УНИВЕРЗИТЕТ У БЕОГРАДУ
МАТЕМАТИЧКИ ФАКУЛТЕТ

Илија Вреһица

СТАТИСТИКА СЕЛМЕРОВИХ ГРУПА У ФАМИЛИЈИ ЕЛИПТИЧКИХ КРИВИХ ПРИДРУЖЕНИХ КОНГРУЕНТНИМ БРОЈЕВИМА

докторска дисертација

Београд, 2022.

UNIVERSITY OF BELGRADE
FACULTY OF MATHEMATICS

Ilija Vrećica

JOINT DISTRIBUTION FOR THE SELMER RANKS OF THE CONGRUENT NUMBER CURVES

Doctoral Dissertation

Belgrade, 2022.

Ментор:

др Горан Ђанковић, ванредни професор, Универзитет у Београду, Математички факултет

Чланови комисије:

др Зоран Петровић, редовни професор, Универзитет у Београду, Математички факултет

др Горан Ђанковић, ванредни професор, Универзитет у Београду, Математички факултет

др Марко Радовановић, ванредни професор, Универзитет у Београду, Математички факултет

др Драган Станков, ванредни професор, Универзитет у Београду, Рударско геолошки факултет

др Тања Стојадиновић, доцент, Универзитет у Београду, Математички факултет

Датум одбране: _____

Посвећено мојој породици, и свим мојим пријатељима.

Захвалница

Захвалио бих се мом ментору, проф. др Горану Ђанковићу, на великој помоћи коју ми је пружио током студија, као и на указивању на два рада који су били основ за тему ове дисертације. Његова помоћ је била кључна у настанку ове дисертације.

Такође бих се захвалио комисији за примедбе које су ми упутили, на основу којих је рад знатно побољшан. Посебно бих се захвалио проф. др Марку Радовановићу за указивање на грешку у петој глави прелиминарне верзије дисертације, што је резултовало побољшањем не само тезе, већ и једног рада.

Додатно, захвалио бих се колегама са којима сам имао успешну сарадњу, која је довела и до неколико заједничких радова. Поред ментора Горана Ђанковића, то су и колеге Никола Лелас, Драган Ђокић и Младен Зекић.

Илија Врећица

Наслов: Статистика Селмерових група у фамилији елиптичких кривих придружених конгруентним бројевима

Резиме: Први део дисертације се бави скуповима збирова $hA = \{a_1 + \cdots + a_h \in \mathbb{Z}^d : a_1, \ldots, a_h \in A\}$, где је A коначни скуп у $\mathbb{Z}^d$. Познато је да постоји константа $h_0 \in \mathbb{N}$ и полином $p_A(X)$ такав да је $p_A(h) = |hA|$ за $h \geqslant h_0$. Међутим, мало се зна о полиному, као и о константи h_0. Конус $\mathcal{C}_A$ над скупом A садржи информације о hA, за свако $h \in \mathbb{N}$. Када скуп A има $d+2$ елемента, могу се експлицитно описати полином p_A и константа h_0. Када A има $d+3$ елемента, налази се горње ограничење за број елемената скупа hA.

Други део дисертације се бави Селмеровим групама у фамилији елиптичких кривих придружених конгруентним бројевима. Бесквадратан природан број n је конгруентан ако и само ако постоји правоугли троугао са целобројним дужинама страница чија површина је n. Познато је да је природан број n конгруентан ако и само ако је ранг елиптичке криве $E_n : y^2 = x^3 - n^2x$ као алгебарске групе различит од нуле. Селмерове групе придружене изогенијама елиптичких кривих E_n су занимљиве, јер њихов ранг није мањи од ранга криве E_n, па када је ранг Селмерових група нула, тада је и ранг криве E_n једнак нули. Елементи Селмерових група се могу представити као партиције одређеног графа, па се на тај начин може наћи дистрибуција ранга Селмерових група.

Кључне речи: симплицијални комплекси, скупови збирова, елиптичке криве, Селмерова група, конгруентни бројеви, теорија графова, Тејт-Шафаревичева група, теорија Хованског, Ерхартова теорија

Научна област: Математика

Ужа научна област: Теорија бројева

УДК број: УДК број

AMC класификација: 11G05, 14H52, 11N45, 11H06, 52B20, 05A15, 11P21

Dissertation title: Selmer group statistics in the congruent number family of elliptic curves

Abstract: First part of dissertation examines sumsets $hA = \{a_1 + \cdots + a_h \in \mathbb{Z}^d : a_1, \ldots, a_h \in A\}$, where A is a finite set in $\mathbb{Z}^d$. It is known that there exists a constant $h_0 \in \mathbb{N}$ and a polynomial $p_A(X)$ such that $p_A(h) = |hA|$ for $h \geqslant h_0$. However, little is known of polynomial p_A and constant h_0. Cone $\mathcal{C}_A$ over the set A contains information about hA, for all $h \in \mathbb{N}$. When A has $d+2$ elements, polynomial p_A and constant h_0 can be explicitly described. When A has $d+3$ elements, an upper bound is found for the number of elements of hA.

Second part of dissertation examines Selmer groups of elliptic curves in the congruent number family. A squarefree natural number is congruent if and only if there exists a right triangle with area n whose sides all have integer lengths. It is known that n is a congruent number if and only if elliptic curve $E_n : y^2 = x^3 - n^2x$ has nonzero rank as an algebraic group. Selmer groups of isogenies on E_n are interesting, because their rank is not smaller than the rank of E_n, so when the Selmer groups have rank zero, then the elliptic curve E_n also has rank zero. Elements of these Selmer groups can be represented as partitions of a particular graph, from which one may find the distribution of ranks of Selmer groups.

Keywords: simplicial complexes, sumsets, elliptic curves, Selmer group, congruent numbers, graf theory, Tate-Shafarevich group, Khovanskii theory, Ehrhart theory

Research area: Mathematics

Research sub-area: Number theory

UDC number: UDC number

AMS Subject Classification: 11G05, 14H52, 11N45, 11H06, 52B20, 05A15, 11P21

Садржај

Увод

Теза је подељена на две целине. Први део је посвећен теорији Хованског и теорији Ерхарта, док је други посвећен Селмеровим групама на елиптичкој кривој. У другом делу ће се ставити нагласак на везу између Селмерових група и одређених графова.

Теза је подељена на осам глава и има следећу структуру. Прва глава уводи основне појмове из теорије Ерхарта, и приказује доказ важне теореме из [E]. У другој глави се уводе основни појмови адитивне комбинаторике и теорије Хованског, и приказује се важан резултат из [Kh]: За коначан скуп $A \subset \mathbb{Z}^d$ постоје полином $p_A(X)$ и константа $h_0 \in \mathbb{N}$ такви да је $|hA| = p_A(h)$ за $h \geqslant h_0$. У трећој глави се примењују технике из Ерхартове теорије на теорију Хованског, при чему се добијају експлицитан полином $p_A(X)$ и константе h_0 за скупове $A \subset \mathbb{Z}^d$ са $d+2$ елемента.

У четвртој и петој глави су приказани оригинални резултати. У четвртој глави дат је алтернативни начин пребројавања броја елемената hA, када је $A \subset \mathbb{Z}^d$ скуп са $d+2$ елемената, као и уопштење резултата из [CG]. У петој глави је за скуп $A \subset \mathbb{Z}^d$ са $d+3$ елемента и симплицијалним конвексним омотачем, техником из треће главе дато горње ограничење за број елемената скупа hA за довољно велико h.

Шеста глава припада другој целини, и уводи конгруентне бројеве, елиптичке криве, и везу између њих. У седмој глави је приказан рад [F] који уводи везу између проблема конгруентних бројева, L функција на елиптичким кривама описаних једначинама $E_n : y^2 = x^3 - n^2x$, и Селмерових група придружених изогенијама на тим кривама. Он је мотивисао даље истраживање Селмерових група помоћу теорије графова (на пример у [FJ], [F], [FX], [HB1], [HB2], [JO]).

У осмој глави је приказан оригинални резултат. Рангови две Селмерове групе на елиптичкој кривој E_n се могу изразити преко ранга Лапласове матрице одређеног графа, чији скупови темена и ивица зависе од простих фактора броја n и Лежандрових симбола између простих фактора броја n. Налажењем вероватноће да природан број n има не само одговарајући број простих фактора, већ и одговарајуће Лежандрове симболе између њих, може се наћи дистрибуција рангова Селмерових група на елиптичким кривама из фамилије E_n.

Глава 1

Ерхартова теорија

1.1 Основни појмови

Један од проблема у теорији бројева је пребројавање целобројних тачака неког политопа. Кључан допринос у том смеру је рад [E], који је индуковао технике примењене не само у овој области, већ и у теорији Хованског.

Дефиниција 1.1.1. *Конвексни омотач* коначног скупа тачака $A = \{a_1, \ldots, a_k\} \subset \mathbb{R}^d$ је најмањи конвексни скуп који садржи скуп A. Другим речима, то је скуп

$$\Delta_A := \{\lambda_1 a_1 + \cdots + \lambda_k a_k \in \mathbb{R}^d \,:\, \lambda_1, \ldots, \lambda_k \geqslant 0\,,\, \lambda_1 + \cdots + \lambda_k = 1\}.$$

Скуп Δ_A се такође зове *конвексни политоп*. Конвексни политоп је *целобројни* ако су координате сваког његовог темена цели бројеви.

