Teorija brojeva

Filip Najman

7. predavanje

10.5.2021.

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 $X^{\tau}FX$, 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 $X'^{\tau}GX'$, gdje je $G = U^{\tau}FU$.

Matrično f možemo zapisati kao $X^\tau FX$, 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 $X'^\tau GX'$, gdje je $G = U^\tau FU$.

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 je $UV \in \Gamma$, slijedi da je je $f \sim h$. $\square$

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

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

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 $G = U^\tau FU$. Ako je $n = X_0^\tau FX_0$, stavimo $X_1 = U^{-1}X_0$, pa imamo

$$X_1^\tau GX_1 = X_1^\tau (U)^\tau FUX_1 = X_0^\tau (U^\tau)^{-1}(U)^\tau FUU^{-1}X_0 = X_0^\tau FX_0 = n.$$

2) Neka je $X_0 = \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$, $X_1 = \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}$.

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 $X_0 = \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$, $X_1 = \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}$.

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 $d_0 = d_1$. $\square$

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 $d_0 = d_1$. $\square$

Sada ćemo opisati redukciju pozitivno definitnih kvadratnih formi. Dakle, pretpostavljamo da je $d < 0$ i $a > 0$, pa je i $c > 0$ (inače $d = b^2 - 4ac$ ne može biti negativno).

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 $d_0 = d_1$. $\square$

Sada ćemo opisati redukciju pozitivno definitnih kvadratnih formi. Dakle, pretpostavljamo da je $d < 0$ i $a > 0$, pa je i $c > 0$ (inače $d = b^2 - 4ac$ ne može biti negativno).

Definicija

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

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 $d_0 = d_1$. $\square$

Sada ćemo opisati redukciju pozitivno definitnih kvadratnih formi. Dakle, pretpostavljamo da je $d < 0$ i $a > 0$, pa je i $c > 0$ (inače $d = b^2 - 4ac$ ne može biti negativno).

Definicija

Reći ćemo da je pozitivno definitna 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

Svaka pozitivno definitna kvadratna forma je ekvivalentna nekoj reduciranoj formi.

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 $d_0 = d_1$. □

Sada ćemo opisati redukciju pozitivno definitnih kvadratnih formi. Dakle, pretpostavljamo da je $d < 0$ i $a > 0$, pa je i $c > 0$ (inače $d = b^2 - 4ac$ ne može biti negativno).

Definicija

Reći ćemo da je pozitivno definitna 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

Svaka pozitivno definitna kvadratna forma je ekvivalentna nekoj reduciranoj formi.

Dokaz: Promotrimo supstitucije čije su matrice

$$U = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{i} \quad V = \begin{pmatrix} 1 & \pm 1 \\ 0 & 1 \end{pmatrix}.$$

Pokažimo da korištenjem konačno mnogo ovih transformacija možemo postići da je

$$|b| \leq a \leq c.$$

Zaista, $U^\tau FU = \begin{pmatrix} c & -b/2 \\ -b/2 & a \end{pmatrix}$, što znači da U zamjenjuje a i c, pa ako smo u F imali $a > c$, onda ćemo u $U^\tau FU$ imati $a < c$. Nadalje

$$V^\tau FV = \begin{pmatrix} a & \pm a + \frac{b}{2} \\ \pm a + \frac{b}{2} & a \pm b + c \end{pmatrix},$$

što znači da V zamjenjuje b s $b \pm 2a$, dok a ostavlja nepromjenjenim.

Pokažimo da korištenjem konačno mnogo ovih transformacija možemo postići da je

$$|b| \leq a \leq c.$$

Zaista, $U^\tau F U = \begin{pmatrix} c & -b/2 \\ -b/2 & a \end{pmatrix}$, što znači da U zamjenjuje a i c, pa ako smo u F imali $a > c$, onda ćemo u $U^\tau F U$ imati $a < c$.
Nadalje

$$V^\tau F V = \begin{pmatrix} a & \pm a + \frac{b}{2} \\ \pm a + \frac{b}{2} & a \pm b + c \end{pmatrix},$$

što znači da V zamjenjuje b s $b \pm 2a$, dok a ostavlja nepromjenjenim.

Stoga koristeći ovu transformaciju konačno mnogo puta možemo postići da je $|b| \leq a$. Ovaj proces mora završiti budući svaka primjena prve transformacije smanjuje vrijednost od a.

Pokažimo da korištenjem konačno mnogo ovih transformacija možemo postići da je

$$|b| \leq a \leq c.$$

Zaista, $U^\tau FU = \begin{pmatrix} c & -b/2 \\ -b/2 & a \end{pmatrix}$, što znači da U zamjenjuje a i c, pa ako smo u F imali $a > c$, onda ćemo u $U^\tau FU$ imati $a < c$. Nadalje

$$V^\tau FV = \begin{pmatrix} a & \pm a + \frac{b}{2} \\ \pm a + \frac{b}{2} & a \pm b + c \end{pmatrix},$$

što znači da V zamjenjuje b s $b \pm 2a$, dok a ostavlja nepromjenjenim.

