikazati kao suma kvadrata 5 prirodnih brojeva.

Rješenje. Vrijedi

$$169 = 13^2 = 12^2 + 5^2 = 12^2 + 4^2 + 3^2 = 11^2 + 4^2 + 4^2 + 4^2$$

pa se 169 može prikazati kao suma m prirodnih brojeva za svaki $m \leq 4$. Znamo da se broj $n - 169$ može prikazati kao suma 4 kvadrata cijelih brojeva. Neka je od ta 4 broja njih $k \leq 4$ prirodnih. Tada možemo uzeti sumu

$$n = (n - 169) + 169 = (\text{suma } k \text{ prirodnih brojeva}) + (\text{suma } 5\text{-k prirodnih brojeva}).$$

Zadatak 4.17. (*) Dokažite da postoji beskonačno mnogo prostih brojeva oblika $a^2 + b^2 + c^2 + 1$.

Rješenje. Po Dirichletovom teoremu znamo da postoji beskonačno mnogo prostih brojeva oblika $8k + 7$. Također, broj $8k + 6$ je prikaziv kao suma 3 kvadrata. Stoga je $p = 8k + 7 = (8k + 6) + 1 = a^2 + b^2 + c^2 + 1$.

Zadatak 4.18. (*) Ako je a prirodan broj takav da je za svaki $n \in \mathbb{N}$ broj $a + n^2$ prikaziv kao suma 2 kvadrata cijelih brojeva, dokažite da je a potpun kvadrat.

Rješenje. Pretpostavimo suprotno i neka je $a = k^2b$, gdje je $b \geq 2$ kvadratno slobodan. Primjenom postupka u rješenju Zadatka 3.27. uz male promjene (detalje CRT-a ostavljamo čitatelju) dobivamo da postoji prost broj $p > a$ oblika $4k + 3$ takav da je $\left(\frac{p}{b}\right) = 1$.

Stoga je $\left(\frac{-b}{p}\right) = \left(\frac{p}{b}\right) = 1$ i postoji $n_0 \in \mathbb{N}$ takav da $p \mid b + n_0^2$. Ako $p^2 \mid b + n_0^2$, umjesto n_0 možemo uzeti $n_0 + p$ pa vrijedi

$$p^2 \nmid b + (n_0 + p)^2 = (b + n_0^2) + p^2 + 2n_0p.$$

Dakle, postoji $n \in \mathbb{N}$ takav da $p \parallel b + n^2$ (tj. $p \mid b + n^2, p^2 \nmid b + n^2$). Zbog uvjeta $p > a$ sada vrijedi $p \parallel k^2(b + n^2) = a + (kn)^2$ pa taj broj nije prikaziv kao suma 2 kvadrata.

Dobili smo kontradikciju pa a mora biti potpun kvadrat.

Zadatak 4.19. (*) Dokažite da se svaki cijeli broj n može prikazati kao suma 5 kubova (ne nužno različitih) cijelih brojeva.

Rješenje. Primijetimo prvo da se svaki cijeli broj djeljiv sa 6 može prikazati kao suma 4 kuba cijelih brojeva

$$6n = (n + 1)^3 + (n - 1)^3 - n^3 - n^3.$$

Još treba pokazati da je svaki ostatak mod 6 kubni ostatak. Imamo

$$\begin{aligned} 0 &= 0^3, \\ 1 &= 1^3, \\ 2 &\equiv 2^3 \pmod{6}, \\ 3 &\equiv 3^3 \pmod{6}, \\ 4 &\equiv (-2)^3 \pmod{6}, \\ 5 &\equiv (-1)^3 \pmod{6}. \end{aligned}$$

Napomena 1: Vrijedi i tvrdnja da se svaki prirodan broj može prikazati kao suma najviše 9 kubova prirodnih brojeva. Slutnja da se svaki cijeli broj može prikazati kao suma 4 kuba cijelih brojeva je otvoren problem iako je dokazana za neke specijalne slučajeve (za $3 \mid n$ te za $n \equiv 1, 7, 8 \pmod{18}$).

Napomena 2: Waringov problem pita sljedeće: postoji li za svaki $k \in \mathbb{N}$ prirodni broj s takav da se svaki prirodan broj može prikazati kao suma $\leq s$ k -tih potencija cijelih brojeva. Ako postoji, koliki je minimalni mogući takav $g(k) := s$?

Dokazano je da je $g(k) = 2^k + \lfloor (\frac{3}{2})^k \rfloor - 2$ za sve $k < 471600000$. Tako je npr. $g(3) = 9, g(4) = 19, g(5) = 37, g(6) = 73, \dots$ Slutnja je da ta tvrdnja vrijedi za sve $k \in \mathbb{N}$. Više o tome može se naći u [1].

Bibliografija

- [1] M. B. Nathanson: *Additive Number Theory: The Classical Bases*, Graduate Texts in Mathematics. Vol. 164. Springer-Verlag. (1996.) 4