UNIVERZITET U BEOGRADU

MATEMATIČKI FAKULTET

MASTER RAD

Aritmetička statistika kubičnih i kvartičnih binarnih formi

Autor
Ilija Vrećica

Mentor
Dr. Goran Đanković

oktobar, 2015.

Sadržaj

Glava 1

Uvod u neke pojmove

1.1 Diskriminanta polinoma

Diskriminanta polinoma sa jednom promenljivom $p(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_0$ je

$$\mathrm{Disc}(p) = a_n^{2n-2} \prod_{1 \le i < j \le n} (r_i - r_j)^2,$$

gde su r_i koreni polinoma p, $i = 1, ..., n$.

Mi ćemo se u ovom radu baviti binarnim kvadratnim, kubičnim i kvartičnim formama. No, i za ove polinome možemo definisati diskriminantu: za

$$p(x, y) = a_n x^n + a_{n-1}x^{n-1}y + ... + a_1 xy^{n-1} + a_0 y^n,$$

posmatrajmo razlomljenu funkciju

$$p_1(x, y) := p(x, y)/y^n = a_n \frac{x^n}{y^n} + a_{n-1}\frac{x^{n-1}}{y^{n-1}} + ... + a_1 \frac{x}{y} + a_0.$$

Diskriminanta binarne forme p će biti upravo diskriminanta polinoma

$$q(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0.$$

Diskriminanta binarne kvadratne forme $f(x,y) = ax^2 + bxy + cy^2$ je

$$\text{Disc}(f) = a^{2\cdot 2-2}(x_1 - x_2)^2 = a^2(x_1 - x_2)^2.$$

No, znamo da je $x_{1,2} = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$, pa važi:

$$\text{Disc}(f) = a^2 \frac{b^2 - 4ac}{a^2} = b^2 - 4ac.$$

Nađimo sada diskriminante polinoma trećeg stepena:

Neka je $f(x) = ax^3 + bx^2 + cx + d$. Nađimo korene ovog polinoma: Neka je $y = x + \frac{b}{3a}$. Tada naš polinom postaje

$$a\left(y - \frac{b}{3a}\right)^3 + b\left(y - \frac{b}{3a}\right)^2 + c\left(y - \frac{b}{3a}\right) + d =$$

$$ay^3 + \left(c - \frac{b^2}{3a}\right)y + \left(d + \frac{2b^3}{27a^3} - \frac{bc}{3a}\right).$$

Drugim rečima, svaki kubni polinom se može smenom promenljive svesti na sledeći oblik:

$$y^3 + Ay = B$$

Sada, neka su $s, t \in \mathbb{R}$ takvi da zadovoljavaju sledeći sistem jednačina:

$$3st = A \tag{1.1}$$

$$s^3 - t^3 = B$$

Tada naš kubni polinom ima sledeći oblik:

$$y^3 + 3sty = s^3 - t^3,$$

i može se videti da je $y = s - t$ jedan koren ovog polinoma. Preostaje samo da nađemo s i t. Prva jednakost (1.1) nam daje $s = \frac{A}{3t}$. Iz druge jednakosti imamo:

$$\frac{A^3}{27t^3} - t^3 = B \Longrightarrow t^6 + Bt^3 - \frac{A^3}{27} = u^2 + Bu - \frac{A^3}{27} = 0,$$

gde je $u = t^3$. Odavde imamo da je

$$u = \frac{-B \pm \sqrt{B^2 - \frac{4A^3}{27}}}{2},$$

tj.

$$t = \sqrt[3]{\frac{-B \pm \sqrt{B^2 - \frac{4A^3}{27}}}{2}},$$

a odavde dobijamo i s. Dakle, pomoću s i t dobijamo jedan koren polinoma, odakle se problem nalaženja korena kubnog polinoma svodi na rešavanje kvadratne jednačine. Iz računa se može videti da je diskiminanta kubnog polinoma

$$\mathrm{Disc}(f) = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd.$$

Diskriminanta binarne kvartične forme $f(x, y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4$ se može videti da je:

$$\mathrm{Disc}(f) = d^2c^2b^2 - 4d^3b^3 - 4d^2c^3a + 18d^3cba - 27d^4a^2 + e\left(-4c^3b^2 + 18dcb^3 + \right. \quad (1.2)$$

$$\left. + 16c^4a - 80dc^2ba - 6d^2b^2a + 144d^2ca^2\right) + e^2\left(-27b^4 + 144cb^2a - 128c^2a^2 - \right.$$

$$\left. - 192dba^2\right).$$

1.2 Matrične grupe i njihovo dejstvo na binarne forme

Grupu 2×2 matrica sa koeficijentima u $\mathbb{R}$ ($\mathbb{Z}$) čije su determinante različite od 0 obeležavamo sa $\mathrm{GL}_2(\mathbb{R})$ ($\mathrm{GL}_2(\mathbb{Z})$).

Grupu 2×2 matrica sa koeficijentima u $\mathbb{R}$ ($\mathbb{Z}$) čije su determinante jednake 1 obeležavamo sa $\mathrm{SL}_2(\mathbb{R})$ ($\mathrm{SL}_2(\mathbb{Z})$).

Grupa $\mathrm{GL}_2(\mathbb{R})$ deluje na prostor binarnih formi na sledeći način: ako je $k \in \mathrm{GL}_2(\mathbb{R})$, i

$$f(x, y) = a_n x^n + a_{n-1} x^{n-1} y + ... + a_0 y^n$$

neka binarna forma n-tog stepena, onda je

$$(k \cdot f)(x, y) = f([x, y] \cdot k)$$

takođe binarna forma n-tog stepena.

Svakoj binarnoj kubnoj formi $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ odgovara Hessian-ova kovarijanta

$$H_f(x, y) := (b^2 - 3ac)x^2 + (bc - 9ad)xy + (c^2 - 3bd)y^2. \tag{1.3}$$

Može se videti da za $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ važi: $\gamma \cdot H_f = H_{\gamma \cdot f}$.

1.3 Iwasawa-ina dekompozicija

Neka je $G = \mathrm{SL}(m, \mathbb{R})$. Označimo: A je grupa dijagonalnih matrica sa pozitivnim koeficijentima, N je grupa gornje trougaonih matrica, koje imaju jedinice na svim mestima na dijagonali, $K = \mathrm{SO}(m)$. Posmatrajmo preslikavanje

$$K \times A \times N \to G$$

$$(k, a, n) \mapsto kan.$$

Neka je $\{e_1, ..., e_m\}$ standardna baza za $\mathbb{R}^m$, $g \in G$ proizvoljno, i posmatrajmo bazu $\{ge_1, ..., ge_m\}$. Gram-Šmitov postupak na ovu bazu nam daje novu ortonormiranu bazu $v_1, ..., v_m$ za koju važi

$$\text{span}\{ge_1, ..., ge_j\} = \text{span}\{v_1, ..., v_j\}$$

$$v_j \in \mathbb{R}^+(ge_j) + \text{span}\{v_1, ..., v_{j-1}\}$$

za $1 \leq j \leq m$. Neka je $k \in \text{O}(m)$ matrica takva da je $k^{-1}v_j = e_j$. Tada je $k^{-1}g$ gornje trougaona sa pozitivnim koeficijentima na dijagonali. Pošto g ima determinantu 1, i k ima determinantu norme 1, to k mora imati determinantu 1. Odavde sledi da je $k \in \text{SO}(m)$, $k^{-1}g \in AN$, i g se može prikazati kao

$$g = k(k^{-1}g) \in K(AN).$$

Dakle, pošto je g bilo proizvoljno, preslikavanje $K \times A \times N \to G$ je na.

Iz $K \cap AN = \{I\}$ sledi da je preslikavanje 1-1: matrice u AN su gornje trougaone, i imaju pozitivne koeficijente na dijagonalama, kada se neka matrica l iz AN pomnoži sa l^*, dobije se matrica j_1 za čije elemente važi $j_{ii} = l_{ii}^2$. Dakle, l mora imati jedinice na dijagonali ako želimo da bude $ll^* = I$, pa je $l \in N$. Posmatrajmo proizvod ll^*:

$$(ll^*)_{ii} = \sum_{k=1}^{m}(l_{ik} \cdot (l)_{ki}^T) = \sum_{k=1}^{m}(l_{ik} \cdot l_{ik}) = \sum_{k=1}^{m}(l_{ik}^2) = \sum_{\substack{k=1 \\ k \neq i}}^{m}(l_{ik}^2) + 1.$$

Prema tome, da bi l bilo u K, svi ostali koeficijenti l van dijagonale moraju biti 0, i $l_{ii} = 1$, za $1 \leq i \leq m$. Dakle, $K \cap AN = \{I\}$. Odavde sledi da je preslikavanje 1-1: ako je $kan = I$, za neke $k \in K$, $a \in A$ i $n \in N$, onda možemo videti an kao inverz od k, tj. $an = k^{-1}$. No, $k^{-1} \in K$, a $an \in AN$ i $K \cap AN = \{I\}$, pa mora biti $k^{-1} = I = an$, a samim tim i $k = I$. Pošto je $an = I$, to a na dijagonali može imati samo jedinice, pa je $a = I$, pa n može biti samo I. Dakle, preslikavanje je 1-1.

Iz formula Gram-Šmitovog postupka se može videti da je inverz gladak.

1.4 Gauss-ov fundamentalan domen

Neka je $\mathcal{F}$ Gauss-ov fundamentalan domen za $\mathrm{GL}_2(\mathbb{Z}) \setminus \mathrm{GL}_2(\mathbb{R})$ u $\mathrm{GL}_2(\mathbb{R})$. Tada skup $\mathcal{F}$ ima sledeći oblik:

$$\mathcal{F} = \{nak\lambda : n \in N'(a), a \in A', k \in K, \lambda \in \Lambda\},$$

gde su

$$N'(a) = \left\{ \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} : n \in \nu(a) \right\}, A' = \left\{ \begin{pmatrix} t^{-1} & 0 \\ 0 & t \end{pmatrix} : t \geq \frac{\sqrt[4]{3}}{\sqrt{2}} \right\},$$

$$\Lambda = \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} : \lambda > 0 \right\},$$

i $K = \mathrm{SO}_2(\mathbb{R})$, pri čemu je $\nu(a)$ unija dva podintervala od $[-\frac{1}{2}, \frac{1}{2}]$.

1.5 Haar-ova mera i p-adični celi

Kompaktne Lijeve grupe imaju bitno svojstvo: na njima se može definisati takozvana Haar-ova mera, tj. nenula regularna Borelova mera koja je invarijantna pod levom translacijom. Neka je μ_l leva Haar-ova mera na kompaktnoj Lijevoj grupi G. Tada G takođe ima i desnu Haar-ovu meru: $\mu_r(E) = \mu_l(E^{-1})$ (E^{-1} je skup inverza iz E). Neka je sada A skup u σ algebri generisan kompaktnim podskupovima od G koji su prebrojivi preseci otvorenih skupova, i neka je I_A karakteristična funkcija za A. Fubinijeva teorema, primenjena na funkciju $(x, y) \mapsto I_A(xy)$, nam daje:

$$\mu_l(G)\mu_r(A) = \int_G \left[\int_G I_A(x) d\mu_r(x) \right] d\mu_l(y) = \int_G \left[\int_G I_A(xy) d\mu_r(x) \right] d\mu_l(y) =$$

$$= \int_G \left[\int_G I_A(xy) d\mu_l(y) \right] d\mu_r(x) = \int_G \left[\int_G I_A(y) d\mu_l(y) \right] d\mu_r(x) = \mu_r(G)\mu_l(A).$$

Pošto su μ_l i μ_r regularne Borelove mere, to ova jednakost važi za sve Borelove skupove A. Prema tome, svaka leva Haar-ova mera je proporcionalna svakoj desnoj Haar-ovoj meri. Postoji samo jedna leva Haarova mera (do na konstantu), i ona je desna Haarova mera, zbog čega možemo razmatrati Haar-ovu meru μ, koja je invarijantna sa obe strane. Ova mera se može normalizovati tako da je $\mu(G) = 1$.

Posmatrajmo sada, za neki prost broj p, topološki prsten p-adičnih celih, $\mathbb{Z}_p$. Prvo, skup p-adičnih racionalnih brojeva, $\mathbb{Q}_p$, se dobija od skupa racionalnih brojeva tako što se na $\mathbb{Q}$ dodaju beskonačne sume oblika $\sum_{i=k}^{\infty} a_i p^i$, gde su a_i elementi skupa $\{0, 1, \ldots, p-1\}$, i k ne mora biti pozitivan celi broj. Drugo, na $\mathbb{Q}$ se može definisati sledeća valuacija, koja se može prirodno proširiti na $\mathbb{Q}_p$: ako $p \nmid ab$, tada je

$$\left| p^n \frac{a}{b} \right|_p = p^{-n}.$$

Skup $\mathbb{Z}_p$ je skup svih redova $\sum_{i=k}^{\infty} a_i p^i$ u $\mathbb{Q}_p$ za koje je $a_i = 0$ za sve $i < 0$, i zove se skup p-adičnih celih. To je topološki prsten, v cija je topologija indukovana sa valuacijom $|\cdot|_p$. Takođe, $\mathbb{Z}_p$ ima meru, i to je Haarova mera aditivne grupe $\mathbb{Z}_p$.

1.6 Neki rezultati iz geometrije brojeva

U ovom delu ćemo dokazati Davenport-ovu teoremu koja će nam biti potrebna u sledeće dve glave.

Definicija 1.6.1. *Multiskup je skup koji sadrži više kopija barem jednog elementa. Broj kopija nekog elementa je njegov multiplicitet.*

Definicija 1.6.2. *Multiskup $\mathcal{R} \subset \mathbb{R}^n$ je merljiv ako je $\mathcal{R}_k$ merljivo za svako k, gde je $\mathcal{R}_k$ skup svih tačaka u $\mathcal{R}$ sa multiplicitetom k. Ako je multiskup merljiv, onda njegovu meru definišemo na sledeći način:*

$$\mathrm{Vol}(\mathcal{R}) = \sum_k \mathrm{Vol}(\mathcal{R}_k),$$

gde je $\mathrm{Vol}(\mathcal{R}_k)$ *euklidska mera* $\mathcal{R}_k$.

Definicija 1.6.3. *Algebarski skup $S \subset \mathbb{R}^n$ je skup koji je opisan sa konačno mnogo polinomijalnih jednakosti ili nejednakosti, ili bilo koja konačna unija takvih skupova. Drugim rečima, on je određen nekim algebarskim nejednakostima i jednakostima*

$$G_j(x_1, ..., x_n) = 0, \quad (j = 1, 2, ..., k_1),$$

$$F_i(x_1, ..., x_n) \geq 0, (i = 1, 2, ..., k_2),$$

gde su F_i i G_j polinomi sa realnim koeficijentima, i stepenima ograničenim nekim prirodnim brojem l.

Definicija 1.6.4. *Unipotentna linearna transformacija prostora $\mathbb{R}^n$ sa matricom A je ona za koju važi da je $A - I$ nilpotentno, tj. $(A - I)^k = 0$, za neko $k \in \mathbb{N}$ (I je jedinična matrica).*

Definicija 1.6.5. *Neka je $\mathcal{R}$ neki podskup od $\mathbb{R}^n$. Tada sa $\overline{\mathcal{R}}$ označavamo projekciju podskupa $\mathcal{R}$ na neki potprostor (koji se dobija od $\mathbb{R}^n$ tako što se neki broj koordinata izjednači sa nulom), takav da je mera $\overline{\mathcal{R}}$ u tom potprostoru najveća mera među merama svih mogućih ovakvih projekcija.*

Teorema 1.6.6. *([D], [BS]) Neka je $\mathcal{R}$ ograničeni, algebarski multiskup u $\mathbb{R}^n$ sa maksimalnim multiplicitetom m, definisan sa najviše k polinomijalnih nejednakosti čiji je stepen najviše l. Neka je $\mathcal{R}'$ slika $\mathcal{R}$ pri bilo kojoj trougaonoj, unipotentnoj transformaciji prostora $\mathbb{R}^n$. Tada je broj integralnih tačaka, tj. tačaka sa celobrojnim koordinatama (računate sa multiplicitetom) u $\mathcal{R}'$ jednak*

$$\mathrm{Vol}(\mathcal{R}) + O(\max\{\mathrm{Vol}(\overline{\mathcal{R}}), 1\}).$$

Implicirana konstanta u drugom sabirku zavisi samo od n, m, k i l.

Ova teorema, koju ćemo upotrebljavati u ovom obliku pri radu sa binarnim kubičnim i kvartičnim formama, je posledica sledeće teoreme ([D]):

Teorema 1.6.7. *Neka je $\mathcal{R}$ kompaktan podskup od $\mathbb{R}^n$. Neka za skup $\mathcal{R}$ i prirodan broj h važe sledeća dva uslova:*

1. *Svaka prava koja je paralelna sa nekom od n osa ima presek sa $\mathcal{R}$ koji se, ako nije prazan, sastoji od najviše h intervala.*
2. *Isto tvrđenje važi i za bilo koju m-dimenzionalnu oblast koja se dobija projektovanjem $\mathcal{R}$ na neki koordinatni prostor koji se dobija tako što se neki izbor $n-m$ koordinata izjednači sa nulom. Ovo važi za svako m od 1 do $n-1$.*

Tada važi

$$|N(\mathcal{R}) - V(\mathcal{R})| \leq \sum_{m=0}^{n-1} h^{n-m} V_m,$$

gde je $V(\mathcal{R})$ zapremina $\mathcal{R}$, $N(\mathcal{R})$ broj celobrojnih tačaka u $\mathcal{R}$, V_m je suma m dimenzionalnih zapremina projekcija $\mathcal{R}$ na koordinatne prostore koji se dobiju tako što se bilo kojih $n-m$ koordinata izjednači sa nulom, i $V_0 = 1$.

Pošto je $\mathcal{R}$ kompaktan, možemo smatrati da su zapremine u teoremi Lebesgueove mere, koje postoje jer su svi skupovi čije zapremine koristimo kompaktni.

Dokaz: Neka je $f(x_1, ..., x_n)$ karakteristična funkcija skupa $\mathcal{R}$. Ona je merljiva, pošto je $\mathcal{R}$ zatvoren. Ako je $i_1 < i_2 < ... < i_m$ bilo koji izbor indeksa iz $1, 2, ..., n$, sa $f(x_{i_1}, ..., x_{i_m})$ obeležavamo funkciju koja je ili 1 ili 0 u zavisnosti od toga da li se za preostalih $n-m$ argumenata mogu izabrati vrednosti tako da je $(x_1, ..., x_n) \in \mathcal{R}$. Dakle, ova funkcija je karakteristična funkcija za m-dimenzionalni skup koji se dobija tako što se $\mathcal{R}$ projektuje na koordinatni prostor u kojem su preostalih $n-m$ koordinata jednake nuli. Pošto je projekcija zatvorenog skupa zatvorena, ova funkcija je takođe merljiva funkcija.

Smatraćemo da su sve sumacije i integracije proširene na neku kocku koja sadrži $\mathcal{R}$, i da su promenljive u sumacijama celobrojne. Specijalan slučaj Fubini-eve teoreme nam kaže da je mera $\mathcal{R}$ jednaka

$$V(\mathcal{R}) = \int dx_1 \int dx_2 ... \int f(x_1, ..., x_n) dx_n,$$

a slično se dobija i za projekcije $\mathcal{R}$.

Imajući ovo u vidu, formula u teoremi postaje:

$$\begin{aligned} &\left| \int dx_1 ... \int f(x_1, ..., x_n) dx_n - \sum_{x_1} ... \sum_{x_n} f(x_1, ..., x_n) \right| \leq \\ &\leq \sum_{m=0}^{n-1} h^{n-m} \sum_{i_1 < ... < i_m} \int dx_{i_1} ... \int f(x_{i_1}, ..., x_{i_m}) dx_{i_m}; \end{aligned} \tag{1.4}$$

u slučaju da je $m = 0$, unutrašnjoj sumi na desnoj strani nejednakosti se dodeljuje vrednost 1.

Teoremu ćemo dokazati indukcijom po dimenziji prostora u kome radimo, tj. po n:

Neka je dimenzija prostora 1. Tada se $\mathcal{R}$, zbog svojstva 1, sastoji od najviše h intervala, pa nejednakost postaje

$$\left| \int f(x) dx - \sum_x f(x) \right| \leq h,$$

što je tačno (na primer, interval $[0, 2]$ ima meru 2, a 3 celobrojne tačke, što nam pokazuje da je za svaki interval broj celobrojnih tačaka ograničen sa njegovom merom plus 1).

Pretpotstavimo da teorema važi ako je dimenzija prostora jednaka $n - 1$, i dokažimo da ona važi i za prostore dimenzije n. Presek $\mathcal{R}$ sa ravni $x_1 = \xi$ daje $(n - 1)$ dimenzioni prostor, pa pošto smo pretpostavili da teorema važi za $n - 1$, to za bilo koju vrednost x_1 znači da je

$$\left| \int dx_2 ... \int f(x_1, ..., x_n) dx_n - \sum_{x_2} ... \sum_{x_n} f(x_1, ..., x_n) \right| \leq$$

$$\leq \sum_{r=0}^{n-2} h^{n-1-r} \sum_{\substack{i_1 < ... < i_r \\ i_1 \geq 2}} \int dx_{i_1} ... \int f(x_1, x_{i_1}, ..., x_{i_r}) dx_{i_r}.$$

Ako integralimo na levoj strani unutar znakova apsolutne vrednosti po x_1, dobijamo

$$\left| \int dx_1 ... \int f(x_1, ..., x_n) dx_n - \sum_{x_2} ... \sum_{x_n} \int f(x_1, ..., x_n) d_{x_1} \right| \leq$$

$$\leq \sum_{r=0}^{n-2} h^{n-1-r} \sum_{\substack{i_1 < ... < i_r \\ i_1 \geq 2}} \int dx_1 \int dx_{i_1} ... \int f(x_1, x_{i_1}, ..., x_{i_r}) dx_{i_r}.$$

Nakon zamene $m = r + 1$, dobijamo na desnoj strani nejednakosti

$$\sum_{m=1}^{n-1} h^{n-m} \sum_{\substack{j_1 < ... < j_m \\ j_1 = 1}} \int dx_{j_1} ... \int f(x_{j_1}, ..., x_{j_m}) dx_{j_m}. \tag{1.5}$$

Iz baze indukcije vidimo da fiksiranjem vrednosti $x_2, ..., x_n$ dobijamo

$$\left| \int f(x_1, ..., x_n) dx_1 - \sum_{x_1} f(x_1, ..., x_n) \right| \leq h f(x_2, ..., x_n).$$

Sada sumiramo po $x_2, ..., x_n$, i koristeći induktivnu hipotezu dobijamo

$$\left| \sum_{x_2} ... \sum_{x_n} \int f(x_1, ..., x_n) dx_1 - \sum_{x_1} ... \sum_{x_n} f(x_1, ..., x_n) \right| \leq h \sum_{x_2} ... \sum_{x_n} f(x_2, ..., x_n) \leq$$

$$\leq \int dx_2 ... \int f(x_2, ..., x_n) dx_n + h \sum_{m=0}^{n-2} h^{n-1-m} \sum_{\substack{i_1 < ... < i_m \\ i_1 \geq 2}} \int dx_{i_1} ... \int f(x_{i_1}, ..., x_{i_m}) dx_{i_m} =$$

$$= \sum_{m=0}^{n-1} h^{n-m} \sum_{\substack{i_1 < ... < i_m \\ i_1 \geq 2}} \int dx_{i_1} ... \int f(x_{i_1}, ..., x_{i_m}) dx_{i_m}. \tag{1.6}$$

Suma izraza (1.5) i (1.6) nam daje gornje ograničenje za levu stranu (1.4). Zbir ova dva izraza nam daje: h^n u (1.6) kada je $m = 0$, i za $1 \leq m \leq n-1$ imamo

$$\sum_{i_1<...<i_m} \int dx_{i_1} ... \int f(x_{i_1}, ..., x_{i_m}) dx_{i_m},$$

što nam daje dokaz teoreme. □

U našem slučaju, skup $\mathcal{R}$ je algebarski, i stepeni polinoma koji ga definišu su ograničeni sa l. Takođe, pretpotstavljamo da nejednakosti impliciraju ograničenost $\mathcal{R}$. Tada važi da je svaka m dimenziona projekcija $\mathcal{R}$ na neki koordinatni prostor takođe definisana sa konačno mnogo algebarskih nejednakosti, gde su broj ovih nejednakosti, kao i njihovi stepeni, ograničeni brojevima koji zavise od n, k, l. $\mathcal{R}$ zadovoljava svojstva 1 i 2, za neko h koje zavisi samo od n, k, l, pa iz teoreme sledi da je

$$|N(\mathcal{R}) - V(\mathcal{R})| < C \max\{\mathrm{Vol}\overline{\mathcal{R}}, 1\},$$

gde je C određeno samo sa $n, k, l, \mathrm{Vol}(\overline{\mathcal{R}})$. Ovde je bitan detalj da C ne zavisi od koeficijenata polinoma F_i.

U slučaju da je $\mathcal{R}$ algebarski multiskup sa multiplicitetom najviše m, i koji je samo ograničen (nije zatvoren), multiskup $\mathcal{R}$ se podeli na polualgebarske skupove sa fiksiranim multiplicitetom, i teorema se primeni na njihova zatvorenja.

Glava 2

Binarne kvadratne forme

Definicija 2.0.8. *Dve binarne kvadratne forme u i v su u istoj klasi u užem smislu ako postoji $k \in \mathrm{SL}_2(\mathbb{Z})$ tako da je $v = k \cdot u$ (tj. ako postoji unimodularna zamena promenljivih koja pretvara u u v), a u širem ako je determinanta k jednaka ili* 1 *ili* -1.

Definicija 2.0.9. *Automorf formi diskriminante d je unimodularna zamena promenljivih koja pretvara forme diskriminante d u same sebe (ako je $k \in \mathrm{GL}_2(\mathbb{Z})$ matrica koja odgovara ovoj smeni, onda je $k \cdot u = u$ za svako u sa ovom diskriminantom).*

Neka je

$$f(x, y) = ax^2 + bxy + cy^2$$

primitivna binarna kvadratna forma (primitivna znači da je najveći zajednički delilac koeficijenata jednak 1). Sa $d = b^2 - 4ac$ obeležavamo diskriminantu polinoma f, sa h_d broj klasa (u užem smislu) sa diskriminantom d. Neka je d ceo broj koji nije kvadrat nekog celog broja, i neka je $\epsilon_d = (t + u\sqrt{d})/2$, gde su t i u najmanja pozitivna celobrojna rešenja za jednačinu $t^2 - du^2 = 4$. Uočimo, ako je $d = 4k$, onda je b parno.

Gaus je svom delu *Disquisitiones Arithmeticae* pokazao da se vrednost $h_{4k} \log \epsilon_{4k}$ asimptotski ponaša kao $\frac{2\pi^2}{7\zeta(3)} k^{\frac{1}{2}}$. U ovoj glavi ćemo pokazati da važi

Teorema 2.0.10 (Carl Ludwig Siegel).

$$\sum_{k\leq N} h_{4k}\log\epsilon_{4k} \sim \frac{4\pi^2}{21\zeta(3)}N^{3/2},\ N\to\infty.$$

Takođe ćemo prikazati dokaz za sledeću formulu:

Teorema 2.0.11 (Carl Ludwig Siegel).

$$\sum_{k\leq N} h_k\log\epsilon_k = \frac{\pi^2}{18\zeta(3)}N^{3/2} + O(N\log N).$$

2.1 Dirihleovi karakteri i nekompletne sume karaktera

Neka je $\chi(k)$ netrivijalan Dirihleov karakter modulo q, i neka je

$$s(n) := \sum_{k=1}^{n}\chi(k),$$

za $n\in\mathbb{N}$. Uvedimo sledeći pojam:

Definicija 2.1.1. *Za svaki karakter χ modula m postoji prirodan broj $m^\star$, koji je najmanji delilac broja m za koji postoji karakter $\chi^\star$ modula $m^\star$, takav da je $\chi = \chi_0\chi^\star$, gde je χ_0 glavni karakter modula m. Karakter χ je primitivan karakter ako je $m^\star = m$.*

Primetimo da je $\chi^\star$ jedinstveno određeno sa χ. Pólya i Vinogradov su pokazali da važi

Teorema 2.1.2 (Pólya-Vinogradov). *Važi sledeće:*

$$\left|\sum_{k=1}^{n}\chi(k)\right| < cm^{1/2}\log m,$$

gde su c apsolutna konstanta, i χ Dirihleov karakter modulo m.

Dokaz: Neka je

$$S_\chi(N) := \sum_{M<n\leq M+N}\chi(n),$$

gde je χ Dirihleov karakter modula m koji nije glavni. Iz [IK], lema 12.1 imamo:

$$|S_\chi(N)| \leq 2\sum_{0<a\leq\frac{m}{2}} a^{-1}|g_\chi(a)|, \tag{2.1}$$

gde je

$$g_\chi(a) = \sum_{x(\mathrm{mod}q)}\chi(x)e\left(\frac{ax}{m}\right).$$

Neka je $\chi^\star \bmod m^\star$ primitivni karakter koji indukuje χ. Tada je ([IK], lema 3.2)

$$g_\chi(a) = g_{\chi^\star}(1)\sum_{d|(a,m/m^\star)} d\overline{\chi}^\star(a/d)\mu(q/dq^\star).$$

Ovo nam daje

$$|g_\chi(a)| \leq \sigma((a,m/m^s tar))\sqrt{m^\star}.$$

Kada ubacimo ovo u (2.1):

$$|S_\chi(N)| \leq 3\tau(m/m^\star)\sqrt{m^\star}\log m.$$

Pošto je $\tau(m) \leq 2\sqrt{m}$, ovo nam daje teoremu. □

(ovaj dokaz se može naći u [IK])

Za prirodan broj N važi:

$$\sum_{n=N+1}^{\infty} \chi(n)n^{-1} = \sum_{n=N+1}^{\infty} (s_n - s_{n-1})n^{-1} = \sum_{n=N}^{\infty} s_n \left(\frac{1}{n} - \frac{1}{n+1}\right) - s_N N^{-1}.$$

Iz gornje ocene koju su dobili Pólia i Landau sledi:

$$\left| \sum_{n=N+1}^{\infty} \chi(n)n^{-1} \right| < 2cN^{-1}m^{1/2}\log m.$$

Posebno, kada je $d \equiv 0$ ili $1 \pmod 4$ i kada d nije kvadrat nekog broja, tada je Ležandrov simbol $\left(\frac{d}{k}\right)$ netrivijalan karakter modulo $|d|$. U sledećoj sekciji ćemo dati skicu dokaza za dve bitne teoreme.

2.2 Automorfi i reprezentacije

Pre nego što navedemo teoreme, podsetićemo se nekih pojmova:
Za svako d postoje barem dva automorfa: identitet ($x = x'$ i $y = y'$) i množenje sa -1 ($x = -x'$ i $y = -y'$). Ako je $d < 0$, to su jedini automorfi osim za $d = -3$ i $d = -4$, i u oba ova slučaja postoji samo jedna klasa formi.

1. Za $d = -3$, predstavnik klase je $x^2 + xy + y^2$, i automorfi su

$$x = -y',\ y = x' + y'$$

i

$$x = x' + y',\ y = -x'$$

i njihovi negativi (obe jednakosti u ovim automorfima daju nove automorfe kada ih pomnožimo sa -1).

2. Za $d = -4$ predstavnik klase je $x^2 + y^2$, i automorf je

$$x = y',\ y = -x'$$

i njegov negativ.

Definicija 2.2.1. *Za $d < 0$, sa $w = w_d$ obeležavamo broj automorfa za forme sa diskriminantom d. Kao što smo već videli, za $d < 0$ važi:*

$$w = \begin{cases} 2 & \text{za } d \neq -4, -3 \\ 4 & \text{za } d = -4 \\ 6 & \text{za } d = -3 \end{cases} \tag{2.2}$$

U slučaju da je $d > 0$, uzimamo da je $w = 1$.

Neka je sada $d > 0$. Svaka forma sa diskriminantom d ima beskonačno mnogo automorfa. Ovi automorfi odgovaraju rešenjima Pelove jednačine

$$t^2 - du^2 = 4.$$

Za formu $ax^2 + bxy + cy^2$, automorfi su dati sa ([L], teorema 202.)

$$\begin{cases} \alpha = \frac{1}{2}(t - bu), & \beta = -cu, \\ \gamma = au, & \delta = \frac{1}{2}(t + bu). \end{cases} \tag{2.3}$$

Trivijalni automorfi odgovaraju rešenjima $t = \pm 2$, $u = 0$. Pelova jednačina ima beskonačno rešenja, i ako je (t_0, u_0) rešenje za koje je $t_0 > 0$, $u_0 > 0$ i u_0 najmanje za koje važe prethodna dva uslova, tada su sva rešenja data sa ([L], teorema 111.)

$$\frac{t + u\sqrt{d}}{2} = \pm \left[\frac{t_0 + u_0\sqrt{d}}{2} \right]^n,$$

za bilo koji ceo broj n. Može se videti, nakon faktorizacije

$$ax^2 + bxy + cy^2 = a(x - \theta y)(x - \theta' y)$$

(θ i θ' su koreni forme), da (2.3) zaista daje automorf oblika

$$\begin{cases} x - \theta y = \frac{(t - u\sqrt{d})(x' - \theta y')}{2}, \\ x - \theta' y = \frac{(t + u\sqrt{d})(x' - \theta' y')}{2}. \end{cases} \tag{2.4}$$

Sada ćemo posmatrati koliki je ukupan broj reprezentacija nekog prirodnog broja n sa skupom formi diskriminante d.

Ako je $d < 0$, tada je broj reprezentacija od n sa bilo kojom formom konačan.

Međutim, za $d > 0$ broj ovakvih reprezentacija je beskonačan, pošto iz jedne reprezentacije možemo dobiti beskonačno mnogo drugih preko automorfa. Zato ćemo uzeti po jednu reprezentaciju iz svakog skupa (u kojima možemo jednu reprezentaciju dobiti iz druge pomoću automorfa), i ispostaviće se da je broj ovih predstavnika konačan. Ove predstavnike zovemo glavnim reprezentacijama.

Neka su x, y i X, Y dve reprezentacije povezane automorfom. Tada je

$$\frac{x - \theta' y}{x - \theta y} = \frac{\frac{1}{2}(t + u\sqrt{d})}{\frac{1}{2}(t - u\sqrt{d})} \cdot \frac{X - \theta' Y}{X - \theta Y}.$$

Neka je $\epsilon_d = (t_0 + u_0\sqrt{d})/2 > 1$. Tada je

$$(t + u\sqrt{d})/2 = \pm \epsilon_d^m,$$

$$(t - u\sqrt{d})/2 = \pm\epsilon_d^{-m},$$

za neki ceo broj m. Za date X i Y postoji tačno jedno m za koje je

$$1 \leq \frac{x - \theta' y}{x - \theta y} < \epsilon_d^2.$$

Možemo takođe smatrati da važi

$$x - \theta y > 0.$$

Reprezentaciju koja zadovoljava ova dva uslova ćemo zvati *glavnom*. Broj glavnih reprezentacija broja n je konačan, jer je količnik linearnih formi $x - \theta y$ i $x - \theta' y$ ograničen po prvom uslovu, i njihov proizvod je jednak n/a, jer je

$$ax^2 + bxy + cy^2 = a(x - \theta y)(x - \theta' y).$$

Definicija 2.2.2. *Ako je $d < 0$, tada ćemo broj reprezentacija prirodnog broja n sa formama diskriminante d obeležavaćemo sa $R(n)$. Za $d > 0$, sa $R(n)$ ćemo obeležavati ukupan broj glavnih reprezentacija broja n sa skupom formi diskriminante d.*

Sada prelazimo na dokazivanje teorema.

2.3 Dirihleova teorema broja klasa

U ovom delu ćemo dokazati Dirihleovu teoremu broja klasa, koju ćemo podeliti u dve teoreme.

Teorema 2.3.1. *Za fundamentalnu diskriminantu $d > 0$ imamo da je*

$$d^{-1/2} h_d \log \epsilon_d = \sum_{n=1}^{\infty} \left(\frac{d}{n}\right) n^{-1}.$$

Teorema 2.3.2. *A kada je $d < 0$, važi*

$$|d|^{-1/2} \, h_d \frac{2\pi}{w_d} = \sum_{n=1}^{\infty} \left(\frac{d}{n}\right) n^{-1}.$$

Pre nego što pređemo na dokaz teorema, dokazaćemo par lema i uvesti neke pojmove:

Definicija 2.3.3. *Neka su n prirodan broj, i f binarna kvadratna forma sa diskriminantom d. Tada je $R(n, f)$ broj reprezentacija od n pomoću f.*

Iz ove definicije svakako sledi

$$R(n) = \sum_{f} R(n, f),$$

gde sumacija ide po predstavnicima klasa sa $a > 0$, pa suma ima h_d članova.

Lema 2.3.4. *Ako je $n > 0$ i $(n, d) = 1$, tada je*

$$R(n) = w \sum_{m|n} \left(\frac{d}{m}\right),$$

gde je w dato sa 2.2.1

(Dokaz se može naći u [L], teorema 204.)

