**SVEUČILIŠTE U ZAGREBU**

**PRIRODOSLOVNO–MATEMATIČKI FAKULTET**

**MATEMATIČKI ODSJEK**

Ivona Mrkalj

# LOKALNO-GLOBALNI PRINCIP

Diplomski rad

Voditelj rada:
prof. dr. sc. Filip Najman

Zagreb, rujan, 2016

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

*Mojoj pranoni, vječnoj gospođi, Kseniji (Pavletić) Granić*

# Sadržaj

# Uvod

Lokalno-globalni princip otkrio je 1920. godine Helmut Hasse (zbog toga je također poznat i kao Hasseov princip) i njime po prvi put ukazao na važnost $p$-adskih brojeva. Ako polinomijalna jednadžba ima globalno rješenje u racionalnim brojevima tada ima i realno i $p$-adsko rješenje za svaki prost broj $p$. Drugim riječima, globalno rješenje daje lokalna rješenja svugdje. Lokalno-globalni princip je pitanje za kakve polinomijalne jednadžbe vrijedi obrat ove tvrdnje. U ovom diplomskom radu dokazati ćemo teorem Hasse-Minkowski koji nam kaže da lokalno globalni princip vrijedi za sve kvadratne forme. Točnije dokazati ćemo Hasse-Minkowski teorem za polje racionalnih brojeva $\mathbb{Q}$, s obzirom da je općeniti slučaj značajno teže dokazati, a nije značajnije poučniji. Važnost Hasse-Minkowski teorema je u tome što je dao novi model za odgovarnje na aritmetička pitanja. Da bi odredili da li kvadratna forma ima racionalna rješenja dovoljno je provjeriti ima li rješenja u skupu realnih i $p$-adskih brojeva, gdje se analitičke metode traženja riješenja (poput Newton-ove metode) primjenjuju.
Opišimo ukratko sadržaj ovog rada. U prvom poglavlju, pod nazivom Uvod u teoriju brojeva, definiramo osnove pojmove teorije brojeva, poput djeljivosti i kongruencija, te ćemo iskazati i dokazati neke osnovne teoreme iz teoriji brojeva. Posebnu pažnju posvetiti ćemo kvadratnim ostacima koji će nam biti potrebni za razumjevanje i dokazivanje pojedinih teoremu u nastavku rada. U drugom poglavlju, definiramo polje $p$-adskih brojeva, te dokazujemo Henselovu lemu. U trećem poglavlju koncentrirati ćemo se na kvadratne forme, posebice u slučaju $n = 3$ gdje uvodimo pojam Hilbertovih simbola koji će nam biti od posebne važnosti u dokazivanju teorema. U četvrtom, i završnom poglavlju, dati ćemo dokaz Hasse-Minkowski teorema za $\mathbb{Q}$. Dokaz uveliko ovisi o broju varijabli $n$ kvadratne forme, te ćemo posebno dokazivati za $n = 1, 2, 3, 4$ i $\geq 5$.

# Poglavlje 1

# Uvod u teoriju brojeva

## 1.1 Djeljivost i kongruencije

Djeljivost je fundamentalni pojam teorije brojeva. Dakle, neka su $a$ i $b$ cijeli brojevi, te neka je $a \neq 0$. Kažemo da je $b$ djeljiv s $a$, odnosno da $a$ dijeli $b$, ako postoji cijeli broj $x$ takav da je $b = ax$. To zapisujemo sa $a \mid b$. Ako $b$ nije djeljiv sa $a$, onda pišemo $a \nmid b$.
Neka su $b$ i $c$ cijeli brojevi. Cijeli broj $a$ koji dijeli oba broja $b$ i $c$ naziva se zajednički djelitelj brojeva $b$ i $c$. Ukoliko je barem jedan od brojeva $b$ i $c$ različit od nule, tada taj broj ima konačno mnogo djelitelja. U tom slučaju postoji i konačno mnogo zajedničkih djelitelja brojeva $b$ i $c$. Najvećeg od njih označavamo s $\mathrm{NZD}(b, c)$. Izraz $\mathrm{NZD}(b, c)$ nazivamo najveći zajednički djelitelj brojeva $b$ i $c$. Slično se defnira i najveći zajednički djelitelj cijelih brojeva $a_1, a_2, \ldots, a_n$ (od kojih je barem jedan različit od nule), koji se označava s $\mathrm{NZD}(a_1, a_2, \ldots, a_n)$. Primijetimo da je $\mathrm{NZD}(b, c)$ uvijek prirodan broj.
Prirodan broj $n$, $n > 1$, nazivamo prostim ukoliko nema niti jednog djelitelja $d$ za koji vrijedi $1 < d < n$. Broj koji nije prost naziva se složen. Primijetimo kako su jedini pozitivni djelitelji prostog broja $p$ brojevi 1 i $p$. Za cijele brojeve $a$ i $b$ kažemo da su relativno prosti ukoliko je $\mathrm{NZD}(a, b) = 1$. Slično, za brojeve $a_1, a_2, \ldots, a_n$ kažemo da su relativno prosti ukoliko je $\mathrm{NZD}(a_1, a_2, \ldots, a_n) = 1$.

**Teorem 1.1.1.** *Svaki prirodan broj $n > 1$ može se prikazati kao produkt prostih brojeva (s jednim ili više faktora).*

*Dokaz.* Teorem ćemo dokazati matematičkom indukcijom. Broj 2 je prost. Pretpostavimo sada da neki $n > 2$, tvrdnja teorema vrijedi za sve $m$ takve da $2 \leq m < n$. Želimo dokazati da se i $n$ može prikazati kao produkt prostih faktora. Ako je n prost, tvrdnja vrijedi. Ako $n$ nije prost broj tada $n = n_1 n_2$, gdje je $1 < n_1 < n$ i $1 < n_2 < n$. Po pretpostavci indukcije $n_1$ i $n_2$ se mogu prikazati kao produkt prostih broja stoga to vrijedi i za $n$. □

Iz ovoga vidimo da se svaki prirodan broj $n$ možemo zapisati u obliku

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

gdje su $p_1, \ldots, p_k$ prosti brojevi a $\alpha_1, \ldots, \alpha_k$ prirodni brojevi. Lako se dokaže da je taj zapis jedinstven do na poredak prostih faktora.

**Teorem 1.1.2.** *(Euklid) Skup svih prostih brojeva je beskonačan.*

*Dokaz.* Pretpostavimo da su $p_1, p_2, ..., p_k$ svi prosti brojevi. Promotrimo broj $n = 1 + p_1 p_2 \cdots p_k$. Uočimo da $n$ nije djeljiv niti s jednim od brojeva $p1, p_1, \ldots, p_k$. Dakle, svaki prosti faktor $p$ od $n$ je različit od $p_1, \ldots, p_k$. Budući da je $n$ ili prost ili ima prosti faktor, dobili smo prost broj različit od $p_1, \ldots, p_k$, što je kontradikcija. □

**Definicija 1.1.3.** *Ako cijeli broj $m \neq 0$ dijeli razliku $a-b$, onda kažemo da je $a$ kongruentan $b$ modulo $m$ i pišemo $a \equiv b \pmod{m}$. U protivnom, kažemo da $a$ nije kongruentan $b$ modulo $m$ i pišemo $a \not\equiv b \pmod{m}$.*

**Propozicija 1.1.4.** *Relacija biti kongruentan modulo $m$ je relacija ekvivalencije na skupu $\mathbb{Z}$.*

*Dokaz.* Trebamo dokazati da vrijedi refleksivnost, simetričnost i tranzitivnost. Reflektivnost slijedi iz činjenice da $m \mid 0$ pa $a \equiv a \pmod{m}$. Neka je $a \equiv b \pmod{m}$. Tada postoji $k \in \mathbb{Z}$ takav da $a - b = km$, pa $b - a = (-k)m$ pa vidimo da i $b \equiv a \pmod{m}$ čime smo dokazali simetričnost. Neka je $a \equiv b \pmod{m}$ i $b \equiv c \pmod{m}$. Iz toga nam slijedi da postoje $k, l \in \mathbb{Z}$ takvi da $a - b = km$ i $b - c = lm$. Zbrajanjem dobijemo $a - c = (k + l)m$ pa $a \equiv c \pmod{m}$ čime smo dokazali i tranzitivost. □

**Definicija 1.1.5.** *Skup $\{x_1, \ldots, x_m\}$ zove se potpuni sustav ostataka modulo $m$ ako za svaki $y \in \mathbb{Z}$ postoji točno jedan $x_i$ takav da je $y \equiv x_i \pmod{m}$. Drugim riječima, potpuni sustav ostataka dobivamo tako da iz svake klase ekvivalencije modulo $m$ uzmemo po jedan član.*

Za $m \in \mathbb{Z}$ označimo s $\overline{x}^m$ (ili s $\overline{x}$) klasu ekvivalencije modulo m za $x \in \mathbb{Z}$.

**Teorem 1.1.6.** *(Dirichletov teorem). Neka su $a$ i $m$ relativno prosti pozitivni cijeli brojevi, tada postoji beskonačno mnogo prostih brojeva koji su kongrunetni s $a$ modulo $m$. Drugim riječima, svaka klasa ostataka mudulo $m$ koja se sastoji od brojeva relativno prostih s $m$ sadrži beskonačno mnogo prostih brojeva.*

Dokaz se može naći u [7].

**Propozicija 1.1.7.** *Neka su $a$, $b$, $c$ i $d$ cijeli brojevi.*

**(1)** *Ako je* $a \equiv b \pmod m$ *i* $c \equiv d \pmod m$*, tada vrijedi i* $a + c \equiv b + d \pmod m$*,* $a - c \equiv b - d \pmod m$*,* $ac \equiv b \pmod m$*.*

**(2)** *Ako je* $a \equiv b \pmod m$ *i* $d \mid m$ *tada* $a \equiv b \pmod d$*.*

**(3)** *Ako* $a \equiv b \pmod m$*, tada je* $ac \equiv bc \pmod{mc}$ *za svaki* $c \neq 0$*.*

*Dokaz.* (1) Neka je $a - b = mk$ i $c - d = ml$. Tada je $(a + c) - (b + d) = m(k + l)$ i $(a - c) - (b - d) = m(k - l)$, pa je $a + c \equiv b + d \pmod m$ i $a - c \equiv b - d \pmod m$. Zbog $ac - bd = a(c - d) + d(a - b) = m(al + dk)$s slijedi da je $ac \equiv bd \pmod m$. (2) Neka je $m = de$. Tada iz $a - b = mk$ slijedi $a - b = d \cdot (ek)$, pa je $a \equiv b \pmod d$. (3) Iz $a - b = mk$ slijedi $ac - bc = (mc) \cdot k$, pa je $ac \equiv bc \pmod{mc}$. □

**Propozicija 1.1.8.** *Neka je* $f$ *polinom s cjelobrojnim koeficijentima. Ako je* $a \equiv b \pmod m$*, onda je* $f(a) \equiv f(b) = \pmod m$*.*

*Dokaz.* Neka je $f(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_0$, gdje su za svaki $i = 0, \ldots, n$ $c_i \in \mathbb{Z}$. Iz $a \equiv b \pmod m$, uzastopnom primjeno propozicije 1.1.7(1) dobijemo $a^2 \equiv b^2 \pmod m$, $a^3 \equiv b^3 \pmod m, \ldots,$ $a^n \equiv b^n \pmod m$. Tada je i $c_i a^i \equiv c_i b^i \pmod m$ pa konačno

$$c_n a^n + c_{n-1}a^{n-1} + \cdots + c_0 \equiv c_n b^n + c_{n-1}b^{n-1} + \cdots + c_0 \pmod m.$$

□

**Propozicija 1.1.9.** *Vrijedi da je* $ax \equiv ay \pmod m$ *ako i samo ako* $x \equiv y \pmod{\frac{m}{NZD(a,m)}}$*. Specijalno, u slučaju da su* $a$ *i* $m$ *relativno prosti tada je* $ax \equiv ay \pmod m$ *ako i samo ako* $x \equiv y \pmod m$*.*

*Dokaz.* Ako je $ax \equiv ay \pmod m$, tada postoji $z \in \mathbb{Z}$ takav da vrijedi $ax - ay = zm$. Dijeleći s NZD$(m, a)$ dobijemo $\frac{a}{NZD(a,m)}(x - y) = \frac{mz}{NZD(a,m)}$ tj. $\frac{m}{NZD(a,m)}$ dijeli $\frac{a}{NZD(a,m)}(x - y) = \frac{mz}{NZD(a,m)}$. S obzirom da su $\frac{a}{NZD(a,m)}$ i $\frac{m}{NZD(a,m)}$ relativno prosti vidimo da $\frac{m}{NZD(a,m)}$ dijeli $x - y$ pa $x \equiv a \pmod{\frac{m}{NZD(a,m)}}$. Obratno, ako je $x \equiv y \pmod{\frac{m}{NZD(a,m)}}$, tada prema propoziciji 1.1.7 (3) dobijemo $ax \equiv ay \pmod{\frac{am}{NZD(a,m)}}$, pa zbog toga što $a \mid NZD(a, m)$ prema propoziciji 1.1.7 (2) $ax \equiv ay \pmod m$. □

**Propozicija 1.1.10.** *Neka je* $\{x_1, \ldots, x_m\}$ *potpuni sustav ostataka modulo m, te neka je* $NZD(a, m) = 1$*. Tada je* $\{ax_1, \ldots, ax_m\}$ *takoder potpuni sustav ostataka modulo m.*

*Dokaz.* Dovoljno je dokazati da je $ax_i \not\equiv ax_j \pmod m$ za $i \neq j$. Pretpostavimo da je $ax_i \equiv ax_j \pmod m$, tada propozicija 1.1.9 povlači da je $x_i \equiv x_j \pmod m$, tj. $i = j$. □

**Definicija 1.1.11.** *Reducirani sustav ostataka modulo m je skup cijelih brojeva $r_i$ sa svojstvom da je NZD$(r_i, m) = 1, r_i \not\equiv r_j \pmod m$ za $i \neq j$, te da za svaki cijeli broj $x$ takav da je NZD$(x, m) = 1$ postoji $r_i$ takav da je $x \equiv r_i \pmod m$. Jedan reducirani sustav ostataka modulo m je skup svih brojeva $a \in \{1, 2, \ldots, m\}$ takvih da je NZD$(a, m) = 1$. Jasno je da svi reducirani sustavi ostataka modulo m imaju isti broj elemenata. Taj broj označavamo s $\varphi(m)$, a funkciju $\varphi$ zovemo Eulerova funkcija. Drugim riječima, $\varphi(m)$ je broj brojeva u nizu $1, 2, \ldots, m$ koji su relativno prosti sa m.*

Primjetimo da ako je $p$ prost broj tada je reuducirani sustav ostataka jednak potpunom sustavu ostataka i $\varphi(p) = p - 1$.

