Teorija brojeva

Filip Najman

6. predavanje

20.4.2023.

Definicija

Neka je Q neparan prirodan broj, te neka je $Q = q_1 \cdots q_s$, gdje su q_i neparni prosti brojevi, ne nužno različiti. Tada se Jacobijev simbol $\left(\frac{a}{Q}\right)$ definira sa

$$\left(\frac{a}{Q}\right) = \prod_{j=1}^{s} \left(\frac{a}{q_j}\right),$$

gdje je $\left(\frac{a}{q_j}\right)$ Legendreov simbol.

Definicija

Neka je Q neparan prirodan broj, te neka je $Q = q_1 \cdots q_s$, gdje su q_i neparni prosti brojevi, ne nužno različiti. Tada se Jacobijev simbol $\left(\frac{a}{Q}\right)$ definira sa

$$\left(\frac{a}{Q}\right) = \prod_{j=1}^{s} \left(\frac{a}{q_j}\right),$$

gdje je $\left(\frac{a}{q_j}\right)$ Legendreov simbol.

Ako je Q prost broj, onda se Legendreov i Jacobijev simbol podudaraju.

Definicija

Neka je Q neparan prirodan broj, te neka je $Q = q_1 \cdots q_s$, gdje su q_i neparni prosti brojevi, ne nužno različiti. Tada se Jacobijev simbol $\left(\frac{a}{Q}\right)$ definira sa

$$\left(\frac{a}{Q}\right) = \prod_{j=1}^{s} \left(\frac{a}{q_j}\right),$$

gdje je $\left(\frac{a}{q_j}\right)$ Legendreov simbol.

Ako je Q prost broj, onda se Legendreov i Jacobijev simbol podudaraju.

Ako je $(a, Q) > 1$, onda je $\left(\frac{a}{Q}\right) = 0$; inače je $\left(\frac{a}{Q}\right) \in \{-1, 1\}$.

Definicija

Neka je Q neparan prirodan broj, te neka je $Q = q_1 \cdots q_s$, gdje su q_i neparni prosti brojevi, ne nužno različiti. Tada se Jacobijev simbol $\left(\frac{a}{Q}\right)$ definira sa

$$\left(\frac{a}{Q}\right) = \prod_{j=1}^{s} \left(\frac{a}{q_j}\right),$$

gdje je $\left(\frac{a}{q_j}\right)$ Legendreov simbol.

Ako je Q prost broj, onda se Legendreov i Jacobijev simbol podudaraju.

Ako je $(a, Q) > 1$, onda je $\left(\frac{a}{Q}\right) = 0$; inače je $\left(\frac{a}{Q}\right) \in \{-1, 1\}$.

Ako je a kvadratni ostatak modulo Q, onda je a kvadratni ostatak modulo q_j za svaki j.

Definicija

Neka je Q neparan prirodan broj, te neka je $Q = q_1 \cdots q_s$, gdje su q_i neparni prosti brojevi, ne nužno različiti. Tada se Jacobijev simbol $\left(\frac{a}{Q}\right)$ definira sa

$$\left(\frac{a}{Q}\right) = \prod_{j=1}^{s} \left(\frac{a}{q_j}\right),$$

gdje je $\left(\frac{a}{q_j}\right)$ Legendreov simbol.

Ako je Q prost broj, onda se Legendreov i Jacobijev simbol podudaraju.

Ako je $(a, Q) > 1$, onda je $\left(\frac{a}{Q}\right) = 0$; inače je $\left(\frac{a}{Q}\right) \in \{-1, 1\}$.

Ako je a kvadratni ostatak modulo Q, onda je a kvadratni ostatak modulo q_j za svaki j.

Zato je $\left(\frac{a}{q_j}\right) = 1$ za svaki j, pa je i $\left(\frac{a}{Q}\right) = 1$.

Primijetimo međutim da $(\frac{a}{Q}) = 1$ *ne povlači* da je a kvadratni ostatak modulo Q.

Primijetimo međutim da $(\frac{a}{Q}) = 1$ *ne povlači* da je a kvadratni ostatak modulo Q.

Na primjer, $(\frac{2}{15}) = (\frac{2}{3})(\frac{2}{5}) = (-1)(-1) = 1$, ali kongruencija $x^2 \equiv 2 \pmod{15}$ nema rješenja.

Primijetimo međutim da $(\frac{a}{Q}) = 1$ *ne povlači* da je a kvadratni ostatak modulo Q.