Нека је $\mathcal{P}$ целобројни, конвексни политоп у $\mathbb{R}^d$, и нека је $p_{\mathcal{P}}(t) := |t \cdot \mathcal{P} \cap \mathbb{Z}^d|$ број целобројних тачака у $t \cdot \mathcal{P} = \{tv \in \mathbb{R}^d \,:\, v \in \mathcal{P}\}$ за позитиван цели број t. У овој глави ће бити доказано да је $p_{\mathcal{P}}(t)$ полином по t, због чега се $p_{\mathcal{P}}(t)$ зове *Ерхартов полином*.

Дефиниција 1.1.2. *(Усмерени) конус* у $\mathbb{R}^d$ је скуп облика

$$\mathcal{C} := \{v + \lambda_1 w_1 + \cdots + \lambda_k w_k \in \mathbb{R}^d \,:\, \lambda_1, \ldots, \lambda_k \in \mathbb{R}, \lambda_1, \ldots, \lambda_k \geqslant 0\},$$

при чему су вектори $v, w_1, \ldots, w_k$ такви да постоји хипер раван H таква да је $H \cap \mathcal{C} = \{v\}$ (другим речима, конус $\mathcal{C}$ је садржан у једном полупростору који је одређен са H).

Вектор v је *врх* конуса $\mathcal{C}$, док су вектори $w_1, \ldots, w_k$ *генератори* конуса $\mathcal{C}$. Димензија конуса $\mathcal{C}$ је димензија афиног простора разапетог генераторима конуса. Конус $\mathcal{C} \subset \mathbb{R}^d$ је *симплицијални конус* ако има тачно d линеарно независних генератора.

Ако су $v, w_1, \ldots, w_k \in \mathbb{Z}^d$, тада се за скуп

$$\{v + \lambda_1 w_1 + \cdots + \lambda_k w_k \in \mathbb{Z}^d \,:\, \lambda_1, \ldots, \lambda_k \in \mathbb{Z}_{\geqslant 0}\}$$

каже да је *целобројни конус*.

Конуси су битни из много разлога. Један од њих је што се могу конструисати конуси над конвексним политопима. Нека је $\mathcal{P} \subset \mathbb{R}^d$ конвексни политоп са теменима $v_1, \ldots, v_k$. Вектори $v_1, \ldots, v_k$ се могу „подићи" у $\mathbb{R}^{d+1}$ тако што се дода 1 као последња координата:

$$\widetilde{v}_1 = (v_1, 1), \ldots, \widetilde{v}_k = (v_k, 1).$$

Сада се може конструисати конус над политопом $\mathcal{P}$ као

$$\mathcal{C}_{\mathcal{P}} := \{\lambda_1 \widetilde{v}_1 + \cdots + \lambda_k \widetilde{v}_k \in \mathbb{R}^{d+1} \,:\, \lambda_1, \ldots, \lambda_k \in \mathbb{R}_{\geqslant 0}\} \subset \mathbb{R}^{d+1}.$$

Важан алат у пребројавању целобројних тачака у политопу је генераторни ред скупа. Нека је $S \subset \mathbb{R}^d$ непразан скуп. Тада се генераторна функција скупа S дефинише као формални ред

$$\sigma_S(z) = \sigma_S(z_1, \ldots, z_d) := \sum_{x \in S \cap \mathbb{Z}^d} z^x \in \mathbb{Z}[[z_1, \ldots, z_d]],$$

при чему се под z^x подразумева $z_1^{x_1} \ldots z_d^{x_d}$ за $x = (x_1, \ldots, x_d) \in S \cap \mathbb{Z}^d$. Нека је $\mathcal{C}$ симплицијални конус са генераторима $v_1, \ldots, v_d$. Тада се дефинише фундаментални паралелепипед као

$$\Pi := \{\lambda_1 v_1 + \cdots + \lambda_d v_d \in \mathbb{R}^d \,:\, 0 \leqslant \lambda_1, \ldots, \lambda_d < 1\}.$$

Теорема 1.1.3. Нека је

$$\mathcal{C} = \{\lambda_1 v_1 + \cdots + \lambda_d v_d \in \mathbb{R}^d \,:\, \lambda_1, \ldots, \lambda_d \geqslant 0\}$$

симплицијални конус са генераторима $v_1, \ldots, v_d \in \mathbb{Z}^d$. Генераторна функција $\sigma_{v+\mathcal{C}}$ конуса $v + \mathcal{C}$ са врхом $v \in \mathbb{R}^d$ може се изразити преко генераторне функције $\sigma_{v+\Pi}$

$$\sigma_{v+\mathcal{C}}(z) = \frac{\sigma_{v+\Pi}(z)}{(1 - z^{v_1}) \ldots (1 - z^{v_d})},$$

где је Π фундаментални паралелепипед за $\mathcal{C}$.

Доказ. У генераторном реду $\sigma_{v+\mathcal{C}}(z)$, свака целобројна тачка $m \in (v + \mathcal{C}) \cap \mathbb{Z}^d$ доприноси z^m. Целобројне тачке m се могу записати као

$$m = v + \lambda_1 v_1 + \cdots + \lambda_d v_d$$

за неке реалне бројеве $\lambda_1, \ldots, \lambda_d \geqslant 0$. Пошто $v_1, \ldots, v_d$ чине базу $\mathbb{R}^d$, овај запис тачке m је јединствен. Свако λ_k се може записати као збир целог и разломљеног дела: $\lambda_k = [\lambda_k] + \{\lambda_k\}$. Сада је

$$m = v + (\{\lambda_1\}v_1 + \cdots + \{\lambda_d\}v_d) + [\lambda_1]v_1 + \cdots + [\lambda_d]v_d,$$

а пошто је $0 \leqslant \{\lambda_k\} < 1$, вектор

$$p := v + \{\lambda_1\}v_1 + \cdots + \{\lambda_d\}v_d$$

припада $v + \Pi$. Штавише, вектор p је елемент $\mathbb{Z}^d$, јер су то и m и $[\lambda_k]v_k$. Дакле, сваки вектор $m \in (v + \mathcal{C}) \cap \mathbb{Z}^d$ се може на јединствен начин записати као

$$m = p + k_1v_1 + \cdots + k_dv_d \tag{1.1}$$

за неко $p \in (v + \Pi) \cap \mathbb{Z}^d$ и неке целе бројеве $k_1, \ldots, k_d \geqslant 0$. Са друге стране,

$$\frac{\sigma_{v+\Pi}(z)}{(1 - z^{v_1}) \ldots (1 - z^{v_d})} = \left(\sum_{p \in (v+\Pi) \cap \mathbb{Z}^d} z^p \right) \left(\sum_{k_1 \geqslant 0} z^{k_1 v_1} \right) \ldots \left(\sum_{k_d \geqslant 0} z^{k_d v_d} \right)$$

Када се измноже сабирци, просечан експонент ће изгледати као (1.1). □

Конус $v+\mathcal{C}$ је поплочан транслатима $v+\Pi$, због чега се генераторна функција за $v+\mathcal{C}$ може изразити преко генераторне функције за $v+\Pi$. Могућност оваквог поплочавања конуса копијама фундаменталног домена је један од разлога зашто је лакше радити са конусима уместо са политопима. Пошто сваки конус има триангулацију на симплицијалне конусе, и пошто је пресек два симплицијална конуса у тријангулацији опет симплицијални конус, важи следећа теорема:

Теорема 1.1.4. За било који усмерени конус

$$\mathcal{C} = \{v + \lambda_1v_1 + \cdots + \lambda_kv_k \in \mathbb{R}^d \,:\, \lambda_1, \ldots, \lambda_k \geqslant 0\}$$

са $v \in \mathbb{R}^d$ и $v_1, \ldots, v_k \in \mathbb{Z}^d$ функција $\sigma_{\mathcal{C}}(z)$ је рационална функција по $z_1, \ldots, z_d$.

1.2 Ерхартова теорема

Теорема 1.2.1. [E, глава 3, теорема 3.3] Ако је $\mathcal{P}$ целобројни конвексни политоп у $\mathbb{R}^d$, тада је $p_{\mathcal{P}}(t)$ полином по t.

За доказ теореме биће неопходна следећа лема:

Лема 1.2.2. Нека су $f, g : \mathbb{Z} \to \mathbb{Z}$. Ако је

$$\sum_{t \geqslant 0} f(t) z^t = \frac{g(z)}{(1-z)^{d+1}},$$

тада је f полином степена d ако и само ако је g полином степена $\leqslant d$ и $g(1) \neq 0$.

Дефиниција 1.2.3. *Триангулација конвексног d-политопа* $\mathcal{P}$ је коначна колекција T која садржи d-симплексе са следећим својствима:

- $\mathcal{P} = \bigcup_{\Delta \in T} \Delta$.
- За све $\Delta_1, \Delta_2 \in T$, пресек $\Delta_1 \cap \Delta_2$ је страна и Δ_1 и Δ_2.