Lema 2.3.5. *Za w iz 2.2.1 važi da je*

$$\lim_{N\to\infty}\frac{1}{N}\sum_{\substack{n=1\\(n,d)=1}}^{N}R(n)=w\frac{\phi(|\ d\ |)}{|\ d\ |}\sum_{m=1}^{\infty}\frac{1}{m}\left(\frac{d}{m}\right).$$

Dokaz:

$$w^{-1}\sum_{\substack{n=1\\(n,d)=1}}^{N}R(n)=\sum_{\substack{m_1m_2\le N\\(m_1m_2,d)=1}}\left(\frac{d}{m_1}\right)=\sum_{m_1\le\sqrt{N}}\left(\frac{d}{m_1}\right)\sum_{\substack{m_2\le N/m_1\\(m_2,d)=1}}1+$$

$$+\sum_{\substack{m_2<N/m_1\\(m_2,d)=1}}\ \sum_{\sqrt{N}<m_1\le N/m_2}\left(\frac{d}{m_1}\right).$$

Prva unutrašnja suma je jednaka

$$\frac{N}{m_1}\frac{\phi(|d|)}{|d|}+O(\phi(|d|)),$$

pa je prva suma

$$N\frac{\phi(|d|)}{|d|}\sum_{m_1\le\sqrt{N}}\frac{1}{m_1}\left(\frac{d}{m_1}\right)+O(\sqrt{N}),$$

za fiksirano d i proizvoljno N. Pošto je $\left(\frac{d}{m_1}\right)$ karakter modula d koji nije glavni, suma njegovih vrednosti kada se prolazi po m_1 je ograničena. Dakle, druga suma je $O(\sqrt{N})$. Prema tome

$$w^{-1} \sum_{\substack{n=1 \\ (n,d)=1}}^{N} R(n) = N\frac{\phi(|d|)}{|d|} \sum_{m\leq\sqrt{N}} \frac{1}{m}\left(\frac{d}{m}\right) + O(\sqrt{N}).$$

Kada proširimo sumu do beskonačnosti, i ocenimo $\sum_{m>\sqrt{N}} \frac{1}{m}\left(\frac{d}{m}\right)$ sa $O(N^{-1/2})$, dobićemo da je

$$\lim_{N\to\infty} \frac{1}{N} \sum_{\substack{n=1 \\ (n,d)=1}}^{N} R(n) = w\frac{\phi(|d|)}{|d|} \sum_{m=1}^{\infty} \frac{1}{m}\left(\frac{d}{m}\right).\square$$

Pomoću leme 2.3.5 smo ocenili srednju vrednost $R(n)$ kada n varira po celim brojevima koji su uzajamno prosti sa d.
Ovaj rezultat možemo videti i ovako: srednja vrednost $R(n)$ u odnosu na n je $w\sum_{n=1}^{\infty}\left(\frac{d}{n}\right)n^{-1}$, jer $\frac{\phi(|d|)}{|d|}$ predstavlja gustinu celih brojeva n koji su uzajamno prosti sa d.

Procenićemo sada

$$\lim_{N\to\infty} \frac{1}{N} \sum_{\substack{n=1 \\ (n,d)=1}}^{N} R(n,f).$$

Ispostaviće se da ovaj limes ne zavisi od f, i kada uporedimo ovaj limes sa prethodnim, dobićemo vezu između h_d i $\sum_{n=1}^{\infty}\left(\frac{d}{n}\right)n^{-1}$.

Dokaz teoreme 2.3.2

Suma

$$\sum_{\substack{n=1 \\ (n,d)=1}}^{N} R(n,f)$$

predstavlja broj parova celih x i y za koje je

$$0 < ax^2 + bxy + cy^2 \leq N,$$

$$(ax^2 + bxy + cy^2, d) = 1.$$

Iz drugog uslova se može videti da su x i y ograničeni na određene parove ostataka modulo $|d|$, i u [L], teorema 206. možemo videti da je broj ovih parova jednak $|d|\phi(|d|)$. Zato smatramo da za x i y važi

$$ax^2 + bxy + cy^2 \leq N,$$

$$x \equiv_{|d|} x_0,\ y \equiv_{|d|} y_0.$$

Prva jednakost kaže da se tačka nalazi u elipsi čiji je centar tačka $(0, 0)$, koja se ravnomerno širi kada $N \to \infty$. Površina ove elipse je

$$\frac{2\pi}{\sqrt{4ac - b^2}} = \frac{2\pi}{|d|^{1/2}} N.$$

Kada podelimo ravan na kvadrate sa stranicom $|d|$, možemo videti da je broj tačaka (x, y) u elipsi koje zadovoljavaju drugi uslov asimptotski jednak

$$\frac{2\pi}{|d|^{5/2}} N$$

kada $N \to \infty$. Pomnožimo ovo sa $|d|\phi(|d|)$:

$$\lim_{N\to\infty} \frac{1}{N} \sum_{\substack{n=1 \\ (n,d)=1}}^{N} R(n, f) = \frac{2\pi\phi(|d|)}{|d|^{3/2}}.$$

Odavde imamo (iz 2.3.5 i 2.3.3) da je

$$h_d = \frac{w|d|^{1/2}}{2\pi} \sum_{n=1}^{\infty} \left(\frac{d}{n}\right) n^{-1}.\square$$

Dokaz teoreme 2.3.1

Kao i ranije, tražimo broj parova celih brojeva koji zadovoljavaju

$$ax^2 + bxy + cy^2 \leq N$$

$$x - \theta y > 0, \quad 1 \leq \frac{x - \theta' y}{x - \theta y} < \epsilon_d^2,$$

$$x \equiv_d x_0, \quad y \equiv_d y_0.$$

Prva dva uslova nam kažu da se ovi parovi nalaze u sektoru hiperbole ograničenom sa dve poluprave. Površinu ovog sektora ćemo izračunati pomoću smene

$$\xi = x - \theta y,$$

$$\eta = x - \theta' y.$$

Za ovu smenu je $\frac{\partial(\xi,\eta)}{\partial(x,y)} = \theta - \theta' = \frac{\sqrt{d}}{a}$. U ovoj ravni sa ξ i η koordinatama, sektor je određen sa

$$\xi\eta \leq \frac{N}{a},\ \xi > 0,\ \xi \leq \eta < \epsilon_d^2 \xi,$$

što je ekvivalentno sa

$$0 < \xi \leq \sqrt{N/a},\ \xi \leq \eta < \min(\epsilon_d^2 \xi, N/a\xi).$$

Ako uzmemo da je $\xi_1 = \epsilon_d^{-1}\sqrt{N/a}$, onda je površina sektora jednaka

$$\int_0^{\xi_1} (\epsilon_d^2 \xi - \xi) d\xi + \int_{\xi_1}^{\sqrt{N/a}} \left(\frac{N}{a\xi} - \xi\right) d\xi =$$

$$= (\epsilon_d^2 - 1)\frac{\xi_1^2}{2} + \sqrt{N/a}\log(N/a) - (N/a)\log\xi_1 - \frac{N}{2a} + \frac{\xi_1^2}{2} = \frac{N\log\epsilon_d}{a}.$$

Ovaj broj delimo sa $\sqrt{d}a^{-1}$ kako bismo dobili površinu u x, y ravni. Zatim, delimo sa d^2 kao u slučaju za $d < 0$, kako bismo našli broj parova (x, y) koji ispunjavaju uslove kongruencije. I na kraju množimo sa $d\phi(d)$ – broj parova (x_0, y_0). Rezultat ovoga je

$$\lim_{N\to\infty} \frac{1}{N} \sum_{\substack{n=1 \\ (n,d)=1}}^{N} R(n, f) = \frac{\phi(d)\log\epsilon_d}{d^{3/2}},$$

što nam zajedno sa 2.3.5 i 2.3.3 daje

$$h_d = \frac{d^{1/2}}{\log\epsilon_d} \sum_{n=1}^{\infty} \left(\frac{d}{n}\right) n^{-1}.\square$$

2.4 Dokaz teoreme 2.0.11

Neka je $N \in \mathbb{N}$. Koristićemo ovo N da kontrolišemo dužinu parcijalne sumacije kojom ćemo aproksimirati $f_d := d^{-1/2} h_d \log\epsilon_d$.

Definicija 2.4.1. *Za $d > 0$ i $N \in \mathbb{N}$:*

$$\sigma_d = \sigma_d(N) := \sum_{n=1}^{N} \left(\frac{d}{n}\right) n^{-1}.$$

Tada je

$$|f_d - \sigma_d| < 2cN^{-1}d^{1/2}\log d,$$

za svako $d \equiv 0$ ili $1 \pmod 4$ koje nije kvadrat. No, takođe važi i

$$|\sigma_d| \leq \sum_{n=1}^{N} n^{-1} < 1 + \log N,$$

što važi i kada je d kvadrat nekog broja.

U sledećoj proceni koja sledi iz ocena $|f_d - \sigma_d|$ i $|\sigma_d|$, sume prolaze po $1 \leq d, t \leq N$, $d, t \equiv r \pmod 4$ (r je ili 0 ili 1), d nije kvadrat:

$$\sum_{d} f_d = \sum_{n=1}^{N} n^{-1} \sum_{t} \left(\frac{t}{n}\right) + O(N^{1/2}\log N) \tag{2.5}$$

kada $N \to \infty$.

Definicija 2.4.2. *Za $N \in \mathbb{N}$ i $r \in \{0, 1\}$, neka je*

$$P_r(n) = P_r(n, N) := \sum_{\substack{1 \leq t \leq N \\ t \equiv_4 r}} \left(\frac{t}{n}\right), \tag{2.6}$$

za svako $n \in \{1, 2, ..., N\}$ (za parno n imamo da je $P_r(n) = 0$).

Posmatraćemo dva slučaja: kada je n kvadrat, i kada n nije kvadrat.

1. Za neparno n, $\chi_1(k) = \left(\frac{t}{n}\right)$ je netrivijalni karakter modulo n, pa iz ocene s_n sledi:

$$P_0(n) = \sum_{4k \leq N} \chi_1(k) = n^{1/2} \log n + O(1).$$

Neka $2^l || n$ ($2^l | n$ i $2^{l+1} \nmid n$). Tada je $n/l = s$ neparan broj i $\left(\frac{t}{n}\right) = \left(\frac{l}{t}\right)\left(\frac{t}{s}\right)$, za neparno t. Karakteri $\chi_2(k) = \left(\frac{4l}{l}\right)\left(\frac{k}{s}\right)$ i $\chi_3(k) = \left(\frac{-4l}{l}\right)\left(\frac{k}{s}\right)$ su modulo 4 i netrivijalni, pa kao za P_0 važi

$$P_1(n) = \frac{1}{2} \sum_{k \leq N} (\chi_2(k) + \chi_3(k)) = n^{1/2} \log n + O(1).$$

Prema tome:

$$P_r(n) = n^{1/2} \log n + O(1), \tag{2.7}$$

za $r = 0, 1$ i $1 \leq n \leq N$, $n \neq 1, 4, 9, ...$

2. Neka je sada $n = u^2$. Tada je broj $P_r(n)$ jednak broju celih u intervalu $[1, N]$ koji su uzajamno prosti sa u i kongruentni sa r po modulu 4, iz čega imamo

$$P_r(u_1^2) = \frac{\varphi(u_1)}{4u_1} N + O(1),$$

$$P_r(u_2^2) = \frac{r\varphi(u_2)}{2u_2} N + O(1),$$

gde je u_1 neparno, a u_2 parno. Ovo nam daje:

$$\sum_{u^2\le N} u^{-2}P_r(u^2) = \frac{N}{4}\sum_{u_1^2\le N} u_1^{-3}\varphi(u_1) + \frac{rN}{2}\sum_{u_2^2\le N} u_2^{-3}\varphi(u_2) + O(\log N) = \quad (2.8)$$

$$= \frac{N}{4}\frac{\zeta(2)}{\zeta(3)}\left(1+\frac{2r-1}{7}\right) + O(\sqrt{N}).$$

Dokaz teoreme 2.0.11: Iz (2.5), (2.6), (2.7) i (2.8) sledi

$$\sum_d f_d = \sum_{n=1}^{N} n^{-1}P_r(n) + O\left(N^{1/2}\log N\right) = \frac{\pi^2 N}{24\zeta(3)}\left(1+\frac{2r-1}{7}\right) + O\left(N^{1/2}\log N\right).$$

Nakon što primenimo parcijalnu sumaciju, dobijamo:

$$\sum_d d^{1/2} f_d = \frac{\pi^2 N^{3/2}}{36\zeta(3)}\left(1+\frac{2r-1}{7}\right) + O(N\log N),$$

gde d ide po celim brojevima u intervalu $[1, N]$ koji su kongruentni sa r po modulu 4 i različiti od kvadrata. No, $d^{1/2}f_d = h_d \log \epsilon_d$, pa gornja jednakost predstavlja jednakost u teoremi 2.0.11, što znači da smo upravo dokazali tu teoremu. □

Definicija 2.4.3. *Sa H_d obeležavamo broj klasa pozitivnih kvadratnih formi $Q(x,y) = ax^2+bxy+cy^2$ sa celobrojnim koeficijentima i diskriminantom d.*

Po definiciji 2.4.3 vidimo da je $H_d = \sum_t h_t$, gde t prolazi po svim deliocima d za koje je dt^{-1} kvadrat.

Lema 2.4.4. *Važi sledeće:*

$$\sum H_{-k} = \frac{\pi}{18}N^{3/2} + O(N\log N).$$

Dokaz: Iz Dirihleove teoreme (2.3.1 i 2.3.2) sledi:

$$\sum_{\substack{k\leq N\\ -k\equiv_4 r}} k^{-1/2}h_{-k} = \frac{\pi N}{24\zeta(3)}\left(1+\frac{2r-1}{7}\right)+O\left(N^{1/2}\log N\right)(r=0,1),$$

$$\sum_{k\leq N} h_{-4k} \sim \frac{4\pi}{21\zeta(3)}N^{3/2},$$

$$\sum_{k\leq N} h_{-k} = \frac{\pi}{18\zeta(3)}N^{3/2}+O(N\log N) \tag{2.9}$$

Iz (2.9) sledi $\sum H_{-k} = \frac{\pi}{18}N^{3/2}+O(N\log N)$. □

Važi i obratno, iz leme 2.4.4 sledi jednakost (2.9) (može se videti preko Mebijusove inverzije).

2.5 Redukovane binarne kvadratne forme

Uočimo, u svakoj klasi pozitivnih kvadratnih formi postoji redukovana forma koja zadovaljava $|b| \leq a \leq c$. Ova forma je jedinstvena ako je $|b| < a < c$.

Neka je $Q(x,y) = ax^2+bxy+cy^2$ nedefinitna kvadratna forma (forma koja uzima i pozitivne i negativne vrednosti) sa realnim koeficijentima, $a \neq 0$, $b^2-4ac = D > 0$. Ako su ρ_1 i ρ_2 koreni jednačine $Q(x,1) = 0$, tada je $Q(x,y) = a(x-\rho_1 y)(x-\rho_2)$. Smatraćemo da je $a(\rho_1-\rho_2) = \sqrt{D}$.

Definicija 2.5.1. *Za $\lambda > 0$, i nedefinitnu kvadratnu formu Q uvodimo sledeću pozitivnu kvadratnu formu:*

$$P(x,y) = P_{\lambda,Q}(x,y) := |a|[\lambda^{-1}(x-\rho_1 y)^2+\lambda(x-\rho_2 y)^2] = \alpha x^2+2\beta xy+\gamma y^2.$$

Koreni jednačine $P(x,1)=0$ su kompleksno konjugovani, pošto forma uzima samo vrednosti veće ili jednake nuli. Dakle, ako je $\tau=\xi+i\eta$ koren sa pozitivnim imaginarnim delom, tada je

$$\frac{\tau-\rho_1}{\tau-\rho_2}=\pm i\lambda.$$

Prema tome, tačke τ određuju polukrug H koji prolazi kroz tačke ρ_1 i ρ_2 u gornjoj poluravni, i taj polukrug je određen jednačinom

$$a(\xi^2+\eta^2)+b\xi+c=0.$$

Definicija 2.5.2. *Za neku nedefinitnu formu Q kažemo da je* **redukovana** *ako i samo ako postoji barem jedno $\lambda>0$ za koje je $P=P_{\lambda,Q}$ redukovano (dakle, kada je $2|\beta|\leq\alpha\leq\gamma$).*

Tada τ leži u fundamentalnom domenu F modularne grupe, definisan nejednakostima $-1/2\leq\xi\leq 1/2$ i $\xi^2+\eta^2\geq 1$. Pošto je $A:=H\cap F$ luk, za svako Q važi da je skup svih λ za koje je P redukovano ili interval $[\lambda_1,\lambda_2]$ ili prazan skup. Neka je $ds=\eta^{-1}(d\xi^2+d\eta^2)^{1/2}$. Tada je dužina A jednaka

$$\mu(a,b,c):=\int_{\lambda_1}^{\lambda_2}\frac{d\lambda}{\lambda}=\log\frac{\lambda_2}{\lambda_1},$$

ako je A neprazan, i $\mu=0$ inače.

2.6 Procena mere skupa redukovanih formi

Posmatrajmo sledeći integral

$$J=\int\int\int_{D<1}\mu da db dc,$$

gde su $a > 0$, i $0 < b^2 - 4ac = D < 1$. Definicija μ nam daje

$$J = \int_0^\infty \left(\int_\tau \int_\epsilon \int_F dadbdc \right) \frac{d\lambda}{\lambda}.$$

Lema 2.6.1. *Integral J ima vrednost $\frac{\pi^2}{18}$.*

Dokaz: Uočimo, za svako $\lambda > 0$ unutrašnji integral predstavlja zapreminu domena R_λ. Mi ćemo umesto a, b i c koristiti α, β i γ pri integraciji. Ako je λ fiksirano, tada je P jedinstveno određeno sa Q. No, takođe možemo videti da su koreni ρ_1 i ρ_2 jedinstveno određeni sa P, pa pošto je

$$\alpha\gamma - \beta^2 = D$$

i $a > 0$, to je Q jedinstveno određeno sa P, kada je λ fiksirano. Dakle, R_λ se preslikava na domen G svih redukovanih P sa $\alpha\gamma - \beta^2 < 1$, i G ne zavisi od λ.

Može se lako proveriti da važi:

$$a^{-1}\alpha = \lambda^{-1} + \lambda,$$

$$a^{-1}\beta = -\lambda^{-1}\rho_1 - \lambda\rho_2,$$

$$a^{-1}\gamma = \lambda^{-1}\rho_1^2 + \lambda\rho_2^2$$

odakle imamo

$$d\alpha = (\lambda^{-1} + \lambda)da,$$

$$\frac{d(a^{-1}\beta, a^{-1}\gamma)}{d(\rho_1, \rho_2)} = \begin{vmatrix} -\lambda^{-1} & -\lambda \\ 2\lambda^{-1}\rho_1 & 2\lambda\rho_2 \end{vmatrix} = 2(\rho_1 - \rho_2).$$

Dalje, važi $a^{-1}b = -\rho_1 - \rho_2$, $a^{-1}c = \rho_1\rho_2$, pa je

$$\frac{d(a^{-1}b, a^{-1}c)}{d(\rho_1, \rho_2)} = \begin{vmatrix} -1 & -1 \\ \rho_2 & \rho_1 \end{vmatrix} = \rho_2 - \rho_1.$$

Prema tome, vrednost Jakobijana je

$$\frac{d(\alpha, \beta, \gamma)}{d(a, b, c)} = -2(\lambda^{-1} + \lambda),$$

pa je

$$J = 1/2 \int_0^\infty \frac{d\lambda}{\lambda^2 + 1} \int_G d\alpha d\beta d\gamma = \frac{\pi}{4} V,$$

gde je V zapremina G. Kako bismo odredili V, integralićemo po D, ξ i η, umesto po α, β i γ. Budući da je $\alpha^{-1}\beta = -\xi$, $\alpha^{-1}\gamma = \xi^2 + \eta^2$, i $D = \alpha\gamma - \beta^2 = (\alpha\eta)^2$, to je

$$\frac{d(\alpha^{-1}\beta, \alpha^{-1}\gamma)}{d(\xi, \eta)} = -2\eta,$$

$$2\alpha\eta d(\alpha\eta) = dD,$$

$$\frac{d(\alpha, \beta, \gamma)}{d(D, \xi, \eta)} = -\alpha\eta^{-1} = -D^{1/2}\eta^{-2},$$

pa je

$$V = \int_0^1 D^{1/2} dD \int_F \frac{d\xi d\eta}{\eta^2} = \frac{2}{3} \int_{-1/2}^{1/2} \frac{d\xi}{\sqrt{1 - \xi^2}} = \frac{2\pi}{9}.$$

Dakle, $J = \frac{\pi^2}{18}$. $\square$

Polukrug H će prolaziti kroz F akko ako jedno od dva temena $1/2(\pm 1 + \sqrt{-3})$ u F pripada polukrugu

$$\xi^2 + \eta^2 + a^{-1}b\xi + a^{-1}c \leq 0, \quad \eta \geq 0.$$

Dakle, za neku redukovanu formu Q mora da važi $a + c \leq \frac{1}{2}|b|$ (za $a > 0$). Pošto je

$$(|b| - a)^2 + 3a^2 = \frac{1}{4}(4a - |b|)^2 + \frac{3}{4}b^2 = D + 4a\left(a + c - \frac{1}{2}|b|\right), \tag{2.10}$$

to imamo sledeće nejednakosti

$$a^2 \leq \frac{1}{3}D, \quad b^2 \leq \frac{4}{3}D, \quad 4a|c| = |b^2 - D| \leq D,$$

za svako redukovano Q sa $a > 0$. Znamo da je P redukovano za svako $\lambda_1 \leq \lambda \leq \lambda_2$, i da je

$$\frac{3}{4}\alpha^2 = \alpha^2 - \frac{1}{4}\alpha^2 \leq \alpha\gamma - \beta^2 = D,$$

pa je

$$a(\lambda^{-1} + \lambda) = \alpha \leq 2\sqrt{D/3},$$

za $\lambda \in [\lambda_1, \lambda_2]$.

Uvedimo sledeće pojmove:

Definicija 2.6.2. *Za $\vartheta > 0$, sa P_ϑ označavamo skup svih redukovanih Q za koje je $a \geq \vartheta$ i $D \leq 1$.*

Imajući u vidu gornje nejednakosti za a^2, b^2 i $|b^2 - D|$, vidimo da je P_ϑ ograničen i zatvoren skup, pa je funkcija μ neprekidna na P_ϑ.

Definicija 2.6.3. *Za $\vartheta > 0$ definišemo* $J_\vartheta := \int\int\int_{P_\vartheta} \mu da db dc.$

Tada je

$$J = \lim_{\vartheta \to 0} J_\vartheta.$$

Sa druge strane je $\mu(qa, qb, qc) = \mu(a, b, c)$ za svako $q \neq 0$, pa ako uzmemo da je $S_1 = S_1(N)$ skup svih redukovanih Q za koje je $a \geq \vartheta N$, $b^2 - 4ac = D \leq N^2$, tada je

$$J_\vartheta = \lim_{N \to \infty} N^{-3} \sum_{Q \in S_1} \mu(a, b, c). \tag{2.11}$$

Lema 2.6.4. *Ako je S skup svih redukovanih formi Q sa celobrojnim koeficijentima čije su diskriminante $\leq N^2$ i nisu kvadrati, onda je*

$$\lim_{N \to \infty} N^{-3} \sum_{Q \in S} \mu(a, b, c) = \frac{\pi^2}{9}.$$

Dokaz: Posmatraćemo različite Q-ove u S_1, i gledati šta se dešava sa gornjim limesom po N.

1. Neka je $Q \in S_1$ sa $D = h^2$. Tada je $4ac = (b+h)(b-h)$ i $0 < h \leq N$. Pošto je $a^2 \leq \frac{2}{4}D$ i $b^2 \leq \frac{4}{3}D$, to je $a^2 \leq \frac{1}{3}N^2$ i $b^2 \leq \frac{4}{3}N^2$. Ako je $b \neq \pm h$, tada je broj delitelja $(b+h)(b-h)$ jednak $o(N)$. Ako je $b = \pm h$, tada je $c = 0$, i $a^2 \leq N^2$. Odavde vidimo da je broj formi čije su diskriminante kvadrati jednak

$$N^2 o(N) + NO(N) = o(N^3).$$

Pošto je $\mu(a,b,c)$ uniformno ograničeno po N za svako ϑ, možemo iz S_1 izbaciti sve Q-ove čije su diskriminante kvadrati, i to neće uticati na J_ϑ.

2. Neka je S_0 skup svih Q sa celobrojnim a, b i c, $0 < a < \vartheta N$, $0 < D \leq N^2$. Na luku A, tačka sa najmanjim η se nalazi na jednom kraju luka, obeležimo ovu tačku sa $\xi_0 + i\eta_0$. Na polukrugu H važi

$$\frac{d\lambda}{\lambda} = \frac{d\tau}{\tau-\rho_1} - \frac{d\tau}{\tau-\rho_2} = \frac{(\rho_1-\rho_2)d\tau}{(\tau-\rho_1)(\tau-\rho_2)} =$$

$$= \frac{(\rho_1-\rho_2)(2\tau-\rho_1-\rho_2)d\xi}{(\tau-\rho_1)(\tau-\rho_2)(\tau-\overline{\tau})} = \frac{2(\rho_1-\rho_2)d\xi}{(\tau-\overline{\tau})^2} = \frac{-D^{1/2}d\xi}{2a\eta^2}$$

odakle sledi

$$\mu(a,b,c) \leq \frac{D^{1/2}}{2a\eta_0^2}\int_{-1/2}^{1/2} d\xi \leq \frac{N}{2a\eta_0^2}. \tag{2.12}$$

No, na osnovu ograničenja α, imamo da važi

$$|\log\lambda| < \log\frac{2}{a}\sqrt{D/3} < \log\frac{2N}{a}$$

$$\mu(a,b,c) < 2\log\frac{2N}{a}.$$

Neka je sada k prirodan broj. Tada je broj prirodnih brojeva u intervalu

$$[(\vartheta N)/2^{k+1}, (\vartheta N)/2^k)$$

manji od $(\vartheta N)/2^k$. Pošto je $b^2 \leq (4/3)N^2$, to za svako ϑ važi

$$\sum_{\substack{Q\in S_0\\ |c|<2N}} \mu(a,b,c) = O(N^2)\sum_{k=0}^{\infty}\frac{\vartheta N}{2^k}\log(2^{k+2}\vartheta^{-1}) = \vartheta\log\vartheta^{-1}O(N^3),$$

Dodatno, na osnovu (2.10) i jednačine polukruga H imamo

$$a\eta_0^2 = -a\xi_0^2 - b\xi_0 - c \leq \frac{1}{2}|b| - c < N - c,$$

za $c < N$ i

$$a\eta_0^2 \geq -\frac{1}{4}a - \frac{1}{2}|b| - c > -N - c \geq \frac{1}{2}|c|,$$

za $|c| \geq 2N$. Iz (2.12) i (2.10) sledi

$$\sum_{\substack{Q\in S_0\\ |c|\geq 2N}} \mu(a,b,c) = O(N^2)\sum_{a,c} c^{-1},$$

gde suma prolazi po celobrojnim a i c za koje je $0 < a < \vartheta N$, $4ac \leq N^2$, $c \geq 2N$. Svakako, imamo procenu

$$\sum_{a,c} c^{-1} = \sum_{a<\vartheta N} O\left(\log\frac{N}{a}\right) = \vartheta\log\vartheta^{-1}O(N).$$

Kada spojimo ove poslednje tri procene, dobijamo

$$N^{-3}\sum_{Q\in S_0}\mu(a,b,c) = \vartheta\log\vartheta^{-1}O(1). \tag{2.13}$$

3. Posmatrajmo sada skup S. Primetimo, $Q \in S \Rightarrow -Q \in S$ i $a \neq 0$. Na osnovu (2.13) i (2.11)

$$\limsup_{N\to\infty} \left| 2J_\vartheta - N^{-3} \sum_{Q\in S} \mu(a,b,c) \right| = \vartheta \log \vartheta^{-1} O(1). \tag{2.14}$$

Videli smo da je $J = \lim_{\vartheta\to 0} J_\vartheta$, i znamo da važi $\lim_{\vartheta\to 0} \vartheta \log \vartheta^{-1} = 0$. Pošto S ne zavisi od ϑ, iz (2.14) i $J = \frac{\pi^2}{18}$. sledi

$$\lim_{N\to\infty} N^{-3} \sum_{Q\in S} \mu(a,b,c) = 2J = \frac{\pi^2}{9}.\square$$

2.7 Dokaz teoreme 2.0.10

Neka je Q primitivna forma, tj. $(a,b,c) = 1$. Matrica linearne transformacije $x \to px + qy$, $y \to rx + sy$, gde su $p,q,r,s \in \mathbb{Z}$ i $ps - qr = 1$, ima oblik

$$\mathfrak{M} = \pm \begin{bmatrix} \frac{t+bu}{2} & au \\ -cu & \frac{t-bu}{2} \end{bmatrix}$$

gde su t i u najmanji prirodni brojevi za koje je $t^2 - Du^2 = 4$. Odgovarajuća modularna zamena fiksira tačke ρ_1 i ρ_2, pa je H invarijatno. Fundamentalan domen na H ciklične grupe ovih modularnih zamena je dat bilo kojim lukom B na H sa neeuklidskom dužinom $2\log\epsilon_D$, $\epsilon_D = \frac{t+u\sqrt{D}}{2}$.

Neka su

$$Q_k = a_k x^2 + b_k xy + c_k y^2$$

$(k = 1, 2, ..., g)$ sve redukovane forme koje su ekvivalentne sa Q, i neka je A_k luk A za Q_k. Tada su luci $A_1, ..., A_g$ ekvivalentni sa lucima na H koji pokrivaju B bez preklapanja i rupa. Dakle,

$$\sum_{k=1}^{g} \mu(a_k, b_k, c_k) = 2 \log \epsilon_D.$$

Ako sumiramo po svim primitivnim Q sa datom diskriminantom D, dobijamo

$$\sum_{\substack{b^2-4ac=D \\ (a,b,c)=1}} \mu(a, b, c) = 2h_D \log \epsilon_D,$$

gde je h_D klasni broj. Iz 2.6.4 i gornje jednakosti sledi

$$g(N) := \sum_{Dq^2 \leq N^2} h_D \log \epsilon_D \sim \frac{\pi^2}{18} N^3,$$

gde suma ide po svim prirodnim brojevima D i q za koje je $Dq^2 \leq N^2$ i D nije kvadrat.

$$\sum_{D \leq N^2} h_d \log \epsilon_D = \sum_{t \leq N} \mu(t) g(t^{-1}N) \sim \frac{\pi^2}{18} \sum_{t \leq N} \mu(t) \left(\frac{N}{t}\right)^3 \sim \frac{\pi^2}{18\zeta(3)} N^3.$$

Posmatrajmo sada sumu na desnoj strani (2.11). Ako iz te sume izbacimo sve članove za koje je ili b neparno, ili su svi a, b i c parni, onda ostatak trojki (a, b, c) čine tačno 3 sistema klasa ostataka modulo 2, pa je ovako dobijena suma jednaka $\frac{3}{8} J_\vartheta$. Kako je $b^2 - 4ac = D = 4k$ deljivo sa 4 i (a, b, c) je neparno, to je

$$\sum_{4kq^2 \leq N^2} h_{4k} \log \epsilon_{4k} \sim \frac{\pi^2}{48} N^3,$$

gde suma ide po svim prirodnim brojevima k i q za koje je $4kq^2 \leq N^2$, q neparno i k nije kvadrat. Odavde sledi Gausova formula:

$$\sum_{k \leq N^2} h_{4k} \log \epsilon_{4k} \sim \frac{\pi^2}{48} \sum_{q \leq N} \mu(q) \left(\frac{2N}{q}\right)^3 \sim \frac{4\pi^2}{21\zeta(3)} N^3. \square$$

Glava 3

Binarne kubične forme

Neka je $V_{\mathbb{R}}$ vektorski prostor binarnih kubičnih formi nad $\mathbb{R}$. Tada grupa $\mathrm{GL}_2(\mathbb{R})$ deluje na $V_{\mathbb{R}}$ na sledeći način:

$$(\gamma \cdot f)(x, y) = f((x, y) \cdot \gamma).$$

Tvrđenje 3.0.1. *Dejstvo* $\mathrm{GL}_2(\mathbb{R})$ *na* $V_{\mathbb{R}}$ *ima tri orbite:* $V_{\mathbb{R}}^0$*, koja se sastoji od elemenata sa pozitivnom diskriminantom,* $V_{\mathbb{R}}^1$*, koja ima elemente sa negativnom diskri minantom, i orbita koja ima elemente čija je diskriminanta nula.*

Dokaz: Neka je $f \in V_{\mathbb{R}}$ sa diskriminantom $\mathrm{Disc}(f)$. Šta se dešava sa diskriminantom pri dejstvu $\mathrm{GL}_2(\mathbb{R})$ na $V_{\mathbb{R}}$? Prvo, kako postoji Iwasawina dekompozicija prostora $\mathrm{GL}_2(\mathbb{R})$, dovoljno je proveriti kako deluju pojedinačne matrice iz

$$\mathrm{O}_2(\mathbb{R}), \quad A_+ = \left\{ \begin{bmatrix} t^{-1} & 0 \\ 0 & t \end{bmatrix} \mid t \in \mathbb{R}_+ \right\}, \quad N = \left\{ \begin{bmatrix} 1 & 0 \\ u & 1 \end{bmatrix} \mid u \in \mathbb{R} \right\} \text{ i}$$

$$\Lambda = \left\{ \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix} \mid \lambda > 0 \right\}$$

na $\mathrm{GL}_2(\mathbb{R})$.

Zato posmatramo po slučajevima:

1. $k \in \Lambda$: Ako je $f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$, i $g = k \cdot f = a_1x^3 + b_1x^2y + c_1xy^2 + d_1y^3$, koliko je Disc$(g)$?

   Znamo da je Disc$(g) = b_1^2c_1^2 - 4a_1c_1^3 - 4b_1^3d_1 - 27a_1^2d_1^2 + 18abcd$. Treba samo izračunati koeficijente a_1,...,d_1, i uvrstiti ih u jednačinu.

$$(k \cdot f)(x,y) = f((x,y) \cdot k) = a\lambda^3x^3 + b\lambda^3x^2y + c\lambda^3xy^2 + d\lambda^3y^3$$

   Odavde vidimo da je Disc$(k \cdot f) = \lambda^{12}$Disc$(f)$. Dakle, elementi iz Λ ne menjaju znak diskriminante.

2. $k = \begin{bmatrix} t^{-1} & 0 \\ 0 & t \end{bmatrix} \in A_+$: Tada je

$$(k \cdot f)(x,y) = f(t^{-1}x, ty) = at^{-3}x^3 + bt^{-2}x^2ty + ct^{-1}xt^2y^2 + dt^3y^3 =$$

$$= at^{-3}x^3 + bt^{-1}x^2y + ctxy^2 + dt^3y.$$

   Dakle, važi

$$\text{Disc}(k \cdot f) = b^2t^{-2}c^2t^2 - 4at^{-3}c^3t^3 - 4b^3t^{-3}dt^3 - 27a^2t^{-6}d^2t^6 + 18at^{-3}bt^{-1}ctdt^3 =$$

$$= \text{Disc}(f).$$

   Elementi iz A_+ uopšte ne utiču na diskriminantu.

3. $k = \begin{bmatrix} 1 & 0 \\ u & 1 \end{bmatrix}, u \in \mathbb{R}$:

$$(k \cdot f)(x, y) = f(x + uy, y) = a(x + uy)^3 + b(x + uy)^2 y + c(x + uy)y^2 + dy^3 =$$

$$= ax^3 + (3au + b)x^2 y + (3au^2 + 2bu + c)xy^2 + (au^3 + bu^2 + cu + d)y^3.$$

Odavde vidimo da je

$$\mathrm{Disc}(k \cdot f) = \mathrm{Disc}(f).$$

Dakle, matrice iz N takođe ne menjaju diskriminantu.

4. $k = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}, \theta \in [0, 2\pi]$:

$$(k \cdot f)(x, y) = f(x\cos\theta - y\sin\theta, x\sin\theta + y\cos\theta) =$$

$$(a\cos^3\theta + b\cos^2\theta\sin\theta + c\cos\theta\sin^2\theta + d\sin^3\theta)x^3 +$$

$$+(-3a\cos^2\theta\sin\theta + b\cos\theta - 3b\cos\theta\sin^2\theta + 3c\cos^2\theta\sin\theta - c\sin\theta + 3d\sin^2\theta\cos\theta)x^2 y +$$

$$+(3a\cos\theta\sin^2\theta + b\sin\theta - 3b\cos^2\theta\sin\theta + c\cos\theta + 3c\sin^2\theta\cos\theta + 3d\sin\theta\cos^2\theta)xy^2 +$$

$$+(-a\sin^3\theta+b\sin^2\theta\cos\theta-c\cos^2\theta\sin\theta+d\cos^3\theta)y^3 = a_1x^3+b_1x^2y+c_1xy^2+d_1y^3,$$

gde sa a_1, b_1, c_1 i d_1 obeležavamo odgovarajuće koeficijente.

Setimo se formule za diskriminantu polinoma $f(x) = a_nx^n + ... + a_1x + a_0$ sa jednom promenljivom:

$$\mathrm{Disc}(f) = a_n^{2n-2} \prod_{1\le i<j\le n} (x_i - x_j)^2,$$

gde su x_i koreni polinoma f. Takođe, diskriminanta neke binarne forme je diskriminanta odgovarajućeg polinoma sa jednom promenljivom. Zbog toga ćemo sa f i $k \cdot f$ takođe obeležavati i polinome koji im odgovaraju.
Neka je $f(u, v) = 0$, za $(u, v) \in \mathbb{R}^2$. Tada je

$$k \cdot f([u, v] \cdot k^{-1}) = f([u, v]kk^{-1}) = f(u, v) = 0.$$

Dakle, ako je (u, v) nula f, onda je $(u', v') = (u, v)k^{-1}$ nula $k \cdot f$. Polinom f je homogen, pa je $f(\frac{u}{v}, 1) = 0$. Odavde vidimo da je, pošto je $f(\frac{u}{v}, 1) = 0$, $k \cdot f(\frac{u'}{v'}, 1) = 0$. No, $\frac{u}{v}$ onda odgovara jednoj od nula x_i, pa onda i $\frac{u'}{v'}$ odgovara jednom od tri korena z_1, z_2 i z_3 od $k \cdot f$.

$$\frac{u'}{v'} = \frac{u\cos\theta + v\sin\theta}{-u\sin\theta + v\cos\theta}$$

Nađimo Disc(k · f): $\mathrm{Disc}(k \cdot f) = a_1^4 \prod_{1\le i<j\le 3} (z_i - z_j)^2$. Pošto je $k \cdot f(z_i) = 0$, to je i

$$k \cdot f(z_i, 1) = f([z_i, 1]k) = f([z_i\cos\theta - \sin\theta, z_i\sin\theta + \cos\theta]) = 0.$$

Dakle,

$$x_i = \frac{z_i \cos\theta - \sin\theta}{z_i \sin\theta + \cos\theta},\ z_i = \frac{x_i \cos\theta + \sin\theta}{\cos\theta - x_i \sin\theta}$$

Kada uvrstimo ove vrednosti za korene z_i u $\mathrm{Disc}(k \cdot f)$ i upotrebimo Vijetove formule, dobijamo da je $\mathrm{Disc}(k \cdot f) = \mathrm{Disc}(f)$.