Na primjer, $(\frac{2}{15}) = (\frac{2}{3})(\frac{2}{5}) = (-1)(-1) = 1$, ali kongruencija $x^2 \equiv 2 \pmod{15}$ nema rješenja.

Da bi a bio kvadratni ostatak modulo Q nužno je i dovoljno da svi $(\frac{a}{q_j})$ budu jednaki 1.

Propozicija

Neka su Q i Q' neparni prirodni brojevi. Tada vrijedi

1) $(\frac{a}{Q})(\frac{a}{Q'}) = (\frac{a}{QQ'})$

Propozicija

Neka su Q i Q' neparni prirodni brojevi. Tada vrijedi

1) $(\frac{a}{Q})(\frac{a}{Q'}) = (\frac{a}{QQ'})$

2) $(\frac{a}{Q})(\frac{a'}{Q}) = (\frac{aa'}{Q})$

Propozicija

Neka su Q i Q' neparni prirodni brojevi. Tada vrijedi

1) $\left(\frac{a}{Q}\right)\left(\frac{a}{Q'}\right) = \left(\frac{a}{QQ'}\right)$

2) $\left(\frac{a}{Q}\right)\left(\frac{a'}{Q}\right) = \left(\frac{aa'}{Q}\right)$

3) Ako je $(a, Q) = 1$*, onda je* $\left(\frac{a^2}{Q}\right) = \left(\frac{a}{Q^2}\right) = 1$.

Propozicija

Neka su Q i Q' neparni prirodni brojevi. Tada vrijedi

1) $\left(\frac{a}{Q}\right)\left(\frac{a}{Q'}\right) = \left(\frac{a}{QQ'}\right)$

2) $\left(\frac{a}{Q}\right)\left(\frac{a'}{Q}\right) = \left(\frac{aa'}{Q}\right)$

3) Ako je $(a, Q) = 1$, *onda je* $\left(\frac{a^2}{Q}\right) = \left(\frac{a}{Q^2}\right) = 1$.

4) Ako je $a \equiv a' \pmod{Q}$, *onda je* $\left(\frac{a}{Q}\right) = \left(\frac{a'}{Q}\right)$.

Propozicija

Neka su Q i Q' neparni prirodni brojevi. Tada vrijedi

1) $\left(\frac{a}{Q}\right)\left(\frac{a}{Q'}\right) = \left(\frac{a}{QQ'}\right)$

2) $\left(\frac{a}{Q}\right)\left(\frac{a'}{Q}\right) = \left(\frac{aa'}{Q}\right)$

3) Ako je $(a, Q) = 1$, *onda je* $\left(\frac{a^2}{Q}\right) = \left(\frac{a}{Q^2}\right) = 1$.

4) Ako je $a \equiv a' \pmod{Q}$, *onda je* $\left(\frac{a}{Q}\right) = \left(\frac{a'}{Q}\right)$.

Dokaz: Sve tvrdnje slijede direktno iz definicije Jacobijevog simbola i Propozicije koja je ranije dokazana. □

Propozicija

Ako je Q neparan prirodan broj, onda je

$$\left(\frac{-1}{Q}\right) = (-1)^{\frac{Q-1}{2}}, \quad \left(\frac{2}{Q}\right) = (-1)^{\frac{Q^2-1}{8}}.$$

Propozicija

Ako je Q neparan prirodan broj, onda je

$$\left(\frac{-1}{Q}\right) = (-1)^{\frac{Q-1}{2}}, \quad \left(\frac{2}{Q}\right) = (-1)^{\frac{Q^2-1}{8}}.$$

Dokaz: Imamo:

$$\left(\frac{-1}{Q}\right) = \prod_{j=1}^{s}\left(\frac{-1}{q_j}\right) = \prod_{j=1}^{s}(-1)^{\frac{q_j-1}{2}} = (-1)^{\sum_{j=1}^{s}\frac{q_j-1}{2}}.$$

Propozicija

Ako je Q neparan prirodan broj, onda je

$$\left(\frac{-1}{Q}\right) = (-1)^{\frac{Q-1}{2}}, \quad \left(\frac{2}{Q}\right) = (-1)^{\frac{Q^2-1}{8}}.$$

Dokaz: Imamo:

$$\left(\frac{-1}{Q}\right) = \prod_{j=1}^{s}\left(\frac{-1}{q_j}\right) = \prod_{j=1}^{s}(-1)^{\frac{q_j-1}{2}} = (-1)^{\sum_{j=1}^{s}\frac{q_j-1}{2}}.$$