Stoga koristeći ovu transformaciju konačno mnogo puta možemo postići da je $|b| \leq a$. Ovaj proces mora završiti budući svaka primjena prve transformacije smanjuje vrijednost od a.

Ako je sada $b = -a$, onda primjenom supstitucije s matricom V možemo postići da je $b = a$, uz nepromjenjeni c. Ako je $a = c$, onda primjenom supstitucije s matricom U možemo postići da je $b \geq 0$.

Teorem

Postoji samo konačno mnogo reduciranih formi s danom diskriminantom d.

Dokaz: Ako je f reducirana, onda je $-d = 4ac - b^2 \geq 3ac$, pa su i a i c i $|b|$ manji od $\frac{1}{3}|d|$.

Teorem

Postoji samo konačno mnogo reduciranih formi s danom diskriminantom d.

Dokaz: Ako je f reducirana, onda je $-d = 4ac - b^2 \geq 3ac$, pa su i a i c i $|b|$ manji od $\frac{1}{3}|d|$.

Dakle, postoji konačno mnogo mogućnosti za a, b, c za fiksni d.

$\square$

Definicija

Broj reduciranih formi s diskriminantom d zove se broj klasa od d i označava se s $h(d)$.

Teorem

Postoji samo konačno mnogo reduciranih formi s danom diskriminantom d.

Dokaz: Ako je f reducirana, onda je $-d = 4ac - b^2 \geq 3ac$, pa su i a i c i $|b|$ manji od $\frac{1}{3}|d|$.

Dakle, postoji konačno mnogo mogućnosti za a, b, c za fiksni d.

$\square$

Definicija

Broj reduciranih formi s diskriminantom d zove se broj klasa od d i označava se s $h(d)$.

Primjer

Izračunajmo $h(-4)$.

Teorem

Postoji samo konačno mnogo reduciranih formi s danom diskriminantom d.

Dokaz: Ako je f reducirana, onda je $-d = 4ac - b^2 \geq 3ac$, pa su i a i c i $|b|$ manji od $\frac{1}{3}|d|$.

Dakle, postoji konačno mnogo mogućnosti za a, b, c za fiksni d.

$\square$

Definicija

Broj reduciranih formi s diskriminantom d zove se broj klasa od d i označava se s $h(d)$.

Primjer

Izračunajmo $h(-4)$.

Rješenje: Iz $3ac \leq 4$ slijedi $a = c = 1$, pa je $b = 0$. Dakle, $h(-4) = 1$.

$\diamondsuit$

Zadatak

Koja je najmanja moguća apsolutna vrijednost diskriminante pozitivno definitne kvadratne forme?

Vrijedi da je $h(d) = 1$ za samo 9 negativnih cijelih brojeva: $d = -3, -4, -7, -8, -11, -19, -43, -67, -163$. Nadalje vrijedi da je $\lim\limits_{d \to -\infty} h(d) = \infty$.

Vrijedi da je $h(d) = 1$ za samo 9 negativnih cijelih brojeva: $d = -3, -4, -7, -8, -11, -19, -43, -67, -163$. Nadalje vrijedi da je $\lim_{d \to -\infty} h(d) = \infty$.

Sljedeći teorem pokazuje da je $h(d)$ upravo broj neekvivalentnih binarnih kvadratnih formi s diskriminatnom d. Napomenimo da analogna tvrdnja za $d > 0$ ne vrijedi.

Teorem

Ako su f i f' dvije ekvivalentne reducirane forme, onda je $f = f'$.

Dokaz: Ako su $x, y \in \mathbb{Z} \setminus \{0\}$ i $|x| \geq |y|$, onda je

$$f(x, y) = ax^2 + bxy + cy^2 \geq |x|(a|x| - |by|) + c|y|^2$$
$$\geq |x|^2(a - |b|) + c|y|^2 \geq a - |b| + c.$$

Dokaz: Ako su $x, y \in \mathbb{Z} \setminus \{0\}$ i $|x| \geq |y|$, onda je

$$f(x,y) = ax^2 + bxy + cy^2 \geq |x|(a|x| - |by|) + c|y|^2$$
$$\geq |x|^2(a - |b|) + c|y|^2 \geq a - |b| + c.$$

Na isti način se provjerava da ako je $|y| \geq |x|$, onda je također $f(x,y) \geq a - |b| + c$.

Dokaz: Ako su $x, y \in \mathbb{Z} \setminus \{0\}$ i $|x| \geq |y|$, onda je

$$f(x, y) = ax^2 + bxy + cy^2 \geq |x|(a|x| - |by|) + c|y|^2$$
$$\geq |x|^2(a - |b|) + c|y|^2 \geq a - |b| + c.$$

Na isti način se provjerava da ako je $|y| \geq |x|$, onda je također $f(x, y) \geq a - |b| + c$.

Dakle, tri najmanje vrijednosti koje može poprimiti $f(x, y)$ su a, c i $a - |b| + c$ i to upravo u tom redosljedu, a poprimaju se za $(x, y) = (1, 0), (0, 1)$, te $(1, 1)$ ili $(1, -1)$.