**Napomena 1.1.12.** *Prsten $\mathbb{Z}/m\mathbb{Z} = \{\overline{x}; x \in \mathbb{Z}\} = \{\overline{01}, \overline{2}, \ldots, \overline{m-1}\}$ zovemo prsten ostataka modulo m. Zbrajanje je definirano se $\overline{x} + \overline{y} = \overline{x+y}$, a množenje s $\overline{xy} = \overline{x+y}$, te se lako vidi da je neutralni element za zbrajanje 0, za množenje 1. Primjetimo da bi $a \in \mathbb{Z}/m\mathbb{Z}$ bio invertibilan mora vrijediti da je NZD$(a, m) = 1$. U suprotnome pretpostavimo da postoji k koji dijeli i a i m, pa možemo pisati $a = kx$ i $m = ky$ za neke $x, y \in \mathbb{Z}$. Za inverz $a^{-1}$ moralo bi vrijediti $aa^{-1} \equiv 1 \pmod m$ tj. postoji $l \in \mathbb{Z}$ takav da $aa^{-1} - 1 = ml$, a to vrijedi ako i samo ako $kxa^{-1} = kyl - 1$. S obzirom da je lijeva strana jednakosti djeliva s k a desna nije vidimo da takav $a^{-1}$ ne postoji. Skup invertibilnih elemenata označavati ćemo s $(\mathbb{Z}/m\mathbb{Z})^\times$, i primjetimo $|\ (\mathbb{Z}/m\mathbb{Z})^\times\ | = \varphi(m)$.*

**Teorem 1.1.13.** *(Eulerov teorem). Ako je NZD$(a, m) = 1$, onda je $a^{\varphi(m)} \equiv 1 \pmod m$.*

*Dokaz.* Neka je $\{r_1, r_2, \ldots, r_{\varphi(m)}\}$ reducirani sustav ostataka modulo $m$. Iz propozicije 1.1.10 lako možemo zaključiti da je i $\{ar_1, ar_2, \ldots, ar_{\varphi(m)}\}$ reducirani sustav ostataka modulo $m$, pa zaključujemo da je

$$\prod_{j=1}^{\varphi(m)} (ar_j) \equiv \prod_{i=1}^{\varphi(m)} r_i \pmod m,$$

odnosno,

$$a^{\varphi(m)} \prod_{j=1}^{\varphi(m)} r_j \equiv \prod_{i=1}^{\varphi(m)} r_i \pmod m.$$

Zbog NZD$(r_i, m) = 1$, primjenom propozicije 1.1.9 dobijemo $a^{\varphi(m)} \equiv 1 \pmod m$. □

**Teorem 1.1.14.** *(Mali Fermatov teorem). Neka je p prost broj. Ako $p \nmid a$, onda je $a^{p-1} \equiv 1$ **(mod** p). Za svaki cijeli broj a vrijedi $a^p \equiv a \pmod p$.*

*Dokaz.* $p$ je prost broj pa $\varphi(p) = p - 1$ te tvrdnja slijedi iz Eulerovog teorema. □

**Teorem 1.1.15.** *(Wilson) Ako je p prost broj, onda je $(p-1)! \equiv -1 \pmod p$.*

*Dokaz.* Za $p = 2$ i $p = 3$ kongruencija je očito zadovoljena. Stoga smijemo pretpostaviti da je $p \geq 5$. Grupirajmo članove skupa $\{2, 3, \ldots, p-2\}$ u parove $(i, j)$ sa svojstvom $ij \equiv 1 \pmod{p}$. Očito je $i \neq j$ jer bi inače broj $(i-1)(i+1)$ bio djeljiv sa $p$, a to je nemoguće zbog $0 < i - 1 < i + 1 < p$. Tako dobivamo $\frac{p-3}{2}$ parova i ako pomnožimo odgovarajućih $\frac{p-3}{2}$ kongruencija, dobit ćemo $2 \cdot 3 \cdots (p-2) \equiv 1 \pmod{p}$, pa je

$$(p-1)! \equiv 1 \cdot 1 \cdot (p-1) \equiv -1 \pmod{p}$$

. □

**Teorem 1.1.16.** *(Kineski teorem o ostatcima). Neka su $m_1, m_2, \ldots, m_k$ u parovima relativno prosti, te neka su $a_1, a_2, \ldots, a_k$ cijeli brojevi. Tada sustav kongruencija*

$$x \equiv a_1 \ (mod\ m_1),\ x \equiv a_2 \ (mod\ m_2), \ldots,\ x \equiv a_k \ (mod\ m_k) \tag{1.1}$$

*ima riješenja. Ako je $x_0$ jedno rješenje, onda su sva rješenja dana sa $x \equiv x_0 \ (mod\ m_1 m_2 \cdots m_k)$.*

*Dokaz.* Neka je $m = m_1 m_2 \cdots m_k$, te neka je $n_i = \frac{m}{m_i}$ za $i = 1, 2, \ldots, k$. Tada je $\text{NZD}(n_i, m_i) = 1$ pa postoji cijeli broj $x_i$ takav da je $n_i x_i \equiv a_i \pmod{m_i}$. Promotrimo sada broj $x_0 = n_1 x_1 + \cdots + n_k x_k$. Vidimo da vrijedi $x_0 \equiv 0 + \cdots + 0 + n_i x_i + 0 + \cdots + 0 \equiv a_i \pmod{m_i}$ pa je $x_0$ rješenje od (1.1).
Ako su $x$ i $y$ dva rješenja od (1.1), tada je $x \equiv y \pmod{m_i}$ za $i = 1, \ldots, k$ pa jer su $m_i$ u parovima relativno prosti dobijemmo $x \equiv y \pmod{m}$. □

## 1.2 Kvadratni ostatci

**Definicija 1.2.1.** *Neka je $(a, m) = 1$. Ako kongruencija $x^2 \equiv a \ (mod\ m)$ ima rješenja, onda kažemo da je a kvadratni ostatak modulo m. U protivnom kažemo da je a kvadratni neostatak modulo m.*

**Definicija 1.2.2.** *Neka je p neparan prost broj. Legendreov simbol $\left(\frac{a}{p}\right)$ defniran je s*

$$\left(\frac{a}{p}\right) = \begin{cases} 1\,, & \text{ako je } a \text{ kvadratni ostatak modulo } p, \\ 0\,, & \text{ako } a \mid p, \\ -1\,, & \text{ako je } a \text{ kvadratni neostatak modulo } p. \end{cases}$$

**Teorem 1.2.3.** *(Eulerov kriterij)*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \ (mod\ p)$$

*Dokaz.* Ako je $\left(\frac{a}{p}\right) = 0$, onda $p \mid q$ pa tvrdnja očito vrijedi. Ako je $\left(\frac{a}{p}\right) = 1$, onda postoji $x_0 \in \mathbb{Z}$ takav da $x_0 \equiv a \pmod{p}$. Sada iz Malog Fermatovog teorema vidimo da vrijedi $a^{\frac{p-1}{2}} \equiv x_0^{p-1} \equiv 1 \equiv \left(\frac{a}{p}\right) \pmod{p}$. Neka je $\left(\frac{a}{p}\right) = -1$. Za svaki $i \in \{1, \ldots, p-1\}$ odaberemo $j \in \{1, \ldots, p-1\}$ tako da vrijedi $ij \equiv a \pmod{p}$ (po propoziciji 1.1.10 znamo da možemo odabrati takve $i$ i $j$). Primjetimo da je $i \neq j$, budući da kongruencija $x^2 \equiv a \pmod{p}$ nema rješenja. Dakle, skup $\{1, \ldots, p-1\}$ se raspada na $\frac{p-1}{2}$ parova $(i, j)$ za koje vrijedi $ij \equiv a \pmod{p}$. Množenjem ovih $\frac{p-1}{2}$ kongruencija, te koristeći Wilsonov teorem, dobivamo

$$a^{\frac{p-1}{2}} \equiv (p-1)! \equiv -1 \pmod{p}.$$

□

**Propozicija 1.2.4.** *Za Legendreov simbol vrijede slijedeće tvrdnje:*

**(1)** *Ako je $a \equiv b \pmod{p}$, onda je $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.*

**(2)** *Legendreov simbol je bilinearan, tj. vrijedi $\left(\frac{a}{p}\right)\left(\frac{ab}{p}\right) = \left(\frac{ab}{p}\right)$.*

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

**(4)** $\left(\frac{1}{p}\right) = 1$, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

*Dokaz.* (1) Ako je $a \equiv b \pmod{p}$, tada kongruencija $x^2 \equiv a \pmod{p}$ ima rješenja ako i samo ako kongruencija $x^2 \equiv b \pmod{p}$ ima rješenja. (2) Iz

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv (ab)^{\frac{p-1}{2}} \equiv \left(\frac{ab}{p}\right) \pmod{p}$$

slijedi $\left(\frac{a}{p}\right)\left(\frac{ab}{p}\right) = \left(\frac{ab}{p}\right)$.
(3) Kongruencija $x^2 \equiv a^2 \pmod{p}$ očito ima rješenje za $x = a$. I naposljetku, prva tvrdnja od (4) je poseban slučaj tvrdnje (3), a druga slijedi uvrštavanjem $a = -1$, u Eulerov kriterij.
□

**Lema 1.2.5.** *Neka su $p$ i $q$ međusobno različiti prosti brojevi. Tada je*

$$\prod_{1 \leq x \leq \frac{pq-1}{2}; x \in (\mathbb{Z}/pq\mathbb{Z})^\times} x \equiv (-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) \text{ (mod } p)$$

*i*

$$\prod_{1 \leq x \leq \frac{pq-1}{2}; x \in (\mathbb{Z}/pq\mathbb{Z})^\times} x \equiv (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) \text{ (mod } q).$$

*Dokaz.* Promotrimo invertibilne elemente modulo $pq$, to su upravo oni elementi koji nisu djeljivi niti s $p$ niti s $q$. Skup invertibilnih elementa $x$ koji se nalaze u $\{1, 2, \ldots, \frac{pq-1}{2}\}$, promatran s modulo $p$ sastoji se od $\frac{q-1}{2}$ nizova $1, 2, \ldots, p-1$ te niza $1, 2, \ldots, \frac{p-1}{2}$, gdje još trebamo isključiti niz $q, 2q, \ldots, \frac{p-1}{2}q$ koji se sastoji od višekratnika broja $q$. Na taj način dobivamo

$$\prod_{1\leq x\leq \frac{pq-1}{2}; x\in(\mathbb{Z}/pq\mathbb{Z})^\times} x \equiv (p-1)!^{\frac{q-1}{2}} \left(\frac{p-1}{2}\right)! \Big/ q^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv (-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) \pmod{p},$$

jer se $\left(\frac{p-1}{2}\right)!$ pokrati, $(p-1)! \equiv -1 \pmod{p}$ prema Wilsonovu teoremu te $q^{\frac{p-1}{2}} \equiv \left(\frac{q}{p}\right) \pmod{p}$ prema Eulerovu kriteriju. Na isti način dobijemo i drugu jednadžbu. □

**Teorem 1.2.6.** *(Kvadratni zakon reciprociteta) Neka su p i q različiti neparni prosti brojevi. Tada vrijedi*

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

*Dokaz.* Pokažimo produkte

$$\prod_{1\leq x\leq \frac{pq-1}{2}; x\in(\mathbb{Z}/pq\mathbb{Z})^\times} x \pmod{p} \; i \prod_{1\leq x\leq \frac{pq-1}{2}; x\in(\mathbb{Z}/pq\mathbb{Z})^\times} x \pmod{q}$$

iz prethodne leme samo pomoći potencija od $-1$. Primijetimo da za svaki $x \in \{1, 2, \ldots, pq-1\}$ točno jedan element skupa $\{x, -x\} \pmod{pq}$ pojavljuje u nizu $1, 2, \ldots, \frac{pq-1}{2}$. Prema tome, među dgovarajućim uređenim parovima ostataka $(a, b) = (x \bmod p, x \bmod q$ pojavljuje se točno jedan od parova $(a, b)$, $(-a, -b)$. Točno po jedan od svakog mogućeg para ostataka $(\bmod p, \bmod q)$ dobivamo uzimajući $1 \leq a \leq p-1$ i $1 \leq b \leq \frac{q-1}{2}$. Na taj način dobijemo

$$\prod_{1\leq x\leq \frac{pq-1}{2}; x\in(\mathbb{Z}/pq\mathbb{Z})^\times} (x, x) \equiv \pm\Big((p-1)!^{\frac{q-1}{2}}, ((q-1)/2)!^{p-1}\Big) \pmod{p, \bmod q} \tag{1.2}$$

jer se svaki $a \in \{1, 2, \ldots, p-1\}$ pojavljuje u točno $\frac{q-1}{2}$ parova, dok se svaki $b \in \{1, 2, \ldots, \frac{q-1}{2}\}$ pojavljuje u točno $p-1$ parova. Pomoću Wilsonovog teorema potencije faktorijela koje se pojavljuju u (1.2) prikazati kao potencije od $-1$. Kako je $(p-1)! \equiv -1 \pmod{p}$, prva komponenta je kongruentna s $(-1)^{\frac{q-1}{2}}$ modulo $p$. Kako bi prikazali i drugu komponentu u obliku potencije od $-1$, primijetimo da vrijedi

$$\begin{aligned} -1 &\equiv (q-1)! \pmod{q} \\ &\equiv 1 \cdot 2 \cdots (q-1)/2 \cdot (-(q-1)/2) \cdots (-2) \cdot (-1) \pmod{q} \\ &\equiv ((q-1)/2)!^2 (-1)^{\frac{q-1}{2}} \pmod{q}. \end{aligned}$$

Prema tome je $((q-1)/2)!^2 \equiv (-1)(-1)^{\frac{q-1}{2}} \pmod{q}$. Potenciranjem dobivamo

$$((q-1)/2)!^{p-1} \equiv (-1)^{\frac{p-1}{2}}(-1)^{\frac{q-1}{2}\cdot\frac{p-1}{2}} \pmod{q}$$

pa kongruencija (1.2) prelazu u

$$\prod_{1\leq x\leq \frac{pq-1}{2}; x\in(\mathbb{Z}/pq\mathbb{Z})^\times} (x,x) \equiv \pm((-1)^{\frac{q-1}{2}}, (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}) \pmod{p, \text{mod } q}. \tag{1.3}$$

Sada izjednačavanjem kongruencije (1.3) i kongruencija iz leme 1.2.5 dobijemo da vrijedi jedan od sljedeća dva slučaja

- $\left(\frac{q}{p}\right) = 1$ i $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$
- $\left(\frac{q}{p}\right) = -1$ i $\left(\frac{p}{q}\right) = -(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$

pa u oba slučaja vrijedi $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$. □

# Poglavlje 2

# $p$-adski brojevi

## 2.1 Polje $p$-adskih cijelih brojeva

**Definicija 2.1.1.** *Neka je $p$ neki prost broj. Niz cijelih brojeva $\{x_n\} = \{x_1, x_2, \ldots, x_n, \ldots\}$ koji zadovoljava*

$$x_n \equiv x_{n-1} \ (mod\ p^n)$$

*za sve $n \geq 1$, određuje objekt koji zovemo p-adski cijeli broj. Skup svih p-adskih cijelih brojeva označavamo s $\mathbb{Z}_p$.*
*Dva niza $\{x_n\}$ i $\{x'_n\}$ određuju isti p-adski cijeli broj ako i samo ako je*

$$x_n \equiv x'_n \ (mod\ p^{n+1}) \text{ za sve } n \geq 0.$$

Ako niz $\{x_n\}$ odruđeuje $p$-adski broj $\alpha$, pisat ćemo $\{x_n\} \to \alpha$.