Ako su a i b neparni, onda je

$$\frac{ab-1}{2} - \left(\frac{a-1}{2} + \frac{b-1}{2}\right) = \frac{(a-1)(b-1)}{2} \equiv 0 \pmod 2,$$

Propozicija

Ako je Q neparan prirodan broj, onda je

$$\left(\frac{-1}{Q}\right) = (-1)^{\frac{Q-1}{2}}, \quad \left(\frac{2}{Q}\right) = (-1)^{\frac{Q^2-1}{8}}.$$

Dokaz: Imamo:

$$\left(\frac{-1}{Q}\right) = \prod_{j=1}^{s}\left(\frac{-1}{q_j}\right) = \prod_{j=1}^{s}(-1)^{\frac{q_j-1}{2}} = (-1)^{\sum_{j=1}^{s}\frac{q_j-1}{2}}.$$

Ako su a i b neparni, onda je

$$\frac{ab-1}{2} - \left(\frac{a-1}{2} + \frac{b-1}{2}\right) = \frac{(a-1)(b-1)}{2} \equiv 0 \pmod 2,$$

pa je

$$\frac{ab-1}{2} \equiv \frac{a-1}{2} + \frac{b-1}{2} \pmod 2.$$

pa je

$$\frac{ab-1}{2} \equiv \frac{a-1}{2} + \frac{b-1}{2} \pmod 2.$$

Koristeći ovu relaciju, lako se indukcijom dokaže da vrijedi

$$\sum_{j=1}^{s} \frac{q_j - 1}{2} \equiv \frac{1}{2}\Big(\prod_{j=1}^{s} q_j - 1\Big) \equiv \frac{Q-1}{2} \pmod 2, \qquad (1)$$

pa je $(\frac{-1}{Q}) = (-1)^{\frac{Q-1}{2}}$.

pa je

$$\frac{ab-1}{2} \equiv \frac{a-1}{2} + \frac{b-1}{2} \pmod 2.$$

Koristeći ovu relaciju, lako se indukcijom dokaže da vrijedi

$$\sum_{j=1}^{s} \frac{q_j - 1}{2} \equiv \frac{1}{2}\Big(\prod_{j=1}^{s} q_j - 1\Big) \equiv \frac{Q-1}{2} \pmod 2, \qquad (1)$$

pa je $(\frac{-1}{Q}) = (-1)^{\frac{Q-1}{2}}$.

Slično, ako su a i b neparni, onda je

$$\frac{a^2b^2-1}{8} - \Big(\frac{a^2-1}{8} + \frac{b^2-1}{8}\Big) = \frac{(a^2-1)(b^2-1)}{8} \equiv 0 \pmod 2,$$

pa je

$$\frac{ab-1}{2} \equiv \frac{a-1}{2} + \frac{b-1}{2} \pmod 2.$$

Koristeći ovu relaciju, lako se indukcijom dokaže da vrijedi

$$\sum_{j=1}^{s} \frac{q_j - 1}{2} \equiv \frac{1}{2}\Big(\prod_{j=1}^{s} q_j - 1\Big) \equiv \frac{Q-1}{2} \pmod 2, \qquad (1)$$

pa je $\left(\frac{-1}{Q}\right) = (-1)^{\frac{Q-1}{2}}$.

Slično, ako su a i b neparni, onda je

$$\frac{a^2b^2-1}{8} - \Big(\frac{a^2-1}{8} + \frac{b^2-1}{8}\Big) = \frac{(a^2-1)(b^2-1)}{8} \equiv 0 \pmod 2,$$

pa je

$$\left(\frac{2}{Q}\right) = \prod_{j=1}^{s}\left(\frac{2}{q_j}\right) = (-1)^{\sum_{j=1}^{s} \frac{q_j^2-1}{8}} = (-1)^{\frac{1}{8}\left(\prod_{j=1}^{s} q_j^2 - 1\right)} = (-1)^{\frac{Q^2-1}{8}}.$$

Propozicija

Ako su P i Q neparni prirodni brojevi i $(P,Q)=1$, onda je

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right)=(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}.$$