Dokaz: Ako su $x, y \in \mathbb{Z} \setminus \{0\}$ i $|x| \geq |y|$, onda je

$$f(x,y) = ax^2 + bxy + cy^2 \geq |x|(a|x| - |by|) + c|y|^2$$
$$\geq |x|^2(a - |b|) + c|y|^2 \geq a - |b| + c.$$

Na isti način se provjerava da ako je $|y| \geq |x|$, onda je također $f(x,y) \geq a - |b| + c$.

Dakle, tri najmanje vrijednosti koje može poprimiti $f(x,y)$ su a, c i $a - |b| + c$ i to upravo u tom redosljedu, a poprimaju se za $(x,y) = (1,0), (0,1)$, te $(1,1)$ ili $(1,-1)$.

Budući da, po Propoziciji 6.2), f' poprima iste vrijednosti za $(x,y) = 1$ kao i f, te budući je f' također reducirana, zaključujemo da je $a = a'$.

Dokaz: Ako su $x, y \in \mathbb{Z} \setminus \{0\}$ i $|x| \geq |y|$, onda je

$$f(x, y) = ax^2 + bxy + cy^2 \geq |x|(a|x| - |by|) + c|y|^2$$
$$\geq |x|^2(a - |b|) + c|y|^2 \geq a - |b| + c.$$

Na isti način se provjerava da ako je $|y| \geq |x|$, onda je također $f(x, y) \geq a - |b| + c$.

Dakle, tri najmanje vrijednosti koje može poprimiti $f(x, y)$ su a, c i $a - |b| + c$ i to upravo u tom redosljedu, a poprimaju se za $(x, y) = (1, 0), (0, 1)$, te $(1, 1)$ ili $(1, -1)$.

Budući da, po Propoziciji 6.2), f' poprima iste vrijednosti za $(x, y) = 1$ kao i f, te budući je f' također reducirana, zaključujemo da je $a = a'$.

Pretpostavimo da je $a < c$. Tada je $a < c < a - |b| + c$. Ako bi bilo $a = c'$, onda bi broj a imao više reprezentacija pomoću forme f' nego pomoću forme f. Iz dokaza Propoziciji 6.1) slijedi da f i f' reprezentiraju n isti broj puta.

Dokaz: Ako su $x, y \in \mathbb{Z} \setminus \{0\}$ i $|x| \geq |y|$, onda je

$$f(x,y) = ax^2 + bxy + cy^2 \geq |x|(a|x| - |by|) + c|y|^2$$
$$\geq |x|^2(a - |b|) + c|y|^2 \geq a - |b| + c.$$

Na isti način se provjerava da ako je $|y| \geq |x|$, onda je također $f(x,y) \geq a - |b| + c$.

Dakle, tri najmanje vrijednosti koje može poprimiti $f(x,y)$ su a, c i $a - |b| + c$ i to upravo u tom redosljedu, a poprimaju se za $(x,y) = (1,0), (0,1)$, te $(1,1)$ ili $(1,-1)$.

Budući da, po Propoziciji 6.2), f' poprima iste vrijednosti za $(x,y) = 1$ kao i f, te budući je f' također reducirana, zaključujemo da je $a = a'$.

Pretpostavimo da je $a < c$. Tada je $a < c < a - |b| + c$. Ako bi bilo $a = c'$, onda bi broj a imao više reprezentacija pomoću forme f' nego pomoću forme f. Iz dokaza Propoziciji 6.1) slijedi da f i f' reprezentiraju n isti broj puta.

Dokaz: Ako su $x, y \in \mathbb{Z} \setminus \{0\}$ i $|x| \geq |y|$, onda je

$$f(x, y) = ax^2 + bxy + cy^2 \geq |x|(a|x| - |by|) + c|y|^2$$
$$\geq |x|^2(a - |b|) + c|y|^2 \geq a - |b| + c.$$

Na isti način se provjerava da ako je $|y| \geq |x|$, onda je također $f(x, y) \geq a - |b| + c$.

Dakle, tri najmanje vrijednosti koje može poprimiti $f(x, y)$ su a, c i $a - |b| + c$ i to upravo u tom redosljedu, a poprimaju se za $(x, y) = (1, 0), (0, 1)$, te $(1, 1)$ ili $(1, -1)$.

Budući da, po Propoziciji 6.2), f' poprima iste vrijednosti za $(x, y) = 1$ kao i f, te budući je f' također reducirana, zaključujemo da je $a = a'$.

Pretpostavimo da je $a < c$. Tada je $a < c < a - |b| + c$. Ako bi bilo $a = c'$, onda bi broj a imao više reprezentacija pomoću forme f' nego pomoću forme f. Iz dokaza Propoziciji 6.1) slijedi da f i f' reprezentiraju n isti broj puta.

Stoga je $a < c'$, pa je $c = c'$, pošto je to 2. najveća vrijednost reprezentirana s f, a time onda i f'.

Iz $b^2 = d + 4ac = b'^2$, dobivamo $|b| = |b'|$. Dakle, još samo treba pokazati da $b = -b'$ povlači $b = 0$.

Iz $b^2 = d + 4ac = b'^2$, dobivamo $|b| = |b'|$. Dakle, još samo treba pokazati da $b = -b'$ povlači $b = 0$.

