Kvadratne forme

Vomš, Martina

Sveučilište J. J. Strossmayera u Osijeku
Fakultet primijenjene matematike i informatike
Sveučilišni prijediplomski studij Matematika

Martina Vomš

Kvadratne forme

Završni rad

Osijek, 2023.

Sveučilište J. J. Strossmayera u Osijeku
Fakultet primijenjene matematike i informatike
Sveučilišni prijediplomski studij Matematika

Martina Vomš

Kvadratne forme

Završni rad

Voditelj: izv. prof. dr. sc. Mirela Jukić Bokun

Osijek, 2023.

Sažetak:

Kvadratna forma je homogeni polinom drugog stupnja od n varijabli, gdje je $n \in \mathbb{N}$. U ovom radu bavit ćemo se kvadratnim formama za koje je $n = 2$ i $n = 3$, tj. binarnim i ternarnim kvadratnim formama. Najprije ćemo uvesti pojam kvadratnih formi te ćemo se zatim baviti binarnim kvadratnim formama, gdje ćemo nešto više reći o ekvivalentnim i reduciranim kvadratnim formama. Dobivene rezultate primjenit ćemo na nekoliko primjera, kao i na sume dva i četiri kvadrata. Na kraju ćemo se baviti ternarnim kvadratnim formama, tj. njihovim svojstvima i primjenama na sume triju kvadrata.

Ključne riječi: Kvadratna forma, binarna kvadratna forma, ekvivalentne kvadratne forme, reducirana kvadratna forma, ternarna kvadratna forma, sume kvadrata

Quadratic forms

Abstract:

The quadratic form is homogeneous polynomial of the second degree of n variables, where $n \in \mathbb{Z}$. In this paper we will deal with quadratic forms for which $n = 2$ and $n = 3$, i.e. binary and ternary quadratic forms. First, we will introduce the concept of quadratic forms, and then we will deal with binary quadratic forms, where we will say something more about equivalent and reduced quadratic forms. We will apply the obtained results to several examples, as well to sums of two and four squares. In the end, we will deal with ternary quadratic forms, i.e. their properties and applications to sums of three squares.

Key words: Quadratic form, binary quadratic form, equivalent quadratic forms, reduced quadratic form, ternary quadratic form, sum of squares

Sadržaj

Uvod

Kvadratna forma je homogeni polinom drugog stupnja od n varijabli gdje je n prirodan broj. S obzirom na broj varijabli govorimo o, primjerice, unarnim, binarnim ili ternarnim formama koje redom imaju jednu, dvije ili tri varijable. U ovom radu najviše ćemo se baviti binarnim i ternarnim kvadratnim formama s cjelobrojnim koeficijentima.

Matematičari već stoljećima proučavaju kvadratne forme s cjelobrojnim koeficijentima, naročito se bave problemom koji glasi: „Može li vrijednost određene kvadratne forme s cjelobrojnim koeficijentima biti cijeli broj?“. Primjeri takvog problema su 'Fermatov teorem u sumi dva kvadrata' i 'Pitagorine trojke'. Brahmagupta, indijski matematičar, proučavao je i pronašao metodu za rješavanje jednadžbi oblika $x^2 - ny^2 = c$ još 628. godine. Jednadžbe takvog oblika danas se nazivaju pellovskim jednadžbama. Tim problemom bavili su se i europski matematičari Euler, Lagrange i Brouncker. Razvoj opće teorije kvadratnih formi pokrenut je 1773. godine. Prvu sustavnu obradu kvadratnih formi napravio je Legendre. Binarnim kvadratnim formama s cjelobrojnim koeficijentima bavio se i Gauss koji je 1801. godine svoja postignuća objavio u „Disquisitiones Arithmeticae“. Gauss je svojim postignućima znatno utjecao na razvoj aritmetičke teorije kvadratnih formi u više od dvije varijable. U teoriji brojeva, kvadratne forme oblika $x^2 + y^2 + 10z^2, x, y, z \in \mathbb{Z}$, poznatije su kao Ramanujanove ternarne kvadratne forme. Ramanujan je zaključio da se neki cijeli brojevi ne mogu prikazati u obliku $ax^2 + by^2 + cz^2, a, b, c \in \mathbb{R}$.

U prvom poglavlju ćemo općenito uvesti kvadratne forme, a zatim ćemo se u drugom poglavlju bazirati na binarne kvadratne forme. Saznat ćemo nešto više o definitnosti binarnih kvadratnih formi, a zatim ćemo nešto više reći i o ekvivalentnosti kvadratnih formi. Dotaknut ćemo se i reduciranih kvadratnih formi te pojmova i tvrdnji vezanih uz njih. U potpoglavlju Primjene, riješit ćemo zanimljive primjere vezane uz binarne kvadratne forme. Na kraju drugog poglavlja bavimo se teoremom o sumi dvaju kvadrata i Lagrangeovim teoremom o četiri kvadrata. U trećem poglavlju kratko ćemo se osvrnuti i na ternarne kvadratne forme, gdje ćemo se bazirati na sume triju kvadrata.

1. Kvadratne forme

Kao što smo spomenuli u Uvodu, u ovom radu ćemo se baviti kvadratnim formama s cjelobrojnim koeficijentima, tj. kvadratnim formama oblika:

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij} x_i x_j, \quad a_{ij} \in \mathbb{Z}, i, j \in \{1, 2, \ldots, n\},$$

te ćemo posebnu pažnju posvetiti kvadratnim formama za koje je $n = 2$, tj. binarnim kvadratnim formama, te kvadratnim formama za koje je $n = 3$, tj. ternarnim kvadratnim formama.

Primjer 1.1. *$f(x, y) = 5x^2 + 4xy - 3y^2$ je primjer binarne kvadratne forme.*

Primjer 1.2. *$f(x, y, z) = 3x^2 - 7y^2 + 4z^2 + 2xy - 8xz - 6yz$ je primjer ternarne kvadratne forme.*

Definitnost kvadratne forme je svojstvo koje se koristi u proučavanju kvadratnih formi pa ga navodimo u nastavku.

Definicija 1.1. *Za kvadratnu formu f kažemo da je:*

- *pozitivno definitna ako je $f(x_1, \ldots, x_n) > 0$, za sve $(x_1, \ldots, x_n) \neq (0, 0, \ldots, 0)$,*
- *negativno definitna ako je $f(x_1, \ldots, x_n) < 0$, za sve $(x_1, \ldots, x_n) \neq (0, 0, \ldots, 0)$,*
- *indefinitna ako postoje $x_1', x_2', \ldots, x_n'$, $\quad (x_1', x_2', \ldots, x_n') \neq (0, 0, \ldots, 0)$, sa svojstvom $f(x_1, \ldots, x_n) > 0$ i $f(x_1', x_2', \ldots, x_n') < 0$,*
- *poludefinitna ako je $f(x_1, \ldots, x_n) \geq 0$ ili $f(x_1, \ldots, x_n) \leq 0$, za sve $(x_1, \ldots, x_n)$.*

2. Binarne kvadratne forme

Neka je dana binarna kvadratna forma:

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

Diskriminanta od f je broj $d = b^2 - 4ac$. Ako je b paran broj, tj. broj oblika $b = 2k, k \in \mathbb{Z}$, tada je $b^2 = 4k^2$ te je $d \equiv 0 \pmod 4$. Ako je b neparan broj, odnosno oblika $b = 2k+1, k \in \mathbb{Z}$, onda je $b^2 = 4k^2 + 4k + 1$ pa je $d \equiv 1 \pmod 4$. Glavne forme s diskriminantom d su 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 $d \equiv 1 \pmod 4$, koje imaju diskriminantu d.

Iz (1) slijedi

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

Koristeći ovaj izraz možemo donijeti zaključke o definitnosti kvadratne forme f prema Definiciji 1.1. Ako je $d < 0$ i $a > 0$, funkcija f poprima samo pozitivne vrijednosti za $(x,y) \neq (0,0)$ pa je f pozitivno definitna kvadratna forma. Ako je $d < 0$ i $a < 0$, onda f poprima samo negativne vrijednosti za sve $(x,y) \neq (0,0)$ pa je f negativno definitna. Ako je $d > 0$, f poprima i pozitivne i negativne vrijednosti pa se zove indefinitna, dok je za $d = 0$, f poludefinitna kvadratna forma.