5. $k = \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix}$, $\theta \in [0, 2\pi]$:

$$k \cdot f(x, y) = f(x\cos\theta + y\sin\theta, x\sin\theta - y\cos\theta)$$

Odavde se vidi da je koeficijent uz x^3 jednak $a_1 = a\cos^3\theta + b\cos^2\theta\sin\theta + c\cos\theta\sin^2\theta + d\sin^3\theta$.

Kao pod 4), koristićemo da je

$$\mathrm{Disc}(f) = a^4 \prod_{1 \le i < j \le 3} (x_i - x_j)^2,$$

gde su x_i koreni polinoma koji odgovara polinomu f. U ovom slučaju se može videti da važi $k^{-1} = k$.

Neka je $f(u, v) = 0$, za $(u, v) \in \mathbb{R}^2$. Tada je

$$k \cdot f([u, v] \cdot k^{-1}) = f(u, v) = 0$$

Dakle, ako je (u, v) nula f, onda je $(u', v') = (u, v) \cdot k$ nula $k \cdot f$. Polinom f je homogen, pa je $f(\frac{u}{v}, 1) = 0$. Pošto je $f(\frac{u}{v}, 1) = 0$, to je $k \cdot f(\frac{u'}{v'}, 1) = 0$. Kako $\frac{u}{v}$ odgovara jednoj nuli x_i od $f(x)$, to $\frac{u'}{v'}$ odgovara nekoj nuli z_i od $k \cdot f(x)$.

$$\frac{u'}{v'} = \frac{u\cos\theta + v\sin\theta}{u\sin\theta - v\cos\theta}$$

Nađimo $\mathrm{Disc}(k \cdot f)$:

$$\mathrm{Disc}(k \cdot f) = a_1^4 \prod_{1 \le i < j \le 3} (z_i - z_j)^2.$$

$$k \cdot f(z_i) = 0 \Rightarrow k \cdot f(z_i, 1) = f(z_i\cos\theta + \sin\theta, z_i\sin\theta - \cos\theta) = 0.$$

Dakle,

$$x_i = \frac{z_i\cos\theta + \sin\theta}{z_i\sin\theta - \cos\theta} \Rightarrow z_i = \frac{x_i\cos\theta + \sin\theta}{x_i\sin\theta - \cos\theta}.$$

Kada uvrsitmo ove vrednosti za korene z_i u $\mathrm{Disc}(k \cdot f)$ i upotrebimo Vijetove formule, dobijamo da je $\mathrm{Disc}(k \cdot f) = \mathrm{Disc}(f)$. $\square$

Kao što možemo videti, elementi $k \in \mathrm{GL}_2(\mathbb{R})$ menjaju diskriminante elemenata iz $V_{\mathbb{R}}$ tako što ih množe sa $\det(k)^6$. Prema tome, elementi sa diskriminantom 0 se slikaju u elemente sa diskriminantom 0, elementi sa pozitivnom diskriminantom u elemente sa poz. diskriminantom i elementi sa negativnom dikriminantom u elemente sa neg. diskriminantom.

Smatramo da su ireducibilne one orbite koje se sastoje od ireducibilnih formi. U ovom odeljku ćemo posmatrati broj $N(V_{\mathbb{Z}}^{(i)}; X)$ ireducibilnih $\mathrm{GL}_2(\mathbb{Z})$-orbita u $V_{\mathbb{Z}}^{(i)} := V_{\mathbb{Z}} \cap V_{\mathbb{R}}^{(i)}$ koje imaju apsolutnu diskriminantu manju od X $(i = 0, 1)$. Štaviše, dokazaćemo sledeću teoremu:

Teorema 3.0.2. *([BST]) Važi sledeća procena za broj elemenata $N(V_{\mathbb{Z}}^{(i)}; X)$:*

$$N(V_{\mathbb{Z}}^{(0)}; X) = \frac{\pi^2}{72}X + O(X^{\frac{5}{6}});$$

$$N(V_{\mathbb{Z}}^{(1)}; X) = \frac{\pi^2}{24}X + O(X^{\frac{5}{6}}).$$

Definicija 3.0.3. *Sa $N(\xi, \eta)$ obeležavamo broj $\mathrm{GL}_2(\mathbb{Z})$-klasa ekvivalencije ireducibilnih celobrojnih binarnih kubničnih formi f koje zadovoljavaju $\xi < \mathrm{Disc}(f) < \eta$.*

Nakon toga ćemo dokazati precizniju teoremu:

Teorema 3.0.4. *([BST]) Važi sledeća procena za broj $N(\xi, \eta)$:*

$$N(0, X) = \frac{\pi^2}{72}X + \frac{\sqrt{3}\zeta(2/3)\Gamma(1/3)(2\pi)^{1/3}}{30\Gamma(2/3)}X^{5/6} + O_\epsilon(X^{3/4+\epsilon});$$

$$N(-X, 0) = \frac{\pi^2}{24}X + \frac{\zeta(2/3)\Gamma(1/3)(2\pi)^{1/3}}{10\Gamma(2/3)}X^{5/6} + O_\epsilon(X^{3/4+\epsilon}).$$

Ovde su $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$, i $\Gamma(s) = \int_0^\infty x^{s-1}e^{-x}dx$.

3.1 Redukcija

Neka je $i \in \{0, 1\}$. Označimo sa n_i kardinalnost stabilizatora u $\mathrm{GL}_2(\mathbb{R})$ za bilo koji element u $V_{\mathbb{R}}^{(i)}$. Tada je za svako $v \in V_{\mathbb{R}}^{(i)}$ skup $\mathcal{F}v$ unija n_i fundamentalnih domena za dejstvo $\mathrm{GL}_2(\mathbb{Z})$ na $V_{\mathbb{R}}^{(i)}$. Pošto ova unija ne mora biti disjunktna, korisno je posmatrati $\mathcal{F}v$ kao multiskup, gde je multiplicitet elementa $x \in \mathcal{F}v$ dat kardinalnošću skupa $\{g \in \mathcal{F} | gv = x\}$. Može se videti da je ovaj broj između 1 i n_i.

Iako je $\mathcal{F}v$ unija n_i fundamentalnih domena, nije svaki element u $\mathrm{GL}_2(\mathbb{Z})\backslash V_{\mathbb{Z}}$ predstavljen u $\mathcal{F}v$ tačno n_i puta. U opštem slučaju, $\mathrm{GL}_2(\mathbb{Z})$-klasa ekvivalencije

nekog elementa $x \in V_{\mathbb{Z}}$ će se pojaviti u skupu $\mathcal{F}v$ tačno $n_i/m(x)$ puta, gde je $m(x)$ kardinalnost stabilizatora x u $\mathrm{GL}_2(\mathbb{Z})$. U sledećoj sekciji ćemo videti da je stabilizator u $\mathrm{GL}_2(\mathbb{Z})$ ireducibilnog elementa $x \in V_{\mathbb{Z}}$ ili trivijalan, ili C_3 (C_3 je ciklična grupa reda 3). Dakle, za bilo koje $v \in V_{\mathbb{R}}^{(i)}$, proizvod $n_i \cdot N(V_{\mathbb{Z}}^{(i)}; X)$ je jednak broju ireducibilnih celih tačaka u $\mathcal{F}v$ sa apsolutnom diskriminantom manjom od X, uz primedbu da se, kao što ćemo videti u sledećem delu, C_3 tačke broje sa težinom $1/3$.

3.2 Procene reducibilnosti

U ovom odeljku ćemo pokazati da što se tiče (3.0.4), da je broj celobrojnih reducibilnih formi, kao i broj formi sa stabilizatorom C_3, zanemarljiv.

Neka je

$$\mathcal{R}_X(v) := \{w \in \mathcal{F}v : |\mathrm{Disc}(w)| < X\},$$

gde je v bilo koji element proizvoljnog kompaktnog podskupa B od $V_{\mathbb{R}}$. Uočimo da ako za kubnu formu $ax^3+bx^2y+cxy^2+dy^3$ važi da je $a = 0$, onda je ona reducibilna, pošto je onda y jedan od faktora te forme.

Lema 3.2.1. *Neka je $v \in B$ bilo koja tačka sa nenula diskriminantom, gde je B bilo koji fiksiran kompaktan podskup od $V_{\mathbb{R}}$ koji sadrži samo elemente sa diskriminantom većom od 1. Tada je broj integralnih binarnih kubičnih formi $ax^3+bx^2y+cxy^2+dy^3 \in \mathcal{R}_X(v)$ koje su reducibilne sa $a \neq 0$ procenjen sa $O(X^{\frac{3}{4}+\epsilon})$, gde implicirana konstanta zavisi samo od B.*

Dokaz: Znamo da za bilo koje

$$f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3 \in \mathcal{R}_X(v)$$

imamo da je $f \in N'A'K\Lambda v$, i da za matricu iz Λ koje učestvuje u dekompoziciji f važi da je $0 < \lambda < X^{1/4}$, pošto je $\mathrm{Disc}(\lambda \cdot v) = \lambda^4\mathrm{Disc}(v)$. Odavde sledi da je $a = O(\lambda/t^3) = O(X^{1/4})$, $ab = O(\lambda^2/t^4) = O(X^{1/2})$, $ac = O(\lambda^2/t^2) = O(X^{1/2})$, $ad = O(\lambda^2) = O(X^{1/2})$, $abc = O(\lambda^3/t^3) = O(X^{3/4})$ i $abd = O(\lambda^3/t) = O(X^{3/4})$.

1. Iz prethodnog zaključujemo da je ukupan broj formi $f \in \mathcal{R}_X(v)$ sa $a \neq 0$ i $d = 0$ jednak $O(X^{3/4+\epsilon})$.

2. Pretpostavimo sada da je $a \neq 0$ i $d \neq 0$. U prethodnom delu dokaza smo videli da je ukupan broj mogućnosti za trojku (a, b, d) jednak $O(X^{3/4+\epsilon})$. Fiksirajmo sada vrednosti $a \neq 0, b, d \neq 0$, i posmatrajmo broj mogućnosti za vrednost c tako da je forma $f(x, y)$ reducibilna. Da bi forma f bila reducibilna, ona mora imati linearan faktor $rx + sy$, gde su $r, s \in \mathbb{Z}$ uzajamno prosti. Tada je forma f oblika

$$(rx + sy)(a_1x^2 + b_1xy + c_1y^2),$$

pa imamo da r deli a, a s deli c, zbog čega postoji $O(X^\epsilon)$ mogućnosti i za r i za s. Imajući u vidu da je

$$f(-s, r) = (-rs + rs)(a_1x^2 + b_1xy + c_1y^2) = 0,$$

odavde zaključujemo da je za svaku petorku (a, b, d, r, s) koeficijent c jedinstveno određen. Pošto je broj mogućnosti za trojku (a, b, d) jednak $O(X^{3/4})$, i pošto svakoj takvoj trojci odgovara $O(X^\epsilon)$ mogućnosti za par (r, s), to je ukupan broj reducibilnih formi $f \in \mathcal{R}_X(v)$ sa $a \neq 0$ jednak $O(X^{3/4+\epsilon})$. □

Lema 3.2.2. *Neka je $v \in V_{\mathbb{R}}$ bilo koja forma sa pozitivnom diskriminantom. Tada je broj tačaka u $V_{\mathbb{Z}} \cap \mathcal{R}_X(v)$ čiji je stabilizator C_3 u $\mathrm{GL}_2(\mathbb{Z})$ jednak $O(X^{3/4+\epsilon})$, gde implicirana konstanta ne zavisi od v.*

Dokaz: Znamo iz [DF] da je broj celobrojnih tačaka u $\mathcal{R}_X(v)$ sa stabilizatorom C_3 u $\mathrm{GL}_2(\mathbb{Z})$ jednak broju klasa izomorfizama kubnih prstena sa diskriminantom manjom od X i prstenom automorfizama C_3. Ovaj broj ne zavisi od v, pa je dovoljno dokazati lemu za bilo koje v.

Neka je $v = x^3 - 3xy^2$. Tada je $H_v(x, y) = 9(x^2 + y^2)$ (H_v je Hesijanova kovarijanta: 1.3), odakle vidimo da se $\mathcal{F}H_v$ sastoji od redukovanih (pozitivno definitnih) binarnih kvadratinih formi $A_1x^2 + A_2xy + A_3y^2$, gde je

$$|A_2| \leq A_1 \leq A_3$$

Prema tome, $\mathcal{F}v$ se sastoji od binarnih kubnih formi koje zadovoljavaju

$$|bc - 9ad| \leq b^2 - 3ac \leq c^2 - 3bd.$$

Ako neka binarna kubna forma $f \in \mathcal{F}v$ ima netrivijalan element $\gamma \in SL_2(\mathbb{Z})$ reda 3 koji ga stabilizuje, onda taj element stabilizuje i H_f. Ali, jedina binarna kvadratna forma koja ima netrivijalan stabilizujući element reda 3 (do na množenje skalarom) je $x^2 + xy + y^2$.

Dakle, svaka binarna kubna forma C_3 tipa $f(x, y) = ax^3+bx^2y+cxy^2+dy^3 \in \mathcal{F}v$ mora da zadovoljava

$$b^2 - 3ac = bc - 9ad = c^2 - 3bd.$$

Odavde vidimo da ako su a, b, d fiksirani, da onda postoji najviše jedna mogućnost za c. Kao što smo videli u dokazu prethodne leme, ukupan broj mogućnosti za trojku $(a, b, d) \in \mathcal{F}v$ je $O(X^{3/4+\epsilon})$, odakle sledi lema. □

Dakle, tačaka C_3 tipa u $V_{\mathbb{Z}}$ ima zanemarljivo malo, što se tiče teoreme 3.0.4.

3.3 Usrednjavanje

Neka je dv uobičajena euklidska mera na $V_{\mathbb{R}}$ (normalizovana tako da je ko-mera $V_{\mathbb{Z}}$ jednaka 1), i neka je $dg = t^{-2}dnd^{\times}tdkd^{\times}\lambda$ Haarova mera na $\mathrm{GL}_2(\mathbb{R})$ dobijena iz Iwasawa-ine dekompozicije $\mathrm{GL}_2(\mathbb{R})$, gde je $dk(\mathrm{SO}_2(\mathbb{R})) = 1$, $d^{\times}t = t^{-1}dt$, $d^{\times}\lambda = \lambda^{-1}d\lambda$.

Tvrđenje 3.3.1. *Za $i \in \{0, 1\}$, neka je $f \in C_0(V_{\mathbb{R}}^{(i)})$, i neka je $v_i \in V_{\mathbb{R}}^{(i)}$ proizvoljno. Tada:*

$$\int_{g\in \mathrm{GL}_2(\mathbb{R})} f(g\cdot v_i)dg = \frac{1}{2\pi}\int_{v\in \mathrm{GL}_2(\mathbb{R})\cdot v_i} f(v)|\mathrm{Disc}(v)|^{-1}dv = \frac{n_i}{2\pi}\int_{v\in V_{\mathbb{R}}^{(i)}} f(v)|\mathrm{Disc}(v)|^{-1}dv.$$

Dokaz: Prva jednakost se dobija smenom promenljive $v = g \cdot v_i$, gde su koordinate za g upravo Iwasawine koordinate (k, t, n, λ), a za v su euklidske (a, b, c, d), $dv = dadbdcdd$. Naredna jednakost sledi iz činjenice da je svaki element u skupu $V_{\mathbb{R}}^{(i)}$ predstavljen tačno n_i puta u multiskupu $\mathrm{GL}_2(\mathbb{R})v_i$. □

Neka je sada $C > 1$ neka konstanta, i definišimo sledeći skup:

$$B = B(C) = \{w = (a, b, c, d) \in V_{\mathbb{R}} : 3a^2 + b^2 + c^2 + 3d^2 \leq C, |\mathrm{Disc}(w)| \geq 1\}.$$

Lema 3.3.2. *Skup B je K-invarijantan.*

Dokaz: Prvo, znamo od ranije da elementi K ne utiču na diskriminante elemenata na koje deluju, jer je $\det(k) = 1$, za svako $k \in \mathrm{SO}_2(\mathbb{R})$. Zatim, neka su $k \in K = \mathrm{SO}_2(\mathbb{R})$ i $w = ax^3 + bx^2y + cxy^2 + dy^3 \in B$ proizvoljni. Da li je $k \cdot w \in B$? Pošto je

$$\mathrm{SO}_2(\mathbb{R}) = \left\{ \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix} \mid \theta \in [0, 2\pi] \right\},$$

postoji neko θ za koje je $k = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}$. Tada je

$$k \cdot w(x, y) = w(x\cos\theta - y\sin\theta, x\sin\theta + y\cos\theta) = a_1x^3 + b_1x^2y + c_1xy^2 + d_1y^3.$$

Odavde se računom proveri da je

$$3a_1^2 + b_1^2 + c_1^2 + 3d_1^2 = 3a^2 + b^2 + c^2 + 3d^2 < C,$$

pa važi da je $k \cdot w \in B$. Dakle, pošto su k i w bili proizvoljni, to je $K \cdot B \subset B$, tj. B je K invarijantno. □

Neka je $V_{\mathbb{Z}}^{\mathrm{irr}}$ skup svih ireducibilnih formi u $V_{\mathbb{Z}}$. Tada iz prvog dela ove glave imamo da je

$$N(V_{\mathbb{Z}}^{(i)};X)=\frac{\displaystyle\int_{v\in B\cap V_{\mathbb{R}}^{(i)}}\#\{x\in\mathcal{F}v\cap V_{\mathbb{Z}}^{\mathrm{irr}}:|\mathrm{Disc}(x)|<X\}|\mathrm{Disc}(v)|^{-1}dv}{n_i\cdot\displaystyle\int_{v\in B\cap V_{\mathbb{R}}^{(i)}}|\mathrm{Disc}(v)|^{-1}dv},$$

gde se tačke $x\in\mathcal{F}v\cap V_{\mathbb{Z}}^{\mathrm{irr}}$ sa stabilizatorom C_3 u $\mathrm{GL}_2(\mathbb{Z})$ računaju sa vičestrukošću $1/3$. Po konstrukciji, delitelj u gornjoj jednakosti je konstanta veća od nule. Izabrali smo $|\mathrm{Disc}|^{-1}dv$ kao meru, jer je ona $\mathrm{GL}_2(\mathbb{R})$ invarijantna.

Posmatrajmo opštiji slučaj: Neka je $S\subset V_{\mathbb{Z}}^{(i)}$ bilo koji $\mathrm{GL}_2(\mathbb{Z})$-invarijantan podskup, $N(S;X)$ broj ireducibilnih $\mathrm{GL}_2(\mathbb{Z})$-orbita u S sa diskriminantom manjom od X, i neka je S^{irr} skup ireducibilnih tačaka u S. Tada:

$$N(S;X)=\frac{\displaystyle\int_{v\in B\cap V_{\mathbb{R}}^{(i)}}\#\{x\in\mathcal{F}v\cap S^{\mathrm{irr}}:|\mathrm{Disc}(v)|<X\}|\mathrm{Disc}(v)|^{-1}dv}{n_i\cdot\displaystyle\int_{v\in B\cap V_{\mathbb{R}}^{(i)}}|\mathrm{Disc}(v)|^{-1}dv},$$

gde se tačke $x\in\mathcal{F}v\cap S^{\mathrm{irr}}$ sa stabilizatorom C_3 u $\mathrm{GL}_2(\mathbb{Z})$ računaju sa višestrukošću $1/3$. Ovo ćemo koristiti kao definiciju $N(S;X)$ za bilo koje $S\subset V_{\mathbb{Z}}$, čak i kada S nije $\mathrm{GL}_2(\mathbb{Z})$-invarijantno. Uočimo, ako su $S_1,S_2\in V_{\mathbb{Z}}$ disjunktni, onda važi:

$$N(S_1\cup S_2;X)=N(S_1;X)+N(S_2;X).$$

Neka je $v_i\in V_{\mathbb{R}}^{(i)}$ proizvoljno, i neka su $H^{(i)}\subset\mathrm{GL}_2(\mathbb{R})$ maksimalni skupovi takvi da je $H^{(i)}\cdot v_i=B\cap V_{\mathbb{R}}^{(i)}$. Tada multiskup $H^{(i)}\cdot v_i$ svaki element iz $B\cap V_{\mathbb{R}}^{(i)}$ predstavlja n_i puta i brojilac u gornjoj jednakosti jednak je

$$\sum_{\substack{x\in S^{\mathrm{irr}}\\ |\mathrm{Disc}(x)|<X}}\int_{v\in B\cap V_{\mathbb{R}}^{(i)}}\#\{g\in\mathcal{F}:x=gv\}|\mathrm{Disc}(v)|^{-1}dv=$$

$$= \frac{2\pi}{n_i} \sum_{\substack{x \in S^{\text{irr}} \\ |\text{Disc}(x)|<X}} \int_{h \in H^{(i)}} \#\{g \in \mathcal{F} : x = ghv_i\} dh,$$

gde tačnost ove jednakosti sledi iz prethodnog tvrđenja. Dalje, desna strana jednakosti jednaka je

$$\frac{2\pi}{n_i} \sum_{\substack{x \in S^{\text{irr}} \\ |\text{Disc}(x)|<X}} \int_{g \in \mathcal{F}} \#\{h \in H^{(i)} : x = ghv_i\} dg =$$

$$= \frac{2\pi}{n_i} \int_{g \in \mathcal{F}} \#\{x \in S^{irr} \cap gH^{(i)}v_i : |\text{Disc}(x)| < X\} dg.$$

Dakle, važi:

$$N(S; X) = \frac{1}{M_i} \int_{g \in \mathcal{F}} \#\{x \in S^{\text{irr}} \cap gB \cap V_{\mathbb{R}}^{(i)} : |\text{Disc}(x)| < X\} dg = \tag{3.1}$$

$$= \frac{1}{M_i} \int_{g \in N'(a)A'\Lambda K} \# \left\{ x \in S^{irr} \cap n \begin{bmatrix} t^{-1} & 0 \\ 0 & t \end{bmatrix} \lambda k B \cap V_{\mathbb{R}}^{(i)} : |\text{Disc}(x)| < X \right\}$$

$$t^{-2} dn d^{\times} t d^{\times} \lambda dk,$$

gde je

$$M_i = \frac{n_i}{2\pi} \int_{v \in B \cap V_{\mathbb{R}}^{(i)}} |\text{Disc}(v)|^{-1} dv.$$

Uvedimo sledeću oznaku:

$$B(n,t,\lambda,X) := n \begin{bmatrix} t^{-1} & 0 \\ 0 & t \end{bmatrix} \lambda B \cap \{v \in V_{\mathbb{R}}^{(i)} : |\mathrm{Disc}(v)| < X\}.$$

Kako je $KB = B$ i $\int_K dk = 1$, to je

$$N(S;X) = \frac{1}{M_i} \int_{g \in N'(a)A'\Lambda} \#\{x \in S^{\mathrm{irr}} \cap B(n,t,\lambda,X)\} t^{-2} dn d^{\times}t d^{\times}\lambda. \tag{3.2}$$

Kako bismo procenili broj tačaka u $B(n,t,\lambda,X)$, upotrebićemo Davenportovu teoremu 1.6.6:

Lema 3.3.3. *Broj celobrojnih tačaka (a,b,c,d) u $B(n,t,\lambda,X)$ sa $a \neq 0$ je*

$$\begin{cases} 0 & \frac{C\lambda}{t^3} < 1; \\ \mathrm{Vol}(B(n,t,\lambda,X)) + O(\max\{C^3t^3\lambda^3, 1\}) & \textit{inače.} \end{cases}$$

Dokaz: Iz opisa B imamo da za bilo koju binarnu kubnu formu u B važi da je koeficijent uz x^3 ograničen sa C. Zbog toga, ako je $C\lambda/t^3 < 1$, onda je $a = 0$ jedina mogućnost za celobrojne binarne kubne forme

$$ax^3 + bx^2y + cxy^2 + dy^3 \in B(n,t,\lambda,X).$$

Ako je $C\lambda/t^3 \geq 1$, onda su λ i t pozitivni brojevi ograničeni odozdo sa $(\sqrt[4]{3}/\sqrt{2})^3/C$ i $\sqrt[4]{3}/\sqrt{2}$, redom. U ovom slučaju, projekcija $B(n,t,\lambda,X)$ na $a = 0$ ima meru $O(C^3t^3\lambda^3)$ a ostale projekcije su ograničene sa ovim brojem puta konstanta (dakle, opet $O(C^3t^3\lambda^3)$). Lema sledi iz Davenport-ove propozicije. □

Uočimo, da bi integrant u jednakosti (3.2) bio nenula, mora da važi $t^3 \leq C\lambda$ (prethodna lema), i $1 \leq \lambda < X^{1/4}$, jer je diskriminanta elemenata $B(n,t,\lambda,X)$ između 1 i X. Dakle, možemo reći sledeće, do na grešku od $O(X^{3/4+\epsilon})$:

$$N(V_{\mathbb{Z}}^{(i)};X)=\frac{1}{M_i}\int_{\lambda=(\sqrt[4]{3}/\sqrt{2})^3/C}^{X^{1/4}}\int_{t=\sqrt[4]{3}\sqrt{2}}^{C^{1/3}\lambda^{1/3}}\int_{N'(t)}(\mathrm{Vol}(B(n,t,\lambda,X))+$$

$$+O(\max\{C^3t^3\lambda^3,1\}))t^{-2}dnd^{\times}td^{\times}\lambda.$$

Integral prvog sabirka iznosi

$$\frac{1}{2\pi M_i}\int_{v\in B\cap V_{\mathbb{R}}^{(i)}}\mathrm{Vol}(\mathcal{R}_X(v))|\mathrm{Disc}(v)|^{-1}dv-\frac{1}{M_i}\int_{\lambda=(\sqrt[4]{3}/\sqrt{2})^3/C}^{X^{1/4}}\int_{t=C^{1/3}\lambda^{1/3}}^{\infty}$$

$$\int_{N'(t)}(\mathrm{Vol}(B(n,t,\lambda,X))dnd^{\times}td^{\times}\lambda.$$

Na početku ove glave smo videli da $\mathrm{Vol}(\mathcal{R}_{\mathrm{X}}(\mathrm{v}))$ ne zavisi od izbora $v\in V_{\mathbb{R}}^{(i)}$, prvi član u drugoj jednakosti je jednak $\mathrm{Vol}(\mathcal{R}_{\mathrm{X}}(\mathrm{v}))/\mathrm{n_i}$, a za drugi sabirak imamo da je jednak

$$O(C^{10/3}X^{5/6}/M_i(C)),$$

pošto je $\mathrm{Vol}(B(n,t,\lambda,X))\ll C^4\lambda^4$. Kako je $C^3t^3\lambda^3\gg 1$, možemo videti da je drugi sabirak u prvoj jednakosti jednak

$$O(C^{10/3}X^{5/6}/M_i(C)).$$

Dakle, za bilo koje $v\in V_{\mathbb{R}}^{(i)}$ važi

$$N(V_{\mathbb{Z}}^{(i)};X)=\frac{1}{n_i}\cdot\mathrm{Vol}(\mathcal{R}_X(v))+O(C^{10/3}X^{5/6}/M_i(C)).$$

Kako bismo dokazali teoremu 3.0.2, ostaje nam da izračunamo fundamentalnu zapreminu $\mathrm{Vol}(\mathcal{R}_X(v))$ za $v\in V_{\mathbb{R}}^{(i)}$.

3.4 Računanje fundamentalne zapremine

Neka je $\mathrm{GL}_2^{\pm 1}(\mathbb{R})$ podgrupa matrica od $\mathrm{GL}_2(\mathbb{R})$ sa determinantom ± 1. Poznato je iz [K] da je

$$\mathrm{Vol}(\mathrm{GL}_2^{\pm 1}(\mathbb{Z}) \setminus \mathrm{GL}_2^{\pm 1}(\mathbb{R})) = \zeta(2)/\pi,$$

pa iz tvrđenja 3.3.1 sledi

$$\frac{1}{n_i} \cdot \mathrm{Vol}(\mathcal{R}_X(v_i)) = \frac{2\pi}{n_i} \int_0^{X^{1/4}} \lambda^4 d^\times \lambda \int_{\mathrm{GL}_2(\mathbb{Z})\setminus \mathrm{GL}_2^{\pm 1}(\mathbb{R})} dh = \frac{2\pi}{n_i} \cdot \frac{X}{4} \cdot \frac{\zeta(2)}{\pi} = \frac{\pi^2}{12 n_i} X.$$

3.5 Preciznija procena

U ovom odeljku ćemo naći precizniju procenu za $N(V_{\mathbb{Z}}^{(i)}; X)$. Dobićemo da je

$$N(V_{\mathbb{Z}}^{(i)}; X) = c_1^{(i)} X + c_2^{(i)} X^{5/6} + O(X^{3/4}),$$

gde su $c_1^{(0)} = \pi^2/72$, $c_1^{(1)} = \pi^2/24$, $c_2^{(0)} = \sqrt{3} r/30$, $c_2^{(1)} = r/10$ i

$$r = \frac{\zeta(2/3)\Gamma(1/3)(2\pi)^{1/3}}{\Gamma(2/3)}.$$

Postupak dobijanja je podeljen na nekoliko koraka.

U (3.1) smo dobili $N(V_{\mathbb{Z}}^{(i)}; X)$ izraženo integralom nad $\mathcal{F}$: fundamantalnim domenom dejstva $\mathrm{GL}_2(\mathbb{Z})$ na $\mathrm{GL}_2(\mathbb{R})$. Procena integrala je zahtevala procenu broja celobrojnih tačaka u multiskupu $B(n, t, \lambda, X)$, za šta smo koristili tvrđenje 1.6.6, i dobili da je njihov broj jednak zapremini $B(n, t, \lambda, X)$ sa greškom $O(t^3\lambda^3)$.

Prvi korak:

Sada ćemo tražiti broj celobrojnih tačaka u skupu $B(n,t,\lambda,X/2,X)$: to je podskup od $B(n,t,\lambda,X)$ čije tačke imaju apsolutnu vrednost diskriminante veću od $X/2$. Kako bismo preciznije procenili broj celobrojnih tačaka u ovom skupu, posmatraćemo skup kao uniju podskupova $B_a(n,t,\lambda,X/2,X)$ (elementi određeni uslovom da je koeficjent uz x^3 jednak a). Tada imamo sledeće razbijanje:

$$\#\{x \in V_{\mathbb{Z}}^{irr} \cap B(n,t,\lambda,X/2,X)\} = \sum_{\substack{a\in\mathbb{Z}\\ a\neq 0}} \#\{x \in V_{\mathbb{Z}}^{irr} \cap B_a(n,t,\lambda,X/2,X).$$

Ovu sumu ćemo proceniti pomoću 1.6.6. Biće nam bitno da razdvojimo ovu sumu na članove sa "velikim" t i na članove sa "malim" t. Odvajamo velike t od malih na sledeći način:

Neka je Ψ glatka funkcija na $\mathbb{R}_{\geq 0}$ takva da je $\Psi(x) = 1$ za $x \leq 2$, i $\Psi(x) = 0$ za $x \geq 3$. Označimo sa Ψ_0 funkciju $1 - \Psi$ i sa $N(V_{\mathbb{Z}}^{(i)}; X/2, X)$ broj $\mathrm{GL}_2(\mathbb{Z})$ orbita na $V_{\mathbb{Z}}^{(i),irr}$ sa diskriminantom između $X/2$ i X. Tada za bilo koje $\kappa > 0$ važi:

$$N(V_{\mathbb{Z}}^{(i)}; X/2, X) = \tag{3.3}$$

$$= \frac{1}{M_i} \int_{N'(a)A'\Lambda} \Psi\left(\frac{t\kappa}{\lambda^{1/3}}\right) \#\{x \in V_{\mathbb{Z}}^{(i),irr} \cap B(n,t,\lambda,X/2,X)\} t^{-2} dn d^{\times}t d^{\times}\lambda +$$

$$+ \frac{1}{M_i} \int_{N'(a)A'\Lambda} \Psi_0\left(\frac{t\kappa}{\lambda^{1/3}}\right) \#\{x \in V_{\mathbb{Z}}^{(i),irr} \cap B(n,t,\lambda,X/2,X)\} t^{-2} dn d^{\times}t d^{\times}\lambda.$$

Za nas će κ biti pomoćni parametar, koji ćemo izabrati kasnije kako bismo optimizovali procenu. Za sada ćemo smatrati samo da je $\lim\limits_{X\to\infty} \kappa = \infty$ i $\kappa < X^{3/4}$.

Prvi sabirak u (3.3) je različit od nule samo ako je $t < 3\lambda^{1/3}/\kappa$, dok je drugi različit od nule samo ako je $t > 2\lambda^{1/3}/\kappa$.

Neka je D_0 konstanta koja ograničava diskriminantu svake tačke u B. Pošto je diskriminanta svake tačke u B ograničena odozdo sa 1, i odozgo sa D_0, to je skup $B(n,t,\lambda,X/2,X)$ prazan osim ako je

$$\left(\frac{X}{D_0}\right)^{1/4} < \lambda < X^{1/4}.$$

Takođe, $\Psi\left(\frac{t\kappa}{\lambda^{1/3}}\right)$ je nula za $\lambda < 27t^3\kappa^3$, pa po 1.6.6 imamo da je prvi sabirak u (3.3) jednak

$$\frac{1}{M_i}\int_{\lambda=\left(\frac{X}{D_0}\right)^{1/4}}^{X^{1/4}}\int_{t=\sqrt[4]{3}/\sqrt{2}}^{3\lambda^{1/3}/\kappa}\int_{N'(t)}\Psi\left(\frac{t\kappa}{\lambda^{1/3}}\right)(\mathrm{Vol}(B(n,t,\lambda,X/2,X))+$$

$$+O(\max\{t^3\lambda^3,1\}))t^{-2}dnd^{\times}td^{\times}\lambda.$$

Integral greške u gornjoj jednakosti se nađe da je:

$$O\left(\int_{\left(\frac{X}{D_0}\right)^{1/4}}^{X^{1/4}}\int_{t=\sqrt[4]{3}/\sqrt{2}}^{\lambda^{1/3}/\kappa}\lambda^3 td^{\times}td^{\times}\lambda\right)=O\left(\frac{X^{5/6}}{\kappa}\right).$$

Prema tome, prvi sabirak u (3.3) iznosi

$$\frac{1}{M_i}\int_{\lambda=\left(\frac{X}{D_0}\right)^{1/4}}^{X^{1/4}}\int_{t=\sqrt[4]{3}/\sqrt{2}}^{\infty}\int_{N'(t)}\Psi\left(\frac{t\kappa}{\lambda^{1/3}}\right)\lambda^4\mathrm{Vol}(B(X/(2\lambda^4),X/\lambda^4))t^{-2}dnd^{\times}td^{\times}\lambda+$$

$$+O\left(\frac{X^{5/6}}{\kappa}\right),$$

gde je $B(d_1,d_2)$ broj tačaka u B sa diskriminantom između d_1 i d_2.