Политоп $\mathcal{P}$ се може триангулисати *без додавања нових темена* ако постоји триангулација T политопа $\mathcal{P}$ таква да су темена било ког $\Delta \in T$ такође темена $\mathcal{P}$.

Може се доказати да се сваки конвексни политоп може триангулисати без додавања темена ([BR, глава 3, теорема 3.1]). Тврђење изгледа интуитивно јасно, али није тривијално да се докаже.

Као што се политопи триангулишу на симплексе, тако се конуси триангулишу на симплицијалне конусе.

Дефиниција 1.2.4. Колекција T симплицијалних конуса је *триангулација конуса* $\mathcal{C}$ ако важи

- $\mathcal{C} = \bigcup_{\mathcal{K} \in T} \mathcal{K}$.
- За било које $\mathcal{K}_1, \mathcal{K}_2 \in T$, пресек $\mathcal{K}_1 \cap \mathcal{K}_2$ је страна и $\mathcal{K}_1$ и $\mathcal{K}_2$.

Конус $\mathcal{C} \subset \mathbb{R}^d$ је могуће триангулисати на симплицијалне конусе *без нових генератора* ако постоји триангулација T од $\mathcal{C}$ таква да су генератори било ког $\mathcal{K} \in T$ такође генератори $\mathcal{C}$.

Као и конвексни политопи, сваки усмерени конус се може триангулисати без нових генератора ([BR, глава 3, Теорема 3.2]).

Доказ теореме 1.2.1. Нека је сада $\mathcal{P}$ конвексни политоп, и $\mathcal{C}_\mathcal{P}$ конус над $\mathcal{P}$. Може се видети да је пресек конуса и хиперравни $x_{d+1} = 1$ копија политопа $\mathcal{P}$. Штавише, пресек хиперравни $x_{d+1} = t$ и конуса је копија раширења $t \cdot \mathcal{P}$. Конус $\mathcal{C}_\mathcal{P}$ је према томе веома користан, јер постоји веза између генераторне функције $\sigma_{\mathcal{C}_\mathcal{P}}$ и генераторних функција $\sigma_{t \cdot \mathcal{P}}$ раширења политопа $\mathcal{P}$:

$$\begin{aligned}\sigma_{\mathcal{C}_\mathcal{P}}(z_1,\dots,z_{d+1}) &= 1+\sigma_\mathcal{P}(z_1,\dots,z_d)z_{d+1}+\sigma_{2\mathcal{P}}(z_1,\dots,z_d)z_{d+1}^2+\dots\\ &= 1+\sum_{t\geqslant 1}\sigma_{t\cdot\mathcal{P}}(z_1,\dots,z_d)z_{d+1}^t.\end{aligned}$$

Пошто је $\sigma_\mathcal{P}(1,\dots,1)=|\mathcal{P}\cap\mathbb{Z}^d|$, важи да је

$$\sigma_{\mathcal{C}_\mathcal{P}}(1,\dots,1,z_{d+1}) = 1+\sum_{t\geqslant 1}\sigma_{t\cdot\mathcal{P}}(1,\dots,1)z_{d+1}^t = 1+\sum_{t\geqslant 1}|t\cdot\mathcal{P}\cap\mathbb{Z}^d|z_{d+1}^t. \tag{1.2}$$

За конвексни политоп $\mathcal{P}$ корисно је дефинисати ред

$$\mathrm{Ehr}_\mathcal{P}(z) := 1+\sum_{t\geqslant 1}p_\mathcal{P}(t)z^t\in\mathbb{Z}[[z]],$$

који се назива *Ерхартов ред* за политоп $\mathcal{P}$. По леми 1.2.2 и једнакости (1.2), довољно је показати да је

$$\mathrm{Ehr}_\mathcal{P}(z)=\frac{g(z)}{(1-z)^{d+1}}$$

за неки полином g са целобројним коефицијентима степена највише d за који је $g(1)\neq 0$. Такође, сваки политоп се може триангулисати без додавања темена, па је довољно доказати теорему када је $\mathcal{P}$ d-симплекс са целобројним теменима. По теореми 1.1.3, $\sigma_{\mathcal{C}_\mathcal{P}}$ се може изразити преко σ_Π, где је Π фундаментални домен конуса $\mathcal{C}_\mathcal{P}$:

$$\sigma_{\mathcal{C}_\mathcal{P}}(z_1,\dots,z_{d+1})=\frac{\sigma_\Pi(z_1,\dots,z_{d+1})}{(1-z^{\widetilde{v}_1})\dots(1-z^{\widetilde{v}_{d+1}})},$$

где је $z=(z_1,\dots,z_{d+1})$. Пошто је паралелепипед ограничен, σ_Π је полином по $z_1,\dots,z_{d+1}$. Прво, $d{+}1$-ва координата било које тачке у Π једнака је $\lambda_1+\dots+\lambda_d$ за $0\leqslant\lambda_i<1$ јер је $d{+}1$-ва координата $\widetilde{v}_i$ једнака 1. Према томе, $d{+}1$-ва координата произвољне тачке у Π је мања од $d{+}1$, па ако је та координата цео број, она може бити највише d. Према томе, z_{d+1}-степен полинома $\sigma_\Pi(1,\dots,1,z_{d+1})$ је највише d. Такође, $\sigma_\Pi(1,\dots,1,1)=|\Pi\cap\mathbb{Z}^{d+1}|\neq 0$, јер координатни почетак припада Π.

Када се уврсти $z_1=\dots=z_d=1$ у $z^{\widetilde{v}_i}$, добија се z_{d+1}^1, одакле је

$$\sigma_{\mathcal{C}_\mathcal{P}}(1,\dots,1,z_{d+1})=\frac{\sigma_\Pi(1,\dots,1,z_{d+1})}{(1-z_{d+1})^{d+1}}.$$

Лева страна једнакости је по (1.2) једнака $\mathrm{Ehr}_\mathcal{P}(z_{d+1})=1+\sum_{t\geqslant 1}p_\mathcal{P}(t)z_{d+1}^t$. □

Глава 2

Теорема Хованског о скуповима збирова

2.1 Скупови збирова и дискретна геометрија

У овој глави ће бити приказано пар резултата из адитивне комбинаторике. То је област комбинаторике која се између осталог бави скуповима збирова, који се дефинишу на следећи начин:

Дефиниција 2.1.1. Нека је G адитивна група, и нека су A и B подскупови од G. Тада је *скуп збирова* елемената из A и B дефинисан са

$$A + B := \{a + b \in G \,:\, a \in A,\, b \in B\}.$$

Посебно, скуп $A + A + \cdots + A$ (h сабирака) ће бити обележен са hA.

За скупове збирова се могу поставити питања следећег облика: Колико елемената има скуп $A+B$? Ако се зна да је скуп $A+B$ мале кардиналности, шта се може рећи о скуповима A и B? Да ли се величина $|A+B|$ може изразити преко $|A|$ и $|B|$? Област је релативно млада, и њен развој је започео математичар Е. Семереди. Један од корисних алата при истраживању скупова збирова је појам *адитивне енергије* скупа који је дефинисан са

$$E^+(A) := \left|\{(a_1, a_2, a_3, a_4) \in A^4 \,:\, a_1 + a_2 = a_3 + a_4\}\right|.$$

Ако су a_1, a_2 и a_3 фиксирани, тада постоји највише једно a_4 за које је једначина задовољена и према томе

$$|A|^2 \leqslant E^+(A) \leqslant |A|^3.$$

Скупови за које је $|A+A|$ мало имају велику адитивну енергију. Ово се може видети на следећи начин: Ако се означи $f_A(b) := |\{(a_1, a_2) \in A^2 : a_1 + a_2 = b\}|$, сваки пар елемената a_1 и a_2 из A учествује у декомпозицији тачно једног елемента $A + A$, па важи $\sum_{b\in A+A} f_A(b) = |A|^2$. По Коши-Шварцовој неједнакости важи

$$E^+(A) = \sum_{b\in A+A} f_A(b)^2 \geqslant \frac{\left(\sum_{b\in A+A} f_A(b)\right)^2}{|A+A|} = \frac{|A|^4}{|A+A|}.$$

Међутим, не важи супротно: за скупове велике адитивне енергије скуп збирова $A + A$ не мора бити мали. Један од кључних резултата ове области је Балог-Семереди-Гауерс теорема, која се управо односи на везу између адитивне енергије скупа A и величине скупа $A + A$. Наиме, ако скуп A има велику адитивну енергију, тада ће A имати подскуп A' велике кардиналности за који је скуп разлика $A'-A'$ мале величине. Једна од квантитативних формулација је следећа:

Теорема 2.1.2. [Sch] Нека је A подскуп адитивне групе G такав да је $E^+(A) = \delta|A|^3$. Тада постоји $A' \subset A$ такав да је $|A'| = \Omega(\delta|A|)$ и

$$|A' - A'| = O(\delta^{-4}|A'|),$$

при чему асимптотска ознака $f(x) = \Omega(g(x))$ када $x \to \infty$ значи да је $\limsup_{x\to\infty} \left|\frac{f(x)}{g(x)}\right| > 0$. Другим речима, $f(x) = \Omega(g(x))$ је негација релације $f(x) = o(g(x))$.