Navest ćemo neke primjere takvih kvadratnih formi:

Primjer 2.1. *Kvadratna forma $f(x,y) = x^2 + y^2$ je pozitivno definitna ($a = 1, d = -4$).*

Primjer 2.2. *Kvadratna forma $f(x,y) = x^2 - 3y^2$ je indefinitna ($d = 12$).*

Primjer 2.3. *Kvadratna forma $f(x,y) = x^2 - 2xy + y^2$ je pozitivno poludefinitna ($d = 0$).*

U sljedećem teoremu vidjet ćemo koji brojevi d mogu biti diskriminante kvadratnih formi.

Teorem 2.1 ([4])**.** *Neka je d cijeli broj. Tada postoji najmanje jedna binarna kvadratna forma s cjelobrojnim koeficijentima i diskriminantom d ako i samo ako vrijedi $d \equiv 0$ ili $1 \pmod 4$.*

Dokaz. Budući da je $b^2 \equiv 0$ ili $1 \pmod 4$ za bilo koji cijeli broj b, za diskiriminantu d vrijedi $d = b^2 - 4ac \equiv 0$ ili $1 \pmod 4$. Obrnuto, pretpostavimo prvo da je $d \equiv 0 \pmod 4$. Tada forma $x^2 - (d/4)y^2$ ima diskriminantu d. Slično, ako je $d \equiv 1 \pmod 4$, onda forma $x^2 + xy - \left(\frac{d-1}{4}\right) y^2$ ima diskriminantu d.

□

2.1. Ekvivalentne binarne kvadratne forme

Definicija 2.1. *Kvadratne forme f i g su ekvivalentne ako se jedna može transformirati u drugu pomoću unimodularnih transformacija, tj. supstitucija oblika*

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

gdje su $p, q, r, s \in \mathbb{Z}$ i $ps - qr = 1$. Tada pišemo $f \sim g$. (Napomena: x i y su varijable od f, a x' i y' su varijable od g.)

f matrično možemo zapisati kao $X^T F X$, gdje je

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

Množenjem $X^T F X$ uistinu se dobiva $f(x, y)$. Supstituciju iz Definicije 2.1 matrično možemo zapisati sa $X = UX'$, gdje je

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

Uvjet unimodularnosti ($ps - qr = 1$) možemo zapisati s $\det U = 1$. Pritom f prelazi u g koji matrično možemo zapisati kao $X'^T G X'$, gdje je $G = U^T F U$.

Ako je $\Gamma = \left\{ \begin{pmatrix} p & q \\ r & s \end{pmatrix} : p, q, r, s \in \mathbb{Z}, ps - qr = 1 \right\}$, onda Γ s obzirom na množenje matrica čini grupu. To možemo lako provjeriti:

- Jedinična matrica $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ ima determinantu 1 pa je element od Γ
- Ako je $B = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \Gamma$, onda je $B^{-1} = \frac{1}{ps-qr} \begin{pmatrix} s & -q \\ -r & p \end{pmatrix}$.

  Kako je $B \in \Gamma$, to je $\det B = ps - qr = 1$ što povlači $B^{-1} = \begin{pmatrix} s & -q \\ -r & p \end{pmatrix}$

  Dobivamo da je $\det B^{-1} = ps - qr = 1$, tj. $B \in \Gamma$.
- Ako su $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, B = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \Gamma$, onda je $AB = \begin{pmatrix} ap + br & aq + bs \\ cp + dr & cq + ds \end{pmatrix}$.

  Matrica AB ima cjelobrojne elemente i $\det AB = \det A \cdot \det B = 1$, što znači da je i $AB \in \Gamma$.

Elementi grupe Γ nazivaju se *unimodularne matrice.*
Uvjet ekvivalentnosti kvadratnih formi jednak je postojanju matrice $U \in \Gamma$ za koju je $G = U^T F U$ (uz oznake od prije).

Napomena 2.1. *Ako imamo dvije kvadratne forme $f(x, y) = ax^2 + bxy + cy^2$ i $g(x, y) = a'x^2 + b'xy + c'y^2$, uz dosadašnje oznake vrijedi i:*

$$a' = f(p, r), \quad b' = 2apq + b(ps + qr) + 2crs, \quad c' = f(q, s). \tag{3}$$

Propozicija 2.1 ([2])**.** *Neka su f, g i h kvadratne forme. Tada vrijedi:*

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

Dakle, $\sim$ je relacija ekvivalencije.

Dokaz. 1. Ako promotrimo supstituciju čija je matrica $U = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, U \in \Gamma$, onda vrijedi $F = U^T F U$, tj. $f \sim f$ (f ovom trasnformacijom prelazi sam u sebe).

2. Iz $f \sim g$ slijedi da postoji $U \in \Gamma$ tako da je $G = U^T F U$. Kada izrazimo F, dobijemo $F = (U^{-1})^T G U^{-1}$. Budući da se U^{-1} nalazi u Γ, dobili smo $g \sim f$.

3. Iz $f \sim g$ i $g \sim h$ slijedi $G = U^T F U$ i $H = V^T G V$, za $U, V \in \Gamma$. Kada u H uvrstimo G, dobivamo $H = (UV)^T F (UV)$, odnosno $f \sim h$ jer je $UV \in \Gamma$.

□

Definicija 2.2. *Binarna 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 je reprezentacija prava, inače je neprava.*

Propozicija 2.2 ([2])**.** *Neka su f i g ekvivalentne kvadratne forme i $n \in \mathbb{Z}$. Tada:*

1. *f reprezentira $n \Leftrightarrow g$ reprezentira n,*

2. *f pravo reprezentira $n \Leftrightarrow g$ pravo reprezentira n,*

3. *diskriminante od f i g su jednake.*

Dokaz. 1. Dovoljno je pokazati jednu implikaciju (zbog Propozicije 2.1), tj. dovoljno je uzeti da se f može transponirati u g. Tada je $G = U^T F U$, odnosno $F = (U^{-0})^T G U^{-1}$. $f(x_0, y_0) = n$ zapisujemo kao $n = X_0^T F X_0$, gdje je $X_0 = \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$. Kada izrazimo n dobijemo $n = (U^{-1}X_0)^T G (U^{-1}X_0)$, tj. g reprezentira n (varijable od g predstavlja matrica $U^{-1}X_0$).

2. Nastavno na prethodno dokazano, označimo s $X_1 := U^{-1}X_0$ te neka je $X_1 = \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}$. Pretpostavimo da je $(x_0, y_0) = 1$. Vrijedi $x_0 = px_1 + qy_1$, $y_0 = rx_1 + sy_1$. Ako se cijeli broj d može prikazati u obliku $d = bx + cy$, tada je (b, c) djelitelj od d. Dakle, (x_1, y_1) je djelitelj od x_0 i od y_0. Kako je $(x_0, y_0) = 1$, onda je i $(x_1, y_1) = 1$.

3. Označimo s d_0 i d_1 diskriminante od f i g. Kako je $F = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$, slijedi da je $\det F = ac - \frac{b^2}{4}$. Dakle, $d_0 = -4 \det F$. Analogno $d_1 = -4 \det G$. Vrijedi $\det G = \det U^T \det F \det U = 1 \cdot \det F \cdot 1 = \det F$. Iz toga slijedi da je $d_0 = d_1$.

□

U sljedećim tvrdnjama vidjet ćemo u kojim uvjetima binarna kvadratna forma s diskriminantom d reprezentira neki broj.

Teorem 2.2 ([4])**.** *Neka su n i d dani cijeli brojevi takvi da je $n \neq 0$. Tada postoji binarna kvadratna forma s diskriminantom d koja pravo reprezentira n ako i samo ako kongruencija $x^2 \equiv d \pmod{4|n|}$ ima rješenja.*

Dokaz. Pretpostavimo da je b rješenje dane kongruencije i da vrijedi $b^2 - d = 4nc$. Tada forma $f(x, y) = nx^2 + bxy + cy^2$ ima cjelobrojne koeficijente i diskriminantu d. Štoviše, $f(1, 0) = n$ je prava reprezentacija od n.