**Definicija 2.1.2.** *Neka su $\alpha$ i $\beta$ p-adski cijeli brojevi određeni nizovima $\{x_n\} \to \alpha$ i $\{y_n\} \to \beta$. Tada suma (produkt) od $\alpha$ i $\beta$ je p-adski cijeli broj određen nizom $\{x_n + y_n\}$ ($\{x_n \cdot y_n\}$).*

**Napomena 2.1.3.** *Lako je provjeriti da $\{x_n + y_n\}$ i $\{x_n \cdot y_n\}$ određuju neki p-adski cijeli broj i da on ovisi samo o $\alpha$ i $\beta$, a ne o izboru nizova koji ih određuju. S ovim operacijama skup p-adskih cijelih brojeva $\mathbb{Z}_p$ postaje komutativni prsten. Djeljivost p-adskih cijelih brojeva definirana je kao u bilo kojem komutativnom prstenu, tj. $\alpha$ dijeli $\beta$ ako postoji p-adski cijeli broj $\gamma$ takav da $\beta = \alpha \cdot \gamma$. Također lako ze vidi da je neutralni element za zbajanje $\{0, 0, \ldots\} \to 0$, a za množenje $\{1, 1, \ldots\} \to 1$. Od posebnog interesa su nam p-adski brojevi koji imaju multiplikativni inverz. Takve brojeve zvati ćemo p-adske **jedinice**. Skup svih p-adskih jedinica ozančavat ćemo s $\mathbb{Z}_p^\times$.*

**Propozicija 2.1.4.** *Element $\alpha \in \mathbb{Z}_p$ je jedinica ako i samo ako $\alpha$ nije djeljiv s p, tj. $x \notin p\mathbb{Z}_p$. Drugim riječima, $\mathbb{Z}_p^\times$ je $\mathbb{Z}/p\mathbb{Z}_p$.*

*Dokaz.* Ako je $\{a_n\} \to \alpha \in \mathbb{Z}_p$ dijeljiv s $p$, tada je $a_1 = 0$, pa $\alpha$ očito nemože biti invertibilan.
Ako $\alpha$ nije dijeljiv s $p$ tada $a_1 \neq 0$. Iz definicije lagano slijedi da $a_n \equiv a_{n-1} \equiv \cdots \equiv a_0 \pmod{p}$, tako da $a_n \not\equiv 0 \pmod{p}$. Sada za bilo koji $n$ možemo naći $b_n$ takav da $a_n b_n \equiv 1 \pmod{p}$. Kako $a_n \equiv a_{n-1} \pmod{p^n}$ i $a_n b_n \equiv a_{n-1} b_{n-1} \pmod{p^n}$ tada je također $b_n \equiv b_{n-1} \pmod{p^n}$ pa vrijedi da $\{b_n\} \to \beta \in \mathbb{Z}_p$. Stoga, $\alpha\beta = 1$, tj. $\beta$ je inverz od $\alpha$ pa je $\alpha$ jedinica. S obzirom da je množenje komutativno vidimo da je i $\alpha$ inverz od $\beta$ pa je i $\beta$ p-adska jedinica. □

**Propozicija 2.1.5.** *Svaki element $\alpha \in \mathbb{Z}_p$ može se na jedinstveni način zapisati kao $p^n u$, gdje je $u \in \mathbb{Z}_p^\times$.*

*Dokaz.* Ako je $\alpha$ jedinica tada za $n = 0$ propozicija vrijedi. Neka je $\{a_n\} \to \alpha \neq 0$ gdje $\alpha$ nije jedinica, pa prema prethodnoj propoziciji $\alpha$ je dijeljiv s $p$ i postoji barem jedan $n$ takav da $a_n = 0$ ($a_1 = 0$). Zbog $\alpha \neq 0$ možemo pronaći najveći $n$ za koji $a_n = 0$. Za taj $n$ vrijedi da $\alpha \equiv 0 \pmod{p^n}$ pa postoji $u \in \mathbb{Z}_p$ takav da je $\alpha = p^n u$. Dokažimo još da je $u$ jedinica. U slučaju da $u$ nije jedinica, tada po prethodnoj propoziciji je $u$ djeljiv s $p$, pa je $a = p^{n+1}$ iz čega nam slijedi da je $a_{n+1} = 0$ što je u kontradikciji s pretpostavkom da $n$ najveći indeks za koji $a_n = 0$.
Dokažimo sad i jedinstvenost zapisa. Pretpostavimo $p^n u_1 = p_2^u$. Ako je $m = n$, tada zbog injektivnosti množenja vrijedi i $u_1 = u_2$. U suprotnom, bez smanjenja općenitosti možemo pretpostaviti $n > m$. Tada je $u_2 = p^{n-m} u_1$, pa prema prethodnoj propoziciji $u_2$ nije jedinica, što je u kontradikcji s pretpostavkom propozicije. □

**Definicija 2.1.6.** *Za svaki $0 \neq a \in \mathbb{Z}_p$, p-adska valuacija od a, s oznakom $v_p(a)$ je najveći cijeli broj n za koji je a u $p^n\mathbb{Z}_p$. Ekvivalentno $v_p(a)$ je za $a = \sum_{i=0}^{\infty} b_i p^i$ najmanji prirodan broj n takav da je $b_m \neq 0$. Također ekvivalentno, ako zapišemo $a = p^n u$, gdje je $u \in \mathbb{Z}_p^\times$, tada je $v_p(a) = m$. Definiramo $v_p(0) = +\infty$.*

## 2.2 Polje $p$-adskih brojeva

Polje razlomka nekog prstena $R$ definira se kao skup uređenih parova $(a, b) \in R^2$, koje se obično zapisuje $\frac{a}{b}$ gdje vrijedi da je $\frac{a}{b} = \frac{c}{d}$ ako vrijedi $ad = bc$.

**Definicija 2.2.1.** *Polje p-adskih brojeva $\mathbb{Q}_p$ je polje razlomaka od $\mathbb{Z}_p$.*

Za $a \in \mathbb{Q}_p$ po definiciji vrijedi $a = \frac{p^n u_1}{p^m u_2} = p^{n-m} u_1 u_2^{-1}$, pa možemo svaki element iz $\mathbb{Q}_p$ zapisati kao $up^k$ za $u \in \mathbb{Z}_p^\times$, $k \in \mathbb{Z}$. Sada možemo proširiti definiciju od $v_p$ na $\mathbb{Q}_p$ tako da za $a = up^k$, $u \in \mathbb{Z}_p^\times$, $k \in \mathbb{Z}$ vrijedi $v_p(up^k) = k$, te je kao i prije $v_p(0) = +\infty$. Primjetimo da je $\mathbb{Z}_p \subset \mathbb{Q}_p$, tj. $\mathbb{Z}_p = \{a \in \mathbb{Q}_p | v_p(a) \geq 0\}$.

Postoji i drugi način definiranja polja $\mathbb{Q}_p$ pomoću apsolutnih vrijednosti.

**Definicija 2.2.2.** *Neka je K polje. Aposolutna vrijednost na K je funkcija* $\| \| : K \to R_{\geq 0}$ *sa sljedećim svojstvima:*

**(1)** $\|x\| = 0$ *ako i samo ako je* $x = 0$*,*

**(2)** $\|xy\| = \|x\| \cdot \|y\|$*,*

**(3)** $\|x + y\| \leq \|x\| + \|y\|$*.*

**Definicija 2.2.3.** *Definiramo p-adsku apsolutnu vrijednost* $| \, |_p$ *na* $\mathbb{Q}_p$ *s*

$$|x|_p = p^{v_p(x)}.$$

**Napomena 2.2.4.** *Primjetimo da pošto je* $\mathbb{Q} \subset \mathbb{Q}_p$*, ovo daje definiciju apsolutne vrijednosti* $| \, |_p$ *na* $\mathbb{Q}$*. Drugi način definiranja polja* $\mathbb{Q}_p$ *je da definiramo* $\mathbb{Q}_p$ *kao upotpunjenje od* $\mathbb{Q}$ *(tj.* $\mathbb{Q}$ *skupa sa svim limesima nizova iz* $\mathbb{Q}$*) s obzirom na aposolutnu vrijednost* $| \, |_p$*. U tom slulaju* $\mathbb{Z}_p$ *definira se kao*

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\},$$

*ili kao upotpunjenje od* $\mathbb{Z}$ *s obzirom na* $| \, |_p$*.*

## 2.3 Henselova lema

**Lema 2.3.1.** *(Henselova lema) Neka je* $F(x_1, \ldots, x_n)$ *polinom s koeficijentima iz* $\mathbb{Z}_p$*. Neka su* $\gamma_1, \ldots, \gamma_n \in \mathbb{Z}_p$ *takvi da za neki i* $(1 \leq i \leq n)$ *vrijedi*

$$F(\gamma_1, \ldots, \gamma_n) \equiv 0 \ (mod\ p),$$
$$\frac{\partial F}{\partial x_i}(\gamma_1, \ldots, \gamma_n) \not\equiv 0 \ (mod\ p),$$

*tada postoje* $\theta_1, \ldots, \theta_n \in \mathbb{Z}_p$ *takvi da*

$$F(\theta_1, \ldots, \theta_n) = 0$$

*i*

$$\theta_i \equiv \gamma_i \ (mod\ p) \ za\ i = 1, \ldots, n.$$

*Dokaz.* Promotrimo polinom u varijabli $x$, $f(x) = F(\gamma_1, \ldots, \gamma_{i-1}, x, \gamma_{i+1}, \ldots, \gamma_n)$. Naći ćemo $\alpha \in \mathbb{Z}_p$ takav da $f(\alpha) = 0$ i $\alpha \equiv \gamma_i \pmod{p}$. Tada ćemo definirati $\theta_j = \gamma_j$ za $i \neq j$ i $\theta_i = \alpha$. Lako se vidi da je ovo dovoljno da se dokaže lema.
Neka je $\gamma_i = \gamma$. Konstruirajmo niz u $\mathbb{Z}_p$

$$\alpha_0, \alpha_1, \ldots, \alpha_m, \ldots$$

kongruentan s $\gamma$ modulo $p$ takav da

$$f(\alpha_m) \equiv 0 \pmod{p^{m+1}}$$

za svaki $m > 0$. Za $m = 0$, uzmimo $\alpha_0 = \gamma$. Konstrukciju niza napraviti ćemo indukcijski. pretpostavimo da je za neki $m \geq 1$, $\alpha_0, \ldots, \alpha_{m-1}$ već određen. Tada $\alpha_{m-1} \equiv \gamma \pmod{p}$ i $f(\alpha_{m-1}) \equiv 0 \pmod{p^m}$. Razvijmo polinom $f(x)$ po potencijama od $x - \alpha_{m-1}$:

$$f(x) = \beta_0 + \beta_1 \cdot (x - \alpha_{m-1}) + \beta_2 \cdot (x - \alpha_{m-1})^2 + \ldots \quad , (\beta_i \in \mathbb{Z}_p).$$

Po pretpostavci indukcije $\beta_0 = f(\alpha_{m-1}) = p^m A$, gdje je $A \in \mathbb{Z}_p$. Dalje, kako je $\alpha_{m-1} \equiv \gamma \pmod{p}$ i $\frac{\partial F}{\partial x_i}(\gamma_1, \ldots, \gamma_n) \not\equiv 0 \pmod{p}$ onda je $\beta_1 = f'(\alpha_{m-1}) = B$, gdje je $B \in \mathbb{Z}_p$ i nije djeljiv s $p$. Stavljajući $x = \alpha_{m-1} + \xi p^m$ dobivamo

$$f(\alpha_{m-1} + \xi p^m) = p^m(A + B\xi) + \beta_2 p^{2m\xi^2} + \ldots \quad .$$

S obizirom da je $B \not\equiv 0 \pmod{p}$ možemo izabrati $\xi_0 = \xi \in \mathbb{Z}_p$ takav da je $A + B\xi \equiv 0 \pmod{p}$. Nadalje, zbog $km > m + 1$ za $k \geq 2$ dobivamo

$$f(\alpha_{m-1} + \xi_0 p^m) \equiv 0 \pmod{p^m + 1}.$$

Prema tome, možemo staviti $\alpha_m = \alpha_{m+1} + \xi_0 p^m$. Kako je $m > 1$ vidimo da $\alpha_m \equiv \gamma \pmod{p}$. Po našoj konstrukciji $v_p(\alpha_m - \alpha_{m-1}) \geq m$ pa niz $\alpha_0, \alpha_1, \ldots, \alpha_m, \ldots$ konvergira. Označimo njegov limes s $\alpha$. Jasno, $\alpha \equiv \gamma \pmod{p}$. Iz $f(a_m) \equiv 0 \pmod{p^{m+1}}$ slijedi $\lim_{m\to\infty} f(a_m) = 0$. Prema tome $f(\alpha) = 0$. □

## 2.4 Kvadrati u polju $p$-adskih brojeva

**Propozicija 2.4.1.** *Neka je $p \geq 3$, i neka je $a \in \mathbb{Q}_p^*$. Nužan i dovoljan uvjet da bi $a$ bio kvadrat u $\mathbb{Q}_p^*$ je da je $v_p(a)$ paran i $\left(\frac{a/p^{v_p(a)}}{p}\right) = 1$. Nadalje, sustav izvodnica za $\mathbb{Q}_p^*/\mathbb{Q}_p^{*^2}$ dan je s $1, a, p$ i $pa$, gdje je $a$ bilo koji broj za cijeli broj za koji vrijedi $\left(\frac{a}{p}\right) = -1$.*

*Dokaz.* Neka je $a \in \mathbb{Q}_p^*$ kvadrat od $b \in \mathbb{Q}_p^*$. Možemo zapisati $a = p^{v(a)}u_a$ i $b = p^{v(b)}u_b$ za $u_a, u_b \in \mathbb{Z}_p^\times$. Sada vidimo da mora vrijediti $v(a) = 2v(b)$ pa $v(a)$ mora biti paran. Također vidimo da mora vrijediti $u_a = u_b^2$ pa $\left(\frac{a/p^{v(a)}}{p}\right) = \left(\frac{u_a}{p}\right) = \left(\frac{u_b^2}{p}\right) = 1$. Nadalje, ako $a$ nije kvadrat u $\mathbb{Q}_p^*$, tada kvocjent bilo kojeg od parova $1, a, p, pa$ nije kvadrat u $\mathbb{Q}_p^*$. Ali svaki $p$-adski broj različit od nule može biti prikazan kao produkt nekog od brojeva $1, a, p, pa$ s nekim kvadratom. □

Za $p = 2$ vrijedi nam slijedeće.