Снага метода адитивне комбинаторике је демонстрирана у доказу Грин-Таове теореме у раду [GT] која каже да се за сваки природан број k може наћи k простих бројева који су у аритметичкој прогресији.

2.2 Теорема Хованског о скуповима збирова

У овом одељку ће бити приказан важан резултат из рада [Kh] у проучавању скупова збирова.

Теорема 2.2.1. [Kh] Нека је G комутативна полугрупа. Ако су A и B произвољни коначни подскупови од G, тада постоји полином $p_{A,B}(X) \in \mathbb{Q}[X]$ такав да за сваки довољно велики природан број N скуп $B + NA = \{b + a_1 + \cdots + a_N \in G : b \in B, a_1, \ldots, a_N \in A\}$ има $p_{A,B}(N)$ елемената. Степен полинома $p_{A,B}$ је мањи од броја елемената скупа A.

Доказ ове теореме следи из следеће општије теореме:

Теорема 2.2.2. Нека су $\overline{G}$ скуп, $\overline{B}$ коначан подскуп од $\overline{G}$. Даље, нека је $\overline{A} = \{\overline{a}_1, \ldots, \overline{a}_m\}$ скуп од m комутирајућих пресликавања скупа $\overline{G}$ на самог себе. Тада постоји полином $p_{\overline{A},\overline{B}}(X) \in \mathbb{Q}[X]$ такав да скуп $\overline{B}(N) = \bigcup_{1 \leqslant i_j \leqslant m} \overline{a}_{i_1} \circ \cdots \circ \overline{a}_{i_N}(\overline{B})$ има $p_{\overline{A},\overline{B}}(N)$ елемената.

Такође ће бити неопходна Хилбертова теорема која ће бити наведена без доказа:

Теорема 2.2.3. [Mu, теорема 6.21] Нека је $A = K[X_0, \ldots, X_m]$ прстен полинома над пољем K. Даље, нека је A такође степенован прстен такав да су X_i елементи степена 1, и нека је $M = \bigoplus_n M_n$ степенован A-модул коначног типа. Тада постоје полином $p(X) \in \mathbb{Q}[X]$ и цео број n_0 такви да је $\dim(M_n) = p(n)$ за све $n > n_0$.

Доказ теореме 2.2.2. Нека су G_i копије скупа $\overline{G}$ које се не секу, за $i = 0, 1, \ldots$ Даље, нека су $\pi_i : \overline{G} \to G_i$ инјективна пресликавања. Са X ће се означити унија $X = \bigcup_i G_i$, а са $\mathcal{L}$ векторски простор свих линеарних пресликавања $L : X \to \mathbb{C}$ која су различита од нуле само на коначним скуповима. Векторски простор $\mathcal{L}$ је генерисан пресликавањима

$$\delta_{x_0}(x) := \begin{cases} 1, & \text{за } x = x_0 \\ 0, & \text{за } x \neq x_0, \end{cases}$$

за $x_0 \in X$. Може се дефинисати степеновање $\mathcal{L} = \bigoplus_k \mathcal{L}_k$: функција $L \in \mathcal{L}$ припада компоненти $\mathcal{L}_k$ степена k ако се L анулира само на скупу G_k. Такође, $\mathcal{L}$ се може видети као градуисани модул над прстеном $\mathbb{C}[X_1, \ldots, X_m]$: за генератор X_i и елемент $x \in X$ дефинише се $X_i \cdot \delta_x = \delta_y$, при чему је $x = \pi_j(g)$ за неко $g \in \overline{G}$ и $j \in \mathbb{N}_0$, и $y = \pi_{j+1}(\overline{a}_i(g))$. Ово дејство може се на јединствен начин проширити на дејство $\mathbb{C}[X_1, \ldots, X_m]$ на $\mathcal{L}$.

Нека је сада $\mathcal{L}_{\overline{B}}$ подмодул модула $\mathcal{L}$ генерисан елементима δ_x, за све елементе облика $x = \pi_0(\overline{b})$, $\overline{b} \in \overline{B}$. Компонента $\mathcal{L}_{\overline{B}}$ степена N је линеаран омотач скупа свих пресликавања облика δ_x, за $x = \pi_N(g)$, $g \in \overline{B}(N)$. Димензија компоненте је једнака броју елемената скупа $\overline{B}(N)$. Примена Хилбертове теореме (теорема 2.2.3) даје резултат. □

Доказ теореме 2.2.1. Нека је $\overline{G}$ скуп свих елемената полугрупе G, нека је $\overline{B}$ једнако B, и нека је $\overline{A} = \{\overline{a}_1, \ldots, \overline{a}_m\}$ скуп пресликавања облика $\overline{a}_i(g) = g + a_i$ која одговарају елементима $a_i \in A$. Тада је скуп $\overline{B}(N)$ једнак $B + NA$, па теорема 2.2.1 следи из теореме 2.2.2. □

Посебно, ако је $G = \mathbb{Z}^d$, $A \subset \mathbb{Z}^d$ коначан подскуп, и ако је $B = \{(0, \ldots, 0)\}$ једночлан скуп који садржи само координатни почетак, тада из теореме 2.2.1 следи да постоји константа h_0 и полином $p_A(X) \in \mathbb{Q}[X]$ такав да је $|hA| = p_A(h)$ за сваки природан број $h \geqslant h_0$.

Поред кардиналности скупова збирова, од интереса је и њихова структура, која је мање позната од кардиналности. Нека је $A \subset \mathbb{Z}^d$ коначан скуп, и нека су Δ_A конвексни омотач скупа A, чији скуп темена ће се обележавати са $\mathrm{ex}(\Delta_A)$, $K_A := \{\sum_{a\in A} k_a a \,:\, k_a \in \mathbb{R}_{\geqslant 0} \text{ за све } a \in A\}$, $L_A := \{\sum_{a\in A} x_a a \,:\, x_a \in \mathbb{Z} \text{ за све } a \in A\}$, $\mathcal{P}_A := \bigcup_{h=1}^{\infty} hA$ и $\mathcal{E}(A) = K_A \cap L_A \setminus \mathcal{P}_A$. Може се видети (на пример у раду [GSW]) да за произвољно $a_0 \in A$ важи

$$hA \subset (h\Delta_A \cap (ha_0 + L_{A-A})) \setminus \left(\bigcup_{a\in \mathrm{ex}(\Delta_A)} (ha - \mathcal{E}(a - A)) \right) \tag{2.1}$$

за сваки природан број h, при чему је $A - A = \{a - b \in \mathbb{Z}^d \,:\, a, b \in A\}$. Један од проблема у проучавању структуре скупова збирова је проналажење случајева када у формули (2.1) стоји једнакост. Показано је у раду [GS] да за сваки коначан скуп $A \subset \mathbb{Z}^d$ постоји природан број h_1 такав да у формули (2.1) важи једнакост за све природне бројеве $h \geqslant h_1$.

У општем случају, константе h_0 и h_1, као и полином p_A, нису познати, и до недавно нису постојале ефективне процене за величину h_0 и h_1. Међутим, у недавно објављеном раду [GSW] нађено је ефективно горње ограничење за h_0 и h_1 у општем случају, што је значајан допринос у теорији Хованског. Наиме, када се дефинише $\omega(A) := \max\limits_{a_1,a_2\in A} |a_1 - a_2|$, тада је показано да важе неједнакости

$$h_0 \leqslant (2|A|\omega(A))^{(d+4)|A|} \text{ и } h_1 \leqslant (d|A|\omega(A))^{13d^6}.$$

Упоређивање константи h_0 и h_1 је један од отворених проблема у теорији Хованског, који није решен ни у једној димензији d, и о коме се веома мало зна. Претпоставља се да важи

$$h_1 \leqslant h_0 \leqslant d!\mathrm{Vol}(\Delta). \tag{2.2}$$

У димензији $d = 1$ је показано у раду [GSW] да за скуп $A \subset \mathbb{Z}$ са бар три елемента важи $h_1, h_0 \leqslant \omega(A) - 1$, али се не зна да ли увек важи $h_1 \leqslant h_0$. Такође, није познат контрапример неједнакости (2.2) у димензијама $d > 1$, због чега проблем доказивања те неједнакости вреди разматрати.

Глава 3

Технике из теорије Ерхарта примењене на теорију Хованског

3.1 Увод

У претходној глави је показано да за скуп $A \subset \mathbb{Z}^d$ постоји полином $p_A \in \mathbb{Q}[X]$ такав да је $|hA| = p_A(h)$ почевши од неког природног броја h_0. Теорема у претходној глави је доказана на различите начине, на пример у [L] је дат геомет–ријски доказ теореме 2.2.1, док је у [Na2] и [NR] дат чисто комбинаторни доказ.

Међутим, теорема 2.2.1 не даје вредности коефицијената полинома p_A, нити одређује вредност параметра h_0. Тренутно је проблем налажења полинома p_A и константе h_0 решен само у посебним случајевима.