Pretpostavimo dakle da je $b = -b'$; sada možemo zaključiti da je $-a < b < a < c$, jer kada bi bilo $a = b$, tada bi bilo $-b' = b = a$, što je u kontradikciji pretpostavkom reduciranosti.

Iz $b^2 = d + 4ac = b'^2$, dobivamo $|b| = |b'|$. Dakle, još samo treba pokazati da $b = -b'$ povlači $b = 0$.

Pretpostavimo dakle da je $b = -b'$; sada možemo zaključiti da je $-a < b < a < c$, jer kada bi bilo $a = b$, tada bi bilo $-b' = b = a$, što je u kontradikciji pretpostavkom reduciranosti.

Neka je $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$ matrica prijelaza iz f u f'. Tada je

$$a' = f'(1,0) = f(p,r), \quad b' = 2apq + b(ps + qr) + 2crs, \quad (1)$$

$$c' = f'(0,1) = f(q,s).$$

Iz $b^2 = d + 4ac = b'^2$, dobivamo $|b| = |b'|$. Dakle, još samo treba pokazati da $b = -b'$ povlači $b = 0$.

Pretpostavimo dakle da je $b = -b'$; sada možemo zaključiti da je $-a < b < a < c$, jer kada bi bilo $a = b$, tada bi bilo $-b' = b = a$, što je u kontradikciji pretpostavkom reduciranosti.

Neka je $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$ matrica prijelaza iz f u f'. Tada je

$$a' = f'(1,0) = f(p,r), \quad b' = 2apq + b(ps + qr) + 2crs, \quad (1)$$

$$c' = f'(0,1) = f(q,s).$$

Budući da je u našem slučaju $a' = a = f(p,r) = ap^2 + bpr + cr^2$, slijedi da je $p = \pm 1$ i $r = 0$.

Iz $b^2 = d + 4ac = b'^2$, dobivamo $|b| = |b'|$. Dakle, još samo treba pokazati da $b = -b'$ povlači $b = 0$.

Pretpostavimo dakle da je $b = -b'$; sada možemo zaključiti da je $-a < b < a < c$, jer kada bi bilo $a = b$, tada bi bilo $-b' = b = a$, što je u kontradikciji pretpostavkom reduciranosti.

Neka je $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$ matrica prijelaza iz f u f'. Tada je

$$a' = f'(1,0) = f(p,r), \quad b' = 2apq + b(ps + qr) + 2crs, \tag{1}$$

$$c' = f'(0,1) = f(q,s).$$

Budući da je u našem slučaju $a' = a = f(p,r) = ap^2 + bpr + cr^2$, slijedi da je $p = \pm 1$ i $r = 0$.

Sada iz $ps - qr = 1$ slijedi $s = \pm 1$, a iz $c = f(q,s)$ slijedi $q = 0$. To znači da je $b = b'$, pa je $b = 0$.

Ostaje razmotriti slučaj $a = c$.

Ostaje razmotriti slučaj $a = c$.

Tada broj a ima barem 4 reprezentacije pomoću f, pa mora imati i barem 4 reprezentacije pomoću f', a to povlači da je $c' = a = c$.

Ostaje razmotriti slučaj $a = c$.

Tada broj a ima barem 4 reprezentacije pomoću f, pa mora imati i barem 4 reprezentacije pomoću f', a to povlači da je $c' = a = c$.

Ponovo dobivamo da je $|b| = |b'|$, ali u ovom slučaju iz definicije reduciranosti imamo da je $b \geq 0$, $b' \geq 0$, pa je $b = b'$. $\square$

Teorem

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 $x^2 \equiv d \pmod{4n}$ ima rješenja.

Teorem

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 $x^2 \equiv d \pmod{4n}$ ima rješenja.

Dokaz: Pretpostavimo da gornja kongruencija ima rješenja i da je $x = b$ rješenje. Definirajmo c s $b^2 - 4nc = d$ i stavimo $a = n$.

Teorem

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 $x^2 \equiv d \pmod{4n}$ ima rješenja.

Dokaz: Pretpostavimo da gornja kongruencija ima rješenja i da je $x = b$ rješenje. Definirajmo c s $b^2 - 4nc = d$ i stavimo $a = n$.

Sada forma $f(x, y) = ax^2 + bxy + cy^2$ ima diskriminantu d i $f(1, 0) = n$, pa f pravo reprezentira broj n.

Teorem

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 $x^2 \equiv d \pmod{4n}$ ima rješenja.

Dokaz: Pretpostavimo da gornja kongruencija ima rješenja i da je $x = b$ rješenje. Definirajmo c s $b^2 - 4nc = d$ i stavimo $a = n$.

Sada forma $f(x, y) = ax^2 + bxy + cy^2$ ima diskriminantu d i $f(1, 0) = n$, pa f pravo reprezentira broj n.

Obratno, pretpostavimo da forma f ima diskriminantu d i da je $n = f(p, r)$ za neke $p, r \in \mathbb{Z}$, $(p, r) = 1$.

Teorem

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 $x^2 \equiv d \pmod{4n}$ ima rješenja.