Dokaz: Neka je $P=\prod_{i=1}^{r}p_i$, $Q=\prod_{j=1}^{s}q_j$. Tada je

$$\begin{aligned}\left(\frac{P}{Q}\right) &= \prod_{j=1}^{s}\left(\frac{P}{q_j}\right)=\prod_{j=1}^{s}\prod_{i=1}^{r}\left(\frac{p_i}{q_j}\right)=\prod_{j=1}^{s}\prod_{i=1}^{r}\left(\frac{q_j}{p_i}\right)(-1)^{\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}}\\ &= \left(\frac{Q}{P}\right)(-1)^{\sum_{j=1}^{s}\sum_{i=1}^{r}\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}}.\end{aligned}$$

Ali, prema (1) je

$$\sum_{j=1}^{s}\sum_{i=1}^{r}\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}=\Big(\sum_{i=1}^{r}\frac{p_i-1}{2}\Big)\Big(\sum_{j=1}^{s}\frac{q_j-1}{2}\Big)$$

$$\equiv\frac{P-1}{2}\cdot\frac{Q-1}{2}\pmod 2,$$

pa je $\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right)=(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}$. □

Zadatak

Izračunati: $\left(\frac{-31}{89}\right)$, $\left(\frac{53}{61}\right)$, $\left(\frac{7}{101}\right)$.

Zadatak

Izračunati: $\left(\frac{-21}{91}\right),\ \left(\frac{-35}{221}\right).$

Kvadratne forme

Promatrat ćemo tzv. *binarne kvadratne forme*

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

tj. homogene polinome od dvije varijable drugog stupnja s cjelobrojnim koeficijentima.

Kvadratne forme

Promatrat ćemo tzv. *binarne kvadratne forme*

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

tj. homogene polinome od dvije varijable drugog stupnja s cjelobrojnim koeficijentima.

Diskriminanta od f je broj $d = b^2 - 4ac$.

Kvadratne forme

Promatrat ćemo tzv. *binarne kvadratne forme*

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

tj. homogene polinome od dvije varijable drugog stupnja s cjelobrojnim koeficijentima.

Diskriminanta od f je broj $d = b^2 - 4ac$.

Očito je $d \equiv 0 \pmod 4$ ako je b paran i $d \equiv 1 \pmod 4$ ako je b neparan.

Kvadratne forme

Promatrat ćemo tzv. *binarne kvadratne forme*

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

tj. homogene polinome od dvije varijable drugog stupnja s cjelobrojnim koeficijentima.

Diskriminanta od f je broj $d = b^2 - 4ac$.

Očito je $d \equiv 0 \pmod 4$ ako je b paran i $d \equiv 1 \pmod 4$ ako je b neparan.

Forme $x^2 - \frac{1}{4}dy^2$ ako je $d \equiv 0 \pmod 4$, te $x^2 + xy + \frac{1}{4}(1-d)y^2$ ako je $d \equiv 1 \pmod 4$, imaju diskriminantu jednaku d i zovemo ih *glavne forme* s diskriminantom d. Dakle za svaki $d \equiv 0, 1 \pmod 4$ postoji kvadratna forma s tom diskriminantom.

Kvadratne forme

Promatrat ćemo tzv. *binarne kvadratne forme*

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

tj. homogene polinome od dvije varijable drugog stupnja s cjelobrojnim koeficijentima.

Diskriminanta od f je broj $d = b^2 - 4ac$.

Očito je $d \equiv 0 \pmod 4$ ako je b paran i $d \equiv 1 \pmod 4$ ako je b neparan.

Forme $x^2 - \frac{1}{4}dy^2$ ako je $d \equiv 0 \pmod 4$, te $x^2 + xy + \frac{1}{4}(1-d)y^2$ ako je $d \equiv 1 \pmod 4$, imaju diskriminantu jednaku d i zovemo ih *glavne forme* s diskriminantom d. Dakle za svaki $d \equiv 0, 1 \pmod 4$ postoji kvadratna forma s tom diskriminantom.

Imamo:

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

pa ako je $d < 0$, onda f poprima ili samo pozitivne ili samo negativne vrijednosti, ovisno o predzanku od a.

U skladu s tim, kažemo da je f *pozitivno*, odnosno *negativno definitna*. Ako je $d > 0$, onda f poprima i pozitivne i negativne vrijednosti, pa se zove *indefinitna*. Ako je $d = 0$, onda kažemo da je f *poludefinitna*.

U skladu s tim, kažemo da je f *pozitivno*, odnosno *negativno definitna*. Ako je $d > 0$, onda f poprima i pozitivne i negativne vrijednosti, pa se zove *indefinitna*. Ako je $d = 0$, onda kažemo da je f *poludefinitna*.