Недавно је посебан случај $A \subset \mathbb{Z}$ привукао пажњу ([GS],[GW],[Na2],[WCC]). Скуп A се може транслирати и раширити без промене у понашању скупова збирова. Према томе, може се сматрати да је најмањи елемент скупа A једнак нули, а да је највећи заједнички делилац елемената из A једнак јединици. Може се доказати да за сваки коначан скуп $A \subset \mathbb{Z}$ постоји коначни скуп $\mathcal{E}(A)$ такав да је

$$\bigcup_{h \geqslant 0} hA = \mathbb{N} \setminus \mathcal{E}(A).$$

У раду [GW, теорема 1] је показано да када се са b обележи највећи елемент скупа A, тада за све $h \geqslant b - |A| + 2$ важи једнакост

$$hA = \{0, 1, \ldots, hb\} \setminus (\mathcal{E}(A) \cup (bh - \mathcal{E}(b - A))), \tag{3.1}$$

при чему се неједнакост $h \geqslant b - |A| + 2$ не може побољшати. Помоћу формуле (3.1) се може одредити број елемената скупова $hA \subset \mathbb{Z}$. На пример, нека је $A = \{0, a, b\} \subset \mathbb{Z}$, при чему је $0 < a < b$ и $(a, b) = 1$. Из [Sy] се може видети да је

$$|\mathcal{E}(A)| = \frac{1}{2}(a-1)(b-1). \tag{3.2}$$

Пошто скуп $\{0, a, 2a, \ldots, (b-1)a\}$ садржи све остатке модуло b, скуп $\mathcal{E}$ је садржан у скупу $[0, ab)$, одакле је $bh - \mathcal{E}(b - A) \subset (bh - (b-a)b, bh]$. Формуле (3.1) и (3.2) заједно дају

$$|hA| = bh - \frac{1}{2}b^2 + \frac{3}{2}b \tag{3.3}$$

за свако $h \geqslant b$, јер су тада скупови $[0, ab)$ и $(bh-(b-a)b, bh]$ дисјунктни. Међутим, из оваквог доказа се не види да ли постоји h мање од b за које важи (3.3). Ово питање је решено у раду [CG]. Као посебан случај наредне теореме 3.1.3, добија се да је

$$|hA| = \begin{cases} \frac{1}{2}h^2 + \frac{3}{2}h + 1, & \text{за } 0 \leqslant h < b-2 \\ bh - \frac{1}{2}b^2 + \frac{3}{2}b, & \text{за } h \geqslant b-2. \end{cases}$$

Једна веза између кардиналности скупа збирова hA и Ерхартовог полинома p_{Δ_A} је лако видљива. Наиме, за коначан скуп $A \subset \mathbb{Z}^d$ и природни број h, сваки елемент скупа hA припада конвексном омотачу скупа $\{ha \in \mathbb{Z}^d : a \in A\}$. Због тога важи

Тврђење 3.1.1. За коначни скуп $A \subset \mathbb{Z}^d$ и природни број h важи

$$|hA| \leqslant p_{\Delta_A}(h).$$

Пример 3.1.2. Нека је $A = \{v_1, \ldots, v_{d+1}\} \subset \mathbb{Z}^d$. Ако су вектори $\widetilde{v}_1, \ldots, \widetilde{v}_{d+1} \in \mathbb{Z}^{d+1}$ линеарно независни, тада се за сваки природан број h сваки елемент скупа hA може записати на јединствен начин као збир од h сабирака из A (јединственост следи из линеарне независности). Према томе, број елемената скупа hA једнак је $\binom{h+d}{d}$.

У овој глави ће бити одређен број елемената скупа hA када скуп A има $d+2$ елемената, $A-A$ генерише $\mathbb{Z}^d$ и конвексни омотач скупа A је d-симплекс. Другим речима, биће доказана следећа теорема:

Теорема 3.1.3. [CG] Нека је $A \subset \mathbb{Z}^d$ скуп са $d+2$ елемента такав да $A - A$ генерише $\mathbb{Z}^d$, чији конвексни омотач је d-симплекс. Тада је

$$|hA| = \binom{h+d+1}{d+1}, \text{ ако је } 0 \leqslant h < \mathrm{Vol}(\Delta_A)d! - d - 1$$

$$|hA| = \binom{h+d+1}{d+1} - \binom{h - \mathrm{Vol}(\Delta_A)d! + d + 1}{d+1}, \text{ ако је } h \geqslant \mathrm{Vol}(\Delta_A)d! - d - 1.$$

Доказ ове теореме је сличан доказу Ерхартове теореме: уместо посматрања сваког hA појединачно, сви hA се утопе у вишедимензиони простор, и проучава се објекат који се добије на тај начин (тај објекат се зове конус над скупом A). За вектор $v = (a_1, \ldots, a_d) \in \mathbb{Z}^d$ дефинише се подизање $\widetilde{v} = (a_1, \ldots, a_d, 1) \in \mathbb{Z}^{d+1}$. За вектор $v = (a_1, \ldots, a_d) \in \mathbb{Z}^d$ и $h \in \mathbb{N}$, пише се (v, h) уместо $(a_1, \ldots, a_d, h)$, при чему се h назива висином вектора (v, h) (висина вектора $a = (a_1, \ldots, a_d, h) \in \mathbb{Z}^{d+1}$ се обележава са $\mathrm{height}(a) = h$). Подсећања ради, наводи се дефиниција (целобројног) конуса над скупом A:

Дефиниција 3.1.4. Нека је $A = \{a_1, \ldots, a_k\} \subset \mathbb{Z}^d$. Целобројни конус над скупом A је

$$\mathcal{C}_A := \mathrm{span}_{\mathbb{N}}(\widetilde{a}_1, \ldots, \widetilde{a}_k) = \{n_1\widetilde{a}_1 + \cdots + n_k\widetilde{a}_k \in \mathbb{Z}^{d+1} \,:\, n_1, \ldots, n_k \in \mathbb{N}_0\}.$$

Конусу $\mathcal{C}_A$ се придружује генераторни ред $\mathcal{C}_A(t) \in \mathbb{Q}[[t]]$:

$$\mathcal{C}_A(t) := \sum_{a \in \mathcal{C}_A} t^{\mathrm{height}(a)}.$$

Са Δ_A ће бити обележен конвексни омотач скупа A. Уколико се не наведе другачије, сви конуси су надаље целобројни.

3.2 Доказ теореме 3.1.3

Нека су $v_1, \ldots, v_{d+1}$ темена Δ_A, и нека је, без умањења општости, $d+2$-ги елемент скупа A управо $\mathbf{0}$. Нека су $\Lambda := \mathrm{span}_{\mathbb{Z}}(\widetilde{v}_1, \ldots, \widetilde{v}_{d+1})$ и $\Lambda^+ := \mathrm{span}_{\mathbb{N}}(\widetilde{v}_1, \ldots, \widetilde{v}_{d+1})$. Опште је познато да се $\mathbb{Z}^{d+1}/\Lambda$ може поистоветити са скупом целобројних тачака фундаменталног домена Λ, и да је број целобројних тачака у фундаменталном домену за Λ једнак детерминанти чије су колоне $\widetilde{v}_i$. (Ово се може видети у [Na1, глава 6, одељак 1]). Према томе, важи

$$|\mathbb{Z}^{d+1}/\Lambda| = \mathrm{Vol}(\Delta_A) \cdot d!.$$

Пошто $A - A$ генерише $\mathbb{Z}^d$, сви вектори $(\mathbf{0}, m)$ са $0 \leqslant m < \mathrm{Vol}(\Delta_A) \cdot d!$ су различити модуло Λ, па је

$$\mathcal{C}_A = \bigsqcup_{m=0}^{\mathrm{Vol}(\Delta_A)\cdot d! - 1} \left((\mathbf{0}, m) + \Lambda^+\right).$$

Одавде следи

$$\mathcal{C}_A(t) = \frac{1 + t + \cdots + t^{\mathrm{Vol}(\Delta_A)\cdot d!-1}}{(1-t)^{d+1}} = \frac{1 - t^{\mathrm{Vol}(\Delta_A)\cdot d!}}{(1-t)^{d+2}}.$$

Овде се може приметити да је

$$\frac{1}{(1-t)^{d+2}} = \sum_{h\geqslant 0} \binom{h+d+1}{h} t^h = \sum_{h\geqslant 0} \binom{h+d+1}{d+1} t^h,$$

док је

$$\frac{t^{\mathrm{Vol}(\Delta_A)\cdot d!}}{(1-t)^{d+2}} = \sum_{h\geqslant 0} \binom{h+d+1}{d+1} t^{h+\mathrm{Vol}(\Delta_A)\cdot d!} = \sum_{h\geqslant \mathrm{Vol}(\Delta_A)\cdot d!} \binom{h-\mathrm{Vol}(\Delta_A)\cdot d!+d+1}{d+1} t^h.$$

Одавде следи теорема.

Глава 4

Скуп збирова за скупове $A \subset \mathbb{Z}^d$ са $d+2$ елемента

4.1 Увод

Нека је $A \subset \mathbb{Z}^d$. Са Δ_A ће бити обележен конвексни омотач скупа A. Нула вектор ће бити обележен са $\mathbf{0} = (0, \ldots, 0) \in \mathbb{Z}^d$.

У овој глави ће бити приказан први резултат из рада [V2], где се даје алтернативан доказ теореме [CG, теорема 1.2].