**Propozicija 2.4.2.** *Nužan i dovoljan uvjet da bi neki $a \in \mathbb{Q}_2^*$ bio kvadrat u $\mathbb{Q}_2^*$ je da je $v(a)$ paran i da $a/2^{v(a)} \equiv 1$ (mod 8). Nadalje, sustav izvodnica za $\mathbb{Q}_2^*/\mathbb{Q}_2^{*^2}$ dan je s $\pm 1, \pm 5, \pm 2$ i $\pm 6$.*

*Dokaz.* Neka je $a = 2^{v(a)}u$ za $u \in \mathbb{Z}_2^\times$. Da je $v(a)$ paran zaključujemo kao prethodnoj propoziciji. Nužnost da ja $u \equiv q \pmod 8$ slijedi iz činjenice da je kvadrat neparnog broja uvijek kongruentan 1 modulo 8. Da dokažemo dovoljnost, stavimo $F(x) = x^2 - u_a$ i sada primjenimo Heneslovu lemu uzimajući $\gamma = 1$. Jer je $F(1) \equiv 0 \pmod 8$ i $F'(1) = 2 \not\equiv 0 \pmod 4$ slijedi d postoji $\theta \equiv 1 \pmod 4$ takva da $F(\theta) = 0$, tj. $u = \theta^2$.
Reducirani sustav ostataka modulo 8 je $\{1, 3, 5, 7\}$ tj. $\{\pm 1, \pm 5\}$ tvore skup predstavnika skupa $\mathbb{Z}_2/\mathbb{Z}_2^2$. Ako još pomnožimo s 2 dobit ćemo $\{\pm 1, \pm 5, \pm 2$ i $\pm 10\}$ tj. $\{\pm 1, \pm 5, \pm 2$ i $\pm 6\}$ dobijemo skup predstavnika za $\mathbb{Q}_2^*/\mathbb{Q}_2^{*^2}$. □

# Poglavlje 3

# Kvadratne forme

Neka je, u ovom poglavlju, K polje karakteristike različite od 2 (ovo će se podrazumjevati dalje u radu te neće biti posebno naglašeno).

## 3.1 Osnovna svojstva kvadratnih forma

**Definicija 3.1.1.** *Kvadratna forma nad poljem K je homogeni polinom* $q(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ *stupnja 2.*

Neka je $V$ vektorski prostor nad $K$ konačne dimenzije $n$. Kvadratnu formu možemo zapisati kao funkciju $q : V \to K$ takvu da vrijedi $q(ax) = a^2 q(x), \forall x \in V, \forall a \in K$.

**Definicija 3.1.2.** *Bilinearna forma na vektorskom prostoru V nad K je funkcija* $B : V \times V \to K$ *za koju vrijedi*

1. $B(v_1 + v_2, w) = B(v_1, w) + B(v_2, w)$*, za sve* $v_1, v_2, w \in V$*,*
2. $B(\lambda v, w) = \lambda B(v, w)$*, za sve* $v, w \in V, \lambda \in K$*,*
3. $B(v, w_1 + w_2) = B(v, w_1) + B(v, w_2)$*, za sve* $v, w_1, w_2 \in V$*.*

**Definicija 3.1.3.** *Bilinearna forma je simetrična ako je* $B(v, w) = B(w, v)$ *za sve* $v, w \in V$*.*

**Napomena 3.1.4.** *Za sve vektorske prostore V, postoji bijekcija*

$$\{\textit{kvadratne forme na } V\} \longleftrightarrow \{\textit{simetrične bilinearne forme na } V\}$$
$$q \mapsto B(x, y) := \frac{q(x+y)-q(x)-q(y)}{2}$$
$$q(x) := B(x, x).$$

*Iz ovoga nam slijedi da svakoj kvadratnoj formi možemo pridružiti jedinstvenu simetričnu matricu A tako da vrijedi* $q(x) = x^T Ax$ *i* $B(x, y) = x^T Ay$*.*

**Definicija 3.1.5.** *Rang kvadratne forme q je rang pridružene simetrične matrice A.*

**Definicija 3.1.6.** *Neka je q kvadratna forma nad K i neka je A pridružena simetrična martica formi q. Neka je det(A) determinanta od A. Diskriminanta od A je kvadratno slobodni dio u det(A) i označavamo je s d(q).*

**Definicija 3.1.7.** *Kvadratna forma q je nedegenerirana ako vrijedi bilo koji od sljedećih uvjeta:*

- *Pridružena simetrična matrica A je invertibilna.*
- *Za svaki* $0 \neq x \in V$*, linearno preslikavanje* $y \mapsto B(x, y)$ *nije nul-preslikavanje.*
- *Rang od q je n.*
- *Diskriminanta* $d(q) \neq 0$*.*

**Definicija 3.1.8.** *Kažemo da su dvije kvadratne forme* $q(x_1, \ldots, x_n)$ *i* $q'(x_1, \ldots, x_n)$ *ekvivalentne nad K ako se razlikuju za linearnu promjenu varijabli, tj. ako vrijedi* $q'(x) = q(Tx)$ *za neku invertibilnu matricu* $T \in GL_n(K)$*.*

**Napomena 3.1.9.** *Neka su q i q′ ekvivalentne kvadratne forme i neka je A pridružena simetrična matrica formu q. Po definiciji znamo da za neku invertibilnu matricu T vrijedi* $q'(x) = q(Tx) = (Tx)^T A(Tx) = x^T T^T ATx$*. Vidimo da je* $T^T AT$ *pridružena matrica formu q′. Znamo da je* $det(T^T AT) = det(A)det(T)^2$*. Sada vidimo da je* $d(q) = d(q')$*.*

**Propozicija 3.1.10.** *Svaka kvadratna forma* $q \in K[x_1, \ldots, x_n]$ *nad K je ekvivalentna nad K nekoj dijagonalnoj kvadratnoj formi*

$$a_1 x_1^2 + a_2 x_2^2 + \cdots + a_n x_n^2.$$

*Dokaz.* Neka je $A$ pridružena simetrična matrica formi $q$. S obziroma da je $A$ simetrična možemo ju dijagonalizirati u ortonormiranoj bazi, tj. postoje matrice $Q$ *i* $D$ takve da $A = QDQ^{-1}$ gdje je $D$ dijagonalna matrica a stupci matrice $Q$ čine ortonormiranu bazu pa vrijedi $QQ^T = I$ tj. $Q = Q^{-1}$. Sada znamo da vrijedi da je $A = QDQ^T$ gdje je $Q$ invertibilna matrica pa vrijedi

$$q(x) = x^T Ax = x^T QDQ^T x = (Q^T x)^T D(Q^T x) = [\text{uz notaciju } T = Q^T] = (Tx)^T D(Tx) = q'(Tx)$$

gdje je $q'$ kvadratna forma s pridruženom matricom D. Vidimo da je $q'$ dijagonalna kvadratna forma te da su $q$ i $q'$ ekvivalentne. □

Primjetimo da ako je $q$ ekvivalentna s dijagonalnom formom $a_1x_1^2 + a_2x_2^2 + \cdots + a_nx_n^2$, tada je rang od $q$ jednak broju $a_i-ova$ različitih od 0. To nam također govori da je kvadratna forma nedegerirana ako i samo ako za njezinu ekvivalentnu dijagonalnu formu $a_1x_1^2+a_2x_2^2+\cdots + a_nx_n^2$ vrijedi da je svaki $a_i \neq 0$.

**Definicija 3.1.11.** *Neka je $q : V \to K$ kvadratna forma i neka je $a \in K$. Kažemo da $q$ reprezentira $a$ ako postoji $0 \neq x \in V$ takav da je $q(x) = a$.*

Uvjet da je $x \neq 0$ vrlo nam je bitan u slučaju $a = 0$ jer bi u suprotnome sve kvadratne forme reprezentirale 0. Slučaj $a = 0$ će nam biti posebno zanimljiv i proučavat ćemo ga u daljnjem dijelu rada.

**Propozicija 3.1.12.** *Ako nedegenerirana kvadratna forma reprezentira 0, tada reprezentira svaki element od $K$.*

*Dokaz.* Neka je $q : V \to K$. Prema pretpostavci propozicije postoji $v \in V^*$ takav da $q(v) = 0$. Pošto je $q$ nedegerirana postoji $w \in V$ takav da $B(v, w) \neq 0$. Primjetimo da su $w$ *i* $v$ linearno nezavisni jer u suprotnome bi vrijedilo $B(v, w) = B(v, \lambda v) = \lambda B(v, v) = \lambda g(v) = \lambda \cdot 0 = 0$ za neki $\lambda \in K$. Neka je $x \in K$. Vrijedi da je

$$q(xv + w) = q(xv) + 2B(xv, w) + q(w) = x^2q(v) + 2xB(v, w) + q(w) = ax + b$$

gdje je $a = 2B(v, x) \neq 0$ i $b = q(w)$. Za svaki $c \in K$ možemo riješiti jednadžbu $ax + b = c$ po x, čime smo dokazali da $q$ reprezentira $c = q(xv + w)$. □

**Napomena 3.1.13.** *Neka su $q(x_1, \ldots, x_n)$ i $q'(x_1, \ldots, x_m)$ kvadratne forme s $n$ i $m$ varijabli. Ortogonalna suma $q \oplus q'$ je kvadratna forma u $n + m$ varijabli definirana kao*

$$(q \oplus q')(x_1, \ldots, x_{n+m}) = q(x_1, \ldots, x_n) + q'(x_{n+1}, \ldots, x_{n+m}).$$

*Također definiramo $q \ominus q' = q \oplus (-q')$.*

**Korolar 3.1.14.** *Neka je $q$ nedegerirana kvadratna forma u $n$ varijabli i neka je $c \in K^*$. Kvadratna forma reprezentira $c$ ako i samo ako kvadrtatna forma $q \ominus cx_0^2$ reprezentira 0 u $K$.*

*Dokaz.* Neka $q$ reprezentira $c$. Ako uzmemo $x_0 = 1$ i $(x_1, \ldots, x_n)$ koji su reprezentacija od c tada vidimo da $q \ominus cx_0^2$ reprezentira 0 u $K$ Obratno, neka $-c\alpha_0^2 + q(\alpha_1, \ldots, \alpha_n) = 0$. Ako je $\alpha_0 \neq 0$ tada je $c = q(\alpha_1/\alpha_0, \ldots, \alpha_n/\alpha_0)$. U slučaju $\alpha_0 = 0$ dobijemo da $q$ reprezentira 0 pa prema propoziciji 3.1.12 reprezentira i svaki $c \in K$. □

**Korolar 3.1.15.** *Neka su $q_1$ i $q_2$ nedegerirane kvadrtane forme i neka je $q = q_1 \ominus q_2$. Sljedeće tvrdnje su ekvivalentne:*

**(1)** *Forma $q$ reprezentira 0.*

**(2)** *Postoji točka $c \in K^*$ koja je reprezentirana i s $q_1$ i s $q_2$.*

**(3)** *Postoji točka $c \in K^*$ takva da i $q_1 \ominus cx_0^2$ i $q_2 \ominus cx_0^2$ reprezentiraju 0.*

*Dokaz.* Ekvivalentnost tvrdnji (2) i (3) slijedi direktno iz prethodnog korolara, a da tvrdanja (2) implicira (1) je trvijalno. Dokažimo da (1) implicira (2). Ako $q = q_1 \ominus q_2$ reprezentira 0 tada postoje $x$ i $y$ takvi da $q_1(x) = q_2(y)$ i da je najviše jedan od njih 0. Uzmimo $c = q_1(x) = q_2(y)$. Ako je $c \neq 0$, tada je (2) dokazano. U suprotnome, pošto je ili $x$ ili $y$ različito od 0, barem jedna od formi, uzmimo npr. $q_1$, reprezentira 0, pa prema propoziciji 3.1.12, $q_1$ reprezentira sve elemente od $K$, pa tako i sve vrijednosti koje postiže $q_2$ različite od 0. □

## 3.2 Hilbertovi simboli

Kod proučavanja kvadratnih formi nad p-adskim poljem vrlo nam je bitan slučaj kvadratnih formi s 3 varijable, pa ćemo ga sada proučiti detaljnije. Kao pomoć pri tome služe nam Hilbertovi simboli. U ovome poglavlju neka je $\mathcal{K}$ upotpunjenje od $\mathbb{Q}$, tj. $\mathbb{Q}_p$ ili $\mathbb{R}$.