Dokaz: Pretpostavimo da gornja kongruencija ima rješenja i da je $x = b$ rješenje. Definirajmo c s $b^2 - 4nc = d$ i stavimo $a = n$.

Sada forma $f(x, y) = ax^2 + bxy + cy^2$ ima diskriminantu d i $f(1, 0) = n$, pa f pravo reprezentira broj n.

Obratno, pretpostavimo da forma f ima diskriminantu d i da je $n = f(p, r)$ za neke $p, r \in \mathbb{Z}$, $(p, r) = 1$.

Tada postoje $q, s \in \mathbb{Z}$ takvi da je $ps - rq = 1$. Sada je f ekvivalentna s f' koja je dobivena iz f pomoću matrice prijelaza $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$ i vrijedi: $a' = f'(1, 0) = f(p, r) = n$.

Teorem

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 $x^2 \equiv d \pmod{4n}$ ima rješenja.

Dokaz: Pretpostavimo da gornja kongruencija ima rješenja i da je $x = b$ rješenje. Definirajmo c s $b^2 - 4nc = d$ i stavimo $a = n$.

Sada forma $f(x, y) = ax^2 + bxy + cy^2$ ima diskriminantu d i $f(1, 0) = n$, pa f pravo reprezentira broj n.

Obratno, pretpostavimo da forma f ima diskriminantu d i da je $n = f(p, r)$ za neke $p, r \in \mathbb{Z}$, $(p, r) = 1$.

Tada postoje $q, s \in \mathbb{Z}$ takvi da je $ps - rq = 1$. Sada je f ekvivalentna s f' koja je dobivena iz f pomoću matrice prijelaza $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$ i vrijedi: $a' = f'(1, 0) = f(p, r) = n$. Ali f i f' imaju istu diskriminantu, pa je

$$b'^2 - 4nc' = d.$$

Dakle, kongruencija $x^2 \equiv d \pmod{4n}$ ima rješenje $x = b'$. $\square$

Teorem

Prirodan broj n se može 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 prosti faktor p za koji je $p \equiv 3 \pmod 4$ javlja s parnom potencijom.

Teorem

Prirodan broj n se može 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 prosti faktor p za koji je $p \equiv 3 \pmod 4$ javlja s parnom potencijom.

Dokaz: Pretpostavimo da je $n = x^2 + y^2$, te da je n djeljiv s prostim brojem $p \equiv 3 \pmod 4$. Tada je $x^2 \equiv -y^2 \pmod p$.

Teorem

Prirodan broj n se može 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 prosti faktor p za koji je $p \equiv 3 \pmod 4$ javlja s parnom potencijom.

Dokaz: Pretpostavimo da je $n = x^2 + y^2$, te da je n djeljiv s prostim brojem $p \equiv 3 \pmod 4$. Tada je $x^2 \equiv -y^2 \pmod p$.

Ako p ne dijeli x i y, onda odavde dobivamo da je $\left(\frac{-1}{p}\right)$, što je kontradikcija.

Teorem

Prirodan broj n se može 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 prosti faktor p za koji je $p \equiv 3 \pmod 4$ javlja s parnom potencijom.

Dokaz: Pretpostavimo da je $n = x^2 + y^2$, te da je n djeljiv s prostim brojem $p \equiv 3 \pmod 4$. Tada je $x^2 \equiv -y^2 \pmod p$.

Ako p ne dijeli x i y, onda odavde dobivamo da je $\left(\frac{-1}{p}\right)$, što je kontradikcija.

Stoga p dijeli x i y, pa je n djeljiv sa p^2. Sada je $(\frac{x}{p})^2 + (\frac{y}{p})^2 = \frac{n}{p^2}$, pa indukcijom slijedi da se p u rastavu broja n javlja s parnom potencijom.

Da bi dokazali obrat, dovoljno je dokazati da ako je n kvadratno slobodan i svi neparni faktori p od n zadovoljavaju $p \equiv 1 \pmod 4$, onda se n može prikazati u obliku $x^2 + y^2$. To vidimo jer ako je $n = x^2 + y^2$, onda je $n \cdot m^2 = (xm)^2 + (ym)^2$.

Da bi dokazali obrat, dovoljno je dokazati da ako je n kvadratno slobodan i svi neparni faktori p od n zadovoljavaju $p \equiv 1 \pmod 4$, onda se n može prikazati u obliku $x^2 + y^2$. To vidimo jer ako je $n = x^2 + y^2$, onda je $n \cdot m^2 = (xm)^2 + (ym)^2$.

Promotrimo sada binarnu kvadratnu formu $f(x, y) = x^2 + y^2$. To je reducirana forma s diskriminantom -4. U Primjeru smo ranije pokazali da je $h(-4) = 1$. Stoga je to jedina reducirana forma s diskriminantom -4.

Da bi dokazali obrat, dovoljno je dokazati da ako je n kvadratno slobodan i svi neparni faktori p od n zadovoljavaju $p \equiv 1 \pmod 4$, onda se n može prikazati u obliku $x^2 + y^2$. To vidimo jer ako je $n = x^2 + y^2$, onda je $n \cdot m^2 = (xm)^2 + (ym)^2$.