Obratno, pretpostavimo da imamo pravu reprezentaciju $f(x_0, y_0)$ od n kojeg reprezentira forma $f(x, y) = ax^2 + bxy + cy^2 = n$ s diskriminantom $d = b^2 - 4ac$. Budući da je $(x_0, y_0) = 1$, možemo odabrati cijele brojeve m_1 i m_2 takve da vrijedi $m_1 m_2 = 4|n|$, $(m_1, y_0) = 1$ i $(m_2, x_0) = 1$. Na primjer uzmimo da je m_1 umnožak onih potencija prostih brojeva p^a od $4n$

za koje vrijedi $p|x_0$ te neka je $m_2 = \frac{4|n|}{m_1}$. Iz jednakosti (2) slijedi $4an = (2ax_0 + by_0)^2 - dy_0{}^2$, stoga je $(2ax_0 + by_0)^2 \equiv dy_0{}^2 \pmod{m_1}$. Kako je $(y_0, m_1) = 1$, postoji cijeli broj $y_0{}'$ takav da je $y_0y_0{}' \equiv 1 \pmod{m_1}$ te kongruencija $u^2 \equiv d \pmod{m_1}$ ima rješenje, recimo $u = u_1 = (2ax_0 + by_0)y_0{}'$. Zamijenimo a i c te x i y te vidimo da kongruencija $u^2 \equiv d \pmod{m_2}$ također ima rješenje, recimo $u = u_2$. Prema *Kineskom teoremu o ostacima*[1] dobivamo cijeli broj w takav da je $w \equiv u_1 \pmod{m_1}$ i $w \equiv u_2 \pmod{m_2}$. Stoga je $w^2 \equiv u_1{}^2 \equiv d \pmod{m_1}$ i $w^2 \equiv u_2{}^2 \equiv d \pmod{m_2}$, odakle dobijemo $w^2 \equiv d \pmod{m_1m_2}$. Kako je posljednji modul jednak $4|n|$, teorem je dokazan.

□

Korolar 2.1 ([4]). *Pretpostavimo da je $d \equiv 0$ ili $1 \pmod 4$. Ako je p neparan prost broj, tada postoji binarna kvadratna forma s diskriminantom d koja reprezentira p ako i samo ako je $\left(\frac{d}{p}\right) = 1$.*

Dokaz. Svaka reprezentacija od p mora biti prava. Dakle, ako je p reprezentiran onda je pravo reprezentiran i stoga po Teoremu 2.2 d mora biti kvadrat modulo $4p$ pa je $\left(\frac{d}{p}\right) = 1$.

Obrnuto, ako je $\left(\frac{d}{p}\right) = 1$, onda je d kvadrat modulo p. Po pretpostavci, d je kvadrat modulo 4. Kako je p neparan, slijedi po *Kineskom teoremu o ostacima* da je d kvadrat modulo $4p$ te je stoga po Teoremu 2.2 p pravo reprezentiran nekom formom s diskriminantom d.

□

Neka je d zadan. Po *Gaussovom kvadratnom zakonu reciprociteta*[2] znamo da su neparni prosti brojevi p za koje je $\left(\frac{d}{p}\right) = 1$ upravo prosti brojevi koji leže u određenim klasama ostataka modulo $4|n|$. Na taj način Gaussov kvadratni zakon reciprociteta igra ulogu u određivanju prostih brojeva koji su reprezentirani kvadratnom formom određene diskriminante.

2.2. Reducirane binarne kvadratne forme

Između definitnih i indefinitnih formi postoje brojne razlike. Indefinitnine kvadratne forme kompliciranije su od definitnih, stoga ćemo se baviti definitnim kvadratnim formama, točnije pozitivno definitnim kvadratnim formama koje su oblika $f(x, y) = ax^2 + bxy + cy^2$.

Kao što smo istaknuli ranije, to su one kvadratne forme kod kojih je $d < 0$ i $a > 0$. Iz $d = b^2 - 4ac < 0$ slijedi da c mora biti veći od 0. U nastavku ćemo opisati redukciju ovakvih kvadratnih formi.

Definicija 2.3. *Za pozitivno definitnu kvadratnu formu $f(x, y) = ax^2 + bxy + cy^2$ kažemo da je reducirana ako je $-a < b \leq a < c$ ili $0 \leq b \leq a = c$.*

Teorem 2.3 ([2]). *Svaka pozitivno definitna kvadratna forma je ekvivalentna nekoj reduciranoj formi.*

Dokaz. Promatrat ćemo supstitucije čije su matrice $U = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ i $V = \begin{pmatrix} 1 & \pm 1 \\ 0 & 1 \end{pmatrix}$.

[1] Neka su $m_1, m_2, ..., m_r$ u parovima relativno prosti brojevi te neka su $a_1, a_2, .., a_r \in \mathbb{Z}$. Tada sustav kongruencija $x \equiv a_1 \pmod{m_1}, x \equiv a_2 \pmod{m_2}, ..., x \equiv a_r \pmod{m_r}$ ima rješenja.

Uz to, ako je x_0 jedno rješenje sustava onda su sva rješenja tog sustava dana s $x \equiv x_0 \pmod{m_1 \cdot m_2 \cdot ... \cdot m_r}$

[2] Za dva različita neparna prosta broja p i q vrijedi: $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Pokazat ćemo da korištenjem konačno mnogo ovih transfromacija možemo dobiti da je $|b| \leq a \leq c$.

Lako se pokaže da vrijedi $U^T F U = \begin{pmatrix} c & -\frac{b}{2} \\ -\frac{b}{2} & a \end{pmatrix}$, što znači da U mijenja a i c, a b-u mijenja predznak, tj. ako smo u F imali $a > c$, u $U^T F U$ ćemo imati $a < c$. Zatim, $V^T F V = \begin{pmatrix} a & \frac{b \pm 2a}{2} \\ \frac{b \pm 2a}{2} & a \pm b + c \end{pmatrix}$, odnosno V mijenja b s $b \pm 2a$, a a ne mijenja. Koristeći ovu transformaciju konačno mnogo puta, možemo postići da je $|b| \leq a$. Ovaj proces je konačan jer svaka primjena prve transformacije smanjuje vrijednost od a koji je kod pozitivno definitne kvadratne forme pozitivan broj.

Sada imamo $-a \leq b \leq a$ i $a < c$, odnosno jedan od uvjeta iz Definicije 2.3 je zadovoljen.

Pogledajmo slučaj $b = -a$. Primjenom supstitucije s matricom V možemo dobiti $b = a$, bez mijenjanja c (kod $\pm$ uzimamo $+$). Ako je $a = c$, primjenom supstitucije s matricom U možemo dobiti $b \geq 0$ (primjenom te supstitucije primijeni se predznak ispred $\frac{b}{2}$) te smo dobili i drugi uvjet iz Definicije 2.3. Ako je i dalje $a < c$, imamo prvi uvjet.

□

Primjer 2.4. *Nađimo reduciranu formu ekvivalentnu sa* $179x^2 + 164xy + 13y^2$.

Rješenje: Krećemo od matrice kvadratne forme $F = \begin{pmatrix} 79 & 32 \\ 32 & 13 \end{pmatrix}$.

Na tu matricu primjenimo matricu $U = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$:

$$U^T F U = \begin{pmatrix} 13 & -32 \\ -32 & 79 \end{pmatrix} = F'$$

Zatim, primjenimo matricu $V^+ = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$:

$$V^T F' V = \begin{pmatrix} 13 & -19 \\ -19 & 28 \end{pmatrix} = F''$$

Opet primjenimo matricu V^+ na dobivenu matricu F'' te dobivamo $\begin{pmatrix} 13 & -6 \\ -6 & 3 \end{pmatrix}$.

Primjenom matrice U na posljednju matricu dobivamo matricu $\begin{pmatrix} 3 & 6 \\ 6 & 13 \end{pmatrix}$.

