4. Kvadratne forme

Definicija 4.1 *Binarna kvadratna forma* je homogeni polinom od dvije varijable drugog stupnja s cjelobrojnim koeficijentima, tj.

$$f(x,y) = ax^2 + bxy + cy^2, \quad a,b,c \in \mathbb{Z}. \tag{1}$$

Diskriminanta binarne kvadratne forme f je broj

$$d = b^2 - 4ac.$$

Uočimo:

- Ako je b paran broj, onda je $d \equiv 0 \pmod 4$;
- Ako je b neparan broj, onda je $d \equiv 1 \pmod 4$;

Obrat:

Forme:

$$f(x,y) = x^2 - \frac{1}{4}dy^2 \text{ za } d \equiv 0 (\mathrm{mod}\, 4),$$

i

$$f(x,y) = x^2 + xy + \frac{1}{4}(1-d)\, y^2 \text{ za } d \equiv 1 (\mathrm{mod}\, 4),$$

imaju diskriminantu jednaku d i nazivamo ih *glavne forme* s diskriminantom d;

Iz (1) imamo:

$$4af(x,y) = (2ax+by)^2 - dy^2.$$

- Ako je $d < 0$ onda f ili poprima samo pozitivne ili samo negativne vrijednosti za $(x,y) \neq (0,0)$ U tom slučaju kažemo da je f *pozitivno*, odnosno *negativno definitna*.

- Ako je $d > 0$ onda f poprima i pozitivne i negativne vrijednosti, pa je nazivamo *indefinitna forma*.

- Ako je $d = 0$, onda je f *poludefinitna*.

Definicija 4.2 Kažemo da su dvije binarne kvadratne forme f i g *ekvivalentne* ako se jedna može transformirati u drugu pomoću cjelobrojnih unimodularnih transformacija, tj. supstitucija oblika

$$x = px' + qy', \quad y = rx' + sy', \tag{2}$$

gdje je $p,q,r,s \in \mathbb{Z}$ i $ps - qr = 1$. Pišemo: $f \sim g$.

Matrično f možemo zapisati kao

$$X^T F X,$$

gdje je

$$F = \begin{bmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{bmatrix}, \quad X = \begin{bmatrix} x \\ y \end{bmatrix},$$

a supstituciju sa

$$X = UX',$$

gdje je

$$U = \begin{bmatrix} p & q \\ r & s \end{bmatrix}, \quad X' = \begin{bmatrix} x' \\ y' \end{bmatrix}.$$

Uvjet unimodularnosti je tada $\det U = 1$. Pritom matrični zapis od f prelazi u (matrični zapis od g)

$$X'^T G X',$$

gdje je

$$G = U^T F U.$$

Označimo s

$$\Gamma = \left\{ \begin{bmatrix} p & q \\ r & s \end{bmatrix} : p, q, r, s \in \mathbb{Z} \text{ i } ps - qr = 1 \right\},$$

tada Γ čini grupu s obzirom na matrično množenje.

Uočimo:

- $$B = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \in \Gamma \Longrightarrow B^{-1} = \frac{1}{ps - qr} \begin{bmatrix} s & -q \\ -r & p \end{bmatrix}$$

$$B \in \Gamma \Longrightarrow \det B = ps - qr = 1 \implies B^{-1} = \begin{bmatrix} s & -q \\ -r & p \end{bmatrix}$$

- $$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \quad B = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \in \Gamma \Longrightarrow$$

$$AB^{-1} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} p & -q \\ -r & s \end{bmatrix} = \begin{bmatrix} ap - br & bs - aq \\ cp - dr & ds - cq \end{bmatrix}$$

i

$$\det\left(AB^{-1}\right) = \det A \cdot (\det B)^{-1} = 1 \Longrightarrow AB^{-1} \in \Gamma.$$

Elemente grupe Γ nazivamo *unimodularne matrice*.

- Uvjet ekvivalentnosti kvadratnih formi (2) je ekvivalentan postojanju matrice $U \in \Gamma$ za koju je $G = U^T F U$ (uz oznake od prije).

Propozicija 4.1 Neka su f, g i h binarne kvadratne forme. Tada vrijedi:

i) $f \sim f$;

ii) $f \sim g \Longrightarrow g \sim f$;

iii) $f \sim g, g \sim h \Longrightarrow f \sim h$.