Promotrimo sada binarnu kvadratnu formu $f(x, y) = x^2 + y^2$. To je reducirana forma s diskriminantom -4. U Primjeru smo ranije pokazali da je $h(-4) = 1$. Stoga je to jedina reducirana forma s diskriminantom -4.

Iz ranije dokazanog Teorema slijedi da je n pravo reprezentiran formom $x^2 + y^2$ ako i samo ako kongruencija $x^2 \equiv d = -4 \pmod{4n}$ ima rješenja.

Ova kongruencija je ekvivalentna sa $z^2 \equiv -1 \pmod{n}$. Neka je $n = p_1 p_2 \cdots p_k$. Po pretpostavci je $p_i \equiv 1 \pmod{4}$, pa kongruencija $z^2 \equiv -1 \pmod{p_i}$ ima rješenje; neka je to rješenje $z = z_i$.

Ova kongruencija je ekvivalentna sa $z^2 \equiv -1 \pmod{n}$. Neka je $n = p_1 p_2 \cdots p_k$. Po pretpostavci je $p_i \equiv 1 \pmod{4}$, pa kongruencija $z^2 \equiv -1 \pmod{p_i}$ ima rješenje; neka je to rješenje $z = z_i$.

Po Kineskom teoremu o ostacima, postoji cijeli broj z koji zadovoljava sustav

$$z \equiv z_1 \pmod{p_1}, \ldots, z \equiv z_k \pmod{p_k}.$$

Sada je $z^2 \equiv z_i^2 \equiv -1 \pmod{p_i}$ za svaki i, pa je $z^2 \equiv -1 \pmod{n}$. $\square$

Teorem

Cijeli broj n se može prikazati u obliku $x^2 - y^2$ ako i samo ako $n \not\equiv 2 \pmod 4$.

Rješenje: Pretpostavimo da je $n \equiv 2 \pmod 4$, te da je $n = x^2 - y^2 = (x - y)(x + y)$.

Teorem

Cijeli broj n se može prikazati u obliku $x^2 - y^2$ ako i samo ako $n \not\equiv 2 \pmod 4$.

Rješenje: Pretpostavimo da je $n \equiv 2 \pmod 4$, te da je $n = x^2 - y^2 = (x-y)(x+y)$.

Budući da je n paran, slijedi da je jedan od faktora $x-y$, $x+y$ paran.

Teorem

Cijeli broj n se može prikazati u obliku $x^2 - y^2$ ako i samo ako $n \not\equiv 2 \pmod 4$.

Rješenje: Pretpostavimo da je $n \equiv 2 \pmod 4$, te da je $n = x^2 - y^2 = (x-y)(x+y)$.

Budući da je n paran, slijedi da je jedan od faktora $x-y$, $x+y$ paran.

No, $x+y = (x-y) + 2y$, pa je i drugi faktor također paran.

Teorem

Cijeli broj n se može prikazati u obliku $x^2 - y^2$ ako i samo ako $n \not\equiv 2 \pmod 4$.

Rješenje: Pretpostavimo da je $n \equiv 2 \pmod 4$, te da je $n = x^2 - y^2 = (x-y)(x+y)$.

Budući da je n paran, slijedi da je jedan od faktora $x - y$, $x + y$ paran.

No, $x + y = (x - y) + 2y$, pa je i drugi faktor također paran.

To znači da je $n \equiv 0 \pmod 4$, pa smo dobili kontradikciju.

Teorem

Cijeli broj n se može prikazati u obliku $x^2 - y^2$ ako i samo ako $n \not\equiv 2 \pmod 4$.

Rješenje: Pretpostavimo da je $n \equiv 2 \pmod 4$, te da je $n = x^2 - y^2 = (x-y)(x+y)$.

Budući da je n paran, slijedi da je jedan od faktora $x-y$, $x+y$ paran.

No, $x+y = (x-y)+2y$, pa je i drugi faktor također paran.

To znači da je $n \equiv 0 \pmod 4$, pa smo dobili kontradikciju.

Neka je sada $n \not\equiv 2 \pmod 4$. Razlikujemo dva slučaja:

1) $n = 2k+1$. Tada je $n = (k+1)^2 - k^2$.

Teorem

Cijeli broj n se može prikazati u obliku $x^2 - y^2$ ako i samo ako $n \not\equiv 2 \pmod 4$.

Rješenje: Pretpostavimo da je $n \equiv 2 \pmod 4$, te da je $n = x^2 - y^2 = (x-y)(x+y)$.

Budući da je n paran, slijedi da je jedan od faktora $x-y$, $x+y$ paran.

No, $x + y = (x-y) + 2y$, pa je i drugi faktor također paran.

To znači da je $n \equiv 0 \pmod 4$, pa smo dobili kontradikciju.

Neka je sada $n \not\equiv 2 \pmod 4$. Razlikujemo dva slučaja:

1) $n = 2k+1$. Tada je $n = (k+1)^2 - k^2$.

2) $n = 4k$. Tada je $n = (k+1)^2 - (k-1)^2$. $\square$

Teorem (Teorem o četiri kvadrata (Lagrange))

Svaki prirodan
broj n može se prikazati u obliku sume kvadrata četiri cijela broja, tj. u obliku $n = x^2 + y^2 + z^2 + w^2$, $x, y, z, w \in \mathbb{Z}$.