Zatim dva puta primjenimo matricu $V^- = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$ i dobivamo $\begin{pmatrix} 3 & 3 \\ 3 & 4 \end{pmatrix}$ i $\begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}$.

Za kraj, primjenimo matricu U koja daje traženu matricu $\begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}$, odnosno reducirana kvadratna forma je oblika $x^2 + 3y^2$.

Uz pomoć Teorema 2.3 možemo izbjeći mnogobrojno množenje matrica ako zapamtimo sljedeće:

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

Sljedeći teorem govori o broju reduciranih kvadratnih formi s diskriminantom d.

Teorem 2.4 ([2]). *Postoji samo konačno mnogo reduciranih formi s danom diskriminantom d.*

Dokaz. Kod reducirane forme vrijedi $b \leq a$ i $b \leq c$ iz čega slijedi $b^2 \leq ac$, odnosno $-b^2 \geq -ac$. iz toga slijedi $-d = 4ac - b^2 \geq 3ac$. Sada je $|d| \geq 3ac$ (kod pozitivno definitnih formi je $a > 0$ i $c > 0$). Zaključujemo da je $a \leq \frac{1}{3}|d|$ i $c \leq \frac{1}{3}|d|$ jer je $a \geq 1$ i $c \geq 1$. Iz $ac \geq b^2$ slijedi da je i $|b| \leq \frac{1}{3}|d|$. Zaključujemo da postoji konačno mnogo cijelih brojeva a, b i c koji mogu biti koeficijenti reduciranih formi.

□

Napomena 2.2. *Uočimo da za reduciranu kvadratnu formu $ax^2+bxy+cy^2$ s diskriminantom d vrijedi $|b| \leq a \leq \sqrt{\frac{-d}{3}}$.*

Primjer 2.5. *Neka je diskriminanta $d = -11$, odnosno $4ac - b^2 = 11$. Iz $0 \leq |b| \leq a \leq \sqrt{\frac{11}{3}} \leq 2$ slijedi da je $a = 1$ ili 2.*
Iz $a = 1$ slijedi $4c - b^2 = 11$. b može biti 0 ili ± 1. Za $b = 0$ ne postoje cjelobrojna rješenja, a za $b = \pm 1$ dobivamo $c = 3$.
Za $a = 2$, b može biti $0, \pm 1$ ili ± 2, ali ni za jedan b ne postoji cjelobrojni c koji odgovara rješenju jednadžbe.
Ostaje nam samo jedno rješenje, a to je $(a, b, c) = (1, 1, 3)$, odnosno postoji jedinstvena reducirana kvadratna forma s diskriminantom -11 koja je oblika $f(x, y) = x^2 + xy + 3y^2$. Tada neparan prost broj p odgovara traženoj kvadratnoj formi ako i samo ako je $\left(\frac{-11}{p}\right) = 1$, odnosno $p \equiv 1 \pmod{11}$.

Sada ćemo uvesti novi pojam - *broj klasa od d.*

Definicija 2.4. *Binarna kvadratna forma $f(x, y) = ax^2 + bxy + cy^2$ je primitivna ako je $(a, b, c) = 1$.*

Definicija 2.5. *Broj klasa od d je broj pozitivno definitnih reduciranih binarnih kvadratnih formi s diskriminantom d. Oznaka: $h(d)$.*

Primjer 2.6. *Izračunajmo $h(-4)$.*

Rješenje: Iz $d = b^2 - 4ac$, uvrštavanjem $d = -4$ slijedi $4 = 4ac - b^2$, a to vrijedi samo za $a = c = 1$ i $b = 0$. Stoga je $h(-4) = 1$.

Poznato je da je $h(d) = 1$ samo za 9 negativnih cijelih brojeva:

$$d = -3, -4, -7, -8, -11, -19, -43, -67, -163.$$

Primjer 2.7. *Izračunajmo $h(-20)$.*

Rješenje: Iz $-d = 4ac - b^2 \geq 3ac \geq 3a^2$ slijedi $a \leq 2$. Dijelimo na dva slučaja:

1) Neka je $a = 1$. Tada je $b \in \{0, 1\}$ zbog $-a < b \leq a$. Iz $4c - b^2 = 20$ slijedi da je b paran, odnosno $b = 0$ i $c = 5$.

2) Neka je $a = 2$. Tada je $b \in \{-1, 0, 1, 2\}$. Iz $8c - b^2 = 20$ slijedi da je opet b paran. Uvrštavanjem b u jednadžbu vidimo da za $b = 0$ nema rješenja, a za $b = 2$ dobivamo $c = 3$.

Dakle, postoje dvije reducirane forme s diskriminantom -20, a to su x^2+5y^2 i $2x^2+2xy+3y^2$, tj. $h(20) = 2$.

Sljedeća lema potrebna je za dokaz teorema nakon nje koji pokazuje da je $h(d)$ broj neekvivalentnih reduciranih binarnih kvadratnih formi s diskriminantom d. Analogna tvrdnja za $d > 0$ ne vrijedi..

Lema 2.1 ([4]). *Neka je $f(x, y) = ax^2 + bxy + cz^2$ reducirana pozitivno definitna kvadratna forma. Ako za neki par cijelih brojeva x i y vrijedi $(x, y) = 1$ i $f(x, y) \leq c$, onda onda je $f(x, y) = a$ ili c i točka (x, y) je jedna od sljedećih točaka $\pm(1, 0), \pm(0, 1), \pm(1, -1)$. Štoviše, broj pravih reprezentacija od a pomoću f je*

- *2, ako je $a < c$,*
- *4, ako je $0 \leq b < a = c$ i*
- *6, ako je $a = b = c$.*

Dokaz. Pretpostavimo da vrijedi $(x, y) = 1$. Ako je $y = 0$, onda je $x = \pm 1$ te vrijedi $f(\pm 1, 0) = a$.
Sada pretpostavimo da je $y = \pm 1$. Ako je $|x| \geq 2$, onda slijedi

$$\begin{aligned} |2ax + by| \geq & |2ax| - |by| \text{ (slijedi iz nejednakosti trokuta)} \\ \geq & 4a - |b| \\ \geq & 3a \text{ (jer je } |b| \leq a) \end{aligned}$$

Tada po (2) zaključujemo da

$$\begin{aligned} 4af(x, y) = & (2ax + by)^2 - dy^2 \\ \geq & 9a^2 - dy^2 \\ = & 9a^2 - d \\ = & 9a^2 + 4ac - b^2 \\ > & a^2 - b^2 + 4ac \text{ (budući da je } a > 0) \\ \geq & 4ac \text{ (budući da je } |b| \leq a) \end{aligned}$$

Prema tome, $f(x, \pm 1) > c$ ako je $|x| \geq 2$. Pretpostavimo da je $|y| \geq 2$. Tada po (2) slijedi:

$$\begin{aligned} 4af(x, y) = & (2ax + by)^2 - dy^2 \\ \geq & -dy^2 \\ \geq & -4d \\ = & 16ac - 4b^2 \\ > & 8ac - 4b^2 \text{ (budući da je } ac > 0) \\ \geq & 4a^2 - 4b^2 + 4ac \text{ (budući da je } 0 < a \leq c) \\ \geq & 4ac \text{ (budući da je } |b| \leq a) \end{aligned}$$

Stoga je $f(x, y) > c$ ako je $|y| \geq 2$. Jedine preostale točke su $\pm(1, 0), \pm(0, 1), \pm(1, -1)$ i $\pm(1, 1)$. Kako je $b > -a$ slijedi $f(1, 1) = a + b + c > c$ te se odgovarajuće reprezentacije od a i c dobivaju iz prva tri para.
Posljednja tvrdnja leme slijedi iz navedenog: $f(1, 0) = a, f(0, 1) = c$ i $f(1, -1) = a - b + c$.
□

Teorem 2.5 ([4]). *Neka su $f(x,y) = ax^2 + bxy + cy^2$ i $g(x,y) = dx^2 + exy + hy^2$ reducirane pozitivno definitne kvadratne forme. Ako je $f \sim g$, onda je $f = g$.*

Dokaz. Pretpostavimo da je $f \sim g$. Po Lemi 2.1 najmanji pozitivan broj pravo reprezentiran kvadratnom formom f je a, a od g je d. Po Propoziciji 2.2 slijedi da je $a = d$.