**Definicija 3.2.1.** *Neka je $a, b \in \mathcal{K}^*$. Pišemo $(a, b) = 1$ ako jednadžba $ax^2 + bx^2 = z^2$ ima netrivijalna rješenja u $\mathcal{K}^*$, inače pišemo $(a, b) = -1$. Broj $(a, b)$ zovemo (lokalni) Hilbertov simbol od a i b.*

Kada koristimo više različitih proširenja pisati ćemo $(a, b)_p$ ili $(a, b)_\infty$ da naglasimo prosti broj, ili jednostavno $(a, b)_v$ da ukažemo na mjesto od $v$.
Jasno je da se $(a, b)$ ne mijenja ako pomnožimo $a$ ili $b$ sa nekim kvadratom različitim od 0. Stoga se $(a, b)$ može smatrati funkcijom koja ide s $(\mathcal{K}^*/\mathcal{K}^{*2}) \times (\mathcal{K}^*/\mathcal{K}^{*2})$ u $\{\pm 1\}$.

**Propozicija 3.2.2.** *Neka su $a, b \in \mathcal{K}^*$. Vrijedi da je $(a, b) = 1$ ako i samo ako $a \in \mathcal{N}(\mathcal{K}(\sqrt{b})^*)$ tj. ako i samo ako je a norma elementa iz skupa $\mathcal{K}(\sqrt{b})^*$, gdje je $\mathcal{K}(\sqrt{b}) = \{x + y\sqrt{b}; x, y \in \mathcal{K}\}$.*

*Dokaz.* Neka je $b$ kvadrat. Tada je $(0, 1, \sqrt{b})$ očito riješenje jednadžbe $ax^2 + by^2 = z^2$ i $\mathcal{K}(\sqrt{b}) = \mathcal{K}$ čime je propozicija dokazana. U drugom slučaju ($b$ nije kvadrat) elementi kvadratnog upotpunjenja $\mathcal{K}(\sqrt{b})$ su oblika $u + v\sqrt{b}$ gdje su $u, v \in \mathcal{K}$, pa znamo da je $a$ norma ako i samo ako je $a = u^2 - bv^2$. U tom slučaju $(1, v, u)$ je rješenje jednadžbe. Obratno, ako $ax^2 + by^2 = z^2$ tada je $x \neq 0$ (inače je $b$ kvadrat) pa vidimo da je $a$ norma od $(z/x) + (y/x)\sqrt{b}$. □

**Propozicija 3.2.3.** *Za Hilbertove simbole vrijede slijedeće formule, u kojima pretpostavljam da su svi elementi različiti od 0:*

**(1)** $(a, b) = (b, a)$ *i* $(a, c^2) = 1$

**(2)** $(a,-a)=1$ *i* $(a,1-a)=1$

**(3)** $(a,b)=1$ *implicira* $(aa',b)=(a',b)$

**(4)** $(a,b)=(a,-ab)=(a,(1-a)b)$

*Dokaz.* (1) je očito. Ako uzmemo $b=-a$ (odnosno $b=1-a$), tada $(1,1,0)$ (odnosno $(1,1,1)$) je netrivijalno rješenje od $ax^2+bx^2=z^2$ čime dokazujemo (2). Za (3) prema prethodnoj propoziciji znamo da ako $(a,b)=1$ tada $a\in\mathcal{N}(K(\sqrt{b})^*)$, stoga zbog multiplikativnosti norme $a'\in\mathcal{N}(K(\sqrt{b})^*)$ ako i samo ako $aa'\in\mathcal{N}(K(\sqrt{b})^*)$. Primjetimo da je ova formula posebni slučaj bilinearnosti Hilbertovog simbola (aa',b)=(a,b)(a',b), koju ćemo kasnije dokazati. Konačno, (4) nam slijedi direktno iz (1),(2) i (3), npr. pošto $(a,-a)=1$, imamo $(a,-ab)=(-ab,a)=(b,a)=(a,b)$. □

**Teorem 3.2.4. (1)** *Za* $\mathcal{K}=\mathbb{R}$*, vrijedi* $(a,b)=-1$ *ako* $a<0$ *i* $b<0$*, i* $(a,b)=1$ *ako su a ili b pozitivni.*

**(2)** *Za* $\mathcal{K}=\mathbb{Q}_p$ *za* $p\neq 2$*, pišemo* $a=p^\alpha a_1$*,* $b=p^\beta b_1$ *tako da su* $a_1,b_1\in\mathbb{Z}_p^\times$*. Tada*

$$(a,b)=(-1)^{\alpha\beta(p-1)/2}\left(\frac{a_1}{p}\right)^\beta\left(\frac{b_1}{p}\right)^\alpha.$$

**(3)** *Za* $\mathcal{K}=\mathbb{Q}_2$ *i istom notacijom imamo*

$$(a,b)=(-1)^{(a_1-1)(b_1-1)/4}\left(\frac{a_1}{p}\right)^\beta\left(\frac{b_1}{p}\right)^\alpha.$$

Dokaz za (1) je trivijalan, pa sada možemo pretpostaviti da je $\mathcal{K}=\mathbb{Q}_p$. Prije nego krenemo na dokaz promotriti ćemo slijedeću lemu koja će nam biti potrebna.

**Lema 3.2.5.** *Pretpostavimo da je* $b\in\mathbb{Z}_p^\times$*. Tada ako jednadžba* $px^2+by^2=z^2$ *ima netrivijalno riješenje u* $\mathbb{Q}_p$*, onda ima barem jedno takvo da je* $x\in\mathbb{Z}_p$ *i y i z su u* $\mathbb{Z}_p^\times$*.*

*Dokaz.* Neka je (x,y,z) netrivijalno riješenje. Dijeleći s $p^v$ gdje je $v=\min(v_p(x),v_p(y),v_p(z))$, možemo pretpostaviti da su $x,y$ i $z$ u $\mathbb{Z}_p$, te da je barem jedan od njih u $\mathbb{Z}_p^\times$. Ako imamo $y\notin\mathbb{Z}_p^\times$, tada $v_p(y)\geq 1$, stoga $v_p(z)\geq 1$ i $v_p(x)\geq 1$ što je u kontradikciji s činjenicom da je jedan od x,y i z u $\mathbb{Z}_p^\times$. Zato vrijedi da je $y\in\mathbb{Z}_p^\times$, pa $z\in\mathbb{Z}_p^\times$ također. □

*Dokaz.* **(2)**. Pretpostavimo $p\neq 2$. Kao što smo već rekli Hilbertov simbol $(a,b)$ se ne mijenja ako pomnožimo $a$ ili $b$ s kvadratom različitim od 0, pa zaključejemo da ovisi samo o parnosti od $\alpha$ i $\beta$, pa bez smanjenja općenitosti možemo pretpostavit da su $\alpha$ i $\beta$ jednaki 0 ili 1. Sada ćemo razmatrati tri moguća slučaja.
**1. slučaj:** $\alpha=\beta=0$.
Lako vidimo da jednadžba $a_1x^2+b_1y^2=z^2$ ima netrivijalno riješenje modulo $p$, pa s

obzirom da su $a_1$ i $b_1$ p-adski brojevi i $p \neq 2$, prema Henselovoj lemi slijedi da jednadžba ima i $p$-adsko rješenje, pa $(a, b) = 1$ kao što tvrdi teorem.
**2. slučaj:** $\alpha = 1,\ \beta = 0$.
Prema 1. slučaju znamo da $(a_1, b_1) = 1$. Prema propoziciji 3.2.3 (3) vrijedi nam $(a, b) = (pa_1, b_1) = (p, b_1)$. Ako je $b_1$ kvadrat u $\mathbb{Q}_p$ tada $(p, b_1) = 1$ i $\left(\frac{b_1}{p}\right) = 1$, pa imamo $(a, b) = \left(\frac{b_1}{p}\right) = 1$. U slučaju da $b_1$ nije kvadrat u $\mathbb{Q}_p$, onda $\left(\frac{b_1}{p}\right) = -1$ tada nam gornja lema implicira da $px^2 + b_1y^2 = z^2$ nema netrivijalna rješenja (u suprotnome, s obzirom da je $y \in \mathbb{Z}_p^\times$, $b_1$ bi bilo kongruentno s $(y/z)^2$ modulo p) pa $(a, b) = \left(\frac{b_1}{p}\right) = -1$.
**3. slučaj:** $\alpha = \beta = 1$.
Prema propoziciji 3.2.3 (4) i koristeći se istim zaključivanjem kao i u 2. slučaju dobijemo da vrijedi

$$(a, b) = (pa_1, pb_1) = (pa_1, -p^2a_1b_1) = (pa_1, -a_1b_1)$$
$$= \left(\frac{-a_1b_1}{p}\right) = (-1)^{(p-1)/2}\left(\frac{a_1}{p}\right)\left(\frac{b_1}{p}\right),$$

pa dobijemo traženu formulu.
**(3)**. pretpostavimo $p = 2$. Dokaz će biti sličan te ponovno razmatramo ista tri slučaja.
**1. slučaj:** $\alpha = \beta = 0$.
Sada moramo dokazati da je $(a_1, b_1) = 1$ ako je ili $a_1$ ili $b_1$ kongruentno s 1 modula 4, u suprotnome $(a, b) = -1$. Pretpostavimo prvo da je $a_1 \equiv 1 \pmod{4\mathbb{Z}_2}$. Tada imamo dva slučaja. Prvi slučaj je da je $a_1 \equiv 1 \pmod{8\mathbb{Z}_2}$, a u tom slučaju $a_1$ je prema propoziciji 2.4.2 kvadrat pa je $(a, b) = 1$. U drugom slučaju $a_1 \equiv 5 \pmod{8\mathbb{Z}_2}$. Tada je $a_1 + 4b_1 \equiv 1 \pmod{8\mathbb{Z}_2}$ pa je $a_1 + 4b_1$ kvadrtat nekog broja $w \in \mathbb{Z}_2$ pa je $(1, 2, w)$ netrivijalno rješenje jednadžbe $a_1x^2 + b_qy^2 = z^2$, pa ponovno dobijemo $(a, b) = 1$.
Pretpostavimo sada da je $a_1 \equiv b_1 \equiv -1 \pmod{4\mathbb{Z}_2}$, pretpostavimo kontradikciju, tj da postoji netrivijalno rješenje $(x, y, z)$ jednadžbe $a_1x^2 + b_qy^2 = z^2$, gdje kao i u gornjem primjeru možemo pretpostaviti da $x, y, z \in \mathbb{Z}_2$ tako da je barem jedan u $\mathbb{Z}_p^\times$. Tada $x^2 + y^2 + z^2 \equiv 0 \pmod{4\mathbb{Z}_2}$, a s obzirom svi kvadratu u $\mathbb{Z}_2$ modulo 4 su 0 ili 1, to nam implicira da x,y i z nisu jedinice, što je kontradikcija s pretpostavkom, pa $(a, b) = -1$ u ovom slučaju.

**2. slučaj:** $\alpha = 1,\ \beta = 0$.
Prvo ćemo dokazati slučaj kada je $a_1 = 1$. U tom slučaju moramo dokazati da je $(2, b_1) = \left(\frac{b_1}{2}\right)$, drugim riječima da je $(2, b_1) = 1$ ako i samo ako je $b_1 \equiv \pm 1 \pmod{8\mathbb{Z}_2}$. Ako je $(2, b_1) = 1$, gornja lema nam kaže da postoje x,y i z u $\mathbb{Z}_2$ i y i z u $U_2$ takvi da vrijedi $2x^2 + b_1y^2 = z^2$. Zato nam slijedi da je $y^2 \equiv z^2 \equiv 1 \pmod{8\mathbb{Z}_2}$, stoga $b_1 \equiv 1 - 2x^2 \pmod{8\mathbb{Z}_2}$, pa $b_1 \equiv \pm 1 \pmod{8\mathbb{Z}_2}$. U slučaju kada je $b_1 \equiv 1 \pmod{8\mathbb{Z}_2}$ tada je $b_1$ kvadrat, pa $(2, b_1) = 1$, a u slučaju $b_1 \equiv -1 \pmod{8\mathbb{Z}_2}$ tada je $-b_1$ kvadrat pa dobijemo da je $(2, b_1) = (2, -1)$, i $(1, 1, 1)$ je netrivijalno rješenje jednadžbe $2x^2 - y^2 = z^2$, pa i u ovom slučaju dobijemo $(2, b_1) = 1$.

Sada ćemo dokazati općeniti slučaj, tj. trebamo dokazati da je $(2a_1, b_1) = (a_1, b_1)(2, b_1)$. Prema propoziciji 3.2.3 (3), ovo vrijedi kada je ili $(2, b_1) = 1$ ili $(a_1, b_1) = 1$, pa pretpostavimo sada da je $(2, b_1) = (a_1, b_1) = -1$. Prema onome što smo dokazali prethodno dobijemo da tada $a_1 \equiv b_1 \equiv -1 \pmod{4\mathbb{Z}_2}$ i $b_1 \equiv \pm 3 \pmod{8\mathbb{Z}_2}$, tj $b_1 \equiv 3 \pmod{8\mathbb{Z}_2}$. Nakon što pomnožimo s brojevima koji su kongruentni s 1 modulo $8\mathbb{Z}_2$, pa su i kvadrati, možemo pretpostaviti da je $a_1 = -1$ i $b_1 = 3$ ili $a_1 = 3$ a $b_1 = -5$. Jednadžbe $-2x^2+3y^2 = z^2$ i $6x^2 - 5y^2 = z^2$ imaju $(1, 1, 1)$ kao netrivijalno rješenje pa dobijemo da je $(2a_1, b_1) = 1$ kao što smo i tvrdili, te time završavamo dokaz u ovom slučaju.

**3. slučaj:** $\alpha = \beta = 1$.

Kao i u slučaju $p > 2$, propozicija 3.2.3 (4) i 2. slučaj pokazuju nam da

$$\begin{aligned}(2a_1, 2b_1) &= (2a_1, -4a_1b_1) = (2a_1, -a_1b_1) = \\ &= (-1)^{(a_1-1)(b_1-1)/4}\left(\frac{-a_1b_1}{2}\right) = (-1)^{(a_1-1)(b_1-1)/4}\left(\frac{-a_1}{2}\right)\left(\frac{b_1}{2}\right),\end{aligned}$$

čime završavamo dokaz teorema. □

Iz ovoga teorema nam je lako zaključiti bilinearnost Hilbertovih simbola, čega je propozicija 3.2.3 (3) poseban slučaj.