Teorem (Teorem o četiri kvadrata (Lagrange))

Svaki prirodan
broj n može se prikazati u obliku sume kvadrata četiri cijela broja,
tj. u obliku $n = x^2 + y^2 + z^2 + w^2$, $x, y, z, w \in \mathbb{Z}$.

Dokaz: Uočimo da vrijedi identitet

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

Stoga je tvrdnju teorema dovoljno provjeriti za proste brojeve, jer ako vrijedi za njih, tada vrijedi za sve brojeve.

Teorem (Teorem o četiri kvadrata (Lagrange))

Svaki prirodan
broj n može se prikazati u obliku sume kvadrata četiri cijela broja, tj. u obliku $n = x^2 + y^2 + z^2 + w^2$, $x, y, z, w \in \mathbb{Z}$.

Dokaz: Uočimo da vrijedi identitet

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

Stoga je tvrdnju teorema dovoljno provjeriti za proste brojeve, jer ako vrijedi za njih, tada vrijedi za sve brojeve.

Jasno je da je $2 = 1^2 + 1^2 + 0^2 + 0^2$, pa pretpostavimo da je p neparan prost broj.

Promotrimo brojeve

$$0^2, 1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2. \tag{3}$$

Nikoja dva među njima nisu kongruentna modulo p, jer $x^2 \equiv a \pmod{p}$ ima najviše 2 rješenja, pa ako je x_0 rješenje, jedino drugo mora biti $-x_0$.

Promotrimo brojeve

$$0^2, 1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2. \tag{3}$$

Nikoja dva među njima nisu kongruentna modulo p, jer $x^2 \equiv a \pmod{p}$ ima najviše 2 rješenja, pa ako je x_0 rješenje, jedino drugo mora biti $-x_0$.

Isto vrijedi i za brojeve

$$-1-0^2, -1-1^2, -1-2^2, \ldots, -1-(\frac{p-1}{2})^2. \tag{4}$$

Promotrimo brojeve

$$0^2, 1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2. \tag{3}$$

Nikoja dva među njima nisu kongruentna modulo p, jer $x^2 \equiv a \pmod{p}$ ima najviše 2 rješenja, pa ako je x_0 rješenje, jedino drugo mora biti $-x_0$.

Isto vrijedi i za brojeve

$$-1-0^2, -1-1^2, -1-2^2, \ldots, -1-(\frac{p-1}{2})^2. \tag{4}$$

U (3) i (4) imamo ukupno $p+1$ brojeva. Po Dirichletovom principu, dva među njima daju isti ostatak pri dijeljenju sa p.

Promotrimo brojeve

$$0^2, 1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2. \tag{3}$$

Nikoja dva među njima nisu kongruentna modulo p, jer $x^2 \equiv a \pmod{p}$ ima najviše 2 rješenja, pa ako je x_0 rješenje, jedino drugo mora biti $-x_0$.

Isto vrijedi i za brojeve

$$-1-0^2, -1-1^2, -1-2^2, \ldots, -1-(\frac{p-1}{2})^2. \tag{4}$$

U (3) i (4) imamo ukupno $p+1$ brojeva. Po Dirichletovom principu, dva među njima daju isti ostatak pri dijeljenju sa p.

To znači da postoje cijeli brojevi x i y takvi da je $x^2 \equiv -1-y^2 \pmod{p}$ i vrijedi $x^2+y^2+1 < 1+2\cdot(\frac{p}{2})^2 < p^2$. Dakle, dobili smo da je $mp = x^2+y^2+1$ za neki cijeli broj $0 < m < p$.

Promotrimo brojeve

$$0^2, 1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2. \qquad (3)$$

Nikoja dva među njima nisu kongruentna modulo p, jer $x^2 \equiv a \pmod{p}$ ima najviše 2 rješenja, pa ako je x_0 rješenje, jedino drugo mora biti $-x_0$.

Isto vrijedi i za brojeve

$$-1-0^2, -1-1^2, -1-2^2, \ldots, -1-(\frac{p-1}{2})^2. \qquad (4)$$

U (3) i (4) imamo ukupno $p+1$ brojeva. Po Dirichletovom principu, dva među njima daju isti ostatak pri dijeljenju sa p.

To znači da postoje cijeli brojevi x i y takvi da je $x^2 \equiv -1-y^2 \pmod{p}$ i vrijedi $x^2+y^2+1 < 1+2\cdot(\frac{p}{2})^2 < p^2$. Dakle, dobili smo da je $mp = x^2+y^2+1$ za neki cijeli broj $0 < m < p$.

Neka je sada l najmanji prirodan broj takav da je $lp = x^2+y^2+z^2+w^2$ za neke $x, y, z, w \in \mathbb{Z}$. Tada je $l \leq m < p$, pošto je $mp = x^2+y^2+1^2+0^2$.

Nadalje, l je neparan. Naime, ako bi l bio paran, onda bi među brojevima x, y, z, w imali parno mnogo neparnih brojeva, pa bi mogli pretpostaviti da su brojevi $x+y$, $x-y$, $z+w$, $z-w$ parni.