Prvo ćemo razmotriti slučaj $a < c$. Tada po Lemi 2.1 postoje točno dvije prave reprezentacije broja a kvadratnom formom f. Po Propoziciji 2.2 slijedi da postoje i točno dvije reprezentacije broja a kvadratnom formom g. Iz Leme 2.1 zaključujemo da je $h > a$. Stoga po toj istoj Lemi vidimo da je c najmanji broj veći od a kojeg pravo reprezentira f pa tako i g. Po Propoziciji 2.2 slijedi da je $c = h$.
Da bismo pokazali da je $b = e$, promotrit ćemo matricu $U \in \Gamma$ koja f transformira u g. Kako je $\det U = ps - qr = 1$, znamo da je $nzd(p,r) = 1$. Stoga po Napomeni 2.1, $f(p,r) = a$ je prava reprezentacija od a. Po Lemi 2.1 slijedi da je prvi stupac od U jednak $\pm \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. Slično, vidimo da je $nzd(q,s) = 1$ pa je po Napomeni 2.1, $f(q,s) = c$ prava reprezentacija od c. Nadalje, po Lemi 2.1, drugi stupac od M jednak je $\pm \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ ili $\pm \begin{pmatrix} -1 \\ 1 \end{pmatrix}$. Jedini kandidati za U su $\pm I$ i $\pm \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$. Štoviše, po Napomeni 2.1 e bi trebao biti jednak $-2a + b$, što nije moguće pošto b i e moraju ležati u intervalu $(-a, a]$. To nam ostavlja samo slučaj $U = \pm I$, iz kojeg nam slijedi da je $f = g$.

Sada promatramo slučaj $a = c$. Iz Leme 2.1 vidimo da a ima barem 4 prave reprezentacije kvadratnom formom f. Iz Propozicije 2.2 slijedi da isto vrijedi i ta g, a po Lemi 2.1 zaključujemo da je $h = a = c$. Stoga po Definiciji 2.3, $0 \leq e \leq d = h = a$. Kako je $b^2 - 4ac = e^2 - 4dh$, slijedi da je $b = e$ pa samim time i $f = g$.

□

Primjer 2.8. *Lako se vidi da su $f(x,y) = 3x^2 + xy + 4y^2$ i $g(x,y) = 3x^2 - xy + 4y^2$ reducirane kvadratne forme. Prema prethodnoj tvrdnji one nisu ekvivalentne kvadratne forme.*

Napomena 2.3. *Uočimo da obje kvadratne forme iz prethodnog primjera imaju diskriminantu $d = -47$ i reprezentiraju iste brojeve, npr. $f(2,-1) = 14 = g(2,1)$. Stoga obrat tvrdnji iz Propozicije 2.2, točnije obrat tvrdnje 3., općenito ne vrijedi.*

2.3. Primjene

U ovom odjeljku vidjet ćemo kako se primjenjuju prethodno iskazane tvrdnje.

Primjer 2.9. *Dokažimo da se prosti broj p može prikazati u obliku $x^2 + 5y^2, x, y \in \mathbb{N}$ ako i samo ako je $p \equiv 1$ ili $9 \pmod{20}$.*

Rješenje: Da bi se prosti broj p mogao prikazati nekom binarnom kvadratnom formom s diskriminantom -20, nužan i dovoljan uvjet je, prema Teoremu 2.2, da kongruencija $x^2 \equiv -20 \pmod{4p}$ ima rješenja. Odnosno, postoji $z \in \mathbb{Z}$ takav da je $z^2 \equiv -5 \pmod{p}$, tj. $\left(\frac{-5}{p}\right) = 1$.
Znamo da postoje točno dvije neekvivalentne forme s diskriminantom -20 kao što smo vidjeli u Primjeru 2.7.

Ako je $p = x^2 + 5y^2$, onda je $x^2 \equiv p \pmod{5}$, tj. $\left(\frac{p}{5}\right) = 1$.

Ako je $p = 2x^2 + 2xy + 3y^2$, onda je $2p = (2x+y)^2 + 5y^2$ pa je $(2x+y)^2 \equiv 2p \pmod{5}$, tj. $\left(\frac{2p}{5}\right) = 1$. Iz $\left(\frac{2p}{5}\right) = \left(\frac{2}{5}\right)\left(\frac{p}{5}\right) = -\left(\frac{p}{5}\right)$ slijedi da je $\left(\frac{p}{5}\right) = -1$.

Uvjeti za tražene brojeve p su $\left(\frac{-5}{p}\right) = 1$ i $\left(\frac{p}{5}\right) = 1$. Kako je $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$, uvjeti su ekvivalentni s $\left(\frac{p}{5}\right) = 1$ i $\left(\frac{-1}{p}\right) = 1$, tj. $p \equiv 1$ ili $4 \pmod 5$ i $p \equiv 1 \pmod 4$, odakle je, prema *Kineskom teoremu o ostacima*, $p \equiv 1$ ili $9 \pmod{20}$.

Teorem 2.6 ([3]). *Neka je p prost broj. Tada je:*

(a) $p = x^2 + y^2$ *ako i samo ako je* $p \equiv 1 \pmod 4$ *ili* $p = 2$.

(b) $p = x^2 + 2y^2$ *ako i samo ako je* $p \equiv 1, 3 \pmod 8$ *ili* $p = 2$.

(c) $p = x^2 + 3y^2$ *ako i samo ako je* $p \equiv 1 \pmod 3$ *ili* $p = 3$.

(d) $p = x^2 + 4y^2$ *ako i samo ako je* $p \equiv 1 \pmod 4$.

(e) $p = x^2 + 7y^2$ *ako i samo ako je* $p \equiv 1, 2, 4 \pmod 7$ *ili* $p = 7$.

Dokaz. Ovdje ćemo napraviti dokaze za (a) i (b) dio teorema.

(a) Korolar 2.1 zahtjeva da je p neparan, stoga moramo odvojeno obraditi slučaj $p = 2$ (koji je očito reprezentiran s $x^2 + y^2$). Za neparan broj p, znamo da je reprezentiran reduciranom formom s diskriminantom -4. Također, u Primjeru 2.6 pokazali smo da je $h(-4) = 1$ pa je $x^2 + y^2$ jedina reducirana kvadratna forma s diskriminantom -4. Znamo da je $\left(\frac{-1}{p}\right) = 1$ ako i samo ako je $p \equiv 1 \pmod 4$ pa je dokaz završen.

(b) Reducirana forma s diskriminantom -8 reprezentira neparan broj p ako i samo ako je $\left(\frac{-2}{p}\right) = 1$ pa, kao i u prethodnom dokazu, moramo odrediti sve reducirane forme s diskriminantom -8. Znamo da je $|b| \leq a \leq \sqrt{8/3} < 2$ pa a mora biti 1. $1 - 4c = -8$ nema cjelobrojnih rješenja pa je jedina reducirana forma s diskriminantom -8 upravo x^2+2y^2. Kako je $\left(\frac{2}{p}\right) = 1$ ako i samo ako je $p \equiv 1, 7 \pmod 8$ to je $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = 1$ ako i samo ako je $p \equiv 1, 3 \pmod 8$.

□

2.4. Sume dvaju i sume četiriju kvadrata

Za prirodan broj n kažemo da se može prikazati u obliku sume dva kvadrata ako postoje $x, y \in \mathbb{Z}$ takvi da vrijedi $n = x^2 + y^2$.