Definicija

Reći ćemo da su dvije kvadratne forme f i g ekvivalentne ako se jedna može transformirati u drugu pomoću cjelobrojnih unimodularnih transformacija, tj. supstitucija oblika

$$x = px' + qy', \qquad y = rx' + sy',$$

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

Matrično f možemo zapisati kao $X^\tau F X$, gdje je

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

a supstituciju sa $X = UX'$, gdje je

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

Uvjet unimodularnosti je tada $\det U = 1$. Pritom f prelazi u $X'^\tau G X'$, gdje je $G = U^\tau F U$.

Matrično f možemo zapisati kao $X^\tau F X$, gdje je

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

a supstituciju sa $X = UX'$, gdje je

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

Uvjet unimodularnosti je tada $\det U = 1$. Pritom f prelazi u ${X'}^\tau G X'$, gdje je $G = U^\tau F U$.

Primjetimo da je diskriminanta od f jednaka $-4 \det F$.

Označimo s Γ (često se koristi i oznaka $\mathrm{SL}_2(\mathbb{Z})$) skup svih matrica oblika $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$, $p, q, r, s, \in \mathbb{Z}$, $ps - qr = 1$.

Označimo s Γ (često se koristi i oznaka $\mathrm{SL}_2(\mathbb{Z})$) skup svih matrica oblika $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$, $p, q, r, s, \in \mathbb{Z}$, $ps - qr = 1$.

Tada Γ čini grupu s obzirom na množenje matrica. Zaista, neka su $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $B = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \Gamma$. Tada je

$$AB^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} s & -q \\ -r & p \end{pmatrix} = \begin{pmatrix} as - br & -aq + bp \\ cs - dr & -cq + dp \end{pmatrix}$$

i

$$\det(AB^{-1}) = \det A \cdot (\det B)^{-1} = 1,$$

pa je $AB^{-1} \in \Gamma$. Elemente grupe Γ zovemo *unimodularne matrice*.

Propozicija

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

1. $f \sim f$,

Propozicija

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

1. $f \sim f$,
2. $f \sim g \Rightarrow g \sim f$,

Propozicija

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

1. $f \sim f$,
2. $f \sim g \Rightarrow g \sim f$,
3. $f \sim g,\ g \sim h \Rightarrow f \sim h$.

Drugim riječima, $\sim$ je relacija ekvivalencije.

Propozicija

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

1. $f \sim f$,
2. $f \sim g \Rightarrow g \sim f$,
3. $f \sim g,\ g \sim h \Rightarrow f \sim h$.

Drugim riječima, $\sim$ je relacija ekvivalencije.

Dokaz: 1) Očito je $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \Gamma$.

Propozicija

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

1. $f \sim f$,
2. $f \sim g \Rightarrow g \sim f$,
3. $f \sim g,\ g \sim h \Rightarrow f \sim h$.

Drugim riječima, $\sim$ je relacija ekvivalencije.

Dokaz: 1) Očito je $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \Gamma$.

2) Ako je $f \sim g$, onda postoji $U \in \Gamma$ tako da je $G = U^\tau F U$. Odavde je $F = (U^{-1})^\tau G U^{-1}$. No, Γ je grupa, pa je $U^{-1} \in \Gamma$, što znači da je $g \sim f$.

Propozicija

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

1. $f \sim f$,
2. $f \sim g \Rightarrow g \sim f$,
3. $f \sim g,\ g \sim h \Rightarrow f \sim h$.

Drugim riječima, $\sim$ je relacija ekvivalencije.

Dokaz: 1) Očito je $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \Gamma$.

2) Ako je $f \sim g$, onda postoji $U \in \Gamma$ tako da je $G = U^\tau F U$. Odavde je $F = (U^{-1})^\tau G U^{-1}$. No, Γ je grupa, pa je $U^{-1} \in \Gamma$, što znači da je $g \sim f$.

3) Ako je $f \sim g$ i $g \sim h$, onda je $G = U^\tau F U$, $H = V^\tau G V$ za neke $U, V \in \Gamma$. Odavde je $H = (UV)^\tau F(UV)$, a budući da je $UV \in \Gamma$, slijedi da je je $f \sim h$. □

Zadatak

Odredite jesu li kvadratne forme $x^2 + 3y^2$ *i* $3x^2 + y^2$ *ekvivalentne.*

Zadatak

Odredite jesu li kvadratne forme $x^2 + 3y^2$ *i* $x^2 - 3y^2$ *ekvivalentne.*

Definicija

Kažemo da kvadratna forma reprezentira cijeli broj n ako postoje $x_0, y_0 \in \mathbb{Z}$ takvi da je $f(x_0, y_0) = n$. Ako je pritom $(x_0, y_0) = 1$, onda kažemo da reprezentacija prava; inače je neprava.