Nadalje, l je neparan. Naime, ako bi l bio paran, onda bi među brojevima x, y, z, w imali parno mnogo neparnih brojeva, pa bi mogli pretpostaviti da su brojevi $x+y$, $x-y$, $z+w$, $z-w$ parni.

Ali tada bi iz

$$\frac{1}{2}lp = \left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 + \left(\frac{z+w}{2}\right)^2 + \left(\frac{z-w}{2}\right)^2$$

dobili kontradikciju s minimalnošću od l.

Nadalje, l je neparan. Naime, ako bi l bio paran, onda bi među brojevima x, y, z, w imali parno mnogo neparnih brojeva, pa bi mogli pretpostaviti da su brojevi $x+y$, $x-y$, $z+w$, $z-w$ parni.

Ali tada bi iz

$$\frac{1}{2}lp = \left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 + \left(\frac{z+w}{2}\right)^2 + \left(\frac{z-w}{2}\right)^2$$

dobili kontradikciju s minimalnošću od l.

Da bi dokazali teorem, moramo pokazati da je $l = 1$. Stoga pretpostavimo da je $l > 1$ i pokušajmo dobiti kontradikciju.

Nadalje, l je neparan. Naime, ako bi l bio paran, onda bi među brojevima x, y, z, w imali parno mnogo neparnih brojeva, pa bi mogli pretpostaviti da su brojevi $x+y$, $x-y$, $z+w$, $z-w$ parni.

Ali tada bi iz

$$\frac{1}{2}lp = \left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 + \left(\frac{z+w}{2}\right)^2 + \left(\frac{z-w}{2}\right)^2$$

dobili kontradikciju s minimalnošću od l.

Da bi dokazali teorem, moramo pokazati da je $l = 1$. Stoga pretpostavimo da je $l > 1$ i pokušajmo dobiti kontradikciju.

Neka su x', y', z', w' najmanji ostatci po apsolutnoj vrijednosti pri dijeljenju brojeva x, y, z, w s l, te neka je

$$n = x'^2 + y'^2 + z'^2 + w'^2.$$

Tada je $n \equiv 0 \pmod{l}$ i $n > 0$, jer bi inače l dijelio p.

Nadalje, l je neparan. Naime, ako bi l bio paran, onda bi među brojevima x, y, z, w imali parno mnogo neparnih brojeva, pa bi mogli pretpostaviti da su brojevi $x+y$, $x-y$, $z+w$, $z-w$ parni.

Ali tada bi iz

$$\frac{1}{2}lp = \left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 + \left(\frac{z+w}{2}\right)^2 + \left(\frac{z-w}{2}\right)^2$$

dobili kontradikciju s minimalnošću od l.

Da bi dokazali teorem, moramo pokazati da je $l = 1$. Stoga pretpostavimo da je $l > 1$ i pokušajmo dobiti kontradikciju.

Neka su x', y', z', w' najmanji ostatci po apsolutnoj vrijednosti pri dijeljenju brojeva x, y, z, w s l, te neka je

$$n = x'^2 + y'^2 + z'^2 + w'^2.$$

Tada je $n \equiv 0 \pmod{l}$ i $n > 0$, jer bi inače l dijelio p.

Nadalje, budući da je l neparan, imamo da je $n < 4 \cdot (\frac{l}{2})^2 = l^2$. Stoga je $n = kl$ za neki cijeli broj k takav da je $0 < k < l$.

Pošto se n i lp mogu zapisati kao sume 4 kvadrata, Iz

$$\begin{aligned}(kl)(lp) &= (x^2+y^2+z^2+w^2)((x')^2+(y')^2+(z')^2+(w')^2) \\ &= (xx'+yy'+zz'+ww')^2+(x'y-y'x+w'z-z'w)^2 \\ &+ (x'z-z'x+y'w-w'y)^2+(x'w-w'x+z'y-y'z)^2 \quad (5)\end{aligned}$$

slijedi da se broj $(kl)(lp)$ može prikazati kao suma kvadrata četiri cijela broja, i štoviše, svaki od tih kvadrata djeljiv je sa l^2.

Pošto se n i lp mogu zapisati kao sume 4 kvadrata, Iz

$$\begin{aligned}(kl)(lp) = (x^2+y^2+z^2+w^2)((x')^2+(y')^2+(z')^2+(w')^2) \\ = \quad (xx'+yy'+zz'+ww')^2+(x'y-y'x+w'z-z'w)^2 \\ + \quad (x'z-z'x+y'w-w'y)^2+(x'w-w'x+z'y-y'z)^2 \end{aligned} \tag{5}$$

slijedi da se broj $(kl)(lp)$ može prikazati kao suma kvadrata četiri cijela broja, i štoviše, svaki od tih kvadrata djeljiv je sa l^2.

Odavde dijeljenjem s l^2 slijedi da se broj kp može prikazati kao suma četiri kvadrata, no to je u kontradikciji s minimalnošću od l. $\square$

Metoda koju smo upotrijebili u posljednjem dijelu dokaza prethodnog Teorema naziva se *Fermatova metoda beskonačnog spusta*.