Teorem 2.7 ([1]). *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 prosti faktor p za koji je $p \equiv 3 \pmod 4$ javlja s parnom potencijom.*

Dokaz. Prvo ćemo provjeriti nužnost. Pretpostavimo da je $n = x^2 + y^2$ i da prost broj $p \equiv 3 \pmod 4$ dijeli n. Tada je $x^2 + y^2 \equiv 0 \pmod p$, tj. $x^2 \equiv -y^2 \pmod p$. -1 je kvadratni neostatak $\pmod p$ pa zaključujemo da p dijeli x i y što povlači da p^2 dijeli n. Imamo $(\frac{x}{p})^2 + (\frac{y}{p})^2 = \frac{n}{p^2}$, iz čega slijedi da se p u rastavu broja n javlja s parnom potencijom.
Za dokaz obrata, dovoljno je pretpostaviti da je n kvadratno slobodan i pokazati da ako svaki neparni prosti djelitelj p zadovoljava $p \equiv 1 \pmod 4$, tada se n može prikazati kao $x^2 + y^2$. Zaista, ako je $n = x^2 + y^2$, onda je $nm^2 = (xm)^2 + (ym)^2$. Kvadratna forma $x^2 + y^2$

je reducirana s diskriminantom -4 i u Primjeru 2.6 smo pokazali da je $h(-4) = 1$. Stoga je to jedina takva reducirana kvadratna forma. Prema Teoremu 2.2 vrijedi sljedeće: n je pravo reprezentiran formom $x^2 + y^2$ ako i samo ako kongruencija $x^2 \equiv -4 \pmod{4n}$ ima rješenja. Toj kongruenciji ekvivalentna je kongruencija $z^2 \equiv -1 \pmod{n}$. n ćemo zapisati kao $n = p_1 \cdot p_2 \cdot \cdots \cdot p_k$. Po pretpostavci teorema vrijedi $p_i \equiv 1 \pmod 4$, stoga $z^2 \equiv -1 \pmod{p_i}$ ima rješenje i označimo ga s $z = z_i$. *Kineski teorem o ostacima* tvrdi da je cijeli broj z rješenje sustava

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

Sada je $z^2 \equiv {z_i}^2 \equiv -1 \pmod{p_i}$ za svaki $i \in \{1, 2, \ldots, k\}$ pa vrijedi $z^2 \equiv -1 \pmod n$

□

Teorem 2.8 (Lagrangeov teorem o četiri kvadrata, [2])**.** *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. Tvrdnju teorema dovoljno je provjeriti za proste brojeve jer vrijedi sljedeći identitet:

$$\begin{aligned}(x^2 + y^2 + z^2 + w^2) \cdot (a^2 + b^2 + c^2 + d^2) = (ax + by + cz + dw)^2 + \\ +(ay - bx + dz - cw)^2 + (az - cx + bw - dy)^2 + (aw - dx + cy - bz)^2.\end{aligned} \tag{4}$$

Pretpostavimo da je p neparan prost broj te promotrimo sljedeće brojeve $0^2, 1^2, 2^2, \ldots, (\frac{p-1}{2})^2$ među kojima nikoja dva nisu kongruentna modulo p. Isto vrijedi i za sljedeće brojeve $-1 - 0^2, -1 - 1^2, -1 - 2^2, \ldots, -1 - (\frac{p-1}{2})^2$. Brojeva koje smo nabrojali ima $p+1$. Po *slaboj formi Dirichletovog principa* [3] dva broja među njima dat će isti ostatak pri dijeljenju s p, odnosno postoje $x, y \in \mathbb{Z}$ takvi da $x^2 \equiv -1-y^2 \pmod p$ i da vrijedi da je $x^2+y^2+1 < 1+2\cdot(\frac{p}{2})^2 < p^2$. Prema tome, dobili smo da je $mp = x^2+y^2+1$ za neki cijeli broj m za koji vrijedi $0 < m < p$.

Pretpostavimo da je k najmanji prirodan broj za koji vrijedi $kp = x^2 + y^2 + z^2 + w^2$, za neke $x, y, z, w \in \mathbb{Z}$ te vrijedi $k \leq m < p$. k mora biti neparan jer da je paran, među x, y, z, w imali bismo parno mnogo neparnih brojeva što bi značilo da su brojevi $x+y, x-y, z+w, z-w$ parni čime bismo iz

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

dobili kontradikciju s pretpostavkom da je takav k najmanji.

Za dokaz teorema, moramo pokazati da je $k = 1$. Stoga, pretpostavimo suprotno, odnosno $k > 1$.

Uzmimo da su x', y', z', w' najmanji ostaci po apsolutnoj vrijednosti pri dijeljenju brojeva x, y, z, w s k te neka je $n = x'^2 + x'y'^2 + z'^2 + w'^2$.
Mora vrijediti $n \equiv 0 \pmod k$ i $n > 0$ jer bi u suprotnom k dijelio p. Kako je n neparan broj, vrijedi $n < 4 \cdot (\frac{k}{2})^2 = k^2$. Prema tome, $n = mk$, za neki $m \in \mathbb{Z}$ za koji vrijedi $0 < m < k$. Iz (4) slijedi da se $(mk)(kp)$ može prikazati kao suma dva kvadrata četiri cijela broja, štoviše, svaki od njih djeljiv je sa k^2. Odakle dobivamo da se mp može prikazati kao suma četiri kvadrata iz čega dobivamo kontradikciju s minimalnočšu od k. Odnosno, $k = 1$.

□

Metoda koju smo upotrijebili u dokazu Teorema 2.8 naziva se *Fermatova metoda beskonačnog spusta.* Ova metoda temelji se na svojstvu skupa prirodnih brojeva koje glasi *"Svaki neprazan podskup skupa prirodnih brojeva ima najmanji element".*

[3] Neka je n prirodan broj. Ako $n + 1$ predmeta bilo kako rasporedimo u n kutija, tada će barem jedna kutija sadržavati barem 2 predmeta.

3. Ternarne kvadratne forme

Ternarnu kvadratnu formu zapisat ćemo u sljedećem obliku:

$$F(x_1, x_2, x_3) = \sum_{k,l=1}^{3} a_{kl} x_k x_l, \quad a_{kl} \in \mathbb{Z}, \quad a_{kl} = a_{lk}, \quad k, l \in \{1, 2, 3\}.$$

Determinanta matrice čiji su elementi a_{kl} naziva se diskriminanta od $F(x_1, x_2, x_3)$.

3.1. Ekvivalentne ternarne kvadratne forme

Teorem 3.1 ([2]). *Ternarna forma $F(x_1, x_2, x_3) = \sum_{k,l=1}^{3} a_{kl} x_k x_l$ s diskiminantom d je pozitivno definitna ako i samo ako vrijedi:*

$$a_{11} > 0, \quad b = a_{11}a_{22} - a_{12}^2 > 0, \quad d > 0.$$

Nadalje, ako je F pozitivno definitna, onda je

$$a_{11}F = (a_{11}x_1 + a_{12}x_2 + a_{13}x_3)^2 + K(x_2, x_3), \tag{5}$$

gdje je $K(x_2, x_3)$ pozitivno definitna binarna kvadratna forma s diskriminantom $a_{11}d$.

Dokaz. Izravnim računom se provjeri da za

$$K(x_1, x_2) = (a_{11}a_{22} - a_{12}^2)x_2^2 + 2(a_{11}a_{23} - a_{12}a_{13})x_2x_3 + (a_{11}a_{33} - a_{13}^2)x_3^2$$

vrijedi $a_{11}F = (a_{11}x_1 + a_{12}x_2 + a_{13}x_3)^2 + K(x_2, x_3)$ te da je diskriminanta od $K(x_2, x_3)$ jednaka

$$\begin{aligned}
&(a_{11}a_{22} - a_{12}^2)(a_{11}a_{33} - a_{13}^2) - (a_{11}a_{23} - a_{12}a_{13})^2 = \\
&= a_{11}(a_{11}a_{22}a_{33} - a_{11}a_{23}^2 + 2a_{12}a_{13}a_{23} - a_{12}^2a_{33} - a_{13}^2a_{22}) = \\
&= a_{11}d.
\end{aligned}$$

Pretpostavit ćemo da je kvadratna forma F pozitivno definitna. Iz $F(1, 0, 0) = a_{11}$ slijedi da je $a_{11} > 0$. Iz (5) slijedi da je $F(x_1, x_2, x_3)$ pozitivno definitna ako i samo ako je $K(x_2, x_3)$ pozitivno definitna. Zaista, ako K nije pozitivno definitna, onda je $K(x_2, x_3) \leq 0$ za neke $(x_2, x_3) \neq (0, 0)$. Tada je i $K(y_2, y_3) \leq 0$ za $y_2 = a_{11}x_2$ i $y_3 = a_{11}x_3$. Jednadžba $a_{11}x_1 + a_{12}y_2 + a_{13}y_3 = 0$ ima cjelobrojno rješenje x_1 pa dobivamo da je $F(x_1, y_2, y_3) = K(y_2, y_3) \leq 0$ što je u kontradikciji s pretpostavkom da je F pozitivno definitna.