Теорема 4.1.1. [V2, теорема 1.3] Нека је $A \subset \mathbb{Z}^d$ скуп са $d+2$ елемента такав да $A - A$ генерише $\mathbb{Z}^d$. Тада је

$$|hA| = \binom{h+d+1}{d+1}, \text{ за } 1 \leqslant h < \mathrm{Vol}(\Delta_A)d!$$

и

$$|hA| = \binom{h+d+1}{d+1} - \binom{h-\mathrm{Vol}(\Delta_A)d!+d+1}{d+1}, \text{ за } h \geqslant \mathrm{Vol}(\Delta_A)d!.$$

Такође ће бити дат доказ малог уопштења теореме 4.1.1.

Теорема 4.1.2. Нека је $A = \{v_1, \ldots, v_{d+2}\} \subset \mathbb{Z}^d$ скуп са $d+2$ елемента такав да никојих $d+1$ елемената не лежи у истој хиперравни. Тада је

$$|hA| = \binom{h+d+1}{d+1}, \text{ за } 1 \leqslant h < \mathrm{Vol}(\Delta_A)d!/D$$

и

$$|hA| = \binom{h+d+1}{d+1} - \binom{h-\mathrm{Vol}(\Delta_A)d!/D+d+1}{d+1}, \text{ за } h \geqslant \mathrm{Vol}(\Delta_A)d!/D,$$

где су $D_i = \det(\widetilde{v}_1, \ldots, \widetilde{v}_{i-1}, \widetilde{v}_{i+1}, \ldots, \widetilde{v}_{d+2})$ за $1 \leqslant i \leqslant d+1$ и $D = \mathrm{НЗД}(D_1, \ldots, D_{d+1})$.

4.2 Коментар о доказу теореме 4.1.1 из рада [CG] у несимплицијалном случају

У овом одељку ће бити посматран случај када конвексни омотач скупа A није симплекс. Специфично, обратиће се пажња на могућност раздвајања конвексног омотача Δ_A на два симплекса. Може се претпоставити да је $\mathbf{0}$ теме Δ_A. Метод рада у претходној верзији [CG] је следећи: Прво, теорема 4.1.1 се докаже за скупове A чији конвексни омотач јесте симплекс. Затим, установи се постојање темена b од Δ_A таквог да права кроз $\mathbf{0}$ и b сече унутрашњост Δ_A (остала темена ће се означити са $v_1, \ldots, v_d$). Конвексни омотач Δ_A се тада подели на два симплекса: σ, конвексни омотач скупа темена $\{\mathbf{0}, b, v_1, \ldots, v_{d-1}\}$, и τ, затворење од $\Delta_A \setminus \sigma$. На крају, примени се теорема 4.1.1 на два симплекса σ и τ. Постоји пар проблема са методом.

Нека је $d = 3$. Ако се Δ_A добија лепљењем два тетраедра по заједничкој страни, тада скуп τ неће бити симплекс. Према томе, овај метод не дели увек скуп Δ_A на два симплекса.

Општије, неки конвексни политопи са $d+2$ темена не могу да се добију лепљењем два симплекса дуж заједничке стране димензије $d-1$. Како би се ово видело, биће неопходна Радонова теорема и њено проширење:

Теорема 4.2.1. Сваки скуп $S \subset \mathbb{R}^d$ од $d+2$ елемента се може раздвојити на два дисјунктна скупа $S = S_1 \sqcup S_2$ тако да се конвексни омотачи S_1 и S_2 секу.

Теорема 4.2.2. Нека је $S = \{x_1, \ldots, x_{d+2}\} \subset \mathbb{R}^d$ скуп такав да никојих $d+1$ тачака не лежи у истој хиперравни. Даље, нека је $S = S_1 \sqcup S_2$ раздвајање такво да се конвексни омотачи скупова S_1 и S_2 секу. Тада два елемента x_i и x_j припадају истом од скупова S_1 и S_2 ако и само ако припадају различитим полупросторима одређеним хиперравни која садржи преосталих d елемената скупа S.

Доказ. Нека два елемента $x_i, x_j \in S$ припадају истом полупростору H_+ одређеном хиперравни H, која садржи преосталих d елемената скупа S. Ако x_i и x_j оба припадају једном од скупова S_1 или S_2 (без умањења општости, може се претпоставити да $x_i, x_j \in S_1$), тада је $S_2 \subset H$ и $S_1 \subset H_+$. Одавде се види да је $S_1 \cap S_2 \subset H$, па се конвексни омотачи скупова $S_1 \setminus \{x_i, x_j\}$ и S_2 секу. Ово је немогуће, јер се скуп $S \setminus \{x_i, x_j\}$ састоји од d тачака у генеричком положају, па су посебно афино независне.

Нека сада два елемента $x_i, x_j \in S$ припадају различитим полупросторима одређеним хиперравни H која садржи преосталих d тачака (без умањења општости, може се претпоставити $x_i \in H_+$ и $x_j \in H_-$). Ако $x_i \in S_1$ и $x_j \in S_2$, тада је

$S_1 \subset H_+$ и $S_2 \subset H_-$, одакле је $S_1 \cap S_2 \subset H$, па се конвексни омотачи скупова $S_1 \setminus \{s_i\}$ и $S_2 \setminus \{x_j\}$ секу. Ово је немогуће, јер се скуп $S \setminus \{x_i, x_j\}$ састоји од d тачака у генеричком положају, па су посебно афино независне. □

Нека је A скуп са $d+2$ темена чији конвексни омотач се раздваја на два d-симплекса. Нека је X_1 скуп темена заједничке стране, и нека је X_2 скуп од преостала два темена. Конвексни омотачи скупова X_1 и X_2 ће се сећи. Пошто је овакво раздвајање јединствено, ако се неки скуп са $d+2$ елемента раздваја на два подскупа чији конвексни омотачи се секу, а нису кардиналности 2 и d, тада се скуп не може раздвојити на два подскупа чији конвексни омотачи су симплекси са заједничком страном.

На пример, нека је $A = \{P_1(1,0,0,0), P_2(0,1,0,0), P_3(0,0,1,0), Q_1(0,0,0,1), Q_2(0,0,0,0), Q_3(1,1,1,-1)\}$. Конвексни омотачи скупова $X_1 = \{P_1, P_2, P_3\}$ и $X_2 = \{Q_1, Q_2, Q_3\}$ се секу у тачки $(\frac{1}{3}, \frac{1}{3}, \frac{1}{3}, 0)$. Може се видети да $A-A$ генерише $\mathbb{Z}^4$. Ако би A имало раздвајање на два симплекса, тада би један од скупова темена имао 4 елемента, а други 2. Пошто у овом случају сваки скуп има по 3 елемента, и пошто су оваква раздвајања јединствена, може се закључити да A нема раздвајање на два подскупа чији конвексни омотачи су симплекси са заједничком страном.

4.3 Доказ теореме 4.1.1

Нека је $A = \{v_1, \ldots, v_{d+2}\} \subset \mathbb{Z}^d$, и нека је h природан број. Прво ће се пронаћи скуп решења за једначину

$$\alpha_1 \widetilde{v}_1 + \cdots + \alpha_{d+2} \widetilde{v}_{d+2} = (\mathbf{0}, 0).$$

Ова једначина је еквивалентна систему једначина

$$\alpha_1 v_1 + \cdots + \alpha_{d+2} v_{d+2} = \mathbf{0},$$

$$\alpha_1 + \cdots + \alpha_{d+2} = 0.$$

Пошто су тачке $v_1, \ldots, v_{d+2}$ афино зависне, постоји нетривијално решење $\mu_1, \ldots, \mu_{d+2}$ система једначина. Како $A - A$ генерише $\mathbb{Z}^d$, постоји $i \in \{1, \ldots, d+2\}$ такво да је $\det(\widetilde{v}_1, \ldots, \widetilde{v}_{i-1}, \widetilde{v}_{i+1}, \ldots, \widetilde{v}_{d+2}) \neq 0$. Без умањења општости, може се претпоставити да је $i = d+2$. Тада је $\mu_{d+2} \neq 0$, јер би иначе тачке $v_1, \ldots, v_{d+1}$ биле афино зависне, па би било $\det(\widetilde{v}_1, \ldots, \widetilde{v}_{d+1}) = 0$.