Drugi korak:

Sada ćemo proceniti drugi sabirak u (3.3) tako što ćemo ga razbiti na sumu po tačkama sa fiksiranim x^3 koeficijentom:

$$\frac{1}{M_i}\sum_{\substack{a\in\mathbb{Z}\\ a\neq 0}}\int_{g\in\mathcal{F}}\Psi_0\left(\frac{t\kappa}{\lambda^{1/3}}\right)\#\{x\in V_{\mathbb{Z}}^{(i),irr}\cap B_a(n,t,\lambda,X/2,X)\}dg.$$

Pošto je B K invarijantno, broj tačaka u $B_a(n,t,\lambda,X/2,X)$ je jednak broju tačaka u $B_a(n,t,\lambda,X/2,X)$. Bitno je primetiti da integrant jednak nuli kada je $a>O(\kappa^3)$, gde implicirana konstanta zavisi samo od B. Ponovo koristeći 1.6.6 vidimo da gornji izraz iznosi

$$\frac{2}{M_i}\sum_{a=1}^{O(\kappa^3)}\int_{\lambda=\left(\frac{X}{D_0}\right)^{1/4}}^{X^{1/4}}\int_{t=\sqrt[4]{3}/\sqrt{2}}^{\infty}\int_{N'(t)}\Psi_0\left(\frac{t\kappa}{\lambda^{1/3}}\right)(\mathrm{Vol}(B_a(n,t,\lambda,X/2,X))+$$

$$+O(\max\{\lambda^2t^4,1\}))t^{-2}dnd^{\times}td^{\times}\lambda.$$

Kao kod prvog sabirka, procenjujemo grešku kod drugog:

$$\sum_{a=1}^{O(\kappa^3)}\int_{\lambda=\left(\frac{X}{D_0}\right)^{1/4}}^{X^{1/4}}\int_{t=\sqrt[4]{3}/\sqrt{2}}^{\lambda^{1/3}/a^{1/3}}\lambda^2t^4t^{-2}d^{\times}td^{\times}\lambda=X^{2/3}\sum_{a=1}^{O(\kappa^3)}O(a^{-2/3})=O(\kappa X^{2/3}).$$

Treći korak:

Od sada ćemo smatrati da je $\kappa\leq\frac{1}{3}X^{1/12}$. Uočimo: za dovoljno veliko X, ako je $\Psi_0\left(\frac{t\kappa}{\lambda^{1/3}}\right)$ različito od nule, onda je $t>\frac{2\lambda^{1/3}}{\kappa}>1$, pošto je $\lambda>(\frac{X}{D_0})^{1/4}$. Prema tome, integral nad $N'(t)$ kod drugog sabirka uvek ide od $-1/2$ do $1/2$. Sada je integral drugog sabirka jednak

$$\frac{2}{M_i}\sum_{a=1}^{\infty}\int_{\lambda=\left(\frac{X}{D_0}\right)^{1/4}}^{X^{1/4}}\int_{t>0}\Psi_0\left(\frac{t\kappa}{\lambda^{1/3}}\right)\mathrm{Vol}(B_a(0,t,\lambda,X/2,X))t^{-2}d^{\times}td^{\times}\lambda=$$

$$= \frac{2}{M_i} \sum_{a=1}^{\infty} \int_{\lambda=\left(\frac{X}{D_0}\right)^{1/4}}^{X^{1/4}} \int_{t>0} \Psi_0 \left(\frac{t\kappa}{\lambda^{1/3}} \right) \lambda^3 t^3 \mathrm{Vol} \left(B_{\frac{at^3}{\lambda}}(X/(2\lambda^4), X/\lambda^4) \right) t^{-2} d^\times t d^\times \lambda,$$

gde je $B_a(d_1, d_2)$ skup formi u B ǩoje imaju a kao koeficijent uz x^3, i apsolutnu vrednost diskriminante između d_1 i d_2. Uvedimo smenu promenljive u desnoj strani gornje jednakosti: $u = t^3 a/\lambda$, $d^\times u = 3 d^\times t$.

$$\frac{2}{3M_i} \sum_{a=1}^{\infty} \int_{\lambda=\left(\frac{X}{D_0}\right)^{1/4}}^{X^{1/4}} \int_{u>0} \Psi_0 \left(\frac{u^{1/3}\kappa}{a^{1/3}} \right) \frac{\lambda^{10/3} u^{1/3}}{a^{1/3}} \mathrm{Vol}(B_u(X/(2\lambda^4), X/\lambda^4)) d^\times u d^\times \lambda.$$

Četvrti korak:

Kako bismo izračunali gornju sumu, uvešćemo sledeće oznake:

$$\Phi(z) = \Psi_0(u^{1/3}/z^{1/3});$$

za funkciju F definisanoj na pozitivnim realnim brojevima, $\widetilde{F}(s)$ je njena Mellin-ova transformacija. Pošto je Ψ_0' glatka funkcija, i pripada Schwartz-ovoj klasi funkcija (postoje realne konstante $C^{\alpha\beta}$ takve da je

$$\sup_{x \in \mathbb{R}^n} |x^\alpha \partial_\beta f(x)| \leq C^{\alpha\beta},$$

Melinova transfotmacija $\widetilde{\Psi_0'}(s)$ je holomorfna, cela i brzo opadajuća funkcija na bilo kojoj vertikali $\sigma + it$ kada $|t| \to \infty$. Jedno od osnovnih svojstva Mellinove transformacije je da važi

$$\widetilde{\Psi_0'}(s+1) = s\widetilde{\Psi_0}(s).$$

Dakle, $\widetilde{\Psi_0}(s)$ i $\widetilde{\Phi}(s)$ imaju moguć pol u nuli, pored koga su cele, i brzo opadaju na vertikalama. Pol funkcije $\widetilde{\Psi_0}(s)$ u nuli je:

$$\widetilde{\Psi_0'}(1) = \int_0^\infty \Psi_0'(y)dy = 1.$$

Dakle,

$$\sum_{a=1}^{\infty} a^{-\frac{1}{3}} \Psi_0\left(\frac{u^{1/3}\kappa}{a^{1/3}}\right) = \int_{Re(s)=2} \zeta(s+1/3)\widetilde{\Phi}(s)\kappa^{3s}ds =$$

$$= 3\int_{Re(s)=2} \zeta(s+1/3)\widetilde{\Psi_0}(-3s)(\kappa^3 u)^s ds =$$

$$= \zeta(1/3) + 3\widetilde{\Psi_0}(-2)(\kappa^3 u)^{2/3} + O_M\left(\min\left\{(\kappa^3 u)^{-M}, 1\right\}\right),$$

za bilo koji celi broj M, gde se poslednja jednakost dobija pomeranjem prave integracije na $\mathrm{Re}(s) = -M$, i računanjem reziduuma u $s = 0$ i $s = \frac{2}{3}$. Prema tome, sumu koju smo računali ima oblik

$$\frac{2}{3M_i}\int_{\lambda=\left(\frac{X}{D_0}\right)^{1/4}}^{X^{1/4}} \int_{u>0} \left[\zeta(1/3) + 3\widetilde{\Psi_0}(-2)(\kappa^3 u)^{2/3}\right] \lambda^{10/3} u^{1/3} \mathrm{Vol}(B_u(X/(2\lambda^4), X/\lambda^4)) d^\times u d^\times \lambda, \tag{3.4}$$

sa greškom

$$O\left(\int_{\lambda=\left(\frac{X}{D_0}\right)^{1/4}}^{X^{1/4}} \int_{u>0} \min\left\{\left(\kappa^3 u\right)^{-1}, 1\right\} \lambda^{10/3} u^{1/3} \mathrm{Vol}(B_u(X/(2\lambda^4), X\lambda^4)) d^\times u d^\times \lambda\right).$$

Peti korak:

Ako uzmemo da je $\kappa = \frac{1}{3}X^{1/12}$, greška postaje

$$O\left(\int_{\lambda=\left(\frac{X}{D_0}\right)^{1/4}}^{X^{1/4}} \int_{u=0}^{\kappa^{-3}} \lambda^{10/3} u^{1/3} d^\times u d^\times \lambda\right) = O\left(\frac{X^{5/6}}{\kappa}\right).$$

Izračunajmo sada integrale sabiraka u izrazu (3.4). Drugi sabirak:

$$\frac{2}{M_i}\int_{\lambda=\left(\frac{X}{D_0}\right)^{1/4}}^{X^{1/4}}\int_{u>0}\widetilde{\Psi_0}(-2)\kappa^2\lambda^{10/3}u\mathrm{Vol}(B_u(X/(2\lambda^4),X/\lambda^4))d^\times u d^\times\lambda =$$

$$=\frac{1}{M_i}\int_{\lambda=\left(\frac{X}{D_0}\right)^{1/4}}^{X^{1/4}}\widetilde{\Psi_0}(-2)\kappa^2\lambda^{10/3}\mathrm{Vol}(B(X/(2\lambda^4),X/\lambda^4))d^\times\lambda =$$

$$=\frac{1}{M_i}\int_{\lambda=\left(\frac{X}{D_0}\right)^{1/4}}^{X^{1/4}}\int_{t=0}^{\infty}\widetilde{\Psi_0}\left(\frac{t\kappa}{\lambda^{1/3}}\right)\lambda^{\frac{10}{3}+\frac{2}{3}}\mathrm{Vol}(B(X/(2\lambda^4),X/\lambda^4))t^{-2}d^\times\lambda.$$

Dakle, glavni izraz u (3.3) ima oblik

$$\frac{1}{M_i}\int_{\lambda=\left(\frac{X}{D_0}\right)^{1/4}}^{X^{1/4}}\int_{t=\sqrt[4]{3}/\sqrt{2}}^{\infty}\int_{N'(t)}\left(\Psi\left(\frac{t\kappa}{\lambda^{1/3}}\right)+\Psi_0\left(\frac{t\kappa}{\lambda^{1/3}}\right)\right)\lambda^4\mathrm{Vol}(B(X/(2\lambda^4)/X/\lambda^4))$$

$$t^{-2}dnd^\times td^\times\lambda =$$

$$=\frac{1}{M_i}\int_{\lambda=\left(\frac{X}{D_0}\right)^{1/4}}^{X^{1/4}}\int_{t=\sqrt[4]{3}/\sqrt{2}}^{\infty}\int_{N'(t)}\mathrm{Vol}(B(n,t,\lambda,X/2,X))t^{-2}dnd^\times td^\times\lambda,$$

što se može izračunati (kao u prethodnom odeljku) da je jednako $c_1^{(i)}X/2$.

Šesti korak:

Sada, nađimo integral prvog sabirka u (3.4):

$$\frac{2}{3M_i}\int_{\lambda=\left(\frac{X}{D_0}\right)^{1/4}}^{X^{1/4}}\int_{u>0}\zeta(1/3)\lambda^{10/3}u^{1/3}\mathrm{Vol}(B_u(X/(2\lambda^4),X/\lambda^4))d^\times u d^\times\lambda.$$

Označimo sa $a(v), b(v), c(v)$ i $d(v)$ četiri koordinate tačaka $v \in B$. Tada je gornji izraz jednak:

$$\frac{1}{3M_i}\zeta(1/3)\int_{\lambda=\left(\frac{X}{D_0}\right)^{1/4}}^{X^{1/4}}\int_{B(X/(2\lambda^4),X/\lambda^4)}\lambda^{10/3}a(v)^{1/3}\frac{dv}{a(v)}d^\times\lambda =$$

$$=\frac{1}{3M_i}\zeta(1/3)\int_{\lambda=\left(\frac{X}{D_0}\right)^{1/4}}^{X^{1/4}}\int_{B(X/(2\lambda^4),X/\lambda^4)}\lambda^{10/3}a(v)^{-2/3}dvd^\times\lambda =$$

$$=\frac{1}{10M_i}\zeta(1/3)\left(1-2^{-5/6}\right)X^{5/6}\int_B|\mathrm{Disc}(v)|^{-5/6}a(v)^{-2/3}dv =$$

$$=\frac{2\pi}{10n_i}\zeta(1/3)\left(1-2^{-5/6}\right)X^{5/6}\frac{\int_B|\mathrm{Disc}(v)|^{-5/6}a(v)^{-2/3}dv}{\int_B|\mathrm{Disc}(v)|^{-1}dv}. \tag{3.5}$$

Sedmi korak:

Sada ćemo izračunati izraz

$$\frac{\int_B|\mathrm{Disc}(v)|^{-5/6}a(v)^{-2/3}dv}{\int_B|\mathrm{Disc}(v)|^{-1}dv}.$$

Njegova vrednost ne zavisi od K invarijantnog skupa B, pa će on za proizvoljno $f \in V_{\mathbb{R}}^{(i)}$ biti jednak

$$|\mathrm{Disc}(f)|^{1/6}\int_K a(\gamma\cdot f)^{-2/3}d\gamma = |\mathrm{Disc}(f)|^{1/6}\int_K f((1,0)\cdot\gamma)^{-2/3}d\gamma =$$

$$= \frac{|\mathrm{Disc}(f)|^{1/6}}{2\pi}\int_0^{2\pi} f(\cos\theta,\sin\theta)^{-2/3}d\theta.$$

Sada ćemo odabrati pogodne tačke $f \in V_{\mathbb{R}}^{(i)}$:

1. $\underline{i=1}$: $f(x,y) = x^3 + xy^2$, $\mathrm{Disc}(f) = -4$. Tada naš izraz postaje

$$\frac{|\mathrm{Disc}(f)|^{1/6}}{2\pi}\int_0^{2\pi} f(\cos\theta,\sin\theta)^{-2/3}d\theta = \frac{2^{1/3}}{2\pi}\int_0^{2\pi}\cos^{-2/3}\theta d\theta =$$

$$= \frac{2^{4/3}}{\pi}\int_0^{\pi/2}\cos^{-2/3}\theta d\theta.$$

Zatim uvodimo smenu $y = \cos\theta$:

$$\frac{2^{4/3}}{\pi}\int_0^{\pi/2}\cos^{-2/3}\theta d\theta = \frac{2^{4/3}}{\pi}\int_0^1 y^{-2/3}(1-y^2)^{-1/2}dy.$$

Smena $z = y^2$:

$$\frac{2^{4/3}}{\pi}\int_0^1 y^{-2/3}(1-y^2)^{-1/2}dy = \frac{2^{1/3}}{\pi}\int_0^1 z^{-5/6}(1-z)^{-1/2}dz = \frac{2^{1/3}}{\pi}B\left(\frac{1}{2},\frac{1}{6}\right) =$$

$$= \frac{2^{1/3}\Gamma(1/6)\Gamma(1/2)}{\pi\Gamma(2/3)}.$$

Odavde možemo videti da je izraz (3.5) jendak $(1-2^{-5/6})c_2^{(1)}X5/6$.

2. $\underline{i=0}$: Biramo $f(x,y) = x^3 - 3xy^2 \in V_{\mathbb{R}}^{(0)}$. Pomoću identiteta $\cos 3\theta = \cos^3\theta - 3\cos\theta\sin^2\theta$, vidimo da će izraz (3.5) biti jednak $(1-2^{-5/6})c_2^{(0)}X^{5/6}$. Dakle,

$$N(V_{\mathbb{Z}}^{(i)}; X/2, X) = c_1^{(i)}X/2 + c_2^{(i)}(1-2^{-5/6})X^{5/6} + O(X^{2/3}\kappa) + O(X^{5/6}/\kappa),$$

što nam za $\kappa = \frac{1}{3}X^{1/12}$ daje traženi rezultat.

Glava 4

Binarne kvartične forme

U ovoj glavi ćemo raditi sa binarnim kvartičnim formama na sličan način kao što smo radili sa binarnim kubičnim formama. Zato, neka je $V_{\mathbb{R}}$ skup svih binarnih kvartičnih formi, tj. homogenih polinoma oblika

$$f(x, y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4,$$

gde su $a, b, c, d, e \in \mathbb{R}$. Za ovakvo $f \in V_{\mathbb{R}}$ kažemo da je *integralno* ili *celobrojno* ako važi $a, b, c, d, e \in \mathbb{Z}$. Kao i uvek, $\mathrm{GL}_2(\mathbb{Z})$ deluje na prostor binarnih kvartičnih formi na sledeći način:

$$\gamma \cdot f(x, y) = f((x, y) \cdot \gamma).$$

Može se videti da je

$$(\gamma_1\gamma_2) \cdot f = \gamma_1 \cdot (\gamma_2 \cdot f). \tag{4.1}$$

Takođe ćemo gledati dejstvo $\mathrm{SL}_2^{\pm}$ na $V_{\mathbb{R}}$, gde je $\mathrm{SL}_2^{\pm} \subset \mathrm{GL}_2(\mathbb{R})$ podgrupa matrica sa determinantom ± 1. No, ovde imamo razliku u odnosu na kubne forme: prsten invarijanti za ovo dejstvo na binarne kvartične forme ima dva nezavisna generatora, a to su

$$I(f) = 12ae - 3bd + c^2,$$
$$J(f) = 72ace + 9bcd - 27ad^2 - 27eb^2 - 2c^3.$$

Neka je sada $\gamma \in \mathrm{GL}_2(\mathbb{R})$. Tada je

$$I(\gamma \cdot f) = (\det \gamma)^4 I(f),$$
$$J(\gamma \cdot f) = (\det \gamma)^6 J(f),$$

i zato I i J zovemo *relativnim invarijantama* za dejstvo $\mathrm{GL}_2(\mathbb{R})$ na $V_{\mathbb{R}}$ stepena 4 i 6, redom.
Pošto je diskriminanta binarne kvartične forme relativna invarijanta stepena 6, ona se može izraziti preko I i J, i to na sledeći način:

$$\Delta(f) = \Delta(I(f), J(f)) = (4I(f)^3 - J(f)^2)/27 = b^2c^2 + 18abcd - 4ac^3 - 4b^3d - 27a^2d^2.$$

Definicija 4.0.1. *Visina binarne kvartične forme f je*

$$H(f) := H(I, J) = \max\left\{|I|^3, J^2/4\right\}.$$

Primetimo, za proizvoljnu formu $V \in V_{\mathbb{Z}}$ i proizvoljno $\gamma \in \mathrm{Stab}(f)$, imamo da je

$$H(f) = H(\gamma \cdot f) = \max\left\{\left|(\det\gamma)^4 I(f)\right|^3, ((\det\gamma)^6 J(f))^2/4\right\} = (\det\gamma)^{12} H(f),$$

odakle imamo da ako je $\gamma \in \mathrm{Stab}(f)$ za neku formu f, da je tada $\det\gamma = \pm 1$.

Za dve forme kažemo da su $\mathrm{GL}_2(\mathbb{Z})$ ekvivalentne ako postoje matrice $\gamma_1, \gamma_2 \in \mathrm{GL}_2(\mathbb{Z})$ takve da je $f = \gamma_1 \cdot g$ i $g = \gamma_2 \cdot f$. No, zbog jednakosti (4.1), važi:

$$f = \gamma_1 \cdot (\gamma_2 \cdot f) = (\gamma_1\gamma_2) \cdot f.$$

Dakle, imamo da je $\gamma_1\gamma_2 \in \mathrm{Stab}(f)$. Pošto su matrice γ_1 i γ_2 celobrojne, to su i njihove determinante celobrojne.

Pretpotstavimo da je $|\det\gamma_1| > 1$. Tada mora biti $|\det\gamma_2| < 1$ ($\gamma_1\gamma_2 \in \mathrm{Stab}(f)$, pa imamo da je $\det(\gamma_1\gamma_2) = \pm 1$), što je nemoguće, jer ne postoji nijedan celi broj čija je apsolutna vrednost strogo manja od 1 i različita od nule. Dakle, mora biti $\det\gamma_1 = \pm 1$.

Neka su sada f i g binarne kvartične forme koje su $\mathrm{GL}_2(\mathbb{Z})$ ekvivalentne. Tada postoji matrica $\gamma \in \mathbb{Z}$ sa determinantom ± 1 takva da je $f = \gamma \cdot g$. Imajući ovo u vidu, vidimo da je

$$I(f) = (\det\gamma)^4 I(g) = I(g) \quad \text{i} \quad J(f) = (\det\gamma)^6 J(g) = J(g),$$

pa forme f i g imaju istu visinu. Dakle, svi elementi u $\mathrm{GL}_2(\mathbb{Z})$ imaju istu visinu, pa možemo definisati visinu jedne takve klase kao visinu nekog njenog predstavnika.

Primetimo da dejstvo $\mathrm{GL}_2(\mathbb{Z})$ na $V_\mathbb{R}$ šalje integralne elemente u integralne elemente. U ovoj glavi tražimo odgovor na sledeća pitanja: Koliko ima $\mathrm{GL}_2(\mathbb{Z})$ klasa u $V_\mathbb{R}$ sa visinom ne većom od X? Koliko $\mathrm{GL}_2(\mathbb{Z})$ klasa ima sa visinom ne većom od X i datim brojem realnih korena?

Definicija 4.0.2. *$V_\mathbb{Z}^{(i)}$ je skup elemenata u $V_\mathbb{Z}$ sa nenula diskriminantom i $4-2i$ realna korena u $\mathbb{P}^1_\mathbb{C}$. Za $S \subset V_\mathbb{Z}$ koji je $\mathrm{GL}_2(\mathbb{Z})$ invarijantan, neka je $N(S;X)$ broj $\mathrm{GL}_2(\mathbb{Z})$ klasa ireducibilnih elemenata $f \in S$ za koje važi $H(f) < X$.*

Uočimo da je $V_\mathbb{R}^{(2)}$ skup definitnih formi u $V_\mathbb{R}$, tj. onih formi f koje uzimaju samo pozitivne ili samo negativne vrednosti u nenula vektorima $(x_0, y_0) \in \mathbb{R}^2$. Označimo sa $V_\mathbb{R}^{(2+)}$ (odnosno $V_\mathbb{R}^{(2-)}$) podskup od $V_\mathbb{R}^{(2)}$ koji se sastoji od pozitivnih definitnih formi (odnosno negativnih definitnih formi). Za $i = 0, 1, 2$ imamo oznake $V_\mathbb{Z}^{(i)} = V_\mathbb{R}^{(i)} \cap V_\mathbb{Z}$, pa analogno definišemo $V_\mathbb{Z}^{(i)} = V_\mathbb{R}^{(i)} \cap V_\mathbb{Z}$ za $i = 2+, 2-$.

Naš cilj u ovoj glavi je da procenimo brojeve $N(V_\mathbb{Z}^{(i)}; X)$. Videćemo da važi sledeća teorema, koju su dokazali Manjul Bhargava i Arul Shankar, [BS]:

Teorema 4.0.3. *Za svako $\epsilon > 0$, imamo da važe sledeće asimptotske formule, kada $X \to \infty$:*

$$N(V_{\mathbb{Z}}^{(0)}; X) = \frac{4}{135}\zeta(2)X^{5/6} + O(X^{3/4+\epsilon});$$

$$N(V_{\mathbb{Z}}^{(1)}; X) = \frac{32}{135}\zeta(2)X^{5/6} + O(X^{3/4+\epsilon});$$

$$N(V_{\mathbb{Z}}^{(2)}; X) = \frac{8}{135}\zeta(2)X^{5/6} + O(X^{3/4+\epsilon}).$$

4.1 Redukciona teorija

U ovom odeljku ćemo naći pogodan oblik fundamentalnog domena za dejstvo $\mathrm{GL}_2(\mathbb{Z})$ na $V_{\mathbb{R}}$.

U [C2], primedba 2, možemo videti da važi:

1. Skup binarnih kvartičnih formi sa fiksiranim invarijantama I i J se sastoji od samo jedne $\mathrm{SL}_2^{\pm}(\mathbb{R})$ orbite ako je $4I^3 - J^2 < 0$, koja se nalazi u $V_{\mathbb{R}}^{(1)}$.
2. Skup binarnih kvartičnih formi sa fiksiranim I i J se sastoji od tri $\mathrm{SL}_2^{\pm}(\mathbb{R})$ orbite ako je $4I^3 - J^2 > 0$, po jedna od ovih orbita se nalaze u $V_{\mathbb{R}}^{(0)}$, $V_{\mathbb{R}}^{(2+)}$ i $V_{\mathbb{R}}^{(2-)}$.

Pošto važi

$$I(g \cdot f) = (\det g)^4 I(f) \quad \text{i} \quad J(g \cdot f) = (\det g)^6 J(f),$$

to znači da su dve forme $f_1, f_2 \in V_{\mathbb{R}}^{(i)}$ $GL_2(\mathbb{R})$ ekvivalentne ako i samo ako postoji neka pozitivna konstanta $\lambda \in \mathbb{R}$ takva da važi

$$I(f_1) = \lambda^2 I(f_2) \quad \text{i} \quad J(f_1) = \lambda^3 J(f_2).$$

Za proizvoljan par $(I, J) \neq (0, 0)$, uvek postoji pozitivna konstanta $\lambda \in \mathbb{R}$ takva da važi

$$H(\lambda^2 I, \lambda^3 J) = \max\{\lambda^6 |I|^3, \lambda^6 J^2/4\} = 1$$

(za $|I|^3 \leq J^2/4$ uzimamo $\lambda = (J^2/4)^{1/6}$, a za $|I|^3 > J^2/4$ uzimamo $\lambda = |I|^{1/2}$). Uzimajući ove dve činjenice zaključujemo da se za $i = 0, 2+$ ili $2-$ (odnosno $i = 1$) može konstruisati *fundamentalan skup* $L^{(i)}$ za dejstvo $\mathrm{GL}_2(\mathbb{R})$ na $V_{\mathbb{R}}^{(i)}$ tako što se izabere jedno $f \in V_{\mathbb{R}}$ sa invarijantama I i J, za svako I i J za koje važi $H(I, J) = 1$ i $4I^3 - J^2 > 0$ (odnosno $4I^3 - J^2 \leq 0$).

Eksplictini oblik ovih skupova je sledeći:

$$L^{(0)} = \left\{ x^3 y - \frac{1}{3} x y^3 - \frac{J}{27} y^4 \in V_{\mathbb{R}}^{(0)} : -2 < J < 2 \right\}$$

$$L^{(1)} = \left\{ x^3 y - \frac{I}{3} x y^3 + \frac{\pm 2}{27} y^4 \in V_{\mathbb{R}}^{(1)} : -1 \leq I < 1 \right\} \bigcup \left\{ x^3 y + \frac{1}{3} x y^3 - \frac{J}{27} y^4 : -2 < J < 2 \right\}$$

$$L^{(2+)} = \left\{ \frac{1}{16} x^4 - \frac{\sqrt{2 - J}}{3\sqrt{3}} x^3 y + \frac{1}{2} x^2 y^2 + y^4 \in V_{\mathbb{R}}^{(2+)} : -2 < J < 2 \right\}$$

$$L^{(2-)} = \left\{ f \in V_{\mathbb{R}}^{(2-)} : -f \in L^{2+} \right\}$$

Primetimo nešto ovde: za svaku binarnu kvartičnu formu u nekom od ovih skupova važi da su joj koeficijenti ograničeni. Dakle, svi $L^{(i)}$ skupovi leže u nekom ograničenom podskupu od $V_{\mathbb{R}}$, odakle sledi da je za svako $h \in G_0 \subset \mathrm{GL}_2(\mathbb{R})$ (gde je G_0 neki kompaktan podskup) $h \cdot L^{(i)}$ takođe fundamentalan skup za dejstvo $\mathrm{GL}_2(\mathbb{R})$ na $V_{\mathbb{R}}$, i tada su svi koeficijenti formi koje pripadaju $h \cdot L^{(i)}$ ograničeni nezavisno od h.

Dokaz sledeće leme odlažemo do odeljka §4.5 (Uslovi kongruencije):

Lema 4.1.1. *Neka je $f \in V_{\mathbb{R}}^{(i)}$ element sa diskriminantom različitom od nule. Tada stabilizator od f u $\mathrm{GL}_2(\mathbb{R})$ ima 8 elemenata ako je $i = 0, 2$ i 4 ako je $i = 1$.*

Za $i = 0, 1, 2+, 2-$, označimo sa $2n_i$ kardinalnost stabilizatora u $\mathrm{GL}_2(\mathbb{R})$ ireducibilnog elementa $v \in V_{\mathbb{R}}^{(i)}$. Tada je po prethodnoj lemi $n_0 = 4 = n_{2+} = n_{2-}$, i $n_1 = 2$.

Za $h \in \mathrm{GL}_2(\mathbb{R})$, posmatrajmo multiskup $\mathcal{F}h \cdot L^{(i)}$ ($\mathcal{F}$ je fundamentalan domen za dejstvo $\mathrm{GL}_2(\mathbb{Z})$ na $\mathrm{GL}_2(\mathbb{R})$), gde je multiplicitet tačke $\mathbf{x} \in \mathcal{F}h \cdot L^{(i)}$ jednak kardinalnosti skupa $\{g \in \mathcal{F} : \mathbf{x} \in gh \cdot L^{(i)}\} \subseteq \mathcal{F}$. Interesuje nas sledeće: kolika je kardinalnost $m(\mathbf{x})$ klase elementa $\mathbf{x}$ pri dejstvu $\mathrm{GL}_2(\mathbb{Z})$ na $V_{\mathbb{R}}^{(i)}$ u skupu $\mathcal{F}h \cdot L^{(i)}$? Preciznije, tražimo multiplicitet tačke $\mathbf{x}' \in \mathcal{F}h \cdot L^{(i)}$, sumiran po svim $\mathbf{x}' \in V_{\mathbb{Z}}$ koji su $GL_2(\mathbb{Z})$ ekvivalentni sa $\mathbf{x}$.

Uočimo, za proizvoljno $\mathbf{x} \in V_{\mathbb{R}}^{(i)}$, postoji jedinstveno $\mathbf{x}_L \in h \cdot L^{(i)}$ koje je $\mathrm{GL}_2(\mathbb{Z})$ ekvivalentno sa $\mathbf{x}$ (neka je $g \cdot \mathbf{x}_L = \mathbf{x}$). Tada za element $g' \in \mathrm{GL}_2(\mathbb{R})$ važi da je $g' \cdot \mathbf{x}_L$ u istoj $\mathrm{GL}_2(\mathbb{Z})$ klasi kao i $\mathbf{x}$ ako i samo ako je $g' = \gamma g g_0$, za neke $\gamma \in \mathrm{GL}_2(\mathbb{Z})$ i $g_0 \in \mathrm{Stab}_{\mathrm{GL}_2(\mathbb{R})}(\mathbf{x}_L)$, tj. ako i samo ako g i g' predstavljaju isti element u prostoru duplih koseta

$$\mathrm{GL}_2(\mathbb{Z}) \setminus \mathrm{GL}_2(\mathbb{R}) / \mathrm{Stab}_{\mathrm{GL}_2(\mathbb{R})}(\mathbf{x}_L)$$

Broj ovih duplih koseta je

$$\frac{\#[g\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{R})}(\mathbf{x}_L)g^{-1}]}{\#[\mathrm{GL}_2(\mathbb{Z}) \cap g\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{R})}(\mathbf{x}_L)g^{-1}]} = \frac{\#\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{R})}(\mathbf{x})}{\#\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{Z})}(\mathbf{x})} =: m(\mathbf{x})$$

Pošto stabilizator u $\mathrm{GL}_2(\mathbb{Z})$ elementa $x \in V_{\mathbb{R}}$ uvek sadrži identičku matricu I i $-I$, to je $m(\mathbf{x})$ broj između 1 i n_i. Takođe, kako je za bilo koje $\gamma \in \mathrm{GL}_2(\mathbb{Z}) \setminus \{I, -I\}$ skup elemenata $\mathbf{x} \in V_{\mathbb{R}}$ koji su fiksirani sa γ mere nula, to iz prebrojivosti skupa $\mathrm{GL}_2(\mathbb{Z})$ sledi da je skup elemenata $\mathbf{x} \in V_{\mathbb{R}}^{(i)}$ za koje je $m(\mathbf{x}) < n_i$ takođe mere nula. Ovo znači da ako je $h \in \mathrm{GL}_2(\mathbb{Z})$ van ovog skupa mere nula, da je multiskup $\mathcal{F}h \cdot L^{(i)}$ unija n_i fundamentalnih domena za dejstvo $\mathrm{GL}_2(\mathbb{Z})$ na $V_{\mathbb{Z}}$.

Dakle, ako uvedemo oznaku

$$\mathcal{R}_X(h \cdot L^{(i)}) := \{w \in \mathcal{F}h \cdot L^{(i)} : |H(w)| < X\},$$

onda važi da je $n_i N(V_{\mathbb{Z}}^{(i)}; X)$ jednako broju ireducibilnih tačaka u $\mathcal{R}_X(h \cdot L^{(i)})$, gde se tačke sa $\mathrm{GL}_2(\mathbb{Z})$ stabilizatorima kardinalnosti $2r$ računaju težinom $1/r$.

4.2 Procene reducibilnosti

U ovom odeljku razmatramo šta se dešava sa reducibilnim, integralnim elementima multiskupa $\mathcal{R}_X(h \cdot L^{(i)})$, gde je $h \in G_0$ proizvoljan element u nekom kompaktnom skupu $G_0 \subset \mathrm{GL}_2(\mathbb{R})$. Ako za binarnu kvartičnu formu $ax^4+bx^3y+cx^2y^2+dxy^3+ey^4$ važi da je $a = 0$, onda ona ima faktor y, pa je reducibilna nad $\mathbb{Q}$. Šta se dešava za $a \neq 0$?

Lema 4.2.1. *Neka je $G_0 \subset \mathrm{GL}_2(\mathbb{R})$ proizvoljan kompaktan podskup, i neka je $h \in G_0$ proizvoljno. Tada je broj reducibilnih nad $\mathbb{Q}$, integralnih binarnih kvartičnih formi $ax^4 + bx^3y + cx^2y^2dxy^3 + ey^4$ sa $a \neq 0$ jednak $O(X^{2/3+\epsilon})$, gde konstanta zavisi samo od G_0 i ϵ.*

Dokaz: Neka je

$$f(x, y) = ax^4 + bx^3y + cx^2y^2dxy^3 + ey^4 \in \mathcal{R}_X(h \cdot L^{(i)})$$

proizvoljno. Pošto je

$$\mathcal{R}_X(h \cdot L^{(i)}) \subset N'A'K\Lambda h \cdot L^{(i)},$$

gde je $h \cdot L^{(i)}$ podskup nekog kompaktnog skupa, i $0 < \lambda < X^{1/24}$. No, svi koeficijenti proizvoljnog elementa $K\Lambda h \cdot L^{(i)}$ su ograničeni sa $O((X^{1/24})^4) = O(X^{1/6})$, pa imamo da u $N'A'K\Lambda h \cdot L^{(i)}$ važi da je $a = O(X^{1/6}), b = O(X^{1/6}), c = O(X^{1/6}), ad = O(X^{2/6}), bd = O(X^{2/6}), ae = O(X^{2/6})$. Ovo znači da je broj elemenata u $\mathcal{R}_X(h \cdot L^{(i)})$ sa $a \neq 0$ i $e = 0$ jednak $O(X^{4/6+\epsilon})$.

Neka je sada $a \neq 0$ i $e \neq 0$. Prvo ćemo proceniti broj formi sa linearnim faktorom. Ako je $px + qy$ linearan faktor od $f(x, y)$ ($p, q \in \mathbb{Z}$ su uzajamno prosti), onda p deli a, a q deli e, pa postoji $O(X^{\epsilon})$ mogućnosti i za p i za q. Kada fiksiramo p i q, i izračunamo $f(-q, p) = 0$, onda dobijamo vrednost c iz jednakosti (dakle, fiksiranjem p i q mi fiksiramo i c). Prema tome, broj formi $f \in \mathcal{R}_X(h \cdot L^{(i)})$ sa racionalnim linearnim faktorom i $a \neq 0$ je $O(X^{4/6+\epsilon})$.

Posmatrajmo sada broj binarnih kvartičnih formi koje se faktorišu na dve ireducibilne kvadratne forme nad $\mathbb{Z}$:

$$ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4 = (px^2 + qxy + ry^2)(p_1x^2 + sxy + r_1y^2),$$

gde su $p, q, r, s, p_1, r_1 \in \mathbb{Z}$ i p, q, r su uzajamno prosti. Pošto je $ae = O(X^{2/6})$ i $a, e \neq 0$, broj mogućnosti za par (a, e) je $O(X^{2/6+\epsilon})$. Dalje, ako ubacimo $x = 0$ i $y = 0$, videćemo da p deli a i r deli e (dakle, $p_1 = \frac{a}{p}$ i $r_1 = \frac{e}{r}$), redom, pa ako fiksiramo a i e, broj mogućnosti za (p, r) je ograničen sa $O(X^{\epsilon})$. Izjednačimo koeficijente:

$$\frac{a}{p}q + ps = b, \quad \frac{e}{r}q + rs = d. \tag{4.2}$$

Imamo dva slučaja:

1. $\frac{ar}{pe} \neq \frac{p}{r}$ - tada je linearan sistem jednačina (4.2) sa promenljivama q i s nesingularan. Dakle, vrednosti b i d jedinstveno određuju q i s, pa je ukupan broj osmorki (a, b, d, e, p, r, q, s) jednak $O(X^{4/6+\epsilon})$, a c je određeno ostalim koeficijentima, pa je boj mogućnosti za (a, b, c, d, e) $O(X^{4/6+\epsilon})$.

2. $\frac{ar}{pe} = \frac{p}{r}$ - tada je sistem (4.2) singularan. Koeficijent b jedinstveno određuje koeficijent $d = br/p$. Pošto za četvorku (a, e, p, r) postoji $O(X^{2/6+\epsilon})$, za (b, c) $O(X^{2/6})$, i d je određeno sa b, to je broj mogućnosti za (a, b, c, d, e) opet $O(X^{4/6+\epsilon})$. $\square$

4.3 Usrednjavanje

U ovom odeljku ćemo, na sličan način kao sa binarnim kubičnim formama, izraziti broj tačaka u fundamentalnim domenima (koje smo izrazili u odeljku §4.1) preko zapremina ovih domena.

Neka je G_0 kompaktan, algebarski, levo K-invarijantni skup u $\mathrm{GL}_2(\mathbb{R})$, zatvorenje nepraznog otvorenog skupa, i neka svaki element u G_0 ima determinantu ≥ 1. Tada za $i = 0, 1, 2+, 2-$ važi

$$N(V_{\mathbb{Z}}^{(i)}; X) = \frac{\displaystyle\int_{h\in G_0} \#\{\mathbf{x} \in \mathcal{F}h \cdot L \cap V_{\mathbb{Z}}^{\mathrm{irr}} : H(\mathbf{x}) < X\} dh}{\displaystyle n_i \int_{h\in G_0} dh}, \tag{4.3}$$

gde su: $V_{\mathbb{Z}}^{irr}$ skup ireducibilnih elemenata u $V_{\mathbb{Z}}$, $L = L^{(i)}$ i dh Haar-ova mera na $\mathrm{GL}_2(\mathbb{R})$. Uzimajući u obzir prirodu Haarove mere, delilac na desnoj strani (4.3) je jednak nekoj konstanti $C_{G_0}^{(i)} > 1$.

Možemo proširiti definiciju funkcije N: ako je $S \subset V_{\mathbb{Z}}^{(i)}$ proizvoljan $\mathrm{GL}_2(\mathbb{Z})$ invarijantan skup, onda uzimamo da je $N(S; X)$ broj ireducibilnih $\mathrm{GL}_2(\mathbb{Z})$ orbita u S sa visinom manjom od X. Ako sa S^{irr} obeležimo skup ireducibilnih tačaka S, onda važi

$$N(S; X) = \frac{\displaystyle\int_{h\in G_0} \#\{\mathbf{x} \in \mathcal{F}h \cdot L \cap S^{\mathrm{irr}} : H(\mathbf{x}) < X\} dh}{C_{G_0}^{(i)}}.$$

Ovako možemo definisati $N(S; X)$ čak i kada S nije $\mathrm{GL}_2(\mathbb{Z})$ invarijantno.