Obrnuto, ako je K pozitivno definitna, onda iz (5) slijedi da je $F(x_1, x_2, x_3) \geq K(x_2, x_3) > 0$ za $(x_2, x_3) \neq (0, 0)$, dok za $(x_2, x_3) = (0, 0)$ i $x_1 \neq 0$ vrijedi $F(x_1, x_2, x_3) = a_{11}x_1^2 > 0$.

Binarna forma $K(x_2, x_3)$ je pozitivno definitna ako i samo ako je $a_{11}a_{22} - a_{12}^2 > 0$ i $a_{11}d > 0$, čime je teorem dokazan.

□

Definicija 3.1. *Dvije ternarne kvadratne forme $F(x_1, x_2, x_3) = \sum_{k,l=1}^{3} a_{kl}x_kx_l$ i $G(x_1, x_2, x_3) = \sum_{k,l=1}^{3} b_{kl}x_kx_l$ su ekvivalentne (pišemo $F \sim G$) ako postoji 3×3 matrica C s cjelobrojnim koeficijentima c_{kl} i determinantom 1 koja prevodi F u G preko transformacija $x_k = \sum_l c_{kl}y_l$, uz to vrijedi $b_{kl} = \sum_{m,n} c_{mk}a_{mn}c_{nl}$.*

Napomena 3.1. *Ekvivalencija ternarnih kvadratnih formi je relacija ekvivalencije.*

Teorem 3.2 ([2]). *Svaka klasa ekvivalencije pozitivno definitnih ternarnih kvadratnih formu sadržava barem jednu formu čiji koeficijenti zadovoljavaju*

$$a_{11} \leq \frac{4}{3}\sqrt[3]{d}, \quad 2|a_{12}| \leq a_{11}, \quad 2|a_{13}| \leq a_{11}.$$

Teorem 3.3 ([2]). *Svaka pozitivno definitna ternarna kvadratna forma s diskriminantom 1 ekvivalentna je formi $x_1^2 + x_2^2 + x_3^2$.*

Dokaz. Prema Teoremu 3.2, svaka takva forma ekvivalentna je nekoj formi za koju vrijedi:

$$a_{11} \leq \frac{4}{3}, \quad 2|a_{12}| \leq a_{11}, \quad 2|a_{13}| \leq a_{11},$$

odakle dobivamo $a_{11} = 1, a_{12} = 0, a_{13} = 0$. Dakle, promatrana klasa sadržava formu oblika $G = x_1^2 + K(x_2, x_3)$, gdje je $K(x_2, x_3) = a_{22}x_2^2 + 2a_{23}x_2x_3 + a_{33}x_3^2$ pozitivno definitna binarna kvadratna forma s diskiminantom 1 te je stoga ekvivalentna formi $x_2^2+x_3^2$, uz transformacijsku matricu oblika $\begin{pmatrix} t & u \\ v & w \end{pmatrix}$ s determinantom 1. Sada matrica $\begin{pmatrix} 1 & 0 & 0 \\ 0 & t & u \\ 0 & v & w \end{pmatrix}$ također transformira formu G u formu $x_1^2 + x_2^2 + x_3^2$.

□

3.2. Sume triju kvadrata

U sljedećem teoremu saznat ćemo koji brojevi se mogu, odnosno ne mogu, prikazati kao sume triju kvadrata.

Teorem 3.4 ([2]). *Svaki prirodan broj n koji nije oblika $n = 4^m(8k + 7), m, k \geq 0$, može se prikazati u obliku $x^2 + y^2 + z^2, x, y, z \in \mathbb{Z}$.*

Dokaz. Ako se broj n može prikazati kao suma triju kvadrata, onda se i broj $4n$ također može prikazati kao suma triju kvadrata. Stoga znamo da n nije djeljiv s 4. Uz to, znamo i da broj $n \equiv 7 \pmod 8$ nije suma tri kvadrata pa ćemo u dokazu promatrati slučajeve $n \equiv 1, 2, 3, 5$ ili $6 \pmod 8$. Prema Teoremu 3.3, za svaki od takvih n-ova dovoljno je pronaći neku pozitivno definitnu ternarnu kvadratnu formu s diskriminantom 1 koja reprezentira n. Trebamo odrediti šest cijelih brojeva $a_{11}, a_{12}, a_{13}, a_{22}, a_{23}, a_{33}$ takvih da ternarna kvadratna forma koju određuju ($f(x_1, x_2, x_3) = \sum_{i,j=1}^{3} a_{ij}x_ix_j$) reprezentira n i da je pozitivno definitna. Prema Teoremu 3.1, ti brojevi moraju zadovoljavati sljedeća tri uvjeta:

$$a_{11} > 0,$$

$$a_{11}a_{22} - a_{12}^2 > 0,$$

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{12} & a_{22} & a_{23} \\ a_{13} & a_{23} & a_{33} \end{vmatrix} = 1.$$

Kako bismo lakše pronašli rješenje koje zadovoljava gore navedene uvjete, fiksirat ćemo tri nepoznanice: $a_{13} = 1, \quad a_{23} = 0, \quad a_{33} = n$.
Sada je $f(x_1, x_2, x_3) = a_{11}x_1^2 + 2a_{12}x_1x_2 + 2x_1x_3 + a_{22}x_2^2 + nx_3^2$. Za $x_1 = 0, x_2 = 0, x_3 = 1$ vrijedi $f(0, 0, 1) = n$, tj. uvjet da f reprezentira n je zadovoljen. Sada imamo

$$\begin{vmatrix} a_{11} & a_{12} & 1 \\ a_{12} & a_{22} & 0 \\ 1 & 0 & n \end{vmatrix} = nb - a_{22},$$

stoga preostale tri nepoznanice a_{11}, a_{12}, a_{22} trebaju zadovoljiti sljedeće uvjete:

$$a_{11} > 0, \quad b = a_{11}a_{22} - a_{12}^2 > 0, \quad a_{22} = bn - 1.$$

Pretpostavit ćemo da je $n > 1$ jer je za $n = 1$ tvrdnja teorema trivijalno zadovoljena. Iz $a_{22} > b - 1 \geq 0$ i $a_{11}a_{22} = a_{12}^2 + b > 0$ slijedi $a_{11} > 0$, tj. prvi uvjet je zadovoljen.
Sada trebamo pronaći prirodni broj b takav da je $-b$ kvadratni ostatak modulo $bn - 1$ jer je $-b \equiv a_{12}^2 \pmod{a_{22}}$. Dokaz ćemo podijeliti na dva slučaja u ovisnosti o tome je li n paran ili neparan. Prvo pretpostavimo da je $n \equiv 2$ ili $6 \pmod 8$. Tvrdimo da postoji prosti broj p oblika $p = bn - 1$ za koji vrijedi da je $\left(\frac{-b}{p}\right) = 1$. Kako su $4n$ i $n - 1$ relativno prosti, iz *Dirichletovog teorema o prostim brojevima u aritmetičkom nizu*[4] slijedi da postoji prost broj oblika $p = (n-1) + 4nv = (4v+1)n - 1$. Da bi vrijedilo $p = bn - 1$ i $b > 0$, stavit ćemo da je $b = 4v + 1$, Iz $n \equiv 2 \pmod 4$ slijedi $p \equiv 1 \pmod 4$ pa imamo

$$\left(\frac{-b}{p}\right) = \left(\frac{b}{p}\right) = \left(\frac{p}{b}\right) = \left(\frac{bn-1}{b}\right) = \left(\frac{-1}{b}\right) = 1.$$