**Korolar 3.2.6.** *Hilbertov simbol je nedegenerirana bilinearna forma na $\mathbb{F}_2$-vektorskom prostoru $\mathcal{K}^*/\mathcal{K}^{*^2}$.*

*Dokaz.* Kada je $\mathcal{K} = \mathbb{R}$, $\mathcal{K}^*/\mathcal{K}^{*^2}$ slijedi iz teorema 3.2.4(1). Kada je $\mathcal{K} = \mathbb{Q}_p$, bilinearnost nam slijedi iz multiplikativnosti Legendre-Kroneckerovog simbola.
Da bi pokazali da je nedegenerirana, neka je $\bar{a} \in \mathcal{K}^*/\mathcal{K}^{*^2}$ takav da nije klasa identiteta. Promatrati ćemo dva slučaja, kad je $p \neq 2$ i $p = 2$. Ako je $p \neq 2$ prema propoziciji 2.4.1 za predstavnika u $\mathcal{K}^*$ možemo uzeti $a = n, p$ ili $np$, gdje je $n$ cjeli broj takav da $\left(\frac{n}{p}\right) = -1$. Tada očito $(n, p) = -1$, pa ako odaberemo redom $b$ takav da je iz klase $p$, $n$ i $n$ vrijedi $(a, b) = -1$ čime smo pokazali da je forma nedegenerirana.Ako je $p = 2$, prema propoziciji 2.4.2 kao predstavnika od $\mathcal{K}^*$ možemo uzeti brojeve 5,-1,-5,2,10,-2,-10 i provjerimo da $(2a_1, 5) = -1$, dok $(5, 2) = (-1, -1) = (-5, -1) = -1$ čime dokazujemo nedegeriranost i u ovom slučaju. □

**Propozicija 3.2.7.** *Neka je $q(x, y, z) = ax^2 + by^2 + cz^2$ nedegenerirana kvadratna forma u tri varijable i koeficijentima u $\mathbb{Q}_p$ (uključujući i $p = \infty$). Neka je $\varepsilon = \varepsilon(q) = (a, b)(a, c)(b, c)$, i neka je $d = d(q) = abc$ diskriminanta od $q$. Tada $q$ reprezentira 0 u $\mathbb{Q}_p$ ako i samo ako je $(-1, d) = \varepsilon$.*

*Dokaz.* Forma $q$ reprezentira 0 ako i samo ako i forma $-cq$ reprezentira 0, tj. ako i samo ako $-acx^2 - bcy^2 = z^2$ ima netrivijalna rješenja. Drugim riječima, mora vrijediti da je $(-ac, -bc) = 1$. Zbog bilinearnosti ovaj uvjet možemo raspisati

$$1 = (-ac, -bc) = (-1,-1)(-1,a)(-1,b)(a,b)(a,c)(b,c)(c,c),$$

i pošto vrijedi $(c,c) = (-1,c)$

$$1 = (-1,-1)(-1,a)(-1,b)(-1,c)(a,b)(a,c)(b,c) = (-1,-abc)(a,b)(a,b)(b,c)$$

pa vidimo da $(-1,abc) = (a,b)(a,c)(b,c)$ čime dokazujemo propoziciju. □

**Korolar 3.2.8.** *Neka je $c \in \mathbb{Q}_p^*$, i neka je $q(x,y) = ax^2 + by^2$ nedegerirana kvadratna forma u dvije varijable. Tada q reprezentira c u $\mathbb{Q}_p$ ako i samo ako $(c,-ab) = (a,b)$.*

*Dokaz.* Prema korolaru 3.1.14, $q$ reprezentira c ako i samo ako forma $q'(x,y,z) = ax^2 + by^2 - cz^2$ reprezentira 0. Prema prethodnoj propoziciji ovo je istina ako i samo ako $(-1,abc) = (a,b)(a,-c)(b,-c)$, a pošto je $(c,-c) = 1$, ako i samo ako

$$(a,b) = (-1,abc)(ab,-c) = (-1,abc)(-c,abc) = (c,abc) = (c,-c)(c,-ab) = (c,-ab).$$

□

**Lema 3.2.9.** *Neka je $\mathcal{K} = \mathbb{Q}_p$ takav da je $p \neq \infty$.*

**(1)** *Vrijedi $| \mathcal{K}^*/\mathcal{K}^{*^2} | = 2^r$ gdje je $r = 2$ za $p \neq 2$ i $r = 3$ za $p = 2$.*

**(2)** *Ako je $a \in \mathcal{K}^*/\mathcal{K}^{*^2}$ i $\varepsilon = \pm 1$, definiramo $H_\varepsilon(a)$ kao skup svih $x \in \mathcal{K}^*/\mathcal{K}^{*^2}$ takvih da $(x,a) = \varepsilon$. Tada $| H_1(1) | = 2^r$, $H_{-1}(1) = \emptyset$ i $| H_\varepsilon(a) | = 2^{r-1}$ ako $a \neq 1$.*

**(3)** *Neka su $a, a' \in \mathcal{K}^*/\mathcal{K}^{*^2}$ i $\varepsilon, \varepsilon' \in \{-1,1\}$, i pretpostavimo da su $H_\varepsilon(a)$ i $H_{\varepsilon'}(a')$ neprazni skupovi. Tada $H_\varepsilon(a) \cap H_{\varepsilon'}(a') = \emptyset$ ako i samo ako $a = a'$ i $\varepsilon = -\varepsilon'$.*

*Dokaz.* Dokaz za (1) u slučaju $p \neq 2$ slijedi iz propozicije 2.4.1, a za slučaj $p = 2$ iz propozicije 2.4.2 . Za (2), slučaj $a = 1$ dokaz je trivijalan. Kada je $a \neq x$, s obzirom da je Hilbertov simbol nedegerirana bilinearna forma $H_1(a)$ je jezgra surjektivne funkcije $x \mapsto (a,x)$, pa prema prvom toremu o izomorfizmu ima $2^{r-1}$ elementa, a isto je istina i za njegov komplement $H_{-1}(a)$. I naposlijetku, za (3), ako su $E = H_\varepsilon(a)$ i $F = H_{\varepsilon'}(a')$ neprazni i disjunktni, tada prema tvrdnji (2) oba skupa imaju $2^{r-1}$ elemenata pa slijedi da su E i F jedan drugome komplementi. Tada je $H_1(a)$ jednak ili E (ako je $\varepsilon = 1$) ili F (ako je $\varepsilon = -1$), i slično $H_1(a')$ je ili E ili F. S obzirom da je $1 \in H_1(a)$ za sve $a$, $H_1(a)$ i $H_1(a')$ nisu disjunktni, pa $H_1(a) = H_1(a')$. To nam govori da za svaki $x$ imamo $(x,a) = (x,a')$, a s obzirom da je Hilbertov simbol nedegerirana forma vrijedi nam da je $a = a'$, pa nužno i $\varepsilon = -\varepsilon'$, kao što smo i tvrdili. □

Neka je $P = \{p : \text{p je prost broj}\} \cup \{\infty\}$.

**Teorem 3.2.10.** *(Produktna formula) Ako su a i b u $\mathbb{Q}^*$ tada $(a,b)_v = 1$ za gotovo svaki $v \in P$ (drugim riječima, za sve osim za njih konačno mnogo), vrijedi nam produktna formula*

$$\prod_{v \in P} (a,b)_v = 1.$$

*Dokaz.* Zbog bilinearnosti dovoljno je dokazati teorem kada su $a$ i $b$ jednaki -1 ili prosti broj. U tim slučajevima teorem 3.2.4 nam daje odgovor:

- Ako je $a = -1$ i $b = -1$ tada $(-1,-1)_\infty = (-1,-1)_2 = -1$, i $(-1,-1)_v = 1$ za $v \neq 2$ *i* $\infty$, pa je produktna formula jednaka 1.
- Ako je $a = -1$ i $b = l$ takav da je $l$ prost broj. Tada u slučaju $l = 2$ imamo $(-1,2)_v = (-1,(1-(-1)))_v = 1$ za svaki $v \in P$. U slušaju $l \neq 2$ onda $(-1,l)_v = 1$ ako je $v \neq 2$ i $l$, i $(-1,l)_2 = (-1,l)_l = (-1)^{(l-1)/2}$, pa je produktna jednak 1, pa produktna formula vrijedi.
- Ako je $a = l$ i $b = l$ tada prema propoziciji 3.2.3 (4) imamo $(l,l)_v = (-1,l)_v$ pa dobijemo isto kao u u prethodnom slučaju.
- Ako je $a = 2$ i $b = l$, takv da je $l$ prost broj, tada $(2,l)_v = 1$ za $v \neq 2$ *i* $l$, i $(2,l)_2 = \left(\frac{l}{2}\right) = \left(\frac{2}{l}\right) = (2,l)_l$, pa dobijemo da je produkt jednako 1.
- Ako je $a = l$ i $b = l'$ gdje su $l$ i $l'$ različiti prosti brojevi, tada $(l,l')_v = 1$ za $v \neq 2, l$ *i* $l'$, i

  $$(l,l')_2 = (-1)^{(l-1)(l'-1)/4},\ (l,l')_l = \left(\frac{l'}{l}\right),\ (l,l')_{l'} = \left(\frac{l}{l'}\right),$$

  pa prema zakonu kvadratne recipročnosti dobijemo da je produkt jednak 1.

□

Za dokaz sljedećeg teorema biti će nam potreban teorem slabe aproksimacije koji ćemo sada i iskazati, a dokaz se može pronaći u knjizi [6].

**Teorem 3.2.11.** *Neka je $p \in P$ i $x_p \in \mathbb{Q}_p$. Tada za svaki $\varepsilon > 0$ postoji $x \in \mathbb{Q}$ takav da*

$$|x - x_p| < \varepsilon.$$

**Teorem 3.2.12.** *Neka je $(a_i)_{i \in I}$ konačni skup elemenata iz $\mathbb{Q}^*$ i neka je $(\varepsilon_{i,v})_{i \in I, v \in P}$ skup brojeva jednakih $\pm 1$. Postoji $x \in \mathbb{Q}^*$ takav da $(a_i, x) = \varepsilon_{i,v}$ za svaki $i \in I$ i za svaki $v \in P$ ako i samo ako su sljedeća tri uvjeta zadovoljena:*

**(1)** *Gotovo svi $\varepsilon_{i,v}$ su jednaki 1.*

**(2)** *Za sve $i \in I$ vrijedi $\prod_{v\in P} \varepsilon_{i,v}$=1.*

**(3)** *Za sve $v \in P$ postoji $x_v \in \mathbb{Q}_v^*$ takav da $(a_i, x_v)_v = \varepsilon_{i,v}$ za sve $i \in I$.*

*Dokaz.* Nužnost uvjeta (1) i (2) slijedi direktno iz prethodnog teorema, a (3) je trivijalan ako uzmemo $x_v = x$. Stoga ostaje nam pokazati da su ovi uvjeti dovoljni.
Nakon što pomnožimo $a_i$ s ne-nul kvadratima možemo pretpostaviti da su $a_i \in \mathbb{Z}$ za svaki $i$. Ozaničimo sa $S$ (konačan) podskup od P koji sadrži $\infty$, 2 i proste faktore od svih $a_i$, a s $T$ (konačan) skup svih $v \in P$ takvih da postoji $i \in I$ za koje vrijedi $\varepsilon_{i,v} = -1$.
Pretpostavimo prvo da $S \cap T = \emptyset$, i definiramo

$$a = \prod_{l\in T, l\neq 2,\infty} l \quad i \quad m = 8 \prod_{l\in S, l\neq 2,\infty} l.$$

S obzirom da $S \cap T = \emptyset$ cijeli brojevi $a$ i $m$ relativno prosti brojevi, pa prema Dirichletovom teoremu postoji prosti broj $p \equiv a \pmod m$ takav da $p \notin S \cup T$. Tvrdimo da $x = ap$ zadovoljava sva svojstva. Razmatramo dva slučajeva.
**1. slučaj:** $v \in S$
S obzirom da $S \cap T = \emptyset$ vrijedi $\varepsilon_{i,v} = 1$ za sve $i$, pa moramo provjeriti da $(a_i, x)_v = 1$. To očito vrijedi za $v = \infty$ zato jer $x > 0$. Ako je $v = l$ prosti broj, tada $x \equiv a^2 \pmod m$, pa $x \equiv a^2 \pmod 8$ za $l = 2$ i $x \equiv a^2 \pmod l$. Zbog toga što je $a$ l-adska jedinica, Henselova lema implicira da je $x$ kvadrat u $\mathbb{Q}_l^*$, pa $(a_i, x)_v = 1$, za sve $i$.
2. slučaj: $v = l \notin S$.
U ovome slučaju $a_i$ je l-adska jedinica, i zbog $l \neq 2$ prema teoremu 3.2.4 dobijemo da za sve $b \in \mathbb{Q}_l^*$ vrijedi

$$(a_i, b)_l = \left(\frac{a_i}{l}\right)^{v_l(b)}.$$

- Ako $l \notin T \cup \{p\}$, tada je $x$ l-adska jedinica, stoga $(a_i, x)_l = 1 = \varepsilon_{i,v}$ zbog $l \notin T$.

- Ako je $l \in T$ tada $v_l(x) = 1$ i uvjet (3) impliciraju da postoji $x_l \in \mathbb{Q}_l^*$ takav da $(a_i, x_l) = \varepsilon_{i,l}$za sve $i \in I$. S obzirom da $l \in T$ barem jedan od $\varepsilon_{i,l}$ je jednak -1, stoga $v_l(x_l) \equiv 1 \pmod 2$ pa prema teoremu 3.2.4, za sve $i \in I$ vrijedi:

$$(a_i, x)_l = \left(\frac{a_i}{l}\right) = (a_i, x_l)_l = \varepsilon_{i,l}.$$

- Konačno, ako je $l = p$ produktna formula implicira da

$$(a_i, x)_p = \prod_{v\neq p} (a_i, x)_p = \prod_{v\neq p} \varepsilon_{i,v} = \varepsilon_{i,p}$$

prema uvjetu (2), čime dokazujemo teorem u posebnom slučaju $S \cap T = \emptyset$.