Sada ćemo $N(S; X)$ izraziti u pogodnom obliku, na koga ćemo primeniti Davenportovu teoremu:

Teorema 4.3.1. *Ako je $S \subset V_{\mathbb{Z}}^{(i)}$ proizvoljno, onda važi:*

$$N(S; X) = \frac{1}{C_{G_0}^{(i)}} \int_{g\in N'(t)A'\Lambda} \#\left\{\mathbf{x} \in S^{\mathrm{irr}} \cap B(n, t, \lambda, X)\right\} t^{-2} dn d^{\times}t d^{\times}\lambda, \tag{4.4}$$

gde su $C_{G_0}^{(i)} = n_i \int_{h \in G_0} dh$ *i*

$$B(n,t,\lambda,X) := n \begin{bmatrix} t^{-1} & 0 \\ 0 & t \end{bmatrix} \lambda G_0 \cdot L \cap \left\{ \mathbf{x} \in V_{\mathbb{R}}^{(i)} : H(\mathbf{x}) < X \right\}.$$

Dokaz: Neka je sada $\mathbf{x} \in V_{\mathbb{R}}^{(i)}$. Tada postoji jedinstveno $\mathbf{x}_L \in L$ koje je $\mathrm{GL}_2(\mathbb{R})$ ekvivalentno sa $\mathbf{x}$, pa važi

$$\frac{1}{C_{G_0}^{(i)}} \sum_{\substack{\mathbf{x} \in S^{\mathrm{irr}} \\ H(\mathbf{x}) < X}} \int_{h \in G_0} \#\{g \in \mathcal{F} : \mathbf{x} = gh \cdot \mathbf{x}_L\} dh.$$

Za dato $\mathbf{x} \in S^{\mathrm{irr}}$ postoji konačno mnogo elemenata $g_1, ...g_n \in \mathrm{GL}_2(\mathbb{R})$ takvih da je $g_j \cdot \mathbf{x}_L = \mathbf{x}$. Tada je:

$$\int_{h \in G_0} \#\{g \in \mathcal{F} : \mathbf{x} = gh \cdot \mathbf{x}_L\} dh = \sum_j \int_{h \in G_0} \#\{g \in \mathcal{F} : gh = g_j\} dh = \sum_j \int_{h \in G_0 \cap \mathcal{F}^{-1} g_j} dh.$$

No, dh je invarijantna mera na G, pa je

$$\sum_j \int_{h \in G_0 \cap \mathcal{F}^{-1} g_j} dh = \sum_j \int_{g \in G_0 g_j^{-1} \cap \mathcal{F}^{-1}} dg = \sum_j \int_{g \in \mathcal{F}} \#\{h \in G_0 : gh = g_j\} dg =$$

$$= \int_{g \in \mathcal{F}} \#\{h \in G_0 : x = gh \cdot \mathbf{x}_L\}.$$

Prema tome, važi:

$$N(S;X) = \frac{1}{C_{G_0}^{(i)}} \sum_{\substack{\mathbf{x} \in S^{\mathrm{irr}} \\ H(\mathbf{x}) < X}} \int_{g \in \mathcal{F}} \#\{h \in G_0 : \mathbf{x} = gh \cdot \mathbf{x}_L\} dg =$$

$$= \frac{1}{C_{G_0}^{(i)}} \int_{g\in\mathcal{F}} \#\{\mathbf{x} \in S^{\text{irr}} \cap gG_0 \cdot L : H(\mathbf{x}) < X\} =$$

$$= \frac{1}{C_{G_0}^{(i)}} \int_{g\in N'(t)A'\Lambda K} \#\left\{\mathbf{x} \in S^{\text{irr}} \cap n \begin{bmatrix} t^{-1} & 0 \\ 0 & t \end{bmatrix} \lambda k G_0 \cdot L : H(\mathbf{x}) < X\right\} t^{-2} dn d^{\times}t d\times \lambda dk.$$

Pošto je $KG_0 = G_0$ i $\int_K dk = 1$, to teorema važi. □

Po konstrukciji $L^{(i)}$, koeficijenti binarnih kvartičnih formi u $G_0 \cdot L$ su svi ograničeni sa nekom konstantom. Neka je C takvo da je C^4 granica apsolutnih vrednosti svih koeficijenata svih formi u $G_0 \cdot L$. Tada:

Tvrđenje 4.3.2. *Broj celobrojnih tačaka* $(a, b, c, d, e) \in B(n, t, \lambda, X)$ *sa* $a \neq 0$ *je*

$$\begin{cases} 0 & za\ C\lambda < t; \\ \text{Vol}(B(n, t, \lambda, X)) + O\left(t^4\lambda^{16}\right) & inače \end{cases}$$

Dokaz: Ako je

$$a^4 + bx^3 + cx^2y^2 + dxy^3 + ey^4 \in B(n, t\lambda, X),$$

tada su $|a|, |b|, |c|, |d|, |e|$ ograničeni sa $C^4\lambda^4/t^4, C^4\lambda^4/t^2, C^4\lambda^4, C^4\lambda^4t^2, C^4\lambda^4t^4$, redom. Ako je $C\lambda < 1$, tada mora da bude $a = 0$ (jer je $|a| < C^4\lambda^4/t^4 < 1$).

Posmatrajmo slučaj kada je $C\lambda/t \geq 1$. Odavde sledi da je λ, kao i t, ograničeno odozdo sa pozitivnom konstantom. Tada su i

$$C^4\lambda^4/t^4, C^4\lambda^4/t^2, C^4\lambda^4, C^4\lambda^4t^2, C^4\lambda^4t^4$$

ograničeni odozdo, gde je $C^4\lambda^4/t^4$ (gornja granica za $|a|$) najmanje od svih. Tada je zapremina k dimenzione projekcije $B(n, t, \lambda, X)$ na potprostor dobijene izjednačavanjem k koeficijenata sa nulom ($1 \leq k \leq 4$) ograničena sa

$$O(\lambda^4/t^2 \cdot \lambda^4 \cdot \lambda^4 t^2 \cdot \lambda^4 t^4) = O(t^4 \lambda^{16}).$$

Rezultat sledi iz Davenportove teoreme 1.6.7. □

Pošto L i $G_0 \cdot L$ sadrže samo tačke sa visinom barem 1 tada će integrand u (4.4) biti različit od nule samo ako je $t \leq C\lambda$ i $\lambda < X^{1/24}$. Dakle,

$$N(V_{\mathbb{Z}}^{(i)}; X) = \frac{1}{C_{G_0}^{(i)}} \int_{\lambda = \sqrt[4]{3}/(\sqrt{2}C)}^{X1/24} \int_{t=\sqrt[4]{3}/\sqrt{2}}^{C\lambda} \int_{N'(t)} (\mathrm{Vol}(B(n,t,\lambda,X)) + \tag{4.5}$$

$$+O(t^4\lambda^{16}))t^{-2} dn d^\times t d^\times \lambda + O(X^{3/4+\epsilon}),$$

gde $O(X^{3/4+\epsilon})$ dolazi iz ograničenosti broja reducibilnih formi i ograničenosti broja formi sa netrivijalnim $\mathrm{GL}_2(\mathbb{Z})$ stabilizatorom. Integral drugog sabirka je $O(X^{3/4+\epsilon})$. Integral prvog sabirka je:

$$\frac{1}{C_{G_0}^{(i)}} \int_{h \in G_0} \mathrm{Vol}(\mathcal{R}_X(h \cdot L)) dh - \int_{\lambda = \sqrt[4]{3}/(\sqrt{2}C)}^{X^{1/24}} \int_{t=C\lambda}^{\infty} \int_{N'(t)} \mathrm{Vol}(B(n,t,\lambda,X)) t^{-2} dn d^\times t d^\times \lambda. \tag{4.6}$$

No, $\mathrm{Vol}(\mathcal{R}_X(h \cdot L))$ ne zavisi od h. Kako je

$$B(n,t,\lambda,C,X) = O(\lambda^{20}),$$

vidimo da je drugi sabirak u gornjem izrazu jednak $O(X^{3/4})$. Vidimo da kada je $t > C\lambda$ da je zapremina kuspidalnog regiona mala. Dakle, važi:

$$N(V_{\mathbb{Z}}^{(i)}; X) = \mathrm{Vol}(\mathcal{R}_X(L))/n_i + O(X^{3/4+\epsilon}). \tag{4.7}$$

4.4 Proračun zapremine

Naš cilj u ovom odeljku je da izračunamo zapreminu

$$\mathcal{R}_X(L^{(i)}) = \{w \in \mathcal{F}h \cdot L^{(i)} : |H(w)| < X\}.$$

Definicija 4.4.1. *Uvodimo oznake:*

$$R^{(i)} := \Lambda \cdot L^{(i)}.$$

gde su $\Lambda = \left\{ \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix} \mid \lambda > 0 \right\}$*, i* $L^{(i)}$ *fundamentalan domen za dejstvo* $\mathrm{GL}_2(\mathbb{R})$ *na* $V_{\mathbb{R}}$*. Označimo sa* $R^{(i)}(X)$ *skup svih elemenata u* $R^{(i)}$ *sa visinom manjom od* X*.*

Ako za $(I, J) \in \mathbb{R} \times \mathbb{R}$ važi da je $\Delta(I, J) > 0$, onda svaki od skupova $R^{(0)}, R^{(2+)}$ i $R^{(2-)}$ sadrži po tačno jednu tačku sa invarijantama I i J; ako je $\Delta(I, J) < 0$, onda $R^{(1)}$ sadrži tačno jednu tačku sa invarijantama I i J. Posmatrajmo sledeće dejstvo $\mathrm{GL}_2(\mathbb{R})$ na $V_{\mathbb{R}}$:

$$\gamma \cdot f(x, y) := f((x, y) \cdot \gamma)/(\det \gamma)^2,$$

gde je $\gamma \in \mathrm{GL}_2(\mathbb{R})$ i $f \in V_{\mathbb{R}}$. Ovime je indukovano dejstvo $\mathrm{PGL}_2(\mathbb{R})$ na $V_{\mathbb{R}}$, gde je $\mathrm{PGL}_2(\mathbb{R}) = \mathrm{GL}_2(\mathbb{R})/S$ i

$$S = \{\mathrm{diag}(\lambda) | \lambda \in \mathbb{R} \setminus \{0\}\}.$$

Definicija 4.4.2. *Sa* $\mathcal{F}_{\mathrm{PGL}_2}$ *označavamo sliku fundamentalnog domena* $\mathcal{F}$ *za dejstvo* $\mathrm{GL}_2(\mathbb{Z})$ *na* $\mathrm{GL}_2(\mathbb{R})$ *u* $\mathrm{PGL}_2(\mathbb{R})$*.*

Uočimo, $\mathcal{F}_{\mathrm{PGL}_2}$ je fundamentalni domen za dejstvo $\mathrm{PGL}_2(\mathbb{Z})$ na $\mathrm{PGL}_2(\mathbb{R})$ (dejstvuje tako što množi sa leve strane). Dalje, imamo da je $\mathcal{R}_X(L^{(i)}) = \mathcal{F}_{\mathrm{PGL}_2} \cdot R^{(i)}(X)$.

Znamo da ako je:

1. $i = 0, 2+, 2-$, da onda postoji bijekcija između $R^{(i)}$ i $\{(I, J) \in \mathbb{R} \times \mathbb{R} : I^3 - J^2/4 > 0\}$;

2. $i = 1$, da onda postoji bijekcija $R^{(i)}$ sa $\{(I, J) \in \mathbb{R} \times \mathbb{R} : I^3 - J^2/4 < 0\}$.

Prema tome, na svakome od $R^{(i)}$ postoji mera, definisana sa $dr = dIdJ$. Ako je ω diferencijal koji generiše modul diferencijala PGL_2 nad $\mathbb{Z}$ ranka 1, onda je ω dobro definisano do na znak. U cilju racunanja zapremine multiskupa $\mathcal{R}_X(L^{(i)}) = \mathcal{F}_{\mathrm{PGL}_2} \cdot R^{(i)}(X)$, koristićemo sledeće tvrđenje, čiji dokaz ćemo izvesti u sledećoj glavi:

Tvrđenje 4.4.3. *Za bilo koju merljivu fukciju ϕ na $V_{\mathbb{R}}$ važi:*

$$\int_{\mathcal{F}_{\mathrm{PGL}_2} \cdot R^{(i)}} \phi(v)dv = \frac{1}{27} \int_{R^{(i)}} \int_{\mathrm{PGL}_2(\mathbb{R})} \phi\left(g \cdot p^{(i)}_{I,J}\right) \omega(g) dIdJ,$$

gde je $p^{(i)}_{I,J} \in R^{(i)}$ tačka sa invarijantama I i J, i $\mathcal{F}_{\mathrm{PGL}_2} \cdot R^{(i)}$ je multiskup.

Sada možemo upotrebiti tvrđenje 4.4.3:

Dokaz teoreme 4.0.3:

$$\int_{\mathcal{R}_X(L^{(i)})} dv = \int_{\mathcal{F}_{\mathrm{PGL}_2} \cdot R^{(i)}(X)} dv = \frac{1}{27} \int_{R^{(i)}(X)} \int_{\mathcal{F}_{\mathrm{PGL}_2}} dg dI dJ = \frac{2\zeta(2)}{27} \int_{R^{(i)}(X)} dI dJ,$$

a ovde smo upotrebili da je

$$\mathrm{Vol}(\mathcal{F}_{\mathrm{PGL}_2}) = \mathrm{Vol}(\mathrm{PGL}_2(\mathbb{Z}) \setminus \mathrm{PGL}_2(\mathbb{R})) = 2\zeta(2).$$

Za $i = 0, 2+, 2-$ imamo:

$$\int_{R^{(i)}(X)} dIdJ = \int_{I=0}^{X^{1/3}} \int_{J=-2I^{3/2}}^{2I^{3/2}} dJdI = \frac{8}{5} X^{5/6}.$$

S druge strane, imamo:

$$\int_{R^{(1)}(X)} dIdJ = \int_{I=0}^{X^{1/3}} \int_{J=-2I^{3/2}}^{2I^{3/2}} dJdI - \mathrm{Vol}\left(R^{(0)}(X)\right) = 8X^{5/6} - \frac{8}{5}X^{5/6} = \frac{32}{5}X^{5/6}.$$

Zaključujemo da važi:

$$\mathrm{Vol}(\mathcal{R}_X(L^{(i)})) = \begin{cases} \frac{16}{135} \cdot \zeta(2)X^{5/6} & \text{za } i = 0, 2+, 2-; \\ \frac{64}{135} \cdot \zeta(2)X^{5/6} & \text{za } i = 1. \end{cases} \tag{4.8}$$

Iz (4.7) i (4.8) sledi teorema 4.0.3, pošto znamo da je $n_0 = n_{2+} = n_{2-} = 4$ i $n_1 = 2$. □

4.5 Uslovi kongruencije

Naš cilj u ovom i sledećem oedljku je da dokažemo neke pomoćne leme koje su nam neophodne za rezultate o rangu eliptičkih krivih u familijama.

Prvo ćemo navesti par definicija:

Definicija 4.5.1. *Sa $W_{\mathbb{Z}}$ obeležavamo prostor parova ternarnih kvadratnih formi sa koeficijentima u $\mathbb{Z}$. Pošto možemo posmatrati ove forme kao matrice sa koeficijentima u $\frac{1}{2}\mathbb{Z}$, to se svaki element $(A, B) \in W_{\mathbb{Z}}$ može videti kao par simetričnih matrica:*

$$2 \cdot (A, B) = \left(\begin{bmatrix} 2a_{11} & a_{12} & a_{13} \\ a_{12} & 2a_{22} & a_{23} \\ a_{13} & a_{23} & 2a_{33} \end{bmatrix}, \begin{bmatrix} 2b_{11} & b_{12} & b_{13} \\ b_{12} & 2b_{22} & b_{23} \\ b_{13} & b_{23} & 2b_{33} \end{bmatrix} \right),$$

gde su $a_{i,j}, b_{i,j} \in \mathbb{Z}$.

Definicija 4.5.2. *Za binarnu kubičnu formu $g(x,y)$ kažemo da je monična binarna kubična forma ako je koeficijent uz x^3 jednak 1, tj. ako je g oblika*

$$x^3 + rx^2y + sxy^2 + ty^3.$$

Skup svih binarnih kubičnih formi nad $\mathbb{Z}$ ćemo nadalje obeležavati sa $U_{\mathbb{Z}}$, a podskup moničnih binarnih kubičnih formi sa $U_{\mathbb{Z},1}$.

Uočimo da postoji utapanje prostora binarnih kvartičnih formi u prostor $W_{\mathbb{Z}}$:

$$\phi : ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4 \mapsto \left(\begin{bmatrix} 0 & 0 & 1/2 \\ 0 & -1 & 0 \\ 1/2 & 0 & 0 \end{bmatrix}, \begin{bmatrix} a & b/2 & 0 \\ b/2 & c & d/2 \\ 0 & d/2 & e \end{bmatrix} \right). \tag{4.9}$$

Definicija 4.5.3. *Sa $W_{\mathbb{Z},1}$ obeležavamo sliku gornjeg utapanja. Za svako $f \in V_{\mathbb{Z}}$, prva matrica u $\phi(f)$ je jednaka $\begin{bmatrix} 0 & 0 & 1/2 \\ 0 & -1 & 0 \\ 1/2 & 0 & 0 \end{bmatrix}$, i ovu matricu ćemo obeležavati sa A_1.*

Definicija 4.5.4. *Sa $F_{\mathbb{Z},1}$ (tj. sa $F_{\mathbb{Q},1}$) obeležavamo grupu 2×2 donje trougaonih matrica nad $\mathbb{Z}$ (tj. nad $\mathbb{Q}$) sa jedinicama na dijagonali.*

Definicija 4.5.5. *Za svako $f \in V_{\mathbb{Z}}$ definišemo moničnu kubičnu rezolventnu formu $g(x,y) = 4\mathrm{Det}(A_1x - B_fy)$, gde je $\phi(f) = (A_1, B_f)$.*

Primetimo sledeće: ako je $(A,B) \in W_{\mathbb{Z}}$ (odnosno $W_{\mathbb{Z},1}$), tada je $4\mathrm{Det}(Ax - By) \in O_{\mathbb{Z}}$ (odnosno $U_{\mathbb{Z}}, 1$). Grupa $F_{\mathbb{Z},1}$ deluje na $U_{\mathbb{Z},1}$ na već poznat način: $\gamma \cdot g(x,y) = g((x,y) \cdot \gamma)$.

Definicija 4.5.6. *Za* $g(x,y) = x^3 + rx^2y + sxy^2 + ty^3 \in U_{\mathbb{Z},1}$*, definišemo:*

$$I(g) := r^2 - 3s,$$

$$J(g) := -2r^3 + 9rs - 27t.$$

Uočimo da su ove funkcije I i J invarijentne u odnosu na dejstvo $F_{\mathbb{Z},1}$ na argument. Takođe, diskriminanta $\Delta(g)$ binarne kubične forme g se može izraziti preko $I(g)$ i $J(g)$:

$$\Delta(g) = (4I(g)^3 - J(g)^2)/27.$$

Definicija 4.5.7. *Visina binarne kubične forme* g *je*

$$H(g) := H(I,J) = \max\left\{\left|I(g)^3\right|, J(g)^2/4\right\}.$$

Za svaku binarnu kubičnu formu g postoji neka $F_{\mathbb{Q},1}$ transformacija γ takva da $\gamma \cdot g$ ima nula koeficijent uz x^2y, zbog čega je svaka binarna kubična forma $F_{\mathbb{Q},1}$ ekvivalentna sa moničnom binarnom kubičnom formom

$$h(x,y) = x^3 - \frac{I(g)}{3}xy^2 - \frac{J(g)}{27}y^3.$$

Neka je sada $f \in V_{\mathbb{Z}}$ proizvoljno, i g monična kubična rezolventa od f. Tada se može videti da je $I(f) = I(g)$ i $J(f) = J(g)$. Eliptička kriva

$$E_f : z^2 = g(x,1),$$

koju ćemo takođe zapisivati i sa

$$z^2 = x^3 - \frac{I(f)}{3}x - \frac{J(f)}{27},$$

je Jakobijan genusa 1 krive C_f u projektivnom prostoru sa težinom $\mathbb{P}(1,1,2)$ određenom jednačinom $z^2 = f(x,y)$. Iz teoreme 5.3.2 znamo da je stabilizator forme f u $\mathrm{PGL}_2(\mathbb{Q})$ izomorfan sa $E_f(\mathbb{Q})[2]$.

Neka je R proizvoljan prsten, i neka je V_R prostor binarnih kvartičnih formi sa koeficijentima u R. Tada možemo definisati dejstvo $\mathrm{GL}_2(R)$ na V_R:

Definicija 4.5.8. *Za $\gamma \in \mathrm{GL}_2(R)$ i $f \in V_R$:*

$$\gamma \cdot f(x,y) := (\det \gamma)^{-2} f((x,y)\cdot\gamma).$$

Uočimo, centar od $\mathrm{GL}_2(R)$ deluje trivijalno na V_R pri ovom dejstvu. Dakle, imamo dejstvo $\mathrm{PGL}_2(R)$ na V_R.

Dokazaćemo sledeću lemu:

Lema 4.5.9. *Neka je $f \in V_{\mathbb{R}}^{(i)}$ (iz definicije 4.0.2) sa nenula diskriminantom. Tada je red stabilizatora f u $\mathrm{GL}_2(\mathbb{R})$ jednak 8, za $i \in \{0,2\}$, ili 2, za $i = 1$.*

Dokaz: Posmarajmo dejstvo $\mathrm{PGL}_2(\mathbb{R})$ na $V_{\mathbb{R}}$, definisano u definiciji 4.5.8. Teorema 5.3.2 nam kaže da je za proizvoljno $f \in V_{\mathbb{R}}$ sa nenula diskriminantom

$$\mathrm{Stab}_{\mathrm{PGL}_2(\mathbb{R})}(f) \cong E(\mathbb{R})[2],$$

pri čemu je E eliptička kriva data sa

$$y^2 = x^3 - \frac{I(f)}{3}x - \frac{J(f)}{27}.$$

Drugim rečima, važi

$$\#\mathrm{Stab}_{\mathrm{PGL}_2(\mathbb{R})}(f) = \begin{cases} 2 & \Delta(f) < 0 \\ 4 & \Delta(f) > 0 \end{cases}.$$

Neka sada $\gamma \in \mathrm{GL}_2(\mathbb{R})$ stabilizuje f pri uobičajenom dejstvu. Pošto je

$$I(\gamma \cdot f) = (\det \gamma)^4 I(f) \quad \text{i} \quad J(\gamma \cdot f) = (\det \gamma)^6 J(f),$$

to je $\det \gamma = \pm 1$, pa će i slika od γ u $\mathrm{PGL}_2(\mathbb{R})$ takođe da stabilizuje f. Pošto u centru od $\mathrm{GL}_2(\mathbb{R})$ postoje 2 elementa koja stabilizuju f, to će veličina stabilizatora u $\mathrm{GL}_2(\mathbb{R})$ nekog elementa $f \in V_{\mathbb{R}}^{(i)}$ biti 4 za $i = 1$ (tj. za $\Delta(f) < 0$), i 8 za $i \in \{0, 2\}$ (tj. za $\Delta(f) > 0$). $\square$

Lema 4.5.10. *Asimptotski broj $F_{\mathbb{Z},1}$ orbita moničnih celobrojnih binarnih kubičnih formi g koje su reducibilne nad $\mathbb{Q}$ i za koje je $H(g) < X$ je $O(X^{1/2+\epsilon})$.*

Dokaz: Neka je

$$g(x, y) = x^3 + rx^2y + sxy^2 + ty^3 \in U_{\mathbb{Z},1}.$$

Tada možemo smatrati da je $r \in \{-1, 0, 1\}$, pošto umesto g možemo smatrati sa nekim njegovim $F_{\mathbb{Z},1}$ translatom kod koga koeficijent uz x^2y pripada skupu $\{-1, 0, 1\}$. Dakle, za svaki element iz $U_{\mathbb{Z},1}$ smatramo da je ovo tačno. Ako je $H(g) < X$, iz činjenice da je

$$|I(g)|^3 = \left|r^2 - 3s\right|^3 \leq H(g) < X$$

sledi da je $s = O(X^{1/3}$, a iz $J(g)^2/4 = (2r^3 + 9rs - 27t)^2/4 \leq H(g) < X$ sledi da je $t = O(X^{1/2})$. Sada ćemo posmatrati broj formi g koje su reducibilne:

1. Neka je $g(x, y) = x^3 + rx^2y + sxy^2 + ty^3$, $t = 0$ (i $r \in \{-1, 0, 1\}$). Tada je g reducibilno, i broj ovakvih g sa $H(g) < X$ je jednak broju mogućih vrednosti koje r i s mogu da uzmu, a to je

$$3 \cdot O(X^{1/3}) = O(X^{1/3}).$$

2. Neka je sada $t \neq 0$, $H(g) < X$ i $r \in \{-1, 0, 1\}$. Ako je $x - my$ faktor od g, onda $m \mid t$, pa ako fiskiramo $t \neq 0$, onda imamo najviše $t^\epsilon = O(X^\epsilon)$ mogućnosti za izbor m. Fiksiramo li r, t i m, pošto je $g(m, 1) = 0$ ($x - my$ je faktor od g), to je s jedinstveno za ovu trojku (r, t, m). Dakle, iz $t = O(X^{1/2})$ sledi da je broj reducibilnih formi g sa $H(g) < X$ asimptotski jednak $O(X^{1/2+\epsilon})$. □

Pre nego što navedemo sledeću lemu, Uvešćemo par pojmova:

Definicija 4.5.11. *Grupa* $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})$ *deluje na* $W_\mathbb{Z}$ *na sledeći način: Za* $g_3 \in \mathrm{SL}_3(\mathbb{Z})$,

$$g_3 \cdot (A, B) := \left(g_3 A g_3^T, g_3 B g_3^T\right),$$

a za $g_2 = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \in \mathrm{GL}_2(\mathbb{Z})$,

$$g_2 \cdot (A, B) := (pA + qB, rA + sB).$$

Prsten polinomijalnih invarijanti dejstva $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})$ na $W_\mathbb{Z}$ je generisan jednim elementom: diskriminantom. Za neki element $(A, B) \in W_\mathbb{Z}$, diskriminanta $\Delta(A, B)$ je data diskriminantom binarne kubne forme $4 \det(Ax - By)$, i prema tome je invarijanta stepena 12 u koeficijentima od A i B.

Teorema 4.5.12. *Preslikavanje* ϕ *dato sa (4.9) daje kanonsku bijekciju između* $\mathrm{PGL}_2(\mathbb{Z})$ *orbita na* $V_\mathbb{Z}$ *i* $F_{\mathbb{Z},1} \times SO(A_1, \mathbb{Z})$ *orbita na* $W_{\mathbb{Z},1}$.

Dokaz: Uočimo sledeće: svaka $F_{\mathbb{Z},1}$ klasa ekvivalencije u $W_{\mathbb{Z},1}$ sadrži jedinstveni element (A_1, B) takav da je gornji desni koeficijent u B jednak nuli. Odavde sledi da je ϕ bijekcija između $V_\mathbb{Z}$ i skupa $F_{\mathbb{Z},1}$ orbiti na $W_{\mathbb{Z},1}$:

$$V_\mathbb{Z} \to W_{\mathbb{Z},1} \to F_{\mathbb{Z},1} \setminus W_{\mathbb{Z},1}.$$

Primetimo, centar od $\mathrm{GL}_2(\mathbb{Z})$ deluje trivijalno na svoju reprezentaciju na binarnim kvadratnim formama

$$px^2 - 2qxy + ry^2,$$

gde je dejstvo definisano sa

$$\gamma \cdot f(x,y) := f((x,y)\cdot\gamma)/(\det\gamma).$$

Ovo dejstvo grupe $\mathrm{GL}_2(\mathbb{Z})$ čuva diskriminantu $4(q^2-pr)$. Zato imamo preslikavanje $\rho : \mathrm{PGL}_2(\mathbb{Z}) \to \mathrm{SL}_3(\mathbb{Z})$, dato sa

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \frac{1}{ad-bc} \begin{bmatrix} d^2 & cd & c^2 \\ 2bd & ad+bc & 2ac \\ b^2 & ab & a^2 \end{bmatrix}.$$

Pošto je A_1 Gramova matrica ternarne forme q^2-pr, to je slika $\rho(\mathrm{PGL}_2(\mathbb{Z}))$ sadržana u ortogonalnoj grupi $\mathrm{SO}(A_1,\mathbb{Z})$.

Može se lako proveriti da za sve $\gamma \in \mathrm{PGL}_2(\mathbb{Z})$ i $f \in V_{\mathbb{Z}}$ važi da $\phi(\gamma\cdot f)$ i $\rho(\gamma)\cdot\phi(f)$ daju isti element u $F_{\mathbb{Z},1} \setminus W_{\mathbb{Z},1}$, što nam daje teoremu. □

Iz teoreme sledi da imamo preslikavanje

$$\psi : \mathrm{PGL}_2(\mathbb{Z}) \setminus V_{\mathbb{Z}} \to (\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})) \setminus W_{\mathbb{Z}} \tag{4.10}$$

koje je dato sa

$$\mathrm{PGL}_2(\mathbb{Z}) \setminus V_{\mathbb{Z}} \to (F_{\mathbb{Z},1} \times \mathrm{SO}(A_1,\mathbb{Z})) \setminus W_{\mathbb{Z},1} \to (\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})) \setminus W_{\mathbb{Z}}.$$

Tvrđenje 4.5.13. *Za svaki element* $(\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})) \setminus W_{\mathbb{Z}}$ *čija je diskriminanta različita od nule postoji najviše* 12 *elemenata iz* $\mathrm{PGL}_2(\mathbb{Z}) \setminus V_{\mathbb{Z}}$ *koji se slikaju sa* ψ *u njega.*

Dokaz: Definicija preslikavanja ψ i teorema 4.5.12 nam kažu da je dovoljno dokazati da za proizvoljan element $w \in \mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z}) \setminus W_{\mathbb{Z}}$ postoji najviše 12 elemenata iz $F_{\mathbb{Z},1} \times \mathrm{SO}(A_1, \mathbb{Z}) \setminus W_{\mathbb{Z},1}$ koji se slikaju u njega (su predslike od njega). Neka je $\{(A_1, B_\alpha)\}_{\alpha \in \mathcal{A}}$ skup $F_{\mathbb{Z},1} \times \mathrm{SO}(A_1, \mathbb{Z})$ neekvivalentnih predslika od $w \in W_{\mathbb{Z},1}$, za neki skup indeksa $\mathcal{A}$. celobrojne binarne kubične forme

$$g_\alpha(x, y) := 4 \det(A_1 x - B_\alpha y)$$

imaju 1 uz x^3 (dakle, $g_\alpha(1, 0) = 1$). Parovi (A_1, B_α) su $F_{\mathbb{Z},1} \times \mathrm{SO}(A_1, \mathbb{Z})$ neekvivalentni, ali su svi međusobno $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})$ ekvivalentni, zbog čega su g_α međusobno $F_{\mathbb{Z},1}$ neekvivalentni, ali $\mathrm{GL}_2(\mathbb{Z})$ ekvivalentni.

U delima [D3] i [E2] nalazimo da jednačina $g(x, y) = 1$ ima najviše 12 rešenja za koja važi $(x, y) \in \mathbb{Z}^2$ (g je celobrojna binarna kubična forma sa nenu;a diskriminantom), odakle sledi da je kardinalnost skupa $\mathcal{A}$ najviše 12. □

Lema 4.5.14. *Broj* $\mathrm{GL}_2(\mathbb{Z})$ *orbita celobrojnih binarnih kvartičnih formi* $f \in V_{\mathbb{Z}}$ *za koje je*

$$\Delta(f) \neq 0, H(f) < X,$$

i čiji stabilizator u $\mathrm{GL}_2(\mathbb{Q})$ *ima kardinalnost veću od* 2 *je* $O(X^{3/4+\epsilon})$.

Dokaz: Neka je $f \in V_{\mathbb{Z}}$ element sa stabilizatorom veličine bar 2 u $\mathrm{PGL}_2(\mathbb{Q})$. Tada teorema 5.3.2 kaže da je za

$$E : y^2 = x^3 - \frac{I(f)}{3} x - \frac{J(f)}{27}$$

skup $E(\mathbb{Q})[2]$ netrivijalan, odakle sledi da je kubična rezolventa g od f reducibilna nad $\mathbb{Q}$. Ako je još i $H(f) < X$, tada nam prethodna lema kaže da je broj izbora za $F_{\mathbb{Z},1}$ orbitu od g asimptotski jednak $O(X^{1/2+\epsilon})$.

Ako fiksiramo $\mathrm{GL}_2(\mathbb{Z})$ orbitu koja sadrži reducibilnu celobrojnu binarnu kubičnu formu g sa visinom manjom od X, tada iz [B], lema 12, imamo da je broj $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})$ orbita na $W_{\mathbb{Z}}$ sa g kao kubičnom resolventnom formom je ograničen sa $O(X^{1/4})$. Ovo, zajedno sa tvrđenjem 4.5.13, nam daje da je broj $\mathrm{PGL}_2(\mathbb{Z})$ orbita

na $V_{\mathbb{Z}}$ sa g kao kubičnom rezolventom je asimptotski jednak $O(X^{1/4})$. Prema tome, broj $\mathrm{PGL}_2(\mathbb{Z})$ orbita na $V_{\mathbb{Z}}$ sa netrivijalnim stabilizatorom u $\mathrm{PGL}_2(\mathbb{Q})$ i visinom manjom od X je asimptotski jednak $O(X^{1/4}X^{1/2+\epsilon}) = O(X^{3/4+\epsilon})$. □

Teorema 4.5.15. *Par $(I, J) \in \mathbb{Z}^2$ je par invarijanti za neku celobrojnu binarnu kvartičnu formu akko zadovoljava jedan od sledećih uslova:*

- $I \equiv_3 0$ *i* $J \equiv_{27} 0$,
- $I \equiv_9 1$ *i* $J \equiv_{27} \pm 2$,
- $I \equiv_9 4$ *i* $J \equiv_{27} \pm 16$,
- $I \equiv_9 7$ *i* $J \equiv_{27} \pm 7$.

Dokaz: Znamo da ako neka celobrojna binarna kvartična forma ima invarijante I i J, da onda njena kubična rezolventa ima iste te invarijante. Obratno, ako celobrojni par (I, J) predstavlja par invarijanti neke celobrojne binarne kubične forme

$$g(x, y) = x^3 + rx^2 + sxy^2 + ty^3,$$

onda forma

$$f(x, y) = x^3y + rx^2y^2 + sxy^3 + ty^4$$

ima kubičnu rezolventu jednakoj g, pa f ima invarijante I i J. Dakle, kako bismo dokazali ovu teoremu, dovoljno je posmatrati celobrojne monične binarne kubične forme.

Neka forma

$$g(x, y) = x^3 + rx^2y + sxy^2 + ty^3 \in U_{\mathbb{Z},1}$$

ima invarijante I i J. Ako delujemo na g sa elementom $F_{\mathbb{Z},1}$, možemo dobiti formu koja uz x^2y ima član skupa $\{-1, 0, 1\}$ (dakle, možemo smatrati da je $r \in \{-1, 0, 1\}$), i ima invarijante I i J. Ako je $I \equiv_3 0$, onda je $r = 0$, pa $27 \mid J$.

Ako $3 \nmid I$, tada je r jednako 1 ili -1, pa je $I \equiv_3 1$, zbog čega I mora biti kongruentno sa $1, 4$ ili 7 modulo 9, a to se dešava kada je s kongruentno sa $0, 2$ ili 1 modulo 3. Pošto je $r^2 = 1$, to je $J \equiv_{27} r(9s - 2)$. odavde imamo da $I \equiv_9 1, 4, 7$ odgovara $J \equiv_{27} \pm 2, \pm 16, \pm 7$.

Dakle, ako je (I, J) par invarijanti za neku celobrojnu moničnu binarnu kubičnu formu, onda on mora da zadovoljava jedan od uslova ove teoreme. Lako se može dokazati i obratno, tako što idemo argumentima u suprotnom smeru. □

4.6 O prihvatljivim funkcijama-prvi deo

U sledeća tri odeljka ćemo uvesti *prihvatljivu* klasu funkcija: definicija 4.8.2. Te funkcije će nam biti potrebne kako bismo procenili lokalno ponašanje broja $N(S; X)$: teorema 4.8.4.

Neka je S podskup od $V_{\mathbb{Z}}$ koji je definisan sa konačno mnogo uslova kongruencije (možemo pretpotstaviti da je S definisano uslovima kongruencije modulo nekog celog broja m). Tada S možemo gledati kao uniju k translata $\mathcal{L}_1, ..., \mathcal{L}_k$ rešetke $m \cdot V_{\mathbb{Z}}$. Za svako $\mathcal{L}_j$ koristimo formulu (4.4) kako bismo izračunali $N(\mathcal{L}_j \cap V_{\mathbb{Z}}^{(i)}; X)$, gde je svaka d-dimenzionalna mera skalirana faktorom $1/m^d$, jer je naša nova rešetka skalirana faktorom m. Sa ovim skaliranjima, maksimalna zapremina projekcija skupa $B(n, t, \lambda, X)$ se asimptotski ponaša kao $O(t^4\lambda^{16})$. Analogno tvrđenju 4.3.2, broj tačaka

$$(a, b, c, d, e) \in B(n, t, \lambda, X) \cap \mathcal{L}_j$$

sa $a \neq 0$ je jednak

$$\begin{cases} 0 & \text{za} \frac{C\lambda}{t} < 1; \\ \frac{1}{m^5}\text{Vol}(B(n, t, \lambda, X)) + O(t^4\lambda^{16}) & \text{u suprotnom.} \end{cases} \tag{4.11}$$

Kada integralimo $N(\mathcal{L}_j \cap V_{\mathbb{Z}}^{(i);X})$ kao u (4.5) i (4.6), dobijamo, analogno (4.7), da je

$$N(\mathcal{L}_j \cap V_{\mathbb{Z}}^{(i)}; X) = \frac{\text{Vol}(\mathcal{R}_X(L^{(i)}))}{n_i \cdot m^5} + O(X^{3/4+\epsilon}).$$

Kada sumiramo po j, dobijamo

$$N(S \cap V_{\mathbb{Z}}^{(i)}; X) = \frac{k\mathrm{Vol}(\mathcal{R}_X(L^{(i)}))}{n_i \cdot m^5} + O(X^{3/4+\epsilon}).$$

Definicija 4.6.1. *Za bilo koji skup S u $V_{\mathbb{Z}}$ koji je definisan uslovima kongruencije, sa $\mu_p(S)$ označimo p-adičnu gustinu p-adičnog zatvorenja S u $V_{\mathbb{Z}_p}$, pri čemu je aditivna mera μ_p na $V_{\mathbb{Z}_p}$ normalizovana tako da je $\mu_p(V_{\mathbb{Z}_p}) = 1$.*

Iz prethodne diskusije (kao i iz (4.7), vrednosti $N(S \cap V_{\mathbb{Z}}^{(i)}; X)$ koju smo izračunali i identifikacije $km^{-5} = \prod_p \mu_p(S)$) sledi sledeća teorema:

Teorema 4.6.2. *Neka je S podskup od $V_{\mathbb{Z}}$ definisan uslovima kongruencije modulo konačno mnogo stepena prostih brojeva. Tada je*

$$N(S \cap V_{\mathbb{Z}}^{(i)}; X) = N(V_{\mathbb{Z}}^{(i)}; X) \prod_p \mu_p(S) + O(X^{3/4+\epsilon}).$$

gde je $\mu_p(S)$ p-adična gustina S u $V_{\mathbb{Z}}$, i implicirana konstanta zavisi samo od S i ϵ.