Definicija

Kažemo da kvadratna forma reprezentira cijeli broj n ako postoje $x_0, y_0 \in \mathbb{Z}$ takvi da je $f(x_0, y_0) = n$. Ako je pritom $(x_0, y_0) = 1$, onda kažemo da reprezentacija prava; inače je neprava.

Propozicija

Neka su f i g ekvivalentne kvadratne forme, te $n \in \mathbb{Z}$. Tada:
1) f reprezentira n ako i samo ako g reprezentira n,

Definicija

Kažemo da kvadratna forma reprezentira cijeli broj n ako postoje $x_0, y_0 \in \mathbb{Z}$ takvi da je $f(x_0, y_0) = n$. Ako je pritom $(x_0, y_0) = 1$, onda kažemo da reprezentacija prava; inače je neprava.

Propozicija

Neka su f i g ekvivalentne kvadratne forme, te $n \in \mathbb{Z}$. Tada:
1) f reprezentira n ako i samo ako g reprezentira n,
2) f pravo reprezentira n ako i samo ako g pravo reprezentira n,

Definicija

Kažemo da kvadratna forma reprezentira cijeli broj n ako postoje $x_0, y_0 \in \mathbb{Z}$ takvi da je $f(x_0, y_0) = n$. Ako je pritom $(x_0, y_0) = 1$, onda kažemo da reprezentacija prava; inače je neprava.

Propozicija

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

1) f reprezentira n ako i samo ako g reprezentira n,

2) f pravo reprezentira n ako i samo ako g pravo reprezentira n,

3) diskriminante od f i g su jednake.

Definicija

Kažemo da kvadratna forma reprezentira cijeli broj n ako postoje $x_0, y_0 \in \mathbb{Z}$ takvi da je $f(x_0, y_0) = n$. Ako je pritom $(x_0, y_0) = 1$, onda kažemo da reprezentacija prava; inače je neprava.

Propozicija

Neka su f i g ekvivalentne kvadratne forme, te $n \in \mathbb{Z}$. Tada:
1) f reprezentira n ako i samo ako g reprezentira n,
2) f pravo reprezentira n ako i samo ako g pravo reprezentira n,
3) diskriminante od f i g su jednake.

Dokaz: 1) Zbog simetričnosti relacije ekvivalencije, dovoljno je provjeriti jednu implikaciju. Neka je $G = U^\tau F U$. Ako je $n = X_0^\tau F X_0$, stavimo $X_1 = U^{-1} X_0$, pa imamo

$$X_1^\tau G X_1 = X_1^\tau U^\tau F U X_1 = X_0^\tau (U^\tau)^{-1} (U)^\tau F U U^{-1} X_0 = X_0^\tau F X_0 = n.$$

2) Neka je $X_0 = \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$, $X_1 = \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}$, gdje $f(x_0, y_0) = n$ i $g(x_1, y_1) = n$.

2) Neka je $X_0 = \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$, $X_1 = \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}$, gdje $f(x_0, y_0) = n$ i $g(x_1, y_1) = n$.

Pretpostavimo da je $(x_0, y_0) = 1$. Iz $x_0 = px_1 + qy_1$, $y_0 = rx_1 + sy_1$ slijedi da je $(x_1, y_1) | (x_0, y_0)$, pa je $(x_1, y_1) = 1$.

2) Neka je $X_0 = \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$, $X_1 = \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}$, gdje $f(x_0, y_0) = n$ i $g(x_1, y_1) = n$.

Pretpostavimo da je $(x_0, y_0) = 1$. Iz $x_0 = px_1 + qy_1$, $y_0 = rx_1 + sy_1$ slijedi da je $(x_1, y_1) | (x_0, y_0)$, pa je $(x_1, y_1) = 1$.

3) Označimo sa d_0 i d_1 diskriminante od f, odnosno g. Tada je $d_0 = -4 \det F$, $d_1 = -4 \det G$, a $\det G = \det U^\tau \det F \det U = \det F$, pa je $d_0 = d_1$. □