Sada ćemo pretpostaviti da je $n \equiv 1, 3$ ili $5 \pmod 8$. Ako je $n \equiv 3 \pmod 8$, stavimo da je $c = 1$, a ako je $n \equiv 1$ ili $5 \pmod 8$ stavimo $c = 3$, tako da je broj $(cn-1)/2$ neparan u oba slučaja. Stoga su $4n$ i $(cn-1)/2$ relativno prosti pa iz *Dirichletovog teorema o prostim brojevima u aritmetičkom nizu* slijedi da postoji prost broj p oblika $p = \frac{cn-1}{2} + 4nv = \frac{1}{2}((8v+c)n - 1)$. Ako stavimo da je $b = 8v + c$, onda vrijedi $2p = bn - 1$ i $b > 0$. Kako je b neparan, vrijedi da je $-b$ kvadratni ostatak modulo 2. Još moramo provjeriti da je $-b$ kvadratni ostatak modulo p. Najprije uočimo da vrijedi:

- ako je $n \equiv 1 \pmod 8$, onda je $b \equiv 3 \pmod 8$ i $p \equiv 1 \pmod 4$,
- ako je $n \equiv 3 \pmod 8$, onda je $b \equiv 1 \pmod 8$ i $p \equiv 1 \pmod 4$,
- ako je $n \equiv 5 \pmod 8$, onda je $b \equiv 3 \pmod 8$ i $p \equiv 3 \pmod 4$.

Zaključujemo da je u svakom slučaju $\left(\frac{-2}{b}\right) = 1$ pa stoga imamo

$$\begin{aligned}\left(\frac{-b}{p}\right) =& (-1)^{(p-1)/2}\left(\frac{b}{p}\right) = (-1)^{\frac{p-1}{2}\frac{b+1}{2}}\left(\frac{p}{b}\right) = \left(\frac{p}{b}\right) = \left(\frac{p}{b}\right)\left(\frac{-2}{b}\right) \\ =& \left(\frac{-2p}{b}\right) = \left(\frac{1-bn}{b}\right) = \left(\frac{1}{b}\right) = 1.\end{aligned}$$

Dobili smo da je $-b$ kvadratni ostatak modulo 2 i modulo p što znači da je $-b$ kvadratni ostatak i modulo $2p = bn - 1$, što je i trebalo dokazati.

□

Propozicija 3.1 ([2]). *Neka je $n = 4^m(8k+7), m, k \geq 0$. Tada se n ne može prikazati u obliku $x^2 + y^2 + z^2, x, y, z \in \mathbb{Z}$.*

Dokaz. Pretpostavit ćemo suprotno onome što treba dokazati, točnije pretpostavit ćemo da je n najmanji prirodni broj za koji vrijedi:

$$n = 4^m(8k+7) = x^2 + y^2 + z^2.$$

[4]Neka su a i b relativno prosti cijeli brojevi. Tada postoji beskonačno mnogo prostih brojeva p takvih da vrijedi $p \equiv a \pmod b$, tj. u aritmetičkom nizu $a + bn$ postoji beskonačno mnogo prostih brojeva.

Kvadrat neparnog broja daje ostatak 1 pri djeljenju s 8, tj. $(2a+1)^2 = 8 \cdot \frac{a(a+1)}{2} + 1$. Ako je neki od brojeva x, y, z neparan, onda je $x^2+y^2+z^2$ oblika $4l+1$, a ako su 2 ili 3 broja neparna, onda je $x^2+y^2+z^2$ oblika $4l+2$ ili $8l+3$. Kako n nije niti jednog od ovih oblika, onda su x, y, z svi parni, npr. $x = 2x', y = 2y', z = 2z'$. Sada je

$$\frac{n}{4} = 4^{m-1}(8k+7) = x'^2 + y'^2 + z'^2,$$

pa smo dobili kontradikciju s minimalnosti od n.

□

U nastavku navest ćemo još neke zanimljive tvrdnje vezane uz sume triju kvadrata. Za razumijevanje prve tvrdnje potrebno je uvesti sljedeću definiciju:

Definicija 3.2. *Cijeli broj n naziva se trokutasti broj ako postoji cijeli broj m takav da je $n = t_m = \frac{m(m+1)}{2}$. Dakle, neki od trokutastih brojeva su: 0,1,3,6,10,15,21,...*

Za lakše razumijevanje trokutastih brojeva, uzmimo točke koje slažemo u obliku jednakostraničnog trokuta na način da svaka stranica ima m točaka te dodajemo sloj po sloj. Ukupan broj točaka u trokutu bit će $m + (m-1) + \cdots + 1 = \frac{m(m+1)}{2}$, odnosno m-ti trokutasti broj.

Teorem 3.5 (Gauss, [2])**.** *Svaki prirodan broj n može se prikazati kao suma triju trokutastih brojeva.*

Dokaz. Broj $8n+3$ može se prikazati kao suma tri kvadrata: $8n+3 = x_1^2 + x_2^2 + x_3^2$. Brojevi x_1, x_2, x_3 su svi neparni jer kvadrati cijelih brojeva pri djeljenju s 8 daju ostatke 0,1 ili 4. Neka je $x_1 = 2m_1 + 1, x_2 = 2m_2 + 1$ i $x_3 = 2m_3 + 1$. Uvrštavanjem x_1, x_2 i x_3 u izraz za $8n+3$ dobivamo

$$8n + 3 = 4m_1(m_1+1) + 4m_2(m_2+1) + 4m_3(m_3+1) + 3,$$

odnosno

$$n = \frac{m_1(m_1+1)}{2} + \frac{m_2(m_2+1)}{2} + \frac{m_3(m_3+1)}{2}.$$

□

Sljedeća tvrdnja bazira se na tvrdnji iz Teorema 3.4:

Propozicija 3.2 ([5])**.** *Bilo koji broj N može se prikazati u obliku*

$$N = x^2 + y^2 + z^2 + du^2, \tag{6}$$

gdje je d bilo koji cijeli broj između 1 i 7, uključujući i njih.

Dokaz. Ako N nije oblika $4^m(8k+7)$, izraz (6) vrijedit će za $u = 0$. Stoga možemo pretpostaviti da je $N = 4^m(8k+7)$.

Prvo, pretpostavimo da je d jednak nekoj od sljedećih vrijednosti: $1, 2, 4, 5, 6$. Neka je $u = 2^m$. Tada broj $N - du^2 = 4^m(8k+7-d)$ nije oblika $4^m(8k+7)$ pa ga je stoga moguće zapisati u obliku $x^2 + y^2 + z^2$.

Zatim, neka je $d = 3$. Ako je $k = 0$, uzmimo $u = 2^m$. Tada je $N - du^2 = 4^{m+1}$. Ako je $k \geq 1$, uzmimo $u = 2^{m+1}$. Tada je $N - d^2 = 4^m(8k-5)$.
U nijednom od ovih slučajeva $N - du^2$ nije oblika $4^m(8k+7)$ pa se može zapisati u obliku $x^2 + y^2 + z^2$.

Neka je $d = 7$. Ako je $k = 0, 1$ ili 2, uzmimo $u = 2^m$. Sada je $N - du^2$ jednako $0, 2 \cdot 4^{m+1}$ ili 4^{m+2}. Ako je $k \geq 3$, uzmimo $u = 2^{m+1}$. Tada je $N - du^2 = 4^m(8k-21)$.
Stoga se u svakom slučaju $N - du^2$ može izraziti u obliku $x^2 + y^2 + z^2$.

□

Literatura

[1] A. Baker, *A concise introduction in theory of numbers*, Cambridge University Press, Cambridge, 1984.

[2] A. Dujella, *Teorija brojeva*, Školska knjiga, Zagreb, 2019.

[3] P. Michaud-Rodgers, , *Quadratic Forms and Three-Square Theorem*, University of Warwick, 2018.

[4] I. Niven, S. Zuckerman, l. Montgomery, *An Introduction to the Theory of Numbers*, John Wiley & Sons, 1991.

[5] S. Ramanujan, *On the expression of a number in the form* $ax^2 + by^2 + cz^2 + du$, Proceedings of the Cambridge Philosophical Society, XIX, 1917, 11-21.

[6] W. Stein, *An Explicit Approach To Elementary Number Theory*, Harvard University, 2001.