Razmotriti ćemo sada općeniti slučaj. Prema teoremu slabe aproksimacije 3.2.11 znamo da postoji $x' \in \mathbb{Q}^*$ takav da $x'/x_v \in \mathbb{Q}_v^{*2}$ za sve $v \in S$ (možemo naprimjer tražiti da $x'/x_v \equiv 1 \pmod{p\mathbb{Z}_p}$ za $v = p \neq 2, \infty$, $x'/x_v \equiv 1 \pmod{8\mathbb{Z}_2}$ za $v = 2$ i $x'/x_v > 0$ za $v = \infty$). Stoga $(a_i, x')_v = (a_i, x_v)_v = \varepsilon_{i,v}$ za sve $v \in S$. Ako definiramo $\eta_{i,v} = (a_i, x')_v, \varepsilon_{i,v}$, tada očito familija $\eta_{i,v}$ zadovoljava uvjete (1),(2) i (3), i prema definiciji $\eta_{i,v} = 1$ ako $v \in S$. Stoga, prema specijalnom slučaju koji smo prethodno dokazali, postoji $y \in \mathbb{Q}^*$ takav da $(a_i, y)_v = \eta_{i,v}$ za sve $i \in I$ i $v \in P$, i očito je da $x = yx'$ ima tražena svojstva. □

## 3.3 Kvadratne forme nad $\mathbb{Q}_p$

Nakon što smo proučili Hilbertove simbole, tj. kvadratne forme s 3 varijeble nad $\mathbb{Q}_p$, sada ćemo lakše razmotriti i generalni slučaj kvadratnih formu nad $\mathbb{Q}_p$. Neka je $q$ kvadratna forma u $n$ varijabli. Prvi cilj nam je naći nužan i dovoljan uvjet da bi $q$ reprezentirao 0 netrivijalno u $\mathbb{Q}_p$. S obzirom da degerirane forme reprezentiraju 0 netrivijalno, uvijek ćemo pretpostaviti da je $q$ nedegerirana. Diskirminantu $d(q)$ od $q$, smatramo elementom od $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$, i ona je invarijanta klase ekvivalencije kvadratnih formi. Definirati ćemo sada i drugu klasu ekvivalencije kvadratnih formi. Do na ekvivalenciju, možemo pretpostaviti da je $q$ dijagonalna froma oblika $q = \sum_{1 \leq i \leq n} a_i x_i^2$, i definiramo

$$\varepsilon((a_1, \ldots, a_n)) = \prod_{1 \leq i < j \leq n} (a_i, a_j),$$

gdje je $(a_i, a_j)$ Hilbertov simbol, pa vrijedi $\varepsilon((a_1, \ldots, a_n)) = \pm 1$. U slučaju n=1, definiramo da je i $\varepsilon = 1$. Za $\varepsilon$ nam vrijedi sljedeći teorem.

**Teorem 3.3.1.** *Vrijednost od $\varepsilon((a_1, \ldots, a_n))$ je neovisna o linearnoj promjeni varijabli koje transformiraju q u dijgonalnu formu, stoga je $\varepsilon$ invarijanta klase skvivalencije kvadratne forme, što ćemo označavai s $\varepsilon(q)$.*

Ovaj teorem nam govori da kao i diskriminanta d(q), $\varepsilon(q)$ je invarijanta klase ekvivalencije od $q$.

**Teorem 3.3.2.** *Neka je q nedegerirana kvadratna forma u n varijabli, i neka je $d = d(q)$ i $\varepsilon = \varepsilon(q)$. Tada q reprezentira 0 u $\mathbb{Q}_p$ ako i samo ako vrijedi nešto od slijedećeg:*

**(1)** $n = 2$ *i* $d = -1$,

**(2)** $n = 3$ *i* $(-1, -d) = \varepsilon$,

**(3)** $n = 4$ *i ili* $d \neq 1$ *ili* $d = 1$ *i* $(-1, -d) = \varepsilon$,

**(4)** $n \geq 5$.

*Posebno, svaka kvadratna forma u barem 5 varijabli reprezentira 0 u* $\mathbb{Q}_p$

*Dokaz.* S obzirom da su $d$ i $\varepsilon$ invarijante klase ekvivalencije možemo pretpostaviti da je $q$ dijagonalna forma. Kada je $n = 1$, očito je da $q$ ne može reprezentirati 0 netrivijalno. U slučaju kada je $n = 2$, $a_1x_1^2 + a_2x_2^2$ reprezentira 0 netrivijalno ako i samo ako je $a_1/a_2 \in \mathbb{Q}_p^{*^2}$, stoga ako i samo ako je $-d = -a_1a_2 \in \mathbb{Q}_p^{*^2}$, što znači da $d = -1 \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*^2}$. Slučaj kada je $n = 3$ analogan je propoziciji 3.2.7.
**Slučaj** $n = 4$.
Prema korolaru 3.1.15 (ekvivalencija (1) i (2)), $q(x) = \sum_{1\le i\le 4} a_ix_i^2$ reprezentira 0 ako i samo ako postoji $c \in \mathbb{Q}_p^*$ takav da je reprezentiran s formama $a_1x_1^2 + a_2x_2^2$ i $-a_3x_3^2 - a_4x_4^2$. Stoga prema korolaru 3.2.8, $q$ reprezentira 0 ako i samo ako postoji $c \in \mathbb{Q}_p^*$ takav da $(c, -a_1a_2) = (a_1, a_2)$ i $(c, -a_3a_4) = (-a_3, -a_4)$. Neka je A skup svih $x \in \mathbb{Q}_p^*$ takvih da $(x, -a_1a_2) = (a_1, a_2)$ i neka je B skup svih $x \in \mathbb{Q}_p^*$ takvih da vrijedi $(x, -a_3a_4) = (-a_3, -a_4)$. Jasno je sada da $q$ ne reprezntira 0 ako i samo ako je $A \cap B = \emptyset$. Primjetimo da su A i B neprazni skupovi (npr. $a_1 \in A$ i $-a_3 \in B$). Koristeći lemu 3.2.9 (3), zaključujemo da je uvjet $A \cap B = \emptyset$ ekvivalentan s $a_1a_2 = a_3a_4$ i $(a_1, a_2) = -(-a_3, -a_4)$. Prvi uvjet znači da je $d = 1 \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*^2}$, i ako je zadovoljen imamo

$$\varepsilon = (a_1, a_2)(a_1a_2, a_3a_4)(a_3, a_4) = (a_1, a_2)(a_3, a_4)(a_3a_4, a_3a_4).$$

Prema elementarnim svojstvima za Hilbertove simbole znamo da za svaki $x \in \mathbb{Q}_p^*$ vrijedi $(x, x) = (-1, x)(-x, x) = (-1, x)$, stoga

$$\begin{aligned}\varepsilon &= (a_1, a_2)(a_3, a_4)(-1, a_3a_4) = (a_1, a_2)(a_3, a_4)(-1, a_3)(-1, a_4)\\ &= (a_1, a_2)(-a_4, a_3)(-a_4, -1)(-1, -1) = (a_1, a_2)(-a_3, -a_4)(-1, -1),\end{aligned}$$

iz čega vidimo da je drug uvjet ekvivalentan s $\varepsilon = -(-1, -1)$, čime dokazujemo teorem u slučaju $n = 4$.
**Slučaj** $n \ge 5$.
Očito nam je dovoljno dokazati slučaj $n = 5$. Prema korolaru 3.2.8 nedegerirana forma stupnja 2, $q_1 = a_1x_1^2 + a_2x_2^2$ reprezentira $c \in \mathbb{Q}_p^*$ ako i samo ako $(c, -a_1a_2) = (a_1, a_2)$. Broj brojeva $c \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*^2}$, koje reprezentira $q_1$ nije 0 (npr. to vrijedi za $a_1$), pa prema lemi 3.2.9 (2) ima ih najmanje $2^{r-1}$, tj. najmanje 2 jer $r \ge 2$. Očito je da ovo vrijedi i za forme s vise od 2 varijable, pa tako i za $q$. Stoga neka je $c \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*^2}$ različit od $d(q)$ i reprezentiran s $q$. Prema lemi 3.1.14 postoji forma $q_1$ s 4 varijable $x_i$, $2 \le i \le 5$ takva da $q = cx_1^2 + q_1$, i očito je da $d(q) = cd(q_1)$. S obzirom da $c \ne d(q)$, $d(q_1) \ne 1 \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*^2}$, pa prema slučaj za $n = 4$ zaključujemo da $q_1$ reprezentira 0, stoga i $q$, čime završavamo dokaz ovog teorema. □

**Korolar 3.3.3.** *Neka je* $c \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*^2}$. *Nedegerirana forma q s n varijabli, invarijantama d i* $\varepsilon$ *reprezentira c ako i samo ako vrijedi jedno od sljedećeg:*

**(1)** $n = 1$ *i* $c = d$

**(2)** $n = 2$ *i* $(c, -d) = \varepsilon$

**(3)** $n = 3$ *i ili* $c \neq -d$ *ili* $(c = -d$ *i* $(-1, -d) = \varepsilon)$

**(4)** $n \geq 4$

*Dokaz.* Prema korolaru 3.1.14, $q$ reprezentira c ako i samo ako nedegerirana forma u $n + 1$ varijabli $q_1 = -cx_0^2 + q$ reprezentira 0. Vrijedi $d(q_1) = -cd(q)$ i $\varepsilon(q_1) = (-c, d(q))\varepsilon(q)$, pa ako primjenimo gornji teorem na $q_1$ zaključujemo tvdrnje ovog korolara koristeći svojstva Hilbertovih simbola (slučaj $n = 2$ je korolar 3.2.8). □

# Poglavlje 4

# Teorem Hasse-Minkowski

**Teorem 4.0.4.** *(Hasse-Minkowski). Neka je K polje i neka je q kvadratna forma u n varijabli i koeficijentima u K. Tada q reprezentira 0 u K ako i samo ako q reprezentira 0 u svakom upotpunjenju od K.*

U ovom radu dokazati ćemo Hasse-Minkowski teorem u slučaju $K = \mathbb{Q}$. Dokazivati ćemo tako što ćemo pretpostaviti da kvadratna forma ima netrivijalno rješenje u svakom upotpunjenju od $\mathbb{Q}$ te ćemo dokazati da tada ima i netrivijalno rješenje u $\mathbb{Q}$.

Za $n = 1$ rezultat je trivijalan pošto $ax^2 = 0$ ima netrivijalna rješenja ako i samo ako je $a = 0$.

## 4.1 Teorem Hasse-Minkowski za $n \leq 2$

Za dokaz u slučaju $n = 2$ biti će nam potrebna sljedeća lema.

**Lema 4.1.1.** *Nad bilo kojim poljem K, kvadratna forma $ax^2+bxy+cy^2 = 0$ ima netrivijalna rješenja ako i samo ako je $b^2 - 4ac$ kvadrat u K.*

*Dokaz.* Ako gornju formu $ax^2 + bxy + cy^2$ pomnožimo s $4a$ dobiti ćemo:

$$\begin{aligned} 4a(x^2 + bxy + cy^2) &= 4a^2x^2 + 4abxy + 4acy^2 \\ &= (2ax)^2 + 4abxy + (by)^2 - b^2y^2 + 4acy^2 \\ &= (2ax + by)^2 - b^2y^2 + acy^2 \\ &= (2ax + by)^2 - y^2(b^2 - 4ac) \end{aligned}$$

Imamo dva slučaja. Neka je $a \neq 0$. Za $(x, y) \neq (0, 0)$ takve da $ax^2 + bxy + cy^2 = 0$ mora vrijediti $y \neq 0$ (inače bi moralo vrijediti $ax^2 = 0$, tj $a = 0$), pa mora vrijediti da je $b^2 - 4ac = \left(\frac{2ax+by}{y}\right)^2$ tj. $b^2 - 4ac$ je kvadrat te ga možemo zapisati $b^2 - 4ac = u^2$. Suprotno,

neka je $b^2 - 4ac = u^2$, tada iz gornje jednakosti dobijemo da (za $a \neq 0$) $(x, y) = (u - b, 2a)$ zadovoljava jednadžbu $ax^2 + bxy + cy^2 = 0$ i $(x, y) \neq (0, 0)$. U drugom slučaju, za $a = 0$ tada je $b^2 - 4ac = b^2$ je kvadrat i $ax^2 + bxy + cy^2 = y(bx + c) = 0$ ima netrivijalna rješenja, npr. za $(x, y) = (1, 0)$. □

**Teorem 4.1.2.** *Neka je q kvadratna forma u 2 varijeble takva da $q = 0$ ima netrivijalna riješenja u $\mathbb{R}$ i u svakom $\mathbb{Q}_p$. Tada $q = 0$ ima netrivjalno rješenje u $\mathbb{Q}$.*

*Dokaz.* Neka je $q(x, y) = ax^2 + bxy + cy^2$ binarna kvadratna forma. Pošto $q$ reprezentira 0 u $\mathbb{R}$ netrivijalno mora vrijediti da je diskriminanta $d = b^2 - 4ac$ nenegativna (trivijalno, ali također slijedi iz gornje leme). Ako je $d = 0$ tada je $q$ kvadrat linearne forme pa tada $q$ reprezentira 0 netrivijalno u $\mathbb{Q}$. U suprotnom, tj. za $d > 0$, neka je $d = \prod_i p_i^{v_i}$ rastav na proste faktore od $d$. Pošto $q$ postiže 0 netrivijalno u svakom $\mathbb{Q}_{p_i}$, prema prethodnoj lemi mora vrijediti da je $d$ kvadrat u $\mathbb{Q}_{p_i}$. Iz toga slijedi da je $v_{p_i}(d) = v_i$ paran broj za svaki $i$, iz čega slijedi da je $d$ kvadrat u $\mathbb{Q}$, pa prema prethodnoj lemi slijedi da $q$ ima netrivijalna riješenja u $\mathbb{Q}$. □

## 4.2 Teorem Hasse-Minkowski za $n = 3$

Najvažniji dio dokaza teorema Hasse-Minkowski je u slučaju $n = 3$, koji ćemo upravo razmatrati.