Drugim riječima, $\sim$ je relacija ekvivalencije.

Dokaz:

Zadatak: Neka su

$f(x, y) = ax^2 + bxy + cy^2$ i $g(x, y) = a'x^2 + b'xy + c'y^2$

dvije ekvivalentne kvadratne forme. Pokažite: ako je

$$U = \begin{bmatrix} p & q \\ r & s \end{bmatrix}$$

martica prijelaza iz f u g, tada je

$$\gcd(p, r) = 1, \quad \gcd(q, s) = 1$$

$$a' = f(p, r), \ c' = f(q, s)$$

$$b' = 2apq + b(ps + qr) + 2crs,$$

Definicija 4.3 Kažemo da binarna kvadratna forma *reprezentira* cijeli broj n ako postoje $x_0, y_0 \in \mathbb{Z}$ takvi da je

$$f\left(x_0, y_0\right) = n.$$

Ako je pritom $\gcd\left(x_0, y_0\right) = 1$, onda kažemo da je reprezentacija *prava*, inače je *neprava*.

Propozicija 4.2 Neka su f i g ekvivalentne binarne kvadratne forme, te $n \in \mathbb{Z}$. Tada:

i) f reprezentira n ako i samo ako g reprezentira n;

ii) f pravo reprezentira n ako i samo ako g pravo reprezentira n;

iii) diskriminante od f i g su jednake.

Dokaz:

Napomena:

- Obrat ovih tvrdnji općenito ne vrijedi. Primjer:

  $f\left(x, y\right) = 2x^2 + xy + 3y^2$ i $g\left(x, y\right) = 2x^2 - xy + 3y^2$

  su neekvivalentne pozitivno definitne binarne kvadratne forme s diskriminantom -23 i reprezentiraju iste brojeve. Npr. $f\left(2, -1\right) = 9 = g\left(2, 1\right)$.

Redukcija pozitivno definitnih kvadratnih formi.

Pretpostavimo: $d < 0$ i $a > 0$, pa je i $c > 0$.

Definicija 4.4 Kažemo da je pozitivno definitna binarna kvadratna forma $f(x, y) = ax^2 + bxy + cy^2$ *reducirana* ako je $-a < b \leq a < c$ ili $0 \leq b \leq a = c$.

Teorem 4.1 Postoji točno jedna reducirana binarna kvadratna forma u svakoj klasi ekvivalencije pozitivno definitnih binarnih kvadratnih formi.

Dokaz:

Primjer:

$$f(x, y) = 2x^2 + xy + 3y^2 \text{ i } g(x, y) = 2x^2 - xy + 3y^2$$

su reducirane pozitivno definitne binarne kvadratne forme s diskriminantom -23. Po prethodnom teoremu, one su neekvivalentne.

Primjer 4.1 Nađimo reduciranu kvadratnu formu ekvivalentnu sa $f(x, y) = 133x^2 + 108xy + 22y^2$.

Zadatak 4.1 Nađite reduciranu kvadratnu formu ekvivalentnu sa $f(x, y) = 7x^2 + 25xy + 23y^2$.

Teorem 4.2 Postoji samo konačno mnogo klasa ekvivalencije pozitivno definitnih binarnih kvadratnih formi s danom diskriminantom d.

Dokaz:

Definicija 4.5 Za binarnu kvadratnu formu $f(x, y) = ax^2 + bxy + cy^2$ kažemo da je *primitivna* ako je $\gcd(a, b, c) = 1$.

Definicija 4.6 Broj primitivnih pozitivno definitnih reduciranih binarnih kvadratnih formi s diskriminantom d naziva se *broj klasa od d* i označava se s $h(d)$.

Primjer 4.2 Izračunajmo $h(-4)$.

Poznato je da je $h(d) = 1$ za samo 13 negativnih cijelih brojeva: $d = -3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163.$

Vrijedi da je $\lim\limits_{d \to \infty} h(d) = \infty.$

Zadatak 4.1 Dokažite da je $h(d) = 1$ za $d = -7$, -8, $-11.$

Primjer 4.3 Izračunajmo $h(-20)$.