Takođe ćemo koristiti i sledeću verziju prethodne teoreme, čiji dokaz je isti:

Teorema 4.6.3. *Neka su $p_1, ..., p_k$ različiti prosti brojevi. Za $j = 1, ..., k$, neka su: $\phi_{p_j} : V_{\mathbb{Z}} \to \mathbb{R}$ neka $\mathrm{GL}_2(\mathbb{Z})$ invarijantna funkcija na $V_{\mathbb{Z}}$ takva da $\phi_{p_j}(f)$ zavisi samo od klase kongruencije f modulo nekog stepena $p_j^{a_j}$; neka je $N_\phi(V_{\mathbb{Z}}^{(i)}; X)$ broj ireducibilnih $\mathrm{GL}_2(\mathbb{Z})$ orbita u $V_{\mathbb{Z}}^{(i)}$ visine ograničene sa X, gde se svaka orbita $\mathrm{GL}_2(\mathbb{Z}) \cdot f$ računa sa težinom*

$$\phi(f) := \prod_{j=1}^{k} \phi_{p_j}(f).$$

Tada je

$$N_\phi\left(V_{\mathbb{Z}}^{(i)}; X\right) = N\left(V_{\mathbb{Z}}^{(i)}; X\right) \prod_{j=1}^{k} \int_{f \in V_{\mathbb{Z}_{p_j}}} \widetilde{\phi}_{p_j}(f) df + O(X^{3/4+\epsilon}),$$

gde je $\widetilde{\phi}_{p_j}$ *proširenje* ϕ_{p_j} *na* $V_{\mathbb{Z}_{p_j}}$, df *je aditivna mera na* $V_{\mathbb{Z}_{p_j}}$ *koja je normalizovana tako da je*

$$\int_{f \in V_{\mathbb{Z}_{p_j}}} df = 1,$$

i implicirana konstanta zavisi samo od funkcija ϕ_{p_j} *i konstante* ϵ.

4.7 O prihvatljivim funkcijama-drugi deo

Definicija 4.7.1. *Za prost broj* p, *sa* $\mathcal{W}_p(V)$ *označavamo skup binarnih kvartičnih formi* $f \in V_{\mathbb{Z}}$ *takve da je*

$$p^2 \mid \Delta(f).$$

Definicija 4.7.2. *Za formu* $f \in \mathcal{W}_p(V)$ *kažemo da je jako deljiva sa* p^2 *ako*

$$p^2 \mid \Delta(f + pg)$$

za svako $g \in V_{\mathbb{Z}}$. *Skup svih ovakvih* f *obeležavamo sa* $\mathcal{W}_p^{(1)}(V)$.

Definicija 4.7.3. *Za formu $f \in \mathcal{W}_p(V)$ kažemo da je slabo deljiva sa p^2 ako postoji $g \in V_{\mathbb{Z}}$ takvo da*

$$p^2 \nmid \Delta(f + pg).$$

Skup svih ovakvih f obeležavamo sa $\mathcal{W}_p^{(2)}(V)$.

Definicija 4.7.4. *Za element $f \in \mathcal{W}_p^{(1)}(V)$ kažemo da je umnožak od p ako je $f \in pV_{\mathbb{Z}}$.*

Definicija 4.7.5. *Za element $f \in \mathcal{W}_p^{(1)}(V)$ kažemo da ima tip račvanja u p jednak $(1^3), (1^2 1^2), (2^2)$ ili (1^4) ako se redukcija f modulo p faktoriše u ireducibilne faktore nad $\mathbb{F}_p$ kao*

$$c(x - \alpha y)^3 (x - \beta y),$$

$$c(x - \alpha y)^2 (x - \beta y)^2,$$

$$c(x^2 + \alpha xy + \beta y^2)^2$$

ili kao $c(x - \alpha y)^4$.

Sledeća teorema je kvantitativna verzija rezultata u [E], dokazana u [B2], teoremi 3.3:

Teorema 4.7.6. *Neka je B kompaktan region u $\mathbb{R}^n$ konačne mere, i neka je Y zatvorena podshema od $\mathbb{A}^n_{\mathbb{Z}}$ kodimenzije 2. Neka su r i M pozitivni realni brojevi. Tada je*

$$\#\left\{v \in rB \cap \mathbb{Z}^n \mid v(mod\ p) \in Y(\mathbb{F}_p)\ za\ neki\ prost\ broj\ p > M\right\} =$$

$$= O\left(\frac{r^n}{M^{k-1}\log M} + r^{n-k+1}\right),$$

gde implicirana konstanta zavisi samo od B i Y.

Definicija 4.7.7. *Za $0 < \epsilon < 1$, označimo sa $\mathcal{F}^{(\epsilon)}_{\mathrm{PGL}_2}$ (setimo se, $\mathcal{F}_{\mathrm{PGL}_2}$ je fundamentalni domen $N'A'K$ za levo dejstvo $\mathrm{PGL}_2(\mathbb{Z})$ na $\mathrm{PGL}_2(\mathbb{R})$) podskup elemenata $n(u)a(t)k \in \mathcal{F}_{\mathrm{PGL}_2}$, gde je t ograničeno odozgo nekom konstantom tako da je*

$$\mathrm{Vol}\left(\mathcal{F}^{(\epsilon)}_{\mathrm{PGL}_2}\right) = (1-\epsilon)\mathrm{Vol}\left(\mathcal{F}_{\mathrm{PGL}_2}\right).$$

Za fiksirano $\epsilon > 0$, skup $\mathcal{F}^{(\epsilon)}_{\mathrm{PGL}_2} \cdot R^{(i)}(X)$ (gde je $R^{(i)}$ definisano u 4.4.1) je ograničeni region u $V_{\mathbb{R}}$ koji se homogeno širi kada X raste.

Imamo sledeću teoremu:

Teorema 4.7.8. *Neka je $0 < \epsilon < 1$. Za $i \in \{0, 1, 2+, 2-\}$, imamo*

$$\#\left\{\mathcal{F}^{(\epsilon)}_{\mathrm{PGL}_2} \cdot R^{(i)}(X) \bigcap \left(\bigcup_{p>M} \mathcal{W}^{(1)}_p(V)\right)\right\} = O\left(X^{5/6}/(M\log M) + X^{2/3}\right),$$

gde implicirana konstanta zavisi samo od ϵ.

Dokaz: Po definiciji, diskriminante elemenata $\mathcal{W}^{(1)}_p(V)$ su strogo deljive sa p^2. Dakle, ova teorema sledi iz teoreme 4.7.6 (za $n = 5, k = 2$ i $r = X^{1/6}$), jer kao što smo primetili u [B2], ako je neki element $v \in V_{\mathbb{Z}}$ ima diskriminantu strogo deljivu sa p^2, onda on leži u $Y(\mathbb{F}_p)$, gde je Y podshema kodimenzije 2 od $V \cong \mathbb{A}^5$ definisana anuliranjem Δ i $\partial\Delta/\partial e$. □

Trebaće nam sledeća teorema ([B], tvrđenje 23):

Teorema 4.7.9. *Neka je $\mathcal{W}_p^{(2)}(W)$ skup elemenata u $W_{\mathbb{Z}}$ čije su diskriminante deljive (ali ne jako) sa p^2. Broj $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{SL}_3(\mathbb{Z})$ orbita na $\mathcal{W}_p^{(2)}(W)$ sa diskriminantom manjom od X je $O(X/p^2)$, gde implicirana konstanta zavisi samo od p.*

Ova procena, zajedno sa tvrđenjem 4.5.13, nam daje sledeće

$$N\left(\mathcal{W}_p^{(2)}(V); X\right) = O\left(X/p^2\right), \tag{4.12}$$

gde implicirana konstanta ne zavisi od X i p.

Definicija 4.7.10. *Za $X > 0$ i $\epsilon > 0$, uvodimo:*

$$R_X^{(\epsilon)} := \mathcal{F}_{\mathrm{PGL}_2}^{(\epsilon)} \cdot R^{(i)}(X)$$

gde je $\mathcal{F}_{\mathrm{PGL}_2}^{(\epsilon)}$ iz definicije 4.7.7, a $R^{(i)}(X)$ iz definicije 4.4.1.

Teorema 4.7.11. *Neka je $0 < \epsilon < 1$ fiksirano. Za $i \in \{0, 1, 2+, 2-\}$, imamo*

$$\#\left\{\mathcal{F}_{\mathrm{PGL}_2}^{(\epsilon)} \cdot R^{(i)}(X) \bigcap \left(\bigcup_{p>M} \mathcal{W}_p^{(2)}(V)\right)\right\} = O(X^{5/6}/\log M),$$

gde implicirana konstanta ne zavisi od X i M.

Dokaz: Izvod Δ po e je nenula kubični polinom. Ako binarna kvartična forma

$$f(x, y) = a_0x^4 + b_0x^3y + c_0x^2y^2 + d_0xy^3 + e_0y^4$$

pripada $\mathcal{W}_p^{(2)}$ tada mora da važi $p^2 \mid \Delta$ i $p \nmid \partial\Delta/\partial e$ (inače bi f bilo u $\mathcal{W}_p^{(1)}$). Kako se $R_X^{(\epsilon)}$ homogeno širi u $V_{\mathbb{R}} = \mathbb{R}^5$, pri čemu je red širenja svake strane $X^{1/6}$, to postoji $O(X^{4/6})$ mogućnosti za izbor četvorke (a_0, b_0, c_0, d_0) tako da je $f(x, y) \in R_X^{(\epsilon)} \cap V_{\mathbb{Z}}$ za

neko e_0. No, za fiksiranu četvorku postoji najviše 3 izbora za ostatak e_0 modulo p tako da $p \mid \Delta$. Kako $p \nmid \partial\Delta/\partial e$, za svaki takav ostatak modulo p postoji jedinstveni ostatak modulo p^2 takav da $p^2 \mid \Delta$. Dakle

$$\# \left\{ R_X^{(\epsilon)} \cap \mathcal{W}_p^{(2)}(V) \right\} = O\left(\max\left\{ X^{5/6}/p^2, X^{4/6} \right\} \right), \tag{4.13}$$

gde, svakako, koristimo prvu oc enu za $p \leq X^{1/12}$, i drugu za $p > X^{1/12}$. Pošto je broj prostih brojeva u intervalu $[1, X^{1/6}]$ asimptotski jednak $O(X^{1/6}/\log X)$ i pošto je

$$\sum_{p > X^{1/6}} 1/p^2 = O\left(1/\left(X^{1/6} \log X \right) \right),$$

to dobijamo

$$\# \left\{ R_X^{(\epsilon)} \bigcap \left(\bigcup_{p>M} \mathcal{W}_p^{(2)}(V) \right) \right\} = O\left(\sum_{p>M} \# \left\{ R_X^{(\epsilon)} \cap \mathcal{W}_p^{(2)}(V) \right\} \right) = O(X^{5/6}/\log M)$$

tako što koristimo (4.13) da procenimo $\#\{R_X^{(\epsilon)} \cap \mathcal{W}_p^{(2)}(V)\}$ kada je $p < X^{1/6}$, i (4.12) kada je $p \geq X^{1/6}$. □

Sada imamo sledeću teoremu:

Teorema 4.7.12. *Za svako $M > 0$ važi*

$$\lim_{X \to \infty} \frac{N\left(\bigcup_{p>M} \mathcal{W}_p(V); X \right)}{X^{5/6}} = O\left(\frac{1}{\log M} \right),$$

gde implicirana konstanta nezavisna od M.

Pre dokaza, uvedimo sledeću definiciju:

Definicija 4.7.13. *Za realan broj $X > 0$, neka je*

$$R(X) := \bigcup_i R^{(i)}(X),$$

gde je $R^{(i)}(X)$ iz definicije 4.4.1.

Dokaz: Iz glave §4.1 imamo:

$$N\left(\bigcup_{p>M} \mathcal{W}_p(V); X\right) \leq \#\left\{\mathcal{F}_{\mathrm{PGL}_2} \cdot R(X) \bigcap \left(\bigcup_{p>M} \mathcal{W}_p(V)\right) \bigcap V_{\mathbb{Z}}^{\mathrm{irr}}\right\} \leq$$

$$\leq \#\left\{\mathcal{F}_{\mathrm{PGL}_2}^{(\epsilon)} \cdot R(X) \bigcap \left(\bigcup_{p>M} \mathcal{W}_p(V)\right)\right\} + \#\left\{\left(\mathcal{F}_{\mathrm{PGL}_2} \setminus \mathcal{F}_{\mathrm{PGL}_2}^{(\epsilon)}\right) \cdot R(X) \cap V_{\mathbb{Z}}^{\mathrm{irr}}\right\}.$$

Po teoremama 4.7.8 i 4.7.11, prvi sabirak u gornjoj nejednakosti je ograničen sa $O(X^{5/6}/\log M + X^{2/3})$. Rezultati u glavama §4.3 i §4.4 nam kažu da je drugi sabirak ograničen sa

$$\mathrm{Vol}\left(\left(\mathcal{F}_{\mathrm{PGL}_2} - \mathcal{F}_{\mathrm{PGL}_2}^{(\epsilon)}\right) \cdot R(X)\right) = O(\epsilon X^{5/6}).$$

Ovo važi za svako ϵ, pa teorema sledi. □

4.8 O prihvatljivim funkcijama-treći deo

Definicija 4.8.1. *Za neku funkciju $\phi : V_{\mathbb{Z}} \to [0,1] \subset \mathbb{R}$ kažemo da je definisana uslovima kongruencije ako za sve proste brojeve p postoje (lokalne) funkcije $\phi_p : V_{\mathbb{Z}_p} \to [0,1]$ tako da važi:*

1. *Za svako $f \in V_{\mathbb{Z}}$, proizvod $\prod_p \phi_p(f)$ konvergira ka $\phi(f)$.*
2. *Za svaki prost broj p, funkcija ϕ_p je lokalno konstantna van nekog zatvorenog skupa $S_p \subset V_{\mathbb{Z}_p}$ mere nula.*

Definicija 4.8.2. *Za funkciju $\phi : V_{\mathbb{Z}} \to [0,1]$ definisanu uslovima kongruencija kažemo da je prihvatljiva ako za dovoljno velike proste brojeve p imamo da je $\phi_p(f) = 1$ kad god $p^2 \nmid \Delta(f)$.*

Definicija 4.8.3. *Za fiksirani ceo broj Y, sa $N_{\psi}^{Y}(V_{\mathbb{Z}}^{(i)}; X)$ (odnosno sa $N_{\psi'}^{Y}(V_{\mathbb{Z}}^{(i)}; X)$) označavamo broj ireducibilnih $\mathrm{GL}_2(\mathbb{Z})$ orbita u $V_{\mathbb{Z}}^{(i)}$ sa visinom manjom od X, gde se svaka orbita $\mathrm{GL}_2(\mathbb{Z}) \cdot f$ računa sa težinom*

$$\prod_p \psi_{p\lfloor Y/p \rfloor}(f) \quad \left(\text{tj. sa} \prod_p \psi'_{p,\lfloor Y/p \rfloor}(f) \right).$$

Sada ćemo dokazati sledeću teoremu:

Teorema 4.8.4. *Neka je $\phi : V_{\mathbb{Z}} \to [0,1]$ neka prihvatljiva funkcija, i neka su $\phi_p : V_{\mathbb{Z}_p} \to [0,1]$ odgovarajuće lokalne funkcije. Tada imamo da je:*

$$N_{\phi}(V_{\mathbb{Z}}^{(i)}; X) = N(V_{\mathbb{Z}}^{(i)}; X) \prod_p \int_{f \in V_{\mathbb{Z}_p}} \phi_p(f) df + o(X^{5/6}).$$

Dokaz: Pošto su ϕ_p lokalno konstantne funkcije van nekog skupa mere nula, to postoji rastući niz funkcija $\psi_{p,1} \leq \psi_{p,2} \leq ...$ koji je ograničen odozgo i konvergira tačka-po-tačka ka ϕ_p, kao i opadajući niz funkcija $1 = \psi'_{p,0} \geq \psi'_{p,1} \geq \psi'_{p,2} \geq ...$ koji je ograničen odozdo i konvergira tačka-po-tačka ka ϕ_p, i važi da su $\psi_{p,n}$ i $\psi'_{p,n}$ definisani na $V_{\mathbb{Z}_p}$ uslovima kongruencije modulo p^n.

Po teoremi o dominantoj konvergenciji imamo da je

$$\lim_{n\to\infty} \int_{V_{\mathbb{Z}_p}} \psi_{p,n}(f)df = \lim_{n\to\infty} \int_{V_{\mathbb{Z}_p}} \psi'_{p,n}(f)df = \int_{V_{\mathbb{Z}_p}} \phi_p(f)df. \tag{4.14}$$

Dodatno, ϕ je prihvatljiva, pa važi

$$1 - \int_{V_{\mathbb{Z}_p}} \phi_p(f)df \leq \int_{\substack{f\in V_{\mathbb{Z}_p} \\ p^2|\Delta(f)}} df \ll p^{-2} \tag{4.15}$$

za dovoljno veliko p. (možemo videti primer u [P], teorema 3.2).

Uočimo, $\lfloor Y/p \rfloor$ uzima nenula vrednosti samo za konačno mnogo prostih brojeva p, za bilo koje Y. Dakle, iz teoreme 4.6.3 sledi da za bilo koje Y imamo

$$\limsup_{X\to\infty} \frac{N_\phi(V_{\mathbb{Z}}^{(i)}; X)}{X^{5/6}} \leq \limsup_{X\to\infty} \frac{N^Y_{\psi'}(V_{\mathbb{Z}}^{(i)}; X)}{X^{5/6}} =$$

$$= \lim_{X\to\infty} \frac{N(V_{\mathbb{Z}}^{(i)}; X)}{X^{5/6}} \prod_p \int_{f\in V_{\mathbb{Z}_p}} \psi'_{p,\lfloor T/p \rfloor}(f)df.$$

Iz nejednakosti (4.15) sledi da proizvod $\prod_p \int_{V_{\mathbb{Z}_p}} \phi_p(f)df$ konvergira. Ako pustimo da Y teži beskonačnosti, (4.14) nam daje

$$\limsup_{X\to\infty} \frac{N_\phi(V_{\mathbb{Z}}^{(i)}; X)}{X^{5/6}} \leq \lim_{X\to\infty} \frac{N(V_{\mathbb{Z}}^{(i)}; X)}{X^{5/6}} \prod_p \int_{f\in V_{\mathbb{Z}_p}} \phi_p(f)df. \tag{4.16}$$

Setimo se da za dovoljno veliko p i $n \geq 1$ važi

$$\psi_{p,n}(f) = \phi_p(f) = 1,$$

osim ako je $p^2 \mid \Delta(f)$. Prema tome, za dovoljno veliko Y imamo

$$\liminf_{X\to\infty} \frac{N_\phi\left(V_{\mathbb{Z}}^{(i)}; X\right)}{X^{5/6}} \geq \liminf_{X\to\infty} \left[\frac{N_\psi^Y(V_{\mathbb{Z}}^{(i)}; X)}{X^{5/6}} - \frac{O\left(N\left(\bigcup_{p>Y} \mathcal{W}_p(V); X\right)\right)}{X^{5/6}} \right] =$$

$$= \lim_{X\to\infty} \frac{N(V_{\mathbb{Z}}^{(i)}; X)}{X^{5/6}} \cdot \prod_p \int_{f\in V_{\mathbb{Z}_p}} \psi_{p,\lfloor Y/p \rfloor}(f) df - O(1/\log Y),$$

gde prva jednakost važi, jer je ϕ gornje ograničenje za $\psi_{p,n}$ (osim za $n = 0$), i poslednja jednakost sledi iz teorema 4.6.3 i 4.7.12. Kada uzmemo da Y teži beskonačnosti, dobijamo

$$\liminf_{X\to\infty} \frac{N_\phi(V_{\mathbb{Z}}^{(i)}; X)}{X^{5/6}} = \lim_{X\to\infty} \frac{N(V_{\mathbb{Z}}^{(i)}; X)}{X^{5/6}} \cdot \prod_p \int_{f\in V_{\mathbb{Z}_p}} \phi_p(f) df, \tag{4.17}$$

pri čemu koristimo (4.15) da zamenimo mesta limesa po Y i proizvoda, i (4.14) da zamenimo mesta limesa po Y i integrala. Teorema sledi sada iz (4.17) i (4.16). □

Glava 5

Rang eliptičkih krivih

5.1 Uvod

U ovoj glavi ćemo pokazati vezu između binarnih kvartičnih formi i ranga eliptičkih krivih, i dokazaćemo jednu veoma bitnu teoremu koja se odnosi na rangove 2-Selmerovih grupa eliptičkih krivih.

Svaka eliptička kriva nad poljem $\mathbb{Q}$ se može napisati u sledećem obliku:

$$E_{A,B} : y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{Z},$$

i za svaki prost broj p važi da $p^6 \nmid B$ kad god $p^4 \mid A$. Sa

$$H(E_{A,B}) := \max\left\{4\left|A^3\right|, 27B^2\right\}$$

obeležavamo visinu, sa

$$\Delta\left(E_{A,B}\right) := -16\left(4A^3 + 27B^2\right)$$

diskriminantu, a sa

$$C(E) = \prod_p p^{f_p(E)},$$

gde je

$$f_p(E) = \begin{cases} 0 & \text{ako } E \text{ ima dobru redukciju u } p \\ 1 & \text{ako } E \text{ ima multiplikativnu redukciju u } p \\ 2 & \text{ako } E \text{ ima aditivnu redukciju u } p \end{cases},$$

konduktor krive E. Ako označimo $I(E) = -3A$ i $J(E) = -27B$, onda krivu $E_{A,B}$ možemo takođe da obeležimo i sa $E^{I,J}$.

Za svaki prost broj p, neka je Σ_p neki zatvoreni podskup od $\mathbb{Z}_p^2 \setminus \{(I,J) : \Delta(E^{I,J}) \neq 0\}$ čija je granica mere nula (sa $\Delta(I,J)$ ćemo podrazumevati $\Delta(E^{I,J}) = (4I^3 - J^2)/27$).

Definicija 5.1.1. *Za familiju eliptičkih krivih $F = F_\Sigma$ definisanih nad $\mathbb{Q}$ za koju važi da $E^{I,J} \in F_\Sigma$ akko $(I,J) \in \Sigma_p$ za svaki prost broj p kažemo da je definisana uslovima kongruencije.*

Primedba 5.1.2. *Takođe ćemo koristiti i F umesto F_Σ.*

Takođe možemo na F_Σ zadati uslove kongruencije u beskonačnosti: ako za krive važi $E^{I,J} \in F_\Sigma$ akko $(I,J) \in \Sigma_\infty = \{(I,J) \in \mathbb{R}^2 : \Delta(I,J) > 0\}$, $\{(I,J) \in \mathbb{R}^2 : \Delta(I,J) < 0\}$ ili $\{(I,J) \in \mathbb{R}^2 : \Delta(I,J) \neq 0\}$.

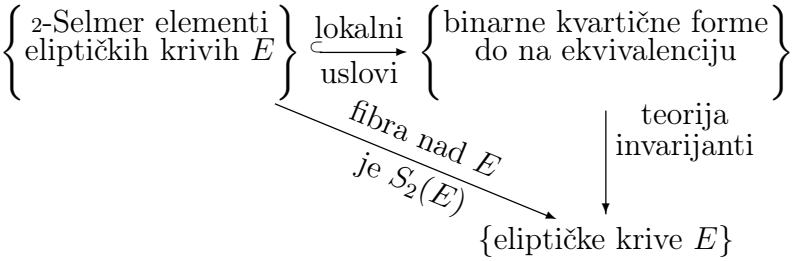
Definicija 5.1.3. *Neka je F proizvoljna neprazna familija eliptičkih krivih nad $\mathbb{Q}$ koja je definisana uslovima kongruencije. Tada sa $\mathrm{Inv}(F)$ obeležavamo skup $\{(I(E), J(E)) : E \in F\}$. Sa $\mathrm{Inv}_p(F)$ obeležavamo skup elemenata u p-adičnom zatvorenju $\mathrm{Inv}(F) \subset \mathbb{Z}_p^2$ za koje važi $\Delta(I,J) = (4I^3 - J^2)/27 \neq 0$, a sa $\mathrm{Inv}_\infty(F)$ obeležavamo $\{(I,J) \in \mathbb{R}^2 : \Delta(I,J) > 0\}$, $\{(I,J) \in \mathbb{R}^2 : \Delta(I,J) < 0\}$ ili $\{(I,J) \in \mathbb{R}^2 : \Delta(I,J) \neq 0\}$, u zavisnosti od toga da li familija F sadrži samo krive sa pozitivnom diskriminantom, samo sa negativnom, ili sadrži i krive sa pozitivnom, i krive sa negativnom diskriminantom.*

Definicija 5.1.4. *Za familiju eliptičkih krivih F definisanu uslovima kongruencije kažemo da je velika ako za sve osim konačno mnogo p skup $\mathrm{Inv}_p(F)$ sadrži sve parove $(I,J) \in \mathbb{Z}_p \times \mathbb{Z}_p$ za koje $p^2 \nmid \Delta(I,J)$.*

U ovoj glavi ćemo pokazati sledeću teoremu, koju su dokazali Manjul Bargava i Arul Shankar, u [BS]:

Teorema 5.1.5. *Kada se sve eliptičke krive E u bilo kojoj velikoj familiji poređaju po visini, prosečna veličina 2-Selmerove grupe $S_2(E)$ je 3.*

U prvom odeljku ćemo se podsetiti Selmerovih grupa, i nekih njihovih svojstava. Zatim ćemo uspostaviti vezu između elemenata 2-Selmerovih grupa eliptičkih krivih i binarnih kvartičnih formi sa racionalnim koeficijentima (do na standardne transformacije) sa nekim lokalnim svojstvima. Klasična teorija invarijanti binarnih kvartičnih formi nam daje vertikalno preslikavanje na sledećem dijagramu:



Zatim, koristeći rezultate iz četvrte glave, brojimo 2-Selmer elemente eliptičkih krivih čije visine su ograničene datom konstantom X. Na kraju, pošto je fibra u gornjem dijagramu jednaka $S_2(E)$, kada podelimo ovaj broj sa brojem eliptičkih krivih visine manje ili jednake X, i uzmemo da X teži beskonačnosti, dobijamo srednju vrednost koju tražimo.

Još uvek se ne zna da li ovaj metod funkcioniše kada korisimo diskriminantu ili konduktor umesto visine, jer ne znamo kako se broj eliptičkih krivih sa diskriminantom ili konduktorom manjim od X ponaša kada X teži beskonačnosti.

5.2 Selmerove grupe

U ovom odeljku ćemo uvesti pojam Selmerovih grupa eliptičkih krivih, i navesti nekoliko svojstava ovih grupa (dokazi ovih svojstava se mogu naći u [S3]). One śu nam jako bitne za rešavanje problema prosečnog ranga eliptičkih krivih koji smo uveli u ovoj glavi (teorema 5.1.5). Pre toga, moramo uvesti Weil-Châtelet grupe.

Definicija 5.2.1. *Neka je E/K eliptička kriva. Glavni homogeni prostor krive E/K je glatka kriva C/K zajedno sa tranzitivnim dejstvom grupe E na C definisanim nad K.*

Definicija 5.2.2. *Dva homogena prostora C/K i C'/K za E/K su ekvivalentna ako postoji izomorfizam $\theta : C \to C'$ definisan nad K za koji važi:*

$$(\forall p \in C)(\forall P \in E)\theta(p + P) = \theta(p) + P.$$

Klasu ekvivalencije koja sadrži E/K (E/K deluje na sebe translacijom) zovemo trivijalnom klasom. Kolekciju klasa ekvivalencija homogenih prostora za E/K zovemo Weil-Châtelet grupom za E/K, koju obeležavamo sa $\mathrm{WC}(E/K)$.

Sada ćemo navesti sledeću teoremu bez dokaza (koji se može naći u [S3], teorema 3.6) koja će nam objasniti zašto $\mathrm{WC}(E/K)$ zovemo grupom.

Teorema 5.2.3. *Neka je E/K eliptička kriva. Postoji prirodna bijekcija*

$$\mathrm{WC}(E/K) \to H^1(G_{\overline{K}/K}, E)$$

Pošto je $H^1(G_{\overline{K}/K}, E)$ grupa, možemo iskoristiti gornju teoremu da posmatramo $\mathrm{WC}(E/K)$ kao grupu.

Neka su sada E/K i E'/K dve eliptičke krive definisane nad brojnim poljem K, i neka je $\phi : E \to E'$ neka nenula izogenija (možemo uzeti na primer $E' = E$ i $\phi = [m]$). Tada postoji tačan niz $G_{\overline{K}/K}$ modula

$$0 \to E[\phi] \to E \to E' \to 0,$$

gde je $E[\phi]$ jezgro od ϕ. Ako posmatramo Galoaovu kohomologiju ovog niza, videćemo jedan dugi tačan niz:

$$0 \to E(K)[\phi] \to E(K) \xrightarrow{\phi} E'(K) \xrightarrow{\delta} H^1(G_{\overline{K}/K}, E[\phi]) \to$$

$$\to H^1(G_{\overline{K}/K}, E) \xrightarrow{\phi} H^1(G_{\overline{K}/K}, E'),$$

i iz ovog niza dobijamo sledeći kratki tačan niz:

$$0 \to E'(K)/\phi(E(K)) \xrightarrow{\delta} H^1(G_{\overline{K}/K}, E[\phi]) \to H^1(G_{\overline{K}/K,E})[\phi] \to 0.$$

Sada ćemo posmatrati lokalna ponašanja druge i treće grupe u ovom kratkom tačnom nizu. Za svako $v \in M_K$ fiksirajmo proširenje v na $\overline{K}$. Ovo nam daje utapanje $\overline{K} \subset \overline{K}_v$ i dekompoziciju grupe $G_v \subset G_{\overline{K}/K}$. Grupa G_v deluje na $E(\overline{K}_v)$ i $E'(\overline{K}_v)$, i kao i pre imamo tačne nizove

$$0 \to E'(K_v)/\phi(E(K_v)) \xrightarrow{\delta} H^1(G_v, E[\phi]) \to H^1(G_v, E)[\phi] \to 0.$$

Inkluzije $G_v \subset G_{\overline{K}/K}$ i $E(\overline{K}) \subset E(\overline{K}_v)$ nam daju sledeći komutativan dijagram:

$$\begin{array}{ccccccccc}
0 & \to & E'(K)/\phi(E(K)) & \xrightarrow{\delta} & H^1(G_{\overline{K}/K}, E[\phi]) & \to & \mathrm{WC}(E/K)[\phi] & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & \prod_{v\in M_K} E'(K_v)/\phi(E(K_v)) & \xrightarrow{\delta} & \prod_{v\in M_K} H^1(G_v, E[\phi]) & \to & \prod_{v\in M_K} \mathrm{WC}(E/K_v)[\phi] & \to & 0
\end{array}$$

Imajući u vidu ovaj dijagram, uvodimo sledeću definiciju:

Definicija 5.2.4. *Neka je $\phi : E/K \to E'/K$ izogenija. ϕ-Selmerova grupa od E/K je sledeća podgrupa od $H^1(G_{\overline{K}/K}, E[\phi])$:*

$$S^{(\phi)}(E/K) = \ker\left\{ H^1(G_{\overline{K}/K}, E[\phi]) \to \prod_{v\in M_K} \mathrm{WC}(E/K_v) \right\}.$$

Šafarevič-Tate grupa od E/K je sledeća podgrupa od $\mathrm{WC}(E/K)$*:*

$$Ш(E/K) = \ker\left\{\mathrm{WC}(E/K) \to \prod_{v\in M_K} \mathrm{WC}(E/K_v)\right\}.$$

U slučaju da je $E = E'$ i izogenija ϕ je množenje sa 2, tada ćemo pisati $S_2(E)$ umesto $S^{([2])}(E)$.

Navešćemo sada neka svojstva ovih grupa.

Teorema 5.2.5. *Neka je $\phi : E/K \to E'/K$ izogenija eliptičkih krivih definisana nad K. Tada:*

1. *Postoji tačan niz*

$$0 \to E'(K)/\phi(E(K)) \to S^{(\phi)}(E/K) \to Ш(E/K)[\phi] \to 0.$$

2. *Selmerova grupa $S^{(\phi)}(E/K)$ je konačna.*

Teorema 5.2.6. *Neka je $\phi : E/K \to E'/K$ izogenija eliptičkih krivih definisana nad K, i neka je $S \subset M_K$ konačan skup mesta koji sadrži*

$$M_K^\infty \cup \left\{v \in M_K^0 : E \text{ ima lošu redukciju u } v\right\} \cup \left\{v \in M_K^0 : v(\deg\phi) > 0\right\}.$$

Tada je

$$S^{(\phi)}(E/K) \subset H^1(G_{\overline{K}/K}, E[\phi]; S).$$

Posmatrajmo sada izogenije $[m^n]$ i $[m]$. Tada imamo sledeći komutativni dijagram:

$$\begin{array}{ccccccc} E(K) & \to & S^{(m^n)}(E/K) & \to & Ш(E/K)[m^n] & \to & 0 \\ \downarrow{\scriptstyle \mathrm{id}} & & \downarrow & & \downarrow{\scriptstyle \text{množenje sa } m^{n-1}} & & \\ E(K) & \to & S^{(m)}(E/K) & \to & Ш(E/K)[m] & \to & 0 \end{array}$$

Teorema 5.2.7. *Neka je E/K eliptička kriva. Za sve cele brojeve $m \geq 2$ i $n \geq 1$, neka je $S^{(m,n)}(E/K)$ slika $S^{(m^n)}(E/K)$ u $S^{(m)}(E/K)$. Tada postoji tačan niz*

$$0 \to E(K)/mE(K) \to S^{(m,n)}(E/K) \to m^{n-1}Ш(E/K)[m^n] \to 0.$$

Teorema 5.2.8. *Neka je E/K eliptička kriva. Tada je $Ш(E/K)$ konačno.*

Teorema 5.2.9. *Neka je E/K eliptička kriva. Tada postoji alternirajuće bilinearno sparivanje*

$$\Gamma : Ш(E/K) \times Ш(E/K) \to \mathbb{Q}/\mathbb{Z},$$

čije je jezgro na svakoj strani podgrupa deljivih elemenata $Ш(E/K)$. Dakle, ako je $\Gamma(\alpha, \beta) = 0$ za sve $\beta \in Ш(E/K)$, tada za svaki ceo broj $N \geq 1$ postoji element $\alpha_N \in Ш(E/K)$ za koji je $N\alpha_N = \alpha$.

5.3 Binarne kvartične forme i 2-pokrivanja eliptičkih krivih

U ovom odeljku ćemo definisati lokalno rešive binarne kvartične forme, i pokazati da postoji veza između 2-Selmerove grupe neke eliptičke krive $E^{I,J}$ nad $\mathbb{Q}$ i lokalno rešivih binarnih kvartičnih formi sa invarijantama $2^4 I$ i $2^6 J$.

Definicija 5.3.1. *Binarna kvartična forma $f(x,y)$ nad poljem K je K-rešiva ako jednačina $z^2 = f(x,y)$ ima rešenje sa $x,y,z \in K$ i $(x,y) \neq (0,0)$. Binarna kvartična forma $f \in V_{\mathbb{Q}}$ je lokalno rešiva ako je $\mathbb{R}$-rešiva i $\mathbb{Q}_p$-rešiva za svaki prost broj p.*

Sada ćemo navesti par teorema koje daju eksplicitan opis grupa $E(K)/2E(K)$ u terminima rešivih binarnih kvartičnih formi, čije dokaze ćemo izostaviti:

Teorema 5.3.2. *Neka je K polje sa* $\mathrm{char}K \neq 2,3$*,*

$$E : y^2 = x^3 - \frac{I}{3}x - \frac{J}{27} \tag{5.1}$$

eliptička kriva nad K. Tada postoji bijekcija između elemenata $E(K)/2E(K)$ i $\mathrm{PGL}_2(K)$-orbita K-rešivih binarnih kvartičnih formi sa invarijantama I i J, koja je data sa

$$(\xi,\eta) + 2E(K) \mapsto \mathrm{PGL}_2(K) \cdot \left(\frac{1}{4}x^4 - \frac{3}{2}\xi x^2 y^2 + 2\eta x y^3 + \left(\frac{I}{3} - \frac{3}{4}\xi^2 \right) y^4 \right).$$

Neutral u $E(K)/2E(K)$ odgovara $\mathrm{PGL}_2(K)$-orbiti binarnih kvartičnih formi koje imaju linearan faktor nad K.