**Teorem 4.2.1.** *Neka je q kvadratna forma u 3 varijeble takva da $q = 0$ ima netrivijalna riješenja u $\mathbb{R}$ i u svakom $\mathbb{Q}_p$. Tada $q = 0$ ima netrivjalno rješenje u $\mathbb{Q}$.*

*Dokaz.* Možemo pretpostaviti da je naša kvadratna forma dijagonalna kvadratna forma $q(x, y, z) = ax^2 + by^2 + cz^2$ . Ako je jedan od koeficjenata jedank 0 tada $q$ očito ima netrivijalna rješenja u $\mathbb{Q}$, pa možemo pretpostaviti da $abc \neq 0$. Nadalje, ako promijenimo $q$ i varijable množeći s racionalnim skalarom možemo pretpostaviti da su $a, b, c \in \mathbb{Z}$, i da je (promijenimo $x$ u $x/a$) $a = 1$, te da su b i c kvadratno slobodni brojevi. Sada možemo promijeniti notaciju te pišemo $q(x, y, z) = x^2 - ay^2 - bz^2$ gdje su a i b cijeli, kvadratno slobodni brojevi, i pretpostavimo $|a| \leq |b|$. Teorem ćemo dokazati indukcijski po m, za $m = |a| + |b|$. Za $m = 2$, imamo $q(x, y, z) = x^2 \pm y^2 \pm z^2$. $q$ ne može biti $x^2 + y^2 + z^2$, jer ta forma ne reprezentira 0 u $\mathbb{R}$ netrivijalno, a u ostalim slučajevima $q$ ima netrivijalna rješenja u $\mathbb{Q}$. Sada možemo pretpostaviti da je $m > 2$, tj. $|b| \geq 2$, i neka je $b = \pm \prod_{1 \leq i \leq k} p_i$ rastav na proste faktore od b. Neka je $p = p_i$ za neki i. Tvrdimo da je $a$ kvadrat modulo p . Ta tvrdnja je trivijalna u slučaju $a \equiv 0 \pmod{p}$, inače $a$ je p-adski broj i po pretpostavci postoji netrivijalno p-adsko rješenje od $ay^2 + bz^2 = x^2$ gdje možemo pretpostaviti da su $x$,$y$ i $z$ u $\mathbb{Z}_p$ takvi da je barem jedan u $\mathbb{Z}_p^\times$. Stoga $x^2 \equiv ay^2 \pmod{p\mathbb{Z}_p}$. Sada slijedi da je $y \in \mathbb{Z}_p^\times$ , jer u suprotnome dobijemo da je $v_p(x) \geq 1$, pa vrijedi da je $v_p(bz^2) \geq 2$ te slijedi $v_p(z) \geq 1$

($b$ nije djeljiv s kvadratom nekog cijelog broja osim 1) što je u suprotnosti s činjenicom da je jedan od brojeva $x$, $y$ i $z$ u $\mathbb{Z}_p^\times$. Slijedi da je $a \equiv (x/y)^2 \pmod{p\mathbb{Z}_p}$, te je $a$ kvadratni modul od $p$ što dokazuje tvrdnju. S obzirom da to vrijedi za sve $p|b$, korištenjem Kineskog teorema o ostatcima 1.1.16 dobijemo da je $a$ kvadratni ostatak od $b$, odnosno da postoji $b'$ i $k$ takvi da $k^2 = a + bb'$, gdje $k$ može biti izabran takav da vrijedi $|k| \leq |b|/2$. S obzirom da je $bb' = k^2 - a$, $bb'$ je norma u $K(\sqrt{a})/K$, gdje je $K = \mathbb{Q}$ ili bilo kojem $\mathbb{Q}_v$. Stoga kao i u dokazu propozicije 3.2.2 zaključujemo da $q$ postiže 0 u K ako i samo ako isto vrijedi i za $q'$, uz $q'(x, y, z) = x^2 - ay^2 - b'z^2$. Posebice, prema pretpostavci $q'$ postiže 0 u svim $\mathbb{Q}_v$. Ali pošto $|b| \geq 2$ i $|a| \leq |b|$, dobijemo:

$$|b'| = \left|\frac{t^2 - a}{b}\right| \leq \frac{|b|}{4} + 1 < |b|.$$

Stoga možemo primijeniti indukcijsku hipotezu na formu $q'$ (točnije na formu $q''$, gdje je $b'$ zamijenjeno s njegovim kvadratno slobodnim dijelom); stoga $q'$ postiže 0 u $\mathbb{Q}$ pa isto vrijedi i za formu $q$. □

Kako bismo mogli dokazati Hasse-Miknowski teorem za $n \geq 4$ varijable trebamo pojačati tvrdnju dobivenu za $n = 3$

**Propozicija 4.2.2.** *Neka je $q(x, y, z)$ kvadratna forma u 3 varijable i pretpostavimo da $q(x, y, z) = 0$ ima netrivijalno rješenje u svakom upotpunjenju od $\mathbb{Q}$ osim u možda jednom. Tada ima i netrivijalno rješenje u $\mathbb{Q}$.*

*Dokaz.* Kao i inače možemo pretpostaviti da je $q$ nedegerirana, jer je u protivnome rezultat trivijalan. Također možemo pretpostaviti da ako promijenimo $q$ u ekvivalentnu formu, $q(x, y, z) = ax^2 + by^2 + cz^2$ je dijagonalna forma. Prema propoziciji 3.2.7 $q$ predstavlja 0 u $\mathbb{Q}_v$ ako i samo ako:

$$(-1, -abc)_v = (a, b)_v(a, c)_v(b, c)_v.$$

Prema pretpostavci ova tvrdnja je istinita za svaki $v$ osim možda jednog. Pošto obje strane zadovoljavaju produktnu formulu slijedi da je jednakost vrijedi za sve $v$. Ponovno prema propoziciji 3.2.7 $q$ predstavlja 0 u $\mathbb{Q}_v$ za svaki $v$ pa prema dokazu teorema Hasse-Minkowski za $n = 3$ predstavlja 0 i u $\mathbb{Q}$. □

## 4.3 Teorem Hasse-Minkowski za $n = 4$

**Teorem 4.3.1.** *Neka je $q$ kvadratna forma u 4 varijeble takva da $q = 0$ ima netrivijalna riješenja u $\mathbb{R}$ i u svakom $\mathbb{Q}_p$. Tada $q = 0$ ima netrivjalno rješenje u $\mathbb{Q}$.*

*Dokaz.* Možemo pretpostaviti da $q = a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2$. Neka je $v \in \mathbb{Q}$. Pošto $q$ predstavlja 0 u $\mathbb{Q}_v$, korolar 3.1.15 govori nam da postoji $c_v \in \mathbb{Q}_v^*$ takav da je predstavljen i s $a_1x_1^2 + a_2x_2^2$ i s $a_3x_3^2 + a_4x_4^2$, i korolar 3.3.3 (2) (koji vrijedi trivijalno i za $\mathbb{R}$) implicira da za svaki $v$ vrijdi

$$(c_v, -a_1a_2)_v = (a_1, a_2)_v \quad i \quad (c_v, -a_3a_4)_v = (a_3, a_4)_v.$$

Prema produktnoj formuli za Hilbertov simbol zaključujemo iz teorema 3.2.12 da postoji $c \in \mathbb{Q}^*$ takav da za svaki $v$ vrijedi $(c, -a_1a_2)_v = (a_1, a_2)_v$ i $(c, -a_3a_4)_v = (a_3, a_4)_v$. Tada forma u 3 varijable $a_1x_1^2 + a_2x_2^2 - cx_0^2$ reprezentira 0 u svakom $\mathbb{Q}_v$, pa prema dokazu terema Hasse-Minkowskog za $n = 3$ slijedi da predstavlja 0 i u $\mathbb{Q}$, pa slijedi da je $c$ predstavljen s $a_1x_1^2+a_2x_2^2$. Analogno dobijemo da je $c$ predstavljen i s $a_3x_3^2+a_4x_4^2$, pa vrijedi da predstavlja 0 u $\mathbb{Q}$. □

## 4.4 Teorem Hasse-Minkowski za $n \geq 5$

**Teorem 4.4.1.** *Neka je q kvadratna forma u 5 varijabli. Pretpostavimo da $q = 0$ ima realno rješenje. Tada $q = 0$ ima rješenje u $\mathbb{Q}$.*

Primjetimo da više ne moramo pretpostaviti da $q$ ima $p$-adsko rješenje jer prema teoremu 3.3.2 znamo da svaka kvadratna forma za broj varijabli $n \geq 5$ ima netrivijlna riješenja u $\mathbb{Q}_p$ za svaki $p$.

*Dokaz.* Dokaz će biti veoma sličan dokazu u slučaju $n = 4$ pa ćemo u ovom slučaju dati samo skicu dokaza.Možemo pretpostaviti da je $q$ regularna i dijagonalna kvadratna forma i zapisaujemo $g = a_1x_1^2 + a_2x_2^2$,$h = -a_3x_3^2 - a_4x_4^2 - a_5x_5^2$, i pretpostavimo da je $a_1 > 0$ i $a_5 < 0$. Pomoću Dirichletovog teorema možemo pronaći cijeli broj $a > 0$ takav da i $g$ i $h$ predstavljaju $a$ u $\mathbb{R}$ i u $\mathbb{Q}_p, \forall p$ osim možda za $p = q$ gdje je $q$ jedinstveni neparni broj koji ne dijeli $a_1a_2a_3a_4a_5$. Također tvrdimo da $g$ i $h$ postižu a u $\mathbb{Q}_p$. Tvrdnja za $g$ slijedi iz propozicije 4.2.2 koristeći pomoćnu formu $g_1 = -ax_0^2 + g$. Za $h$, zbog $a_5 < 0$ vrijedi

$$(-1, d(h)) = (-1, -a_3a_4a_5) = (-1, a_3)(-1, a_4)(-1, -a_5) = (a_3, -1)(-1, a_4) = (-a_3, -a_4) = \varepsilon(h)$$

pa prema teoremu 3.2.7 znamo da ima netrivijalno rješenje u $\mathbb{Q}_p$ pa predstvalja sve elemente iz $\mathbb{Q}_p$ prema propoziciji 3.1.12 čime potvrđujemo gornju tvrdnju. Koristeći korolar 3.1.14 vidimo da forme $g_1 = -ax_0^2 + g$ i $h_1 = -ax_0^2 + h$ s tri i četiri varijable imaju netrivijalna rješenja u svakom upotpunjenju od $\mathbb{Q}$, pa prema teoremu Hasse-Minkowski za forme s tri i četiri varijable slijedi da $g_1$ i $h_1$ imaju rješenje i u $\mathbb{Q}$ pa je a predstavljn s $g$ i $h$ i u $\mathbb{Q}$, čime kao i prije dokazujemo da $q = 0$ ima netrivijalno racionalno rješenje. □

**Korolar 4.4.2.** *Neka je q kvadratna forma u $n \geq 5$ varijabli,i pretpostavimo da q predstavlja 0 u $\mathbb{R}$. Tada q predstavlja 0 i u $\mathbb{Q}$.*

*Dokaz.* Možemo pretpostaviti da je $q$ regularna i dijagonalna forma i da je $a_1 > 0$ te $a_5 < 0$. Tada $q = q_1 + q_2$ tako da $q_1 = \sum_{1 \leq i \leq 5} a_i x_i^2$. Prema gornjem teoremu $q_1 = 0$ ima netrivijalno rješenje, i izaberemo $x_i = 0$ za $5 < i \leq n$, čime dokazujemo korolar. □

Ovime smo završili dokaz teorema Hasse-Minkowski za $K = \mathbb{Q}$.

# Bibliografija


[1] H. Cohen, *Number Theory, Volume I: Tools and Diophantine Equations, Springer*, 2007

[2] Andrej Dujella, *Uvod u teoriju brojeva (skripta), PMF - Matematički odjel, Sveučilište u Zagrebu*(https://web.math.pmf.unizg.hr/ duje/utb/utblink.pdf)

[3] Ivan Matić, *Uvod u teoriju brojeva,Osijek*,2014 (https://www.mathos.unios.hr/ imatic/uvod

[4] Filip Najman, *Aritmetička geometrija, PMF - Matematički odjel, Sveučilište u Zagrebu*, 2015/2016

[5] Lee Dicker, *The Hasse–Minkowski Theorem, University of Minnesota*, REU Summer 2001 (http://www.math.umn.edu/ garrett/students/reu/hasse_minkowski.pdf)

[6] Andrew V. Sutherland, *Introduction to Arithmetic Geometry*, MIT, 2003

[7] Mateja Škledar, *Dirichletov teorem*, PMF-Matematički odsjek, Sveučilište u Zagrebu, 2015 (http://digre.pmf.unizg.hr/4324/)

# Sažetak

Tema ovog diplomskog rada je lokalno-globalni princip. Dokazati ćemo jedanu od najznačajnijih posljedica lokalno-globalnog principa teorem Hasse-Minkowskog, koji tvrdi da lokalno globalni princip vrijedi za kvadratne forme. U prvom poglavlju ćemo se upoznati s osnovnim pojmovima i rezultatima teorije brojeva. U drugom i trećem poglavlju smo definirali p-adske brojeve i kvadratne forme, te dokazali teoreme i tvrdnje koje će biti od velike važnosti u dokazivanju teorema Hasse-Minkowski. Ovaj rad zaključiti ćemo s dokazom Hasse-Minkowski teorema, koji ćemo provoditi zasebno za kvadratne forme s 1,2,3,4 i više od 5 varijabli.

# Summary

The theme of this master thesis is the local-global principle. We are going to prove one of the most significant results of the local-global principle the Hasse-Minkowski theorem, which claims that local-global principle is valid for quadratic forms. In the first chapter we are going to get familiar with basic terms and results of number theory. In the second and third chapter we define $p$-adic numbers and quadratic forms, and prove theorems and statements that will be of significant importance in proving the Hasse-Minkowski theorem. We will conclude this master thesis with a proof of the Hasse-Minkowski theorem, which we will conduct by proving it separately for quadratic forms with 1,2,3,4, and more than 5 variables.

# Životopis

Moje ime je Ivona Mrkalj. Rođena sam 13.07.1990. u Rijeci. Završila sam Osnovnu školu Gornja Vežica u Rijeci, te Gimnaziju Andrije Mohorovičića Rijeka, također u Rijeci. Nakon završetka srednje škole, 2009. godine, upisala sam Prirodoslovno matematički fakultet, smjer Matematika, u Zagrebu. Titulu sveučilišne prvostupnice (baccalaureus) matematike stekla sam 2013. godine, te iste godine upisala diplomski studij Financijska i poslovna matematika na istom fakultetu.