Када се помножи једнакост $\mu_1 \widetilde{v}_1 + \cdots + \mu_{d+2} \widetilde{v}_{d+2} = (\mathbf{0}, 0)$ са $1/\mu_{d+2}$, добија се

$$\frac{\mu_1}{\mu_{d+2}} \widetilde{v}_1 + \cdots + \frac{\mu_{d+1}}{\mu_{d+2}} \widetilde{v}_{d+1} = -\widetilde{v}_{d+2}. \tag{4.1}$$

По Крамеровом правилу, важи

$$\frac{\mu_i}{\mu_{d+2}} = \frac{\det(\widetilde{v}_1, \ldots, \widetilde{v}_{i-1}, -\widetilde{v}_{d+2}, \widetilde{v}_{i+1}, \ldots, \widetilde{v}_{d+1})}{\det(\widetilde{v}_1, \ldots, \widetilde{v}_{d+1})}.$$

Нека су $\lambda_i := \det(\widetilde{v}_1, \ldots, \widetilde{v}_{d+1}) \cdot \frac{\mu_i}{\mu_{d+2}} = \det(\widetilde{v}_1, \ldots, \widetilde{v}_{i-1}, -\widetilde{v}_{d+2}, \widetilde{v}_{i+1}, \ldots, \widetilde{v}_{d+1}) \in \mathbb{Z}$ за $1 \leqslant i \leqslant d+2$. Множењем једнакости (4.1) са $\det(\widetilde{v}_1, \ldots, \widetilde{v}_{d+1})$ добија се

$$\lambda_1 \widetilde{v}_1 + \cdots + \lambda_k \widetilde{v}_k + \lambda_{k+1} \widetilde{v}_{k+1} + \cdots + \lambda_{d+2} \widetilde{v}_{d+2} = (\mathbf{0}, 0). \tag{4.2}$$

Без умањења општости, може се претпоставити да је $\lambda_1, \ldots, \lambda_k \geqslant 0$ и $\lambda_{k+1}, \ldots, \lambda_{d+2} < 0$. Из једнакости (4.2) се види да се конвексни омотачи скупова $X_1 = \{v_1, \ldots, v_k\}$ и $X_2 = \{v_{k+1}, \ldots, v_{d+2}\}$ секу. Посебно, ако је $k = 1$, тада је конвексни омотач скупа X_2 симплекс, и X_1 садржи теме v_1 које припада унутрашњости тог симплекса, па је конвексни омотач скупа A симплекс.

Нека је $w \in hA$ елемент са две репрезентације:

$$w = \alpha_1 v_1 + \cdots + \alpha_{d+2} v_{d+2} = \beta_1 v_1 + \cdots + \beta_{d+2} v_{d+2},$$

где су $\alpha_1, \ldots, \alpha_{d+2}, \beta_1, \ldots, \beta_{d+2}$ ненегативни цели бројеви такви да је $\alpha_1 + \cdots + \alpha_{d+2} = \beta_1 + \cdots + \beta_{d+2} = h$. Разлика две репрезентације елемента $w \in hA$ је $\mathbf{0}$. Штавише, сума коефицијената разлике је $\sum_{i=1}^{d+2}(\alpha_i - \beta_i) = 0$. Према томе, разлика две репрезентације истог елемента мора бити умножак целим бројем израза $\lambda_1 v_1 + \cdots + \lambda_k v_k + \lambda_{k+1} v_{k+1} + \cdots + \lambda_{d+2} v_{d+2}$. Сваком елементу $w \in hA$ одговара тачно једна репрезентација $w = \alpha_1 v_1 + \cdots + \alpha_{d+2} v_{d+2}$ за коју је $\alpha_i < \lambda_i$ за бар једно $1 \leqslant i \leqslant k$. Наиме, ако је $\alpha_i \geqslant \lambda_i$ за $1 \leqslant i \leqslant k$, тада w има репрезентацију $w = (\alpha_1 - \lambda_1)\widetilde{v}_1 + \cdots + (\alpha_{d+2} - \lambda_{d+2})\widetilde{v}_{d+2}$. Према томе, број елемената $|hA|$ једнак је броју свих репрезентација за које је $\sum_{i=1}^{d+2} \alpha_i = h$ умањеног бројем свих репрезентација за које је $\sum_{i=1}^{d+2} \alpha_i = h$ и $\alpha_i \geqslant \lambda_i$, за $1 \leqslant i \leqslant k$. Према томе, ако је $r := \lambda_1 + \cdots + \lambda_k \leqslant h$, тада је

$$|hA| = \binom{d+h+1}{h} - \binom{d+1+h-r}{h-r} = \binom{d+h+1}{d+1} - \binom{d+1+h-r}{d+1}.$$

У супротном, важи

$$|hA| = \binom{d+h+1}{d+1}.$$

Сада треба одредити r. Нека је Δ_i симплекс одређен теменима $v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_{d+2}$. Може се видети да је $\lambda_i = \pm \mathrm{Vol}(\Delta_i) d!$.

Докажимо да је свака тачка Δ_A (која није садржана у некој $d-1$ димензионој страни) садржана у тачно два симплекса Δ_i и Δ_j. При томе, темена v_i и v_j припадају различитим скуповима X_1 и X_2 у раздвајању скупа $\{v_1, \ldots, v_{d+2}\}$ на два дисјунктна подскупа чији се конвексни омотачи секу.

Наиме, ако је $x \in \Delta_i$, нека је l полуправа са почетком у v_i која пролази кроз x, и нека је y последња тачка пресека l са Δ_i припада страни $(v_1, \ldots, v_{i-1}, v_{i+1}, \ldots$ $\ldots, v_{j-1}, v_{j+1}, \ldots, v_{d+2})$. Тада је Δ_j једини други симплекс који садржи тачку x. Ово се може видети на следећи начин: Нека је Δ_k још један симплекс који садржи тачку x. Тада Δ_k не може садржати цео сегмент $[v_i, y]$, јер Δ_k не сече унутрашњост стране којој y припада. Са друге стране, ако је пресек полуправе l и Δ_k празан, тада $x \notin \Delta_k$. Према томе, постоји тачка $z \in l$ између тачака v_i и y таква да је $[v_i, z] = l \cap \Delta_k$. Ако би x припадало Δ_k, онда x не би припадало Δ_i, што је у контрадикцији са почетном претпоставком.

Пошто се унутрашњости симплекса Δ_i и Δ_j секу, темена v_i и v_j припадају истом полупростору одређеном хиперравни која је разапета са преосталих d темена. По Радоновој теореми, једно од темена v_i и v_j припада X_1, а друго X_2.

Према томе, Δ_A има покривање

$$\Delta_A = \Delta_1 \cup \cdots \cup \Delta_k = \Delta_{i+1} \cup \cdots \cup \Delta_{d+2}.$$

Пошто пресек два симплекса Δ_i и Δ_j за $1 \leqslant i, j \leqslant k$ (односно $k+1 \leqslant i, j \leqslant d+2$) има запремину 0, и пошто је $\lambda_1, \ldots, \lambda_k \geqslant 0$, тада је

$$r = \lambda_1 + \cdots + \lambda_k = \mathrm{Vol}(\Delta_1)d! + \cdots + \mathrm{Vol}(\Delta_k)d! = \mathrm{Vol}(\Delta_A)d!.$$

4.4 Доказ теореме 4.1.2

Пример 4.4.1. Нека је $A = \{(1,0), (-1,0), (0,1), (0,-1)\}$. Тада се може лако видети да је $|hA| = (h+1)^2$, $\mathrm{Vol}(\Delta_A) = 2$, $r = 4$, и да је

$$\binom{d+h+1}{d+1} - \binom{d+1+h-r}{d+1} = \binom{h+3}{3} - \binom{h-1}{3} = 2h^2 + 2 \neq |hA|.$$

До разлике долази зато што $A - A$ не генерише $\mathbb{Z}^d$. Теорема 4.1.2 објашњава и овај случај.

Нека је сада $A = \{v_1, \ldots, v_{d+2}\} \subset \mathbb{Z}^d$ скуп такав да никојих $d+1$ елемената не лежи у истој хиперравни у $\mathbb{Z}^d$. Нека су $D_i = \det(\widetilde{v}_1, \ldots, \widetilde{v}_{i-1}, \widetilde{v}_{i+1}, \ldots, \widetilde{v}_{d+2})$ за $1 \leqslant i \leqslant d+1$. Тада је

$$\begin{aligned} D_i &= \begin{vmatrix} v_1 - v_{d+2} & v_2 - v_{d+2} & \ldots & v_{i-1} - v_{d+2} & v_{i+1} - v_{d+2} & \ldots & v_{d+1} - v_{d+2} & v_{d+2} \\ 0 & 0 & \ldots & 0 & 0 & \ldots & 0 & 1 \end{vmatrix} \\ &= \begin{vmatrix} v_1 - v_{d+2} & v_2 - v_{d+2} & \ldots & v_{i-1} - v_{d+2} & v_{i+1} - v_{d+2} & \ldots & v_{d+1} - v_{d+2} \end{vmatrix}. \end{aligned}$$

Ове детерминанте одређују да ли $A - A$ генерише $\mathbb{Z}^d$. Наиме, важи следећа лема.

Лема 4.4.2. Ако је $A \subset \mathbb{Z}^d$ скуп са $d+2$ елемента такав да $A - A$ генерише $\mathbb{Z}^d$, тада је највећи заједнички делилац детерминанти D_i једнак 1.