Takođe, stabilizator u $\mathrm{PGL}_2(K)$ bilo koje binarne kvartične forme sa ne-nula invarijantama I i J je izomorfan sa $E(K)[2]$, gde je E eliptička kriva definisana sa (5.1).

(Dokaz se može naći u [CS], tvrđenje 2.2 i [CF], §3 − 5 i primedba 1)

Tvrđenje 5.3.3. *Neka je*

$$E : y^2 = x^3 - \frac{I}{3}x - \frac{J}{27}$$

eliptička kriva nad $\mathbb{Q}$. Tada postoji bijekcija između klasa izomorfizama lokalno rešivih 2-pokrivanja E i $\mathrm{PGL}_2(\mathbb{Q})$-orbita lokalno rešivih binarnih kvartičnih formi u $V_{\mathbb{Q}}$ sa invarijantama I i J.

Dalje, skup racionalnih binarnih kvartičnih formi sa racionalnim linearnim faktorom i invarijantama I i J leže u jednoj $\mathrm{PGL}_2(\mathbb{Q})$-orbiti, i ova orbita odgovara identitetu u 2-Selmerovoj grupi od E.

(Dokaz se može naći u [BSD], lema 2)

Lema 5.3.4. *Neka je $f \in V_{\mathbb{Q}}$ lokalno rešiva binarna kvartična forma sa celobrojnim invarijantama I i J takva da je*

$$(2^4 \cdot 3) \mid I \quad \text{i} \quad (2^6 \cdot 3^3) \mid J$$

Tada je f u istoj $\mathrm{PGL}_2(\mathbb{Q})$-orbiti kao i neka binarna kvartična forma sa celobrojnim koeficijentima.

(Dokaz se može naći u [BSD], leme 3, 4 i 5)

Pošto je eliptička kriva (5.1) izomorfna eliptičkoj krivoj

$$y^2 = x^3 - \frac{2^4 I(E)}{3} x - \frac{2^6 J(E)}{27}$$

to nam tvrđenje 5.3.4 i lema 5.3.3 daju:

Teorema 5.3.5. *Neka je $E = E^{I,J}$ eliptička kriva nad $\mathbb{Q}$. Tada su elementi 2-Selmerove grupe od E u 1-1 vezi sa $\mathrm{PGL}_2(\mathbb{Q})$ klasama ekvivalencije lokalno rešivih celobrojnih binarnih kvartičnih formi sa invarijantama $2^4 I$ i $2^6 J$.*

Dalje, skup celobrojnih binarnih kvartičnih formi koje imaju racionalan linearan faktor i invarijante $2^4 I$ i $2^6 J$ leži u jednoj $\mathrm{PGL}_2(\mathbb{Q})$ orbiti, a ova orbita odgovara neutralu u 2-Selmerovoj grupi od E.

5.4 Skup $S(F)$ lokalno rešivih kvartičnih formi i njihove težine

U prethodnoj glavi smo izračunali asimptotsko ponašanje broja $\mathrm{GL}_2(\mathbb{Z})$-orbita ireducibilnih celobrojnih binarnih kvartičnih formi sa ograničenom visinom. U lemi 4.2.1 smo videli da je broj $\mathrm{GL}_2(\mathbb{Z})$-orbita formi sa ograničenom visinom koje su

proizvod dve ireducibilne kvadratne forme zanemarljiv. Takođe, $\mathrm{GL}_2(\mathbb{Z})$-orbite na $V_\mathbb{Z}$ su isto što i $\mathrm{PGL}_2(\mathbb{Z})$ na $V_\mathbb{Z}$. Prema tome, asimptotska formula za broj $\mathrm{PGL}_2(\mathbb{Z})$ orbita celobrojnih binarnih kvartičnih formi sa ograničenom visinom bez racionalnog linearnog faktora je jednak asimptotskoj formuli za broj $\mathrm{GL}_2(\mathbb{Z})$ orbita formi sa istim svojstvima.

Mi želimo da izračunamo broj $\mathrm{PGL}_2(\mathbb{Q})$ klasa elvivalencije lokalno rešivih celobrojnih binarnih kvartičnih formi ograničene visine bez racionalnog linearnog faktora. Kako bismo to uradili, računaćemo svaku $\mathrm{PGL}_2(\mathbb{Z})$ orbitu $(\mathrm{PGL}_2(\mathbb{Z}) \cdot f)$ sa težinom $\frac{1}{n(f)}$, gde je $n(f)$ broj $\mathrm{PGL}_2(\mathbb{Z})$ orbita u $\mathrm{PGL}_2(\mathbb{Q})$ klasi od f u $V_\mathbb{Z}$. Biće nam dovoljno da računamo broj $\mathrm{PGL}_2(\mathbb{Z})$ orbita lokalno rešivih celobrojnih binarnih kvartičnih formi ograničene visine bez racionalnog linearnog faktora, računajući svaku orbitu $\mathrm{PGL}_2(\mathbb{Z}) \cdot f$ težinom $\frac{1}{m(f)}$ pri čemu je definicija $m(f)$ sledeća:

Definicija 5.4.1. *Globalna težina elementa $f \in V_\mathbb{Z}$ je*

$$m(f) := \sum_{f' \in B(f)} \frac{\#\mathrm{Aut}_\mathbb{Q}(f')}{\#\mathrm{Aut}_\mathbb{Z}(f')} = \sum_{f' \in B(f)} \frac{\#\mathrm{Aut}_\mathbb{Q}(f)}{\#\mathrm{Aut}_\mathbb{Z}(f')},$$

gde su $B(f)$ skup predstavnika dejstva $\mathrm{PGL}_2(\mathbb{Z})$ na $\mathrm{PGL}_2(\mathbb{Q})$ klasu ekvivalencije od f u $V_\mathbb{Z}$, i $\mathrm{Aut}_\mathbb{Q}(f)$ (tj. $\mathrm{Aut}_\mathbb{Z}(f)$) je stabilizator f u $\mathrm{PGL}_2(\mathbb{Q})$ (tj. $\mathrm{PGL}_2(\mathbb{Z})$).

Razlog zašto možemo prebrojavati težinom $\frac{1}{m(f)}$ umesto težinom $\frac{1}{n(f)}$ je sledeći (po lemi 4.5.14):

Sve osim zanemarljivo mnogo $\mathrm{PGL}_2(\mathbb{Z})$ orbita formi sa nenula diskrimunantom i ograničenom visinom imaju trivijalan stabilizator u $\mathrm{PGL}_2(\mathbb{Q})$, zbog čega za sve osim zanemarljivo mnogo $\mathrm{PGL}_2(\mathbb{Z})$ klasa formi nenula diskriminante i ograničene visine važi $m(f) = n(f)$.

Definicija 5.4.2. *Sa $S(F)$ obeležavamo skup svih lokalno rešivih celobrojnih binarnih kvartičnih formi sa invarijantama $2^4 I$ i $2^6 J$, pri čemu $(I, J) \in \mathrm{Inv}(F)$ (gde je $\mathrm{Inv}(F)$ iz definicije 5.1.3).*

Ako pridružimo svakom elementu $f \in S(F)$ težinu $\frac{1}{m(f)}$, tada će broj ireducibilnih $\mathrm{PGL}_2(\mathbb{Z})$ orbita sa visinom manjom od X u $S(F)$ biti asimptotski jednak broju 2-Selmer elemenata (različitih od identiteta) svih eliptičkih krivih visine manje od X u F. Zbog ovoga, mi ćemo računati broj ireducibilnih orbita u $S(F)$ ograničene visine.

Definicija 5.4.3. *Neka je p proizvoljan prost broj, i $f \in V_{\mathbb{Z}_p}$ neka binarna kvartična forma. Tada je*

$$m_p(f) := \sum_{f' \in B_p(f)} \frac{\#\mathrm{Aut}_{\mathbb{Q}_p}(f')}{\#\mathrm{Aut}_{\mathbb{Z}_p}(f')} = \sum_{f' \in B_p(f)} \frac{\#\mathrm{Aut}_{\mathbb{Q}_p}(f)}{\#\mathrm{Aut}_{\mathbb{Z}_p}(f')}$$

lokalna težina elementa f, gde su $B_p(f)$ skup predstavnika dejstva $\mathrm{PGL}_2(\mathbb{Z}_p)$ na $\mathrm{PGL}_2(\mathbb{Q}_p)$ klasu ekvivalencije od f u $V_{\mathbb{Z}_p}$, a $\mathrm{Aut}_{\mathbb{Q}_p}(f)$ (tj. $\mathrm{Aut}_{\mathbb{Z}_p}(f)$) je stabilizator od f u $\mathrm{PGL}_2(\mathbb{Q}_p)$ (tj. $\mathrm{PGL}_2(\mathbb{Z}_p)$).

Definicija 5.4.4. *Za $f \in V_{\mathbb{Z}}$, sa $\mathrm{PGL}_2(\mathbb{Q})_f$ (odnosno sa $\mathrm{PGL}_2(\mathbb{Q}_p)_f$) obeležavamo skup elemenata $\gamma \in \mathrm{PGL}_2(\mathbb{Q})$ (tj. skup elemenata $\gamma \in \mathrm{PGL}_2(\mathbb{Q}_p)$) takav da je $\gamma \cdot f \in V_{\mathbb{Z}}$ (odnosno $\gamma \cdot f \in V_{\mathbb{Z}_p}$).*

Sada imamo prirodno preslikavanje iz $\mathrm{PGL}_2(\mathbb{Q})_f$ u skup $\mathrm{PGL}_2(\mathbb{Z})$ orbita na $\mathrm{PGL}_2(\mathbb{Q})$ klasu ekvivalncije od $f \in V_{\mathbb{Z}}$ dato sa

$$\gamma \mapsto \mathrm{PGL}_2(\mathbb{Z})\gamma \cdot f. \tag{5.2}$$

Dva elementa u $\mathrm{PGL}_2(\mathbb{Q})_f$ se slikaju u istu orbitu akko se slikaju u isti element u prostoru duplih koseta

$$\mathrm{PGL}_2(\mathbb{Z}) \setminus \mathrm{PGL}_2(\mathbb{Q})_f / \mathrm{Aut}_{\mathbb{Q}}(f).$$

Sledeće tvrđenje nam je veoma bitno, jer pomoću njega određujemo globalnu težine forme pomoću lokalnih težina te forme:

Tvrđenje 5.4.5. *Neka je $f \in V_{\mathbb{Z}}$ sa nenula diskriminantom. Tada je*

$$m(f) = \prod_p m_p(f).$$

Kako bismo dokazali tvrđenje, moramo prvo uvesti par pojmova iz [PR]:

Definicija 5.4.6. *Neka su K algebarsko brojno polje, M_K skup svih neekvivalentnih valuacija nad poljem K, i K_v kompletiranje polja K valuacijom $v \in M_K$. Tada sa $\mathbb{A} = \mathbb{A}_K$ obeležavamo skup adela - podskup direktnog proizvoda $\prod_{v \in M_K} K_v$ koji sadrži sve elemente $x = (x_v)$ takve da je $x_v \in \mathcal{O}_v$ za sve osim konačno mnogo $v \in M_K^\infty$ (sa M_K^0 obeležavamo skup nearhimedovskih valuacija na K, a $\mathcal{O}_v$ je valuacioni prsten - $\{a \in K_v : |a|_v \leq 1\}$).*

Primedba 5.4.7. *Skup adela $\mathbb{A}$ je prsten u odnosu na operacije u proizvodu $\prod_{v \in M_K} K_v$, na kome se može definisati topologija čija baza ima skupove oblika*

$$\prod_{v \in S} W_v \times \prod_{v \in M_K \setminus S} \mathcal{O}_v,$$

pri v cemu su - S konačan podskup od M_K koji sadrži M_K^∞ (M_K^∞ je skup arhimedovskih valuacija nad K), i $W_v \subset K_v$ su otvoreni podskupovi za sve $v \in S$.

Definicija 5.4.8. *Za algebarsko brojno polje K, skup*

$$\mathbb{A}(\infty) = \mathbb{A}_K(\infty) = \prod_{v \in M_K^\infty} K_v \times \prod_{v \notin M_K^\infty} \mathcal{O}_v$$

zovemo prsten celobrojnih adela.

Definicija 5.4.9. *Može se pokazati da postoji dijagonalno utapanje $K \to \mathbb{A}_K$, dato sa $x \mapsto (x, x, ...)$ (to se može videti u [PR], odeljak 1.2). Sliku tog utapanja zovemo prsten glavnih adela, koji identifikujemo sa K.*

Definicija 5.4.10. *Za skup adela $\mathbb{A} = \mathbb{A}_K$ nad algebarskim brojnim poljem K i linearnu algebarsku K-grupu G, grupa adela $G_{\mathbb{A}}$ predstavlja skup svih elemenata $g = (g_v) \in \prod_v G_{K_v}$ za koje je $g_v \in G_{\mathcal{O}_v}$ za sve osim konačno mnogo $v \in M_K^0$, pri čemu koristimo sledeće oznake:*

1. *Za algebarski varijetet X nad algebarskim brojnim poljem K i prsten adela $\mathbb{A}$, skup $X_{\mathbb{A}}$ je skup svih n-torki $(a_1, ..., a_n)$ adela koji zadovoljavaju sve jednačine varijeteta X.*
2. *$G_{\mathcal{O}_v} = G \cap GL_n(\mathcal{O}_v)$*

Definicija 5.4.11. *Za skup adela $\mathbb{A}$ nad algebarskim brojnim poljem K, i linearnu algebarsku K-grupu G, podgrupu M_K^∞-celobrojnih adela obeležavamo sa*

$$G_{\mathbb{A}(\infty)} = \prod_{v \in M_K^\infty} G_{K_v} \times \prod_{v \notin M_K^\infty} G_{\mathcal{O}_v}.$$

Definicija 5.4.12. *Za skup adela $\mathbb{A}$ nad algebarskim brojnim poljem i linearnu algebarsku K-grupu G, sa G_K obeležavamo sliku grupe K-racionalnih tačaka u G pri dijagonalnom utapanju u $G_{\mathbb{A}}$, i tu sliku zovemo grupom glavnih adela.*

Sledeću teoremu navodimo bez dokaza (koji se može naći u [PR]):

Teorema 5.4.13. *Neka je $G_{\mathbb{A}}$ grupa adela od linearne grupe G (pri čemu je $\mathbb{A} = \mathbb{A}_K$ prsten adela nad algebarskim brojnim poljem K). Ona se može rastaviti na sledeći način:*

$$G_{\mathbb{A}} = \bigcup_{i=1}^{h} G_{\mathbb{A}(\infty)} x_i G_K,$$

gde su x_i neki elementi grupe $G_{\mathbb{A}}$. Tada najmanje h za koje postoji ovo rastavljanje zovemo klasni broj grupe G, koji obično obeležavamo sa $cl(G)$. O klasnim brojevima i adelima ima više u [PR].

Dokaz tvrđenja 5.4.5: Za preslikavanje (5.2), broj elemenata u $\mathrm{PGL}_2(\mathbb{Z})\backslash\mathrm{PGL}_2(\mathbb{Q})_f$ koji se slikaju u fiksiranu orbitu $\mathrm{PGL}_2(\mathbb{Z})\cdot f'$ je jednak $\#\mathrm{Aut}_{\mathbb{Q}}(f)/\#\mathrm{Aut}_{\mathbb{Z}}(f')$, odakle je

$$\#[\mathrm{PGL}_2(\mathbb{Z}) \setminus \mathrm{PGL}_2(\mathbb{Q})_f] = \sum_{f' \in B(f)} \frac{\#\mathrm{Aut}_{\mathbb{Q}}(f)}{\#\mathrm{Aut}_{\mathbb{Z}}(f')} = m(f).$$

Na sličan način dobijamo da je

$$\#[\mathrm{PGL}_2(\mathbb{Z}_p) \setminus \mathrm{PGL}_2(\mathbb{Q}_p)_f] = \sum_{f' \in B_p(f)} \frac{\#\mathrm{Aut}_{\mathbb{Q}_p}(f)}{\#\mathrm{Aut}_{\mathbb{Z}_p}(f')} = m_p(f).$$

Posmatrajmo sada dijagonalno utapanje

$$\tau : \mathrm{PGL}_2(\mathbb{Z}) \setminus \mathrm{PGL}_2(\mathbb{Q})_f \to \prod_p \mathrm{PGL}_2(\mathbb{Z}_p) \setminus \mathrm{PGL}_2(\mathbb{Q}_p)_f.$$

Iz tvrđenja 5.8.2 (koje ćemo kasnije dokazati) imamo da je

$$\mathrm{PGL}_2(\mathbb{Q}_p)_f = \mathrm{PGL}_2(\mathbb{Z}_p)$$

za svako prosto p koje ne deli diskriminantu od f, pa je proizvod

$$\prod_p \mathrm{PGL}_2(\mathbb{Z}_p) \setminus \mathrm{PGL}_2(\mathbb{Q}_p)_f$$

konačan. Funkcija τ je dakle dobro definisana i 1-1 (ako se $\gamma_1, \gamma_2 \in \mathrm{PGL}_2(\mathbb{Q})_f$ slikaju u isti element sa τ, tada $\gamma_1\gamma_2^{-1}$ pripada $\mathrm{PGL}_2(\mathbb{Q})$ i $\mathrm{PGL}_2(\mathbb{Z}_p)$ za svako p, pa je $\gamma_1\gamma_2^{-1} \in \mathrm{PGL}_2(\mathbb{Z})$, što smo tražili).

Grupa $\mathrm{PGL}_2(\mathbb{Q})$ ima klasni broj 1 (ovo se može videti u [PR], glava 8), pa ako je

$$\sigma \in \prod_p \mathrm{PGL}_2(\mathbb{Z}_p) \setminus \mathrm{PGL}_2(\mathbb{Q}_p)_f,$$

tada postoji $\gamma \in \mathrm{PGL}_2(\mathbb{Q})$ takvo da se γ slika u σ pod τ. Pošto je $\gamma \cdot f \in V_{\mathbb{Z}_p}$ za svako p, tada je $\gamma \cdot f \in V_{\mathbb{Z}}$, pa je $\gamma \in \mathrm{PGL}_2(\mathbb{Q})_f$. Dakle, τ je na. □

Pošto je $m(f) = \prod_p m_p(f)$, to možemo izraziti globalnu gustinu (sa težinom) skupa $S(F)$ u $V_{\mathbb{Z}}$ kao proizvod lokalnih gustina (sa težinom) zatvorenja skupa $S(F)$ u $V_{\mathbb{Z}_p}$. Uvodimo sledeću oznaku:

Definicija 5.4.14. *Sa $S_p(F)$ obeležavamo p-adično zatvorenje $S(F)$ u $V_{\mathbb{Z}_p}$.*

5.5 Lokalne gustine u $S(F)$ posmatrane pomoću lokalnih masa 2-pokrivanja eliptičkih krivih u F

U ovom odeljku ćemo uvesti lokalne p-adične mase, i pomoću njih odrediti p-adičnu gustinu $S_p(F)$.

Navedimo prvo tvrđenje koje će nam biti potrebno u ovom odeljku, čiji dokaz odlažemo do sledeće sekcije:

Tvrđenje 5.5.1. *Neka su p prost broj, i ϕ neprekidna funkcija na $V_{\mathbb{Z}_p}$. Tada je*

$$\int_{V_{\mathbb{Z}_p}} \phi(f)df = \left|\frac{1}{27}\right|_p \int_{\substack{(I,J)\in\mathbb{Z}_p^2 \\ \Delta(I,J)\neq 0}} \left(\sum_{f \in \frac{V_{\mathbb{Z}_p}(I,J)}{\mathrm{PGL}_2(\mathbb{Z}_p)}} \frac{1}{\#\mathrm{Aut}_{\mathbb{Z}_p}(f)} \int_{g\in\mathrm{PGL}_2(\mathbb{Z}_p)} \phi(g\cdot f)w(g) \right) dIdJ,$$

gde je $\frac{V_{\mathbb{Z}_p}(I,J)}{\mathrm{PGL}_2(\mathbb{Z}_p)}$ skup predstavnika dejstva $\mathrm{PGL}_2(\mathbb{Z}_p)$ na elemente u $V_{\mathbb{Z}_p}$ sa invarijantama I i J.

Ako dodatno vrednosti $\phi(f)$ računamo težinom $\frac{1}{m_p(f)}$, prethodna jednakost ima sledeći oblik:

Posledica 5.5.2. *Neka je p prost broj, i ϕ neprekidna $\mathrm{PGL}_2(\mathbb{Q}_p)$-invarijantna funkcija na $V_{\mathbb{Z}_p}$ takva da svako $f \in V_{\mathbb{Z}_p}$ u nosaču funkcije ϕ ima diskriminantu različitu od nule, je rešivo i zadovoljava $2^4 \cdot 3 \mid I(f)$ i $2^6 \cdot 3^3 \mid J(f)$. Tada:*

$$\int_{V_{\mathbb{Z}_p}} \frac{\phi(f)}{m_p(f)} df = \left|\frac{1}{27}\right|_p \mathrm{Vol}(\mathrm{PGL}_2(\mathbb{Z}_p)) \int_{\substack{(I,J)\in\mathbb{Z}_p^2 \\ \Delta(I,J)\neq 0}} \frac{1}{\#E[2](\mathbb{Q}_p)} \left(\sum_{\sigma \in E(\mathbb{Q}_p)/2E(\mathbb{Q}_p)} \phi(f_\sigma) \right) dI dJ,$$

gde je f_σ bilo koji element u $V_{\mathbb{Z}_p}$ koji odgovara σ po teoremi 5.3.2.

Dokaz: Tvrđenje 5.5.1 nam daje

$$\int_{V_{\mathbb{Z}_p}} \frac{\phi(f)}{m_p(f)} df = \left|\frac{1}{27}\right|_p \int_{\substack{(I,J)\in\mathbb{Z}_p^2 \\ \Delta(I,J)\neq 0}} \left(\sum_{f \in \frac{V_{\mathbb{Z}_p}(I,J)}{\mathrm{PGL}_2(\mathbb{Z}_p)}} \frac{1}{\#\mathrm{Aut}_{\mathbb{Z}_p}(f)} \int_{g\in \mathrm{PGL}_2(\mathbb{Z}_p)} \frac{\phi(g\cdot f)}{m_p(g\cdot f)} dg \right) dI dJ =$$

$$= \left|\frac{1}{27}\right|_p \mathrm{Vol}(\mathrm{PGL}_2(\mathbb{Z}_p)) \int_{\substack{(I,J)\in\mathbb{Z}_p^2 \\ \Delta(I,J)\neq 0}} \left(\sum_{f \in \frac{V_{\mathbb{Z}_p}(I,J)}{\mathrm{PGL}_2(\mathbb{Z}_p)}} \frac{\phi(f)}{m_p(f)\#\mathrm{Aut}_{\mathbb{Z}_p}(f)} \right) dI dJ,$$

pošto su ϕ i m_p invarijantni u odnosu na $\mathrm{PGL}_2(\mathbb{Z}_p)$. Procenimo sada sumu u integralu u prethodnoj jednakosti. Za $f \in V_{\mathbb{Z}_p}$, neka je $\{f_1, f_2, ..., f_k\}$ skup svih elemenata u $\frac{V_{\mathbb{Z}_p}(I,J)}{\mathrm{PGL}_2(\mathbb{Z}_p)}$ koji su $\mathrm{PGL}_2(\mathbb{Z}_p)$ ekvivalentni sa f. Tada iz $\mathrm{PGL}_2(\mathbb{Q}_p)$ invarijantnosti ϕ i m_p dobijamo

$$\sum_{i=1}^{k} \frac{\phi(f_i)}{m_p(f_i)\#\mathrm{Aut}_{\mathbb{Z}_p}(f_i)} = \frac{\phi(f)}{m_p(f)} \sum_{i=1}^{k} \frac{1}{\#\mathrm{Aut}_{\mathbb{Z}_p}(f_i)} =$$

$$= \phi(f) \left(\sum_{i=1}^{k} \frac{\#\mathrm{Aut}_{\mathbb{Q}_p}(f)}{\#\mathrm{Aut}_{\mathbb{Z}_p}(f_i)} \right)^{-1} \sum_{i=1}^{k} \frac{1}{\#\mathrm{Aut}_{\mathbb{Z}_p}(f_i)} = \frac{\phi(f)}{\#\mathrm{Aut}_{\mathbb{Q}_p}(f)}$$

Dakle, imamo

$$\int_{V_{\mathbb{Z}_p}} \frac{\phi(f)}{m_p(f)} df = \left| \frac{1}{27} \right|_p \mathrm{Vol}(\mathrm{PGL}_2(\mathbb{Z}_p)) \int_{\substack{(I,J)\in\mathbb{Z}_p^2 \\ \Delta(I,J)\neq 0}} \left(\sum_{f \in \frac{V_{\mathbb{Z}_p}(I,J)}{\mathrm{PGL}_2(\mathbb{Q}_p)}} \frac{\phi(f)}{\#\mathrm{Aut}_{\mathbb{Q}_p}(f)} \right) dI dJ, \tag{5.3}$$

gde je $\frac{V_{\mathbb{Z}_p}(I,J)}{\mathrm{PGL}_2(\mathbb{Q}_p)}$ skup koji se sastoji od po jednog elementa svake $\mathrm{PGL}_2(\mathbb{Q})$ klase ekvivalencije u $V_{\mathbb{Z}_p}$. Teorema 5.3.2 i lema 5.3.4 nam kažu da su rešivi elementi $\frac{V_{\mathbb{Z}_p}(I,J)}{\mathrm{PGL}_2(\mathbb{Q}_p)}$ u bijekciji sa elementima $E(\mathbb{Q}_p)/2E(\mathbb{Q}_p)$. Teorema 5.3.2 nam dalje kaže da je

$$\mathrm{Aut}_{\mathbb{Q}_p}(f) \cong E^{I(f),J(f)}[2](\mathbb{Q}_p),$$

pa ova posledica sledi iz jednakosti (5.3). □

Definicija 5.5.3. *Za prost broj p i familiju eliptičkih krivih F, lokalna p-adična V-masa familije F je*

$$M_p^V(F) := \int_{(I,J)\in \mathrm{Inv}_p(F)} \frac{\#(E^{I,J}(\mathbb{Q}_p)/2E^{I,J}(\mathbb{Q}_p))}{\#E^{I,J}(\mathbb{Q}_p)[2]} dI dJ.$$

Ako zamenimo ϕ sa 1, i primenimo prethodnu definiciju, onda dobijamo sledeću teoremu:

Tvrđenje 5.5.4. *Važi sledeće:*

$$\int_{S_p(F)} \frac{1}{m_p(f)} df = \left| \frac{2^{10}}{27} \right|_p \cdot \mathrm{Vol}(\mathrm{PGL}_2(\mathbb{Z}_p)) \cdot M_p^V(F).$$

Dokaz: Skup $S_p(F)$ se sastoji od svih $\mathbb{Q}_p$ rešivih binarnih kvartičnih formi sa invarijantama $2^4 I$ i $2^6 J$, gde su $(I, J) \in \mathrm{Inv}_p(F)$. Pošto je $E^{I,J}(\mathbb{Q}_p)$ izomorfno sa $E^{2^4 I, 2^6 J}(\mathbb{Q}_p)$, i zapremina skupa

$$\left\{2^4 I, 2^6 J \mid (I, J) \in \mathrm{Inv}(F)\right\}$$

je jedaka $|2^{10}|_p \cdot \mathrm{Vol}(\mathrm{Inv}_p(F))$, to ovo tvrđenje sledi iz posledice 5.5.2. □

5.6 Promena mere

U ovom odeljku ćemo dokazati tvrđenja koja smo koristili ranije u ovom radu, 4.4.3 i 5.5.1.

Tvrđenje 5.6.1. *Neka su w, dv i $dIdJ$ definisani kao u tvrđenju 4.4.3. Neka je $R \subset \mathbb{C}^2$ otvoren podskup, i $s : R \to V_{\mathbb{C}}$ neprekidna funkcija ($V_{\mathbb{C}}$ je skup binarnih kvartičnih formi nad $\mathbb{C}$) takva da $(\forall (I, J) \in R)$ binarna kvartična forma*

$$s_{I,J} := s(I, J)$$

ima invarijante jednake I i J. Tada postoji racionalan broj $\mathcal{J} \neq 0$ takav da je za svaku merljivu funkciju $\phi : V_{\mathbb{C}} \to \mathbb{R}$ sledeće tačno:

$$\int_{v \in \mathrm{PGL}_2(\mathbb{C}) \cdot s(R)} \phi(v) dv = |\mathcal{J}| \int_R \int_{\mathrm{PGL}_2(\mathbb{C})} \phi(g \cdot s_{I,J}) w(g) dI dJ,$$

gde $\mathrm{PGL}_2(\mathbb{C}) \cdot s(R)$ posmatramo kao multiskup.

Dokaz: Prvo ćemo posmatrati poseban slučaj kada je funkcija s lokalno analitička. Tada znamo da je

$$\int_{v \in \mathrm{PGL}_2(\mathbb{C}) \cdot s(R)} \phi(v) dv = \int_{(I,J) \in \mathbb{C}^2} \int_{\mathrm{PGL}_2(\mathbb{C})} \mathcal{J}_s(g, I, J) \phi(g \cdot s_{I,J}) w(g) dI dJ, \qquad (5.4)$$

gde je $\mathcal{J}_s(g, I, J)$ Jakobijan smene promenljivih preslikavanjem

$$\psi_s : \mathrm{PGL}_2(\mathbb{C}) \times R \to V_{\mathbb{C}}$$

$$(g, (I, J)) \mapsto g \cdot s_{I,J}.$$

Uočimo, $\mathcal{J}_s(g, I, J)$ je neprekidno u g, I i J. Sada ćemo dokazati u nekoliko koraka da $\mathcal{J}_s(g, I, J)$ ne zavisi od g, I, J i s:

1. $\mathcal{J}_s(g, I, J)$ **ne zavisi od** $g \in \mathrm{PGL}_2(\mathbb{C})$**:**
   Pretpotstavimo da postoje $(I, J) \in R$ i $g_1, g_2 \in \mathrm{PGL}_2(\mathbb{C})$ takvi da je

   $$\mathcal{J}_s(g_1, I, J) \neq \mathcal{J}_s(g_2, I, J).$$

   Tada iz neprekidnosti i činjenice da je $w(g)$ $\mathrm{PGL}_2(\mathbb{C})$ invarijantno sledi da postoji otvoren skup $B_1 \subset \mathrm{PGL}_2(\mathbb{C})$ koji sadrži g_1 takav da je

   $$\int_{B_1} \mathcal{J}_s(g, I, J)w(g) \neq \int_{g_2 g_1^{-1} B_1} \mathcal{J}_s(g, I, J)w(g).$$

   Iz neprekidnosti takođe imamo da postoji otvoren skup $N \subset R$ koji sadrži (I, J) takav da je

   $$\int_{(I,J)\in N} \int_{B_1} \mathcal{J}_s(g, I, J)w(g)dIdJ \neq \int_{(I,J)\in N} \int_{g_2 g_1^{-1} B_1} \mathcal{J}_s(g, I, J)w(g)dIdJ. \tag{5.5}$$

   Iz jednakosti (5.4) sledi da je leva strana nejednakosti (5.5) jednaka meri $B_1 \cdot N$, dok je desna strana jednaka meri $g_2 g_1^{-1} B_1 \cdot N$. Pošto preslikavanje $g_2 g_1^{-1} : V_{\mathbb{C}} \to V_{\mathbb{C}}$ predstavlja dejstvo nekim elementom iz $\mathrm{SL}(V_{\mathbb{C}})$, to imamo kontradikciju. Dakle, $\mathcal{J}_s(g, I, J)$ ne zavisi od g.

2. $\mathcal{J}_s(I,J) := \mathcal{J}_s(g,I,J)$ **ne zavisi od** s**:**

Neka je $s' : R \to V_{\mathbb{C}}$ neka druga lokalno analitička funkcija takva da su invarijante od $s'_{I,J} := s'(I,J)$ jednake I i J za svako $(I,J) \in R$. Pošto su $\mathrm{PGL}_2(\mathbb{C}) \cdot s(R)$ i $\mathrm{PGL}_2(\mathbb{C}) \cdot s'(R)$ isti multiskupovi, imamo da je

$$\int_{v \in \mathrm{PGL}_2(\mathbb{C}) \cdot s'(R)} \phi(v)dv = \int_{v \in \mathrm{PGL}_2(\mathbb{C}) \cdot s(R)} \phi(v)dv =$$

$$= \int_{(I,J) \in \mathbb{C}^2} \int_{\mathrm{PGL}_2(\mathbb{C})} \mathcal{J}_s(I,J)\phi(g \cdot s_{I,J})w(g)dIdJ.$$

Izaberimo $g_{I,J} \in \mathrm{PGL}_2(\mathbb{C})$ za svako $(I,J) \in \mathbb{C}^2$ takvo da je $g_{I,J} \cdot s_{I,J} = s'_{I,J}$. Pošto je $w(g)$ i leva i desna Haarova mera, imamo da je

$$\int_{(I,J) \in \mathbb{C}^2} \int_{g \in \mathrm{PGL}_2(\mathbb{C})} \mathcal{J}_s(I,J)\phi(g \cdot s_{I,J})w(g)dIdJ =$$

$$= \int_{\mathbb{C}^2} \int_{\mathrm{PGL}_2(\mathbb{C})} \mathcal{J}_s(I,J)\phi(gg_{I,J} \cdot s_{I,J})w(g)dIdJ =$$

$$= \int_{\mathbb{C}^2} \int_{\mathrm{PGL}_2(\mathbb{C})} \mathcal{J}_s(g,I,J)\phi(g \cdot s'_{I,J})w(g)dIdJ.$$

Odavde sledi:

$$\int_{v \in \mathrm{PGL}_2(\mathbb{C}) \cdot s'(R)} \phi(v)dv = \int_{(I,J) \in \mathbb{C}^2} \int_{\mathrm{PGL}_2(\mathbb{C})} \mathcal{J}_s(I,J)\phi(g \cdot s'_{I,J})w(g)dIdJ.$$

Dakle, $\mathcal{J}_{s'}(I,J) = \mathcal{J}_s(I,J)$.

3. $\mathcal{J}(I,J) := \mathcal{J}_s(I,J)$ **je nenula polinom po** I **i** J **sa racionalnim koeficijentima:**

   Pošto $\mathcal{J}(I,J)$ ne zavisi od s, možemo izabrati s takvo da su koeficijenti od $s_{I,J}$ racionalni polinomi od I i J, na primer:

$$s_{I,J} := x^3y - \frac{I}{3}xy^3 - \frac{J}{27}y^4.$$

   Pošto je $\mathcal{J}(I,J)$ determinanta od 5×5 matrice čiji su elementi polinomi od koeficijanata od $s_{I,J}$, to je $\mathcal{J}(I,J)$ racionalan polinom u I i J. Kako je $\psi_s(\mathrm{PGL}_2(\mathbb{C}), \mathbb{C}^2)$ skup najveće mere u $V_{\mathbb{C}}$, to je $\mathcal{J}(I,J)$ nenula polinom.

4. $\mathcal{J} := \mathcal{J}(I,J)$ **je nenula racionalna konstanta:**

   Neka je $G_0 \subset \mathrm{PGL}_2(\mathbb{C})$ ograničen podskup mere 1, i neka je R_0 proizvoljan ograničeni merljiv skup u $\mathbb{C}^2$. Uvodimo oznaku:

$$B = B(R_0) := \{s_{I,J} : (I,J) \in R_0\}.$$

   Tada je

$$\int_{G_0 \cdot B} dv = \int_{(I,J)\in R_0} \mathcal{J}(I,J)dIdJ, \tag{5.6}$$

   gde $G_0 \cdot B$ gledamo kao multiskup. Iz jednakosti (5.6) sledi da za bilo koje $c \in \mathbb{C}$ važi

$$\int_{cG_0 \cdot B} dv = |c|^5 \int_{G_0 \cdot B} dv = |c|^5 \int_{(I,J)\in R_0} \mathcal{J}(I,J)dIdJ,$$

   jer je $V_{\mathbb{C}}$ dimenzije 5. Sa druge strane imamo sledeću procenu:

$$\int_{cG_0 \cdot B} dv = \int_{G_0 \cdot cB} dv = \int_{(c^{-2}I, c^{-3}J) \in R_0} \mathcal{J}(I,J) dI dJ =$$

$$= \int_{(I',J') \in R_0} \mathcal{J}(c^2 I', c^3 J') |c^2| dI' |c^3| dJ',$$

jer su I i J homogeni polinomi stepena 2 i 3. Dakle:

$$\int_{(I,J) \in R_0} \mathcal{J}(I,J) dI dJ = \int_{(I,J) \in R_0} \mathcal{J}(c^2 I, c^3 J) dI dJ.$$

Kako je $\mathcal{J}(I,J)$ nenula polinom po I i J, i pošto je gornja jednakost tačna za sve R_0 i c, to zaključujemo da je $\mathcal{J}(I,J)$ nenula racionalna konstanta.

Konačno, po Stone-Weierstrass teoremi, svaka neprekidna funkcija se može lokalno, uniformno aproksimirati sa lokalno analitičkim funkcijama, što je kraj dokaza. □

Iz ovog tvrđenja sledi tvrđenje 4.4.3 (samo što umesto konstante 1/27 imamo $\mathcal{J}$), zajedno sa:

Tvrđenje 5.6.2. *Neka su $K \in \{\mathbb{R}, \mathbb{C}, \mathbb{Z}_p \mid p \text{ je prost broj}\}$, dv standardna aditivna mera na V_K (prostor svih binranih kvartičnih formi sa koeficijentima u K), R otvoren podskup od K^2, i $s : R \to V_K$ neprekidna funkcija takva da su invarijante od $s_{I,J} := s(I,J)$ jednake I i J. Tada postoji racionalna nenula konstanta $\mathcal{J}$ takva da je za svaku merljivu funkciju ϕ na V_K sledeće tačno:*

$$\int_{v \in \mathrm{PGL}_2(K) \cdot s(R)} \phi(v) dv = |\mathcal{J}| \int_R \int_{\mathrm{PGL}_2(K)} \phi(g \cdot s_{I,J}) w(g) dI dJ,$$

gde su $\mathrm{PGL}_2(K) \cdot s(R)$ multiskup, w je mera definisana u prethodnoj glavi, i $|\mathcal{J}|$ je apsolutna vrednost $\mathcal{J}$ kao elementa K.