Teorem 4.3 Neka su $d < 0$ i $n > 0$ cijeli brojevi. Tada je n pravo reprezentiran nekom binarnom kvadratnom formom s diskriminantom d ako i samo ako kongruencija $x^2 \equiv d (\bmod 4n)$ ima rješenja.

Dokaz:

Primjer 4.4 Dokažimo da se prost broj p može prikazati u obliku $x^2 + 5y^2$, $x, y \in \mathbb{N}$ ako i samo ako je $p \equiv 1$ ili $9 \pmod{20}$.

Teorem 4.4 Prirodan broj n se može prikazati u obliku $x^2 + y^2$, $x, y \in \mathbb{Z}$ ako i samo ako se u rastavu broja n na proste faktore svaki prost faktor p za koji je $p \equiv 3 \pmod{4}$ javlja s parnom potencijom.

Dokaz:

Teorem 4.6 Cijeli broj n se može prikazati u obliku $x^2 - y^2$, $x, y \in \mathbb{Z}$ ako i samo ako $n \not\equiv 2 \pmod{4}$.

Dokaz:

Primjer 4.5 Neka je $r(n)$ broj uređenih parova (x, y) cijelih brojeva takvih da je $\gcd(x, y) = 1$ i $x^2 + y^2 = n$, te neka je $N(n)$ broj rješenja kongruencije $z^2 \equiv -1 \pmod n$.

i) Tada je $r(n) = 4N(n)$;

ii) Neka je $n = \prod\limits_{p-prost} p^{\alpha(p)}$. Ako je $\alpha(2) = 0$ ili 1, te $\alpha(p) = 0$ za sve $p \equiv 3 \pmod 4$, onda je $r(n) = 2^{t+2}$, gdje je t prost broj faktora od n oblika $4k + 1$. U protivnom je $r(n) = 0$.

iii) Ako je p prost broj oblika $4k + 1$, onda je prikaz broja p u obliku $x^2 + y^2$, $x, y \in \mathbb{N}$ jedinstven do na poredak pribrojnika.

Teorem 4.6 (Teorem o četiri kvadrata) Svaki prirodan broj n može se prikazati u obliku sume kvadrata četiri cijela broja, tj. u obliku

$$n = x^2 + y^2 + z^2 + w^2, \quad x, y, z, w \in \mathbb{Z}.$$

Dokaz:

Napomena: Tvrdnju Teorema 4.6 dovoljno je provjeriti za proste brojeve budući da vrijedi identitet

$$\left(x^2+y^2+z^2+w^2\right)\left(a^2+b^2+c^2+d^2\right)= \\ =(ax+by+cz+dw)^2+(ay-bx+dz-cw)^2+ \\ +(az-cx+bw-dy)^2+(aw-dx+cy-bz)^2 \tag{3}$$

Napomena: Metoda upotrebljena u posljednjem dijelu dokaza prethodnog teorema naziva se *Frematova metoda beskonačnog spusta*.

Metoda beskonačnog spusta:

- koristi se kad radimo s prirodnim brojevima (tj. koristimo činjenicu da svaki podskup od $\mathbb{N}$ ima najmanji element);
- Ideja:
  - Pretpostavimo da je neka tvrdnja točna za neki prirodan broj;
  - Pokažemo da je ta tvrdnja točna za neki manji prirodan broj (manji od danog);
  - Ovo znači da je tvrdnja točna za neki strogo padajući (beskonačni) niz prirodnih brojeva, što je kontradikcija (s činjenicom da svaki podskup od $\mathbb{N}$ ima minimalni element).

Legendere i Gauss su dokazali:

Prirodan broj n može prikazati kao suma tri kvadrata ako i samo ako n nije oblika $4^m(8k+7)$, $m, k \geq 0$.

Nužnost: Primjer 4.6.

Dovoljnost: Dosta teža, koristi teoriju tenarnih formi.

Primjer 4.6 Neka je $n = 4^m(8k+7)$, $m, k \geq 0$. Tada se n ne može prikazati kao suma tri kvadrata, tj. kao $n = x^2 + y^2 + z^2$, $x, y, z \in \mathbb{Z}$.

Zadatak 4.2 Dokažite da postoji beskonačno prirodnih brojeva koji se ne mogu prikazati kao suma kvadrata četiri prirodna broja, ali da se svaki prirodan broj n, $n > 169$ može prikazati kao suma kvadrata pet prirodnih brojeva.