Sada ćemo pokazati sledeće tvrđenje:

Tvrđenje 5.6.3. *Neka su* $K \in \{\mathbb{R}, \mathbb{C}, \mathbb{Z}_p : p \text{ je prosto }\}$, *i* ϕ *merljiva funkcija na* V_K. *Tada postoji racionalna konstanta* $\mathcal{J}$ *koja ne zavisi od* K *i* ϕ *takva da je*

$$\int_{V_K} \phi(f)df = |\mathcal{J}| \int_{\substack{(I,J)\in K^2 \\ \Delta(I,J)\neq 0}} \left(\sum_{f \in \frac{V_K(I,J)}{\mathrm{PGL}_2(K)}} \frac{1}{\#\mathrm{Aut}_K(f)} \int_{g\in \mathrm{PGL}_2(K)} \phi(g\cdot f)w(g) \right) dIdJ,$$

gde je $\frac{V_K(I,J)}{\mathrm{PGL}_2(K)}$ *skup predstavnika dejstva* $\mathrm{PGL}_2(K)$ *na elemente* V_K *sa invarijantama* I *i* J.

Dokaz: Znamo da je svaka neprekidna funkcija na $V_{\mathbb{Z}_p}$ lokalno konstantna van nekog skupa proizvoljno male mere, pa ćemo smatrati da je funkcija ϕ lokalno konstantna. Biće nam dovoljno da pokažemo da tvrđenje važi lokalno, tj. da za svaki element $f \in V_{\mathbb{Z}_p}$ (možemo smatrati da je $\Delta(f) \neq 0$) postoji okolina B_f od f takva da, ako je ϕ karakteristična funkcija od B_f, da je onda jednakost u tvrđenju 5.5.1 tačna.

Uzmimo sada $f \in V_{\mathbb{Z}_p} \setminus \{\Delta = 0\}$, i konstruišimo B_f. Fiksirajmo $P \subset V_{\mathbb{Z}}$, neku dvodimenzionalnu ravan koja prolazi kroz f definisanu sa linearnim jednačinama. Tada postoji okolina $P_0 \subset P$ od f takva da:

1. Invarijante od bilo koja dva elementa u P_0 su različite u $\mathbb{Z}_p^2$;

2. Veličine stabilizatora u $\mathrm{PGL}_2(\mathbb{Z}_p)$ bilo koja dva elementa u P_0 su jednake.

Prva tvrdnja sledi iz teoreme o inverznoj funkciji u lokalnim poljima ([S], tvrđenje 4.3) primenjenoj na uobičajeno preslikavanje koje ide iz $\mathrm{PGL}_2(\mathbb{Z}_p) \times P$ u $V_{\mathbb{Z}_p}$. Sada uzimamo da je B_f jednako $\mathrm{PGL}_2(\mathbb{Z}_p) \cdot P_0$ kao skup (ne kao multiskup). Pošto je ravan P data linearnim jednačinama nad $\mathbb{Q}$, tvrđenje 5.6.1 nam daje

$$\#\mathrm{Aut}_{\mathbb{Z}_p}(f) \cdot \mathrm{Vol}(B_f) = |\mathcal{J}|_p \cdot \mathrm{Vol}(\mathrm{PGL}_2(\mathbb{Z}_p)) \cdot \int_{\mathrm{Inv}_p(P_0)} dIdJ,$$

gde je $\mathrm{Inv}_p(P_0)$ skup svih $(I, J) \in \mathbb{Z}_p^2$ koji se pojavljuju kao invarijante nekog elmenta u P_0. Dakle, imamo ne samo ovo tvrđenje, već smo dokazali i 5.5.1, samo što umesto $1/27$ imamo $\mathcal{J}$. □

Kako bismo završili dokaz tvrđenja 5.5.1, moramo pokazati da je apsolutna vrednost $\mathcal{J}$ jednaka $1/27$. Kako bismo to uradili, mi ćemo izračunati $|\mathcal{J}|_p$ za svako prosto p. Naime, za svako prosto p ćemo izabrati odgovarajući skup $S \subset V_{\mathbb{Z}_p}$, i onda iskoristiti tvrđenje 5.6.2 da izrazimo $|\mathcal{J}|_p$ preko mere skupa S. Zatim posmatramo redukciju S modulo p, koju označavamo sa $\overline{S}$, i određujemo njegovu kardinalnost kako bismo izračunali meru S, a samim tim i vrednost $|\mathcal{J}|$. Zbog ovoga dokazujemo sledeće tvrđenje:

Tvrđenje 5.6.4. *Neka su p prost broj, $S \subset V_{\mathbb{Z}_p}$ skup definisan uslovima kongruencije modulo p, i $\overline{S} \subset V_{\mathbb{F}_p}$ redukcija S modulo p. Ako pretpotstavimo da je $S = \pi^{-1}(\pi(S))$ ($\pi : V_{\mathbb{Z}_p} \to \mathbb{Z}_p^2$ je definisano sa $\pi(f) = (I, J)$, gde su $f \in V_{\mathbb{Z}_p}$, i I i J su invarijante od f), onda imamo da je*

$$|\mathcal{J}|_p = \frac{\#\mathrm{PGL}_2(\mathbb{F}_p) \cdot \left(\sum_{f \in \mathrm{PGL}_2(\mathbb{F}_p) \setminus S} \frac{1}{\#\mathrm{Aut}_{\mathbb{Z}_p}(f)} \right)}{p^{\dim V} \cdot \mathrm{Vol}(\mathrm{PGL}_2(\mathbb{Z}_p)) \cdot \left(\int_{(I,J) \in \pi(S)} \sum_{f \in \frac{V_{\mathbb{Z}_p}(I,J)}{\mathrm{PGL}_2(\mathbb{Z}_p)}} \frac{1}{\#\mathrm{Aut}_{\mathbb{Z}_p}(f)} dI dJ \right)}.$$

Dokaz: Ako u tvrđenju 5.6.3 umesto ϕ stavimo karakterističnu funkciju za S, dobijamo

$$\mathrm{Vol}(S) = |\mathcal{J}|_p \, \mathrm{Vol}(\mathrm{PGL}_2(\mathbb{Z}_p)) \int_{(I,J) \in \pi(S)} \left(\sum_{f \in \frac{V_{\mathbb{Z}_p}(I,J)}{\mathrm{PGL}_2(\mathbb{Z}_p)}} \frac{1}{\#\mathrm{Aut}_{\mathbb{Z}_p}} \right) dI dJ.$$

Pošto je S definisano uslovima kongruencije modulo p, i kako je $\overline{S}$ invarijantno u odnosu na $\mathrm{PGL}_2(\mathbb{F}_p)$ (jer je S invarijantno u odnosu na $\mathrm{PGL}_2(\mathbb{Z}_p)$), imamo da je

$$\mathrm{Vol}(S) = \frac{\#\overline{S}}{p^{\dim V}} = \frac{1}{p^{\dim V}} \#\mathrm{PGL}_2(\mathbb{F}_p) \cdot \left(\sum_{f \in \mathrm{PGL}_2(\mathbb{F}_p) \setminus S} \frac{1}{\#\mathrm{Aut}_{\mathbb{F}_p}(f)} \right),$$

gde poslednja jednakost sledi iz formule orbita-stabilizator. Ove dve jednakosti nam daju tvrđenje. □

Mi ćemo uzeti da je skup S skup binarnih kvartičnih formi sa nekim fiksiranim invarijantama (I, J) modulo p. Kako bismo procenili desnu stranu jednakosti u tvrđenju 5.6.4, koristićemo sledeću lemu:

Lema 5.6.5. *Neka su p prost broj i $(I, J) \in \mathbb{Z}_p^2$ element u slici π takav da $p^2 \nmid \Delta(I, J)$. Tada je*

$$\sum_{f \in \frac{V_{\mathbb{Z}_p}(I,J)}{\mathrm{PGL}_2(\mathbb{Z}_p)}} \frac{1}{\#\mathrm{Aut}_{\mathbb{Z}_p}(f)} = 1.$$

Neka su sada $p \neq 3$ prost broj i $(I, J) \in \mathbb{F}_p^2$ element takav da je $\Delta(I, J) \neq 0$. Tada je

$$\sum_{f \in \frac{V_{\mathbb{F}_p}(I,J)}{\mathrm{PGL}_2(\mathbb{F}_p)}} \frac{1}{\#\mathrm{Aut}_{\mathbb{F}_p}(f)} = 1.$$

Dokaz: Pošto $p^2 \nmid \Delta(I, J)$, teorema 5.3.2 i tvrđenje 5.8.2 (koje ćemo dokazati kasnije) nam daju

$$\mathrm{Aut}_{\mathbb{Z}_p}(f) = \mathrm{Aut}_{\mathbb{Q}_p}(f) = E^{I,J}(\mathbb{Q}_p)[2].$$

Za neparan prost broj p teorema (5.3.2) i [CF], leme 3 i 4 nam kažu da je broj $\mathrm{PGL}_2(\mathbb{Q}_p)$ klasa ekvivalencija u $V_{\mathbb{Z}_p}$ sa invarijantama I i J jednak $\#(E^{I,J}(\mathbb{Q}_p)/2E^{I,J}(\mathbb{Q}_p))$, dok nam [CS], sekcija 6, kaže da je broj $\mathrm{PGL}_2(\mathbb{Q}_2)$ klasa ekvivalencije u $V_{\mathbb{Z}_2}$ sa invarijantama I i J jednak

$$\frac{1}{2}\#(E^{I,J}(\mathbb{Q}_2)/2E^{I,J}(\mathbb{Q}_2)).$$

Prvi deo ove leme sada sledi iz leme 5.8.6.

Za $p \geq 5$, drugi deo leme sledi iz teoreme 5.3.2 (samo što se K zameni sa $\mathbb{F}_p$) i činjenice da je

$$\#\left(E^{I,J}(\mathbb{F}_p)/2E^{I,J}(\mathbb{F}_p)\right)/\#E^{I,J}(\mathbb{F}_p)[2] = 1.$$

Za $p = 2$ imamo konačan račun. □

Sada ćemo izabrati skup $S \subset V_{\mathbb{Z}_p}$ za svaki prost broj p. Za $p \neq 3$, neka je $(I_0, J_0) \in \mathbb{F}_p^2$ fiksirani element takav da je $\Delta(I_0, J_0) \neq 0$. Tada uzimamo da je S skup svih $f \in V_{\mathbb{Z}_p}$ takvih da je redukcija $(I(f), J(f))$ modulo p jednaka (I_0, J_0). Tada nam tvrđenje 5.6.4 i lema 5.6.5 daju

$$|\mathcal{J}|_p = \frac{\#\mathrm{PGL}_2(\mathbb{F}_p)}{p^5 \mathrm{Vol}(\mathrm{PGL}_2(\mathbb{Z}_p))(1/p^2)} = 1.$$

Za $p = 3$, definicija Δ u terminima I i J zahteva deljenje sa 27, pa ako uzmemo neke vrednosti (I, J) modulo 3, to ne znači da je $3 \nmid \Delta(I, J)$. Dakle, S ćemo uzeti da je određeno uslovima na invarijantama (I, J) modulo nekog stepena broja 3. Neka je zato S skup svih $f \in V_{\mathbb{Z}_3}$ takvih da je $I(f) \equiv 3$ modulo 9. Dokaz teoreme 4.5.15 nam kaže da ako je $f \in V_{\mathbb{Z}_3}$ i $I(f) \equiv 0$ modulo 3, da je jedini uslov na J upravo $J(f) \equiv 0$ modulo 27. Dakle, ako je

$$f(x, y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4 \in S,$$

onda $\Delta(f) \not\equiv 0$ modulo 27, i možemo primeniti prvi deo leme (5.6.5). Dalje, primetimo da je $I(f) \equiv 3$ modulo 9 samo kada je $c \equiv_3 0$ i $ae - bd \equiv_3 1$. Označimo sa $\overline{a}, \overline{b}, \overline{c}, \overline{d}$, i $\overline{e}$ redukcije modulo 3 od a, b, c, d i e. Tada je $f \in S$ akko $\overline{c} = 0$ i $\overline{ae} - \overline{bd} = 1$. Postoje 24 vrednosti za $(\overline{a}, \overline{b}, \overline{c}, \overline{d}, \overline{e}) \in \mathbb{F}_p^2$ koje zadovaljavaju ova dva uslova. Dakle:

$$|\mathcal{J}|_3 = \frac{24}{3^5 \mathrm{Vol}(\mathrm{PGL}_2(\mathbb{Z}_p))\mathrm{Vol}(\pi(S))} = \frac{24}{3^5(1 - 1/3^2)(1/3^5)} = 27.$$

Ovo je kraj dokaza tvrđenja (5.5.1). □

5.7 Broj eliptičkih krivih ograničene visine u velikoj familiji

Neka je F velika familija eliptičkih krivih. U ovom odeljku ćemo odrediti asimptotsko ponašanje broja eliptičkih krivih ograničene visine u familija F.

Pošto je svaka eliptička kriva određena invarijantama I i J, tražićemo broj parova $(I, J) \in \mathrm{Inv}(F)$ visine manje od X. Uvedimo sledeći region u $\mathbb{R}^2$:

Definicija 5.7.1. *Za realan broj $X > 0$, neka je*

$$R_X^{\pm} := \left\{(i, j) \in \mathbb{R}^2 : |i| < X^{1/3}, |j| < 2X^{1/2}, \pm(4i^3 - j^2) > 0\right\}$$

Primenom Davenportove teoreme 1.6.6 možemo videti da je broj parova $(I, J) \in \mathbb{Z}^2$ sa $H(I, J) < X$ i $4I^3 - J^2 > 0$ (odnosno $H(I, J) < X$ i $4I^3 - J^2 < 0$) jednak zapremini R_X^+ (odnosno R_X^-), sa greškom $O(X^{1/2})$.

Definicija 5.7.2. *Neka je $S \subset \mathbb{Z}^2$ proizvoljno, i $X > 0$ neki realan broj. Označavamo:*

$$N(S; X) := \#\{(I, J) \in S : H(I, J) < X, \Delta(I, J) \neq 0\}.$$

Skup $\mathrm{Inv}(F) \subset \mathbb{Z}^2$ je definisan uslovima kongruencije, kojih može biti besko načno mnogo, zbog čega nam treba sledeće tvrđenje kako bismo odredili asimptotsko ponašanje za $N(\mathrm{Inv}(F); X)$.

Tvrđenje 5.7.3. *Broj eliptičkih krivih nad $\mathbb{Q}$ sa visinom manjom od X i diskriminantama deljivim sa p^2 je $O(X^{5/6}/p^{3/2})$, i implicirana konstanta ne zavisi od p.*

Dokaz: Neka je $U_{\mathbb{Z}}$ skup svih celobrojnih binarnih kubičnih formi. Skup $\mathrm{GL}_2(\mathbb{Z})$ deluje na $U_{\mathbb{Z}}$ kao i inače. Neka su ψ_1 utapanje skupa $\{x^3 + Ax + B : A, B \in \mathbb{Z}\}$ u skup $U_{\mathbb{Z}}$ sa

$$\psi_1(X^3 + Ax + B) = x^3 + Axy^2 + by^3,$$

$\psi_2 : U_{\mathbb{Z}} \to \mathrm{GL}_2(\mathbb{Z}) \setminus U_{\mathbb{Z}}$ količničko preslikavanje, i $\psi = \psi_2 \circ \psi_1$.

Pokazaćemo da za svaki element u $\mathrm{GL}_2(\mathbb{Z}) \setminus U_{\mathbb{Z}}$ postoji najviše 12 različitih elemenata koji se sa ψ slikaju u njega. Neka je $v \in U_{\mathbb{Z}}$, i neka je $\psi(f) = [v]$. Tada postoji $\gamma \in \mathrm{GL}_2(\mathbb{Z})$ takvo da je $\gamma \cdot v = \psi_1(f)$. Tada je $v((1,0)\cdot\gamma) = 1$. Iz [D3] i [E2] sledi da postoji najviše 12 rešenja $(a,b) \in \mathbb{Z}^2$ za jednačinu $v(a,b) = 1$, a pošto svaki element koji se sa ψ slika u v daje različito rešenje ove jednačine, to postoji najviše 12 elemenata koji se sa ψ slikaju u v. Iz [DH], tvrđenje 1, vidimo da je broj $\mathrm{GL}_2(\mathbb{Z})$ orbita na $U_{\mathbb{Z}}$ sa diskriminantom deljivom sa p^2 ograničen sa $O(X/p^2)$, zbog čega je broj eliptičkih krivih visine manje od X i diskriminante deljive sa p^2 ograničen sa $O(X/p^2)$. Posmatraćemo dva slučaja:

Eliptička kriva $E_{A,B} : y^2 = x^3 + Ax + B$ ima aditivnu redukciju u prostom broju $p > 3$

Ovo se dešava akko je $p \mid A$ i $p \mid B$ (videti [S3], odeljak VII.5). Broj ovakvih parova $(A,B) \in \mathbb{Z}^2$ sa visinom manjom od X (obeležimo ovaj broj sa $f(X,p)$) je ograničen sa

$$O(X^{5/6}/p^2 + X^{1/2}/p + 1),$$

pa je broj eliptičkih krivih sa aditivnom redukcijom u p i visinom manjom od X ograničen sa $O(X/p^2)$ i sa $O(X^{5/6}/p^2 + X^{1/2}/p + 1)$. Dakle postoje konstante C_1 i C_2, i realni brojevi X_1 i X_2 takvi da je $|f(X,p)| \le C_1 \frac{X}{p^2}$ za $X > X_1$ i $|f(X,p)| \le C_2 \left(\frac{X^{5/6}}{p^2} + \frac{X^{1/2}}{p} + 1 \right)$ za $X > X_2$. Kombinovanjem ova dva rezultata dobijamo ograničenje od $O(X^{5/6}/p^{5/3})$:

Naime, znamo da je $\frac{\sqrt[3]{X}}{p} \le \frac{\sqrt{X}}{p}$, pa imamo tri mogućnosti:

1. $1 \le \frac{\sqrt[3]{X}}{p} \le \frac{\sqrt{X}}{p}$: Tada, kada pomnožimo nejednakost $1 \le \frac{\sqrt[3]{X}}{p}$ sa $\frac{\sqrt{X}}{p}$, dobijamo da je

$$1 \le \frac{\sqrt{X}}{p} \le \frac{X^{5/6}}{p^2},$$

pa je $\frac{X^{5/6}}{p^2}$ najveći član u izrazu $X^{5/6}/p^2 + X^{1/2}/p + 1$. Dakle, $X^{5/6}/p^2 + X^{1/2}/p + 1 \leq 3X^{5/6}/p^2$, pa je

$$|f(X,p)| \leq 3C_2\frac{X^{5/6}}{p^2} = 3C_2\frac{1}{p^{1/3}}\frac{X^{5/6}}{p^{5/3}} \overset{\frac{1}{p^{1/3}}<1}{\leq} 3C_2\frac{X^{5/6}}{p^{5/3}},$$

2. $\frac{\sqrt[3]{X}}{p} \leq 1 \leq \frac{\sqrt{X}}{p}$: Tada, kada pomnožimo nejednakost $\frac{\sqrt[3]{X}}{p} \leq 1$ sa $\frac{\sqrt{X}}{p}$, dobijamo da je $\frac{X^{5/6}}{p^2} \leq \frac{\sqrt{X}}{p}$ pa je $\frac{\sqrt{X}}{p}$ najveći član u izrazu $X^{5/6}/p^2 + X^{1/2}/p + 1$. Dakle, $X^{5/6}/p^2 + X^{1/2}/p + 1 \leq 3\sqrt{X}/p$, pa je

$$|f(X,p)| \leq 3C_2\frac{\sqrt{X}}{p} \overset{\frac{\sqrt{X}}{p}\geq 1}{\leq} 3C_2\left(\frac{\sqrt{X}}{p}\right)^{5/3} = 3C_2\frac{X^{5/6}}{p^{5/3}}$$

3. $\frac{\sqrt[3]{X}}{p} \leq \frac{\sqrt{X}}{p} \leq 1$:

$$|f(X,p)| \leq C_1\frac{X}{p^2} = C_1\left(\frac{\sqrt{X}}{p}\right)^2 \overset{\frac{\sqrt{X}}{p}\leq 1}{\leq} C_1\left(\frac{\sqrt{X}}{p}\right)^{5/3} = C_1\frac{X^{5/6}}{p^{5/3}}.$$

Uzmemo li da je $C = \max\{C_1, 3C_2\}$ i da je $X > \max\{X_1, X_2\}$, imamo da je $|f(X,p)| \leq C\frac{X^{5/6}}{p^{5/3}}$ kada $X \to \infty$, odakle je $f(X,p) = O(X^{5/6}/p^{5/3})$.

Eliptička kriva $E_{A,B} : y^2 = x^3 + Ax + B$ ima multiplikativnu redukciju u prostom broju $p > 3$

Za ovakvu krivu važi da $p \nmid A$. Pošto je visina $E_{A,B}$ ograničena sa X, postoji $O(X^{1/3})$ mogućnosti za A i $O(X^{1/2})$ mogućnosti za B. Ako fiksiramo A, tada postoji $O(1)$ mogućnosti za B modulo p^2. Dakle, broj ovakvih krivih je ograničen sa

$$O(X^{1/3} \cdot (X^{1/2}/p^2 + 1)),$$

i sa $O(X/p^2)$. Kada kombinujemo ova dva rezultata, dobijamo da je broj ovakvih krivih ograničen sa $O(X^{5/6}/p^{3/2})$. □

Definišimo sada sledeće mase:

Definicija 5.7.4. *Za familiju F, njena p-adična masa je:*

$$M_p(F) := \int_{(I,J)\in \mathrm{Inv}_p(F)} dIdJ,$$

Sada definišemo lokalne mase u beskonačnosti familije F:

$$M_\infty(F;X) := \int_{\substack{(I,J)\in \mathrm{Inv}_\infty(F) \\ H(I,J)<X}} dIdJ,$$

$$M_\infty^V(F;X) := \int_{\substack{(I,J)\in \mathrm{Inv}_\infty(F) \\ H(I,J)<X}} \frac{\#(E^{I,J}(\mathbb{R})/2E^{I,J}(\mathbb{R}))}{\#E^{I,J}(\mathbb{R})[2]} dIdJ.$$

Iz tvrđenja 5.7.3 sledi sledeća teorema (na sličan način na koji teorema 4.8.4 sledi iz teoreme 4.7.12):

Teorema 5.7.5. *Neka je F velika familija eliptičkih krivih i neka je $N(F;X)$ broj eliptičkih krivih $E \in F$ za koje je $H'(E) < X$. Tada je*

$$N(F;X) = M_\infty(F;X) \prod_p M_p(F) + o(X^{5/6}).$$

5.8 Dokaz teoreme 5.1.5

U ovoj glavi povezujemo sve prethodno, i dokazujemo teoremu 5.1.5.

Definicija 5.8.1. *Za formu $f \in V_{\mathbb{Z}}$ kažemo da je loša u prostom broju p ako f nije $\mathbb{Q}_p$ rešivo, ili ako je $m_p(f) \neq 1$.*

Tvrđenje 5.8.2. *Ako je celobrojna binarna kvartična forma f loša u prostom broju $p > 2$, onda $p^2 \mid \Delta(f)$.*

Dokaz: Gledamo dva slučaja - kada je $m_p(f) \neq 1$, i kada f nije $\mathbb{Q}_p$ rešivo.

Neka je $m_p(f) \neq 1$. Tada postoji $\gamma \in \mathrm{PGL}_2(\mathbb{Q}_p) \setminus \mathrm{PGL}_2(\mathbb{Z}_p)$ takvo da je $\gamma \cdot f \in V_{\mathbb{Z}_p}$. Kako možemo umesto f posmatrati neki član njegove $\mathrm{PGL}_2(\mathbb{Z}_p)$-klase, to možemo smatrati da je $\gamma = \begin{bmatrix} p^\alpha & 0 \\ 0 & 1 \end{bmatrix}$, gde je $\alpha < 0$, $\alpha \in \mathbb{Z}$. Tada je koeficijent za f uz x^4 deljiv sa p^2, i koeficijent za f uz x^3y je deljiv sa p:

Neka je $f(x, y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4$. Tada je

$$\begin{bmatrix} p^\alpha & 0 \\ 0 & 1 \end{bmatrix} \cdot f(x, y) = ap^{4\alpha} + bx^3yp^{3\alpha} + cx^2y^2p^{2\alpha} + dxy^3p^\alpha + ey^4.$$

Kako su $a, b \in \mathbb{Z}$, to je $a = p^{a'}a_1$, $b = p^{b'}b_1$, za neke prirodne brojeve a' i b'. No, $\gamma \cdot f \in V_{\mathbb{Z}_p}$, pa je $|ap^{4\alpha}|_p = p^{-4\alpha-4a'} < 1$, odakle je $a' > -4\alpha \geq 4$. Slično, $b' \geq 3$. Dakle, $p^2 \mid a$ i $p \mid b$.

Odavde sledi da $p^2 \mid \Delta(f)$ (gde je $\Delta(f)$ je diskriminanta forme-(1.2)).

Neka f nije $\mathbb{Q}_p$ rešivo. Pokazaćemo da tada f ima tip račvanja (1^21^2), (2^2) ili (1^4) u p, odakle će slediti da $p^2 \mid \Delta(f)$. Ako je diskriminanta od $f \in V_{\mathbb{Z}_p}$ uzajamno prosta sa p, tada za f znamo da je $\mathbb{Q}_p$ rešivo po [C], glava 3.6. Ako je tip račvanja f u p (1^211) ili (1^31), tada redukcija f modulo p ima prost koren u $\mathbb{P}^1(\mathbb{F}_p)$, odakle po Henselovoj lemi redukcija ima koren u $\mathbb{P}^1(\mathbb{Q}_p)$. Dakle, f je $\mathbb{Q}_p$ rešivo.

Neka sada $f \in V_{\mathbb{Z}_p}$ ima (1^22) kao tip račvanja u p. Tada redukcija f modulo p ima oblik

$$\overline{a}x^2(x^2 - \overline{n}y^2),$$

gde je $\overline{n}$ "neostatak" modulo p. Prema tome,

$$f(x, y) = a(x^2 - kpy^2)(x^2 - ny^2),$$

gde su $a, n, k \in \mathbb{Z}_p$, $n \in \mathbb{Z}_p$ je "neostatak" kada se redukuje modulo p, i $p \nmid a$. Ako je a kvadrat u $\mathbb{Q}_p$, tada je $f(1, 0)$ kvadrat u $\mathbb{Q}_p$, i tvrđenje je dokazano. Dakle, smatramo da a nije kvadrat. Za proizvoljno $x_0 \in \mathbb{Z}_p$, ako $p \nmid x_0$, onda je $x_0 - kp$ kvadrat u $\mathbb{Q}_p$, pa je dovoljno dokazati da postoji $\overline{x}_0 \in \mathbb{F}_p^\times$ takvo da je $\overline{x}_0^2 - \overline{n}$ kvadratni "neostatak" modulo p. Neka je $\overline{x}_0^2 = (c + 1)\overline{n}$ prvi kvadratni ostatak koji se pojavljuje u nizu $\overline{n}, 2\overline{n}, ..., (p - 1)\overline{n}$. Tada je

$$\overline{x}_0^2 - \overline{n} = (c + 1)\overline{n} - \overline{n} = c\overline{n}$$

kvadratni "neostatak". □

Definicija 5.8.3. *Analogno skupovima $S_p(F)$, sa $S_\infty(F)$ obeležavamo skup svih $\mathbb{R}$ rešivih binarnih kvartičnih formi u $V_\mathbb{R}$ čije invarijante pripadaju* $\mathrm{Inv}_\infty(F)$.

Pošto je

$$\frac{\#(E^{I,J}(\mathbb{R})/2E^{I,J}(\mathbb{R}))}{\#E^{I,J}(\mathbb{R})[2]} = \frac{1}{2},$$

to iz (4.8) i definicije 5.7.4 imamo

$$N(V_\mathbb{Z} \cap S_\infty(F); X) = \frac{1}{27}\mathrm{Vol}(\mathrm{PGL}_2(\mathbb{Z}) \setminus \mathrm{PGL}_2(\mathbb{R}))M_\infty^V(F; X) + O(X^{3/4+\epsilon}).$$

Dokazaćemo sledeću teoremu, iz koje sledi teorema 5.1.5.

Teorema 5.8.4. *Neka je F velika familija eliptičkih krivih. Tada je*

$$\lim_{X\to\infty} \frac{\sum\limits_{\substack{E\in F\\ H'(E)<X}} (\#S_2(E)-1)}{\sum\limits_{\substack{E\in F\\ H'(E)<X}} 1} =$$

$$= \mathrm{Vol}(\mathrm{PGL}_2(\mathbb{Z})\setminus \mathrm{PGL}_2(\mathbb{R}))\frac{M_\infty^V(F;X)}{M_\infty(F;X)}\prod_p \left[\mathrm{Vol}(\mathrm{PGL}_2(\mathbb{Z}_p))\frac{M_p^V(F)}{M_p(F)}\right].$$

Primedba 5.8.5. *$M_\infty^V(F;X)$ je iz definicije 5.5.3, a $M_\infty(F;X)$ je iz definicije 5.7.4.*

Dokaz: Po teoremi 5.3.5, leva strana jednakosti u 5.8.4 je jednaka broju lokalno rešivih $\mathrm{PGL}_2(\mathbb{Z})$ orbita na $S(F^{\mathrm{inv}})$ sa visinom manjom od $2^{12}X$ i bez racionalnog linearnog faktora, i svaka orbita $\mathrm{PGL}_2(\mathbb{Z})\cdot f$ se računa sa težinom $1/m(f)$. Po tvrđenjima 5.4.5, 5.5.4, 5.8.2 i teoremi 4.8.4, imamo

$$\sum_{\substack{E\in F\\ H'(E)<X}} (\#S_2(E)-1) = N(V_{\mathbb{Z}}\cap S_\infty(X); 2^{12}X)\prod_p \int_{S_p(F)} \frac{1}{m_p(f)}df + o(X^{5/6}) =$$

$$= \frac{2^{10}}{27}\mathrm{Vol}(\mathrm{PGL}_2(\mathbb{Z})\backslash\mathrm{PGL}_2(\mathbb{R}))M_\infty^V(F;X)\prod_p \left|\frac{2^{10}}{27}\right|_p \mathrm{Vol}(\mathrm{PGL}_2(\mathbb{Z}_p))M_p^V(F)+o(X^{5/6}). \tag{5.7}$$

Pošto za elemente $a\in\mathbb{Q}\setminus\{0\}$ važi $|a|\cdot\prod\limits_p |a|_p = 1$, to se izraz (5.7) skraćuje u:

$$\mathrm{Vol}(\mathrm{PGL}_2(\mathbb{Z})\setminus \mathrm{PGL}_2(\mathbb{R}))M_\infty^V(F;X)\prod_p \mathrm{Vol}(\mathrm{PGL}_2(\mathbb{Z}_p))M_p^V(F) + o(X^{5/6}).$$

Sa druge strane, teorema 5.7.5 nam kaže da je

$$\sum_{\substack{E\in F\\ H'(E)<X}} 1 = M_\infty(F;X)\prod_p M_p(F) + o(X^{5/6}).$$

Razlomak ova dva izraza nam daje rezultat koji tražimo. □

Kako bismo procenili desnu stranu jednakosti u teoremi 5.8.4, trebaće nam lema 3.1 iz [BK], i definicija Tamagawinog broja iz [PR]:

Lema 5.8.6. *Neka je E eliptička kriva nad $\mathbb{Q}_p$. Tada je*

$$\#(E(\mathbb{Q}_p)/2E(\mathbb{Q}_p)) = \begin{cases} \#E(\mathbb{Q}_p)[2], & p\neq 2;\\ 2\cdot\#E(\mathbb{Q}_p)[2], & p=2.\end{cases}$$

Definicija 5.8.7. *Tamagawin broj linearne algebarske grupe G je Tamagawina mera skupa $G_{\mathbb{A}}/G_K$ (pri čemu su $\mathbb{A}$ adeli, i $G_{\mathbb{A}}$ adelična grupa grupe G nad brojnim poljem K), ako postoji, i obeležava se sa $\tau(G)$. Više o Tamagawinom broju i Tamagawinoj meri se može naći u [PR].*

Dokaz teoreme 5.1.5: Kada kombinujemo lemu 5.8.6 sa definicijama 5.5.3 i 5.7.4, dobijamo da je

$$\frac{M_p^V(F)}{M_p(F)} = \frac{\displaystyle\int_{(I,J)\in \mathrm{Inv}_p(F)} \frac{\#(E^{I,J}(\mathbb{Q}_p)\setminus 2E^{I,J}(\mathbb{Q}_p))}{\#E^{I,J}(\mathbb{Q}_p)[2]}dIdJ}{\displaystyle\int_{(I,J)\in \mathrm{Inv}_p(F)} dIdJ} = \begin{cases} 1, & p\neq 2\\ 2, & p=2\end{cases}$$

No, takođe znamo da je

$$\frac{M_\infty^V(F;X)}{M_\infty(F;X)} = \frac{1}{2},$$

pa nam teorema 5.8.4 kaže da je

$$\frac{\sum\limits_{\substack{E\in F\\ H'(E)<X}} (\#S_2(E)-1)}{\sum\limits_{\substack{E\in F\\ H'(E)<X}} 1} = \mathrm{Vol}(\mathrm{PGL}_2(\mathbb{Z})\setminus \mathrm{PGL}_2(\mathbb{R}))\prod_p \mathrm{Vol}(\mathrm{PGL}_2(\mathbb{Z}_p)) =$$

$$= 2\zeta(2)\prod_p (1-p^{-2}) = 2.$$

No, 2 je Tamagawa-in broj od $\mathrm{PGL}_2(\mathbb{Q})$, pa nam ovo daje dokaz teoreme 5.1.5. $\square$

Literatura

[B] M. Bhargava, *The density of discriminants of quartic rings and fields*, Ann. of Math. 162, 1031-1063., (2005)

[B2] M. Bhargava, *The geometric sieve and squarefree values of polynomial discriminants and other invariant polynomials*, arXiv:1402.0031v1, (2014).

[BS] M. Bharhava, A. Shankar, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, Ann. of Math. 181 (2015), 192-242.

[BST] M. Bhargava, A. Shankar, J. Tsimerman, *On the Davenport-Heilbronn theorems and second order terms*, Inventiones mathematicae, Volume 193, Issue 2 Springer-Verlag, Vol. 193, no. 2 (2013.), 439-499.

[BSD] B. J. Birch, H. P. F. Swinnerton-Dyer, *Notes on elliptic curves I*, J. Reine Angew. Math. 212 (1963), 7-25.

[BK] A. Brumer, K. Kramer, *The rank of elliptic curves*, Duke Math. J. 44 (1997), no. 4, 715-743.

[C] J.E. Cremona, *Algorithms for modular elliptic curves*, 2nd edn., Cambridge University Press, 1997.

[C2] J. E. Cremona, *Reduction of binary cubic and quartic forms*, LMS J. Comput. Math. 2 (1999), 64-94.

[CF] J. E. Cremona, T. Fisher, *On the equivalence of binary quartics*, Journal of Symbolic Computation 44 (2009), 673-682.

[CS] J. E. Cremona, M. Stoll, *Minimal models for 2-coverings of elliptic curves*, LMS J. Comput. Math. 5 (2002), 220-243 (electronic).

[D] H. Davenport, *On a principle of Lipschitz*, J. London Math. Soc. (1951), 179-183.

[D2] H. Davenport, *Multiplicative Number Theory*, Second Edition, Graduate Texts in Mathematics, Vol. 74, Springer-Verlag, (1982)

[DH] H. Davenport, H. Heilbronn, *On the density of discriminants of cubic fields II*, Proc. Roy. Soc. London Ser. A 322 (1971), no. 1551, 405-420.

[D3] B. N. Delone, *Uber die Darstellung der Zahlen durch die binare kubischen Formen von negativer Diskriminante*, Math. Z. 31 (1930), 1-26.

[DF] B. N. Delone, D. K. Faddeev, *The theory of irrationalities of the third degree*, AMS Translations of Mathematical Monographs 10, 1964.

[E] T. Ekedahl, *An infinite version of the Chinese remainder theorem*, Comment. Math. Univ. St. Paul. 40 (1991), 53-59.

[E2] J. H. Evertse, *On the representation of integers by binary cubic forms of positive discriminant*, Invent. Math. 73 (1983), no. 1, 117-138.

[H] Wei Ho, *How many rational points does a random curve have?*, Bulletin of American Mathematical Society, Volume 51, Number 1, January 2014, Pages 27-52.

[IK] H. Iwaniec, E. Kowalski, *Analytic number thoery*, American Mathematical Society, Providence, Rhode Island, (2004)

[K] A.W. Knapp, *Lie groups beyond an introduction, Second ed.*, Progress in Mathematics, 140, Birkhäuser, Boston, 2002.

[L] Edmund Landau, *Vorlesungen über Zahlentheorie*, Chelsea Publishing Co., New York, (1927)

[PR] V. Platonov, A. Rapinchuk, *Algebraic groups and number theory*, Translated from the 1991 Russian original by Rachel Rowen, Pure and Applied Mathematics 139, Academic Press, Inc., Boston, MA, 1994.

[P] B. Poonen, *Squarefree values of multivariable polynomials*, Duke Math. J. 118 (2003), no. 2, 353-373.

[S] P. Schneider, *p-adic Lie groups*, Springer, 2011.

[S2] C. L. Siegel, *The average measure of quadratic forms with given determinant and signature*, Annals of Mathematics, Second Series, Vol. 45, No. 4 (Oct., 1944), pp. 667-685

[S3] Joseph H. Silverman, *The arithmetic of elliptic curves, Second ed.*, (2008)