Доказ: Ако су e_i вектори канонске базе $\mathbb{Z}^d$, тада је јединична матрица једнака $E = [e_1 \dots e_d]$, и детерминанта је 1. Са друге стране, пошто $A - A$ генерише $\mathbb{Z}^d$, сваки вектор e_i се може изразити као линеарна комбинација са целобројним коефицијентима вектора $v_1 - v_{d+2}, \dots, v_{d+1} - v_{d+2}$. Према томе, детерминанта јединичне матрице је линеарна комбинација детерминанти D_i са целобројним коефицијентима. Ако би НЗД$(D_1, \dots, D_{d+1})$ био већи од 1, тада би постојао природан број већи од 1 који дели детерминанту матрице E, што је немогуће. □

Наставља се са доказом теореме 4.1.2. Нека је сада $D = \text{НЗД}(D_1, \dots, D_{d+1})$. Као у доказу теореме 4.1.1, две репрезентације елемента $w \in hA$

$$w = \alpha_1 v_1 + \dots + \alpha_{d+2} v_{d+2} = \beta_1 v_1 + \dots + \beta_{d+2} v_{d+2}$$

су исте ако је њихова разлика умножак од

$$\frac{1}{D}\left(\lambda_1 v_1 + \dots + \lambda_k v_k + \lambda_{k+1} v_{k+1} + \dots + \lambda_{d+2} v_{d+2}\right),$$

где су $\lambda_i = \det(\widetilde{v}_1, \dots, \widetilde{v}_{i-1}, -\widetilde{v}_{d+2}, \widetilde{v}_{i+1}, \dots, \widetilde{v}_{d+1})$ (узима се да су $\lambda_1, \dots, \lambda_k \geqslant 0$, и $\lambda_{k+1}, \dots, \lambda_{d+2} < 0$). Према томе, слично као у доказу теореме 4.1.1, ако је $r_D := \frac{1}{D}(\lambda_1 + \dots + \lambda_k) \leqslant h$, тада је

$$|hA| = \binom{d+h+1}{h} - \binom{d+1+h-r_D}{h-r_D} = \binom{d+h+1}{d+1} - \binom{d+1+h-r_D}{d+1}.$$

У супротном, важи

$$|hA| = \binom{d+h+1}{d+1}.$$

На сличан начин као у доказу теореме 4.1.1 може се показати да је $r_D = \text{Vol}(\Delta_A)d!/D$. □

Вратимо се примеру 4.4.1. Детерминанте D_i су

$$D_1 = \begin{vmatrix} -1 & 0 & 0 \\ 0 & 1 & -1 \\ 1 & 1 & 1 \end{vmatrix} = -2,\ D_2 = \begin{vmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 1 & 1 & 1 \end{vmatrix} = 2,\ D_3 = \begin{vmatrix} 1 & -1 & 0 \\ 0 & 0 & -1 \\ 1 & 1 & 1 \end{vmatrix} = 2,$$

па је $D = 2$, и $r_D = 2$, па је по теореми 4.1.2

$$|hA| = \binom{h+3}{3} - \binom{h+1}{3} = (h+1)^2$$

за $h \geqslant 2$.

Напомена 1. Ако $A - A$ генерише $\mathbb{Z}^d$, тада је $D = 1$, па теорема 4.1.1 следи из теореме 4.1.2.

Глава 5

Скупови збирова за скупове $A \subset \mathbb{Z}^d$ са $d+3$ елемента

5.1 Увод

У овој глави ће бити приказан други резултат из рада [V2], који се односи на скупове $A \subset \mathbb{Z}^d$ са $d+3$ елемената са симплицијалним конвексним омотачем. Прецизније, биће доказана следећа теорема

Теорема 5.1.1. [V2, теорема 1.4] Нека је $A = \{\mathbf{0}, v_1, \ldots, v_{d+1}, w\} \subset \mathbb{Z}^d$ скуп са $d+3$ елемената, чији конвексни омотач је симплекс са теменима $v_1, \ldots, v_{d+1}$ која генеришу $\mathbb{Z}^d$. Тада се вектор $(w,1)$ може записати као $(w,1) = \frac{a_1}{q_1}\widetilde{v}_1 + \cdots + \frac{a_{d+1}}{q_{d+1}}\widetilde{v}_{d+1}$, где су a_i и q_i ненегативни цели бројеви такви да је $q_i > 0$, $0 \leqslant a_1 \leqslant q_i$, $\sum_{i=1}^{d+1} \frac{a_i}{q_i} = 1$ и $(a_i, q_i) = 1$, и важи

$$|hA| \leqslant \begin{cases} \sum\limits_{m=0}^{h} \binom{m+d+1}{m}, & h \leqslant o_w - 1 \\ \sum\limits_{m=0}^{o_w-1} \binom{h+d+1-m}{h-m}, & o_w \leqslant h \leqslant N_\Lambda - 1 \\ \sum\limits_{m=0}^{o_w-1} \binom{h+d+1-m}{h-m} - \sum\limits_{m=0}^{h-N_\Lambda} \binom{m+d+1}{m}, & N_\Lambda \leqslant h \leqslant N_\Lambda + o_w - 1 \\ \sum\limits_{m=0}^{o_w-1} \binom{h+d+1-m}{h-m} - \sum\limits_{m=0}^{o_w-1} \binom{h-N_\Lambda+d+1-m}{h-N_\Lambda-m}, & h \geqslant N_\Lambda + o_w, \end{cases}$$

где су $\Lambda = \operatorname{span}_{\mathbb{Z}}(\widetilde{v}_1, \ldots, \widetilde{v}_{d+1})$, N_Λ ред групе $\mathbb{Z}^{d+1}/\Lambda$ и $o_w = \text{НЗС}(q_1, \ldots, q_{d+1})$ ред елемента $(w,1)$ у групи $\mathbb{Z}^{d+1}/\Lambda$.

5.2 Помоћне леме

За $v = (v_1, \ldots, v_d) \in \mathbb{Z}^d$ дефинише се подизање $\widetilde{v} = (v_1, \ldots, v_d, 1) \in \mathbb{Z}^{d+1}$ вектора v. Ако је $v = (v_1, \ldots, v_d) \in \mathbb{Z}^d$ и $h \in \mathbb{N}$, тада се са (v, h) обележава $(v_1, \ldots, v_d, h)$, и h је висина вектора $(v_1, \ldots, v_d, h)$.

Решетка у $\mathbb{R}^n$ је подгрупа облика $\Lambda = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_m \leqslant \mathbb{R}^n$, где су $v_1, \ldots, v_m \in \mathbb{R}^n$ линеарно независни вектори. За m-торку вектора $v_1, \ldots, v_m$ се каже да је *база* решетке Λ, и дефинише се *фундаменталнi домен* решетке као

$$\Pi := \{\lambda_1 v_1 + \cdots + \lambda_m v_m \in \mathbb{R}^n \,:\, \lambda_i \in [0, 1)\}.$$

Може се показати ([Ne, глава 1, одељак 4, тврђење 4.2]) да је подгрупа Λ од $\mathbb{R}^n$ решетка ако и само ако је Λ дискретна подгрупа од $\mathbb{R}^n$. Подсећања ради, целобројни конус скупа A и његов генераторни ред су дефинисани у дефиницији 3.1.4:

$$\mathcal{C}_A := \operatorname{span}_{\mathbb{N}}(\widetilde{v}_1, \ldots, \widetilde{v}_k) = \{n_1\widetilde{v}_1 + \cdots + n_k\widetilde{v}_k \in \mathbb{Z}^{d+1} \,:\, n_1, \ldots, n_k \in \mathbb{N}_0\}.$$

$$\mathcal{C}_A(t) := \sum_{a \in \mathcal{C}_A} t^{\operatorname{height}(a)} \in \mathbb{Z}[[t]].$$

Пошто тачке конуса висине h формирају копију hA утопљену у $\mathbb{Z}^{d+1}$, важи да је

$$\mathcal{C}_A(t) = \sum_{h \geqslant 0} |hA| t^h.$$

Нека је $A \subset \mathbb{Z}^d$ скуп са $d+3$ елемента чији конвексни омотач (који ће се обележавати са Δ_A) је d-симплекс такав да $A - A$ генерише $\mathbb{Z}^d$. Даље, нека су $v_1, \ldots, v_{d+1}$ темена Δ_A. Тада је $\Lambda = \operatorname{span}_{\mathbb{Z}}(\widetilde{v}_1, \ldots, \widetilde{v}_{d+1}) \subset \mathbb{Z}^{d+1}$ решетка у $\mathbb{R}^{d+1}$. За овакву решетку, нека је

$$\Pi_{\mathbb{Z}} := \left\{ \sum_{i=1}^{d+1} \lambda_i \widetilde{v}_i \in \mathbb{R}^{d+1} \,:\, 0 \leqslant \lambda_i < 1 \right\} \cap \mathbb{Z}^{d+1}.$$

Број елемената скупа $\Pi_{\mathbb{Z}}$ ће се обележавати са N_Λ. Такође, са Λ^+ ће се обележавати $\Lambda^+ = \operatorname{span}_{\mathbb{N}}(\widetilde{v}_1, \ldots, \widetilde{v}_{d+1})$. Конус $\mathcal{C}_A$ ће бити подељен на класе π модуло Λ, и свака таква класа се може представити елементом $\Pi_{\mathbb{Z}}$. За елемент $\pi \in \Pi_{\mathbb{Z}}$, скуп елемената скупа $\mathcal{C}_A$ конгруентних са π модуло Λ се обележава са $\mathcal{S}_\pi$. Елемент $(g, N) \in \mathcal{S}_\pi$ је *минималан* ако $(g, N) - \widetilde{v}_i$ није елемент $\mathcal{C}_A$ ни за једно i.

Подсећања ради, у доказу теореме 3.1.3 установљено је да се за решетку Λ у $\mathbb{Z}^{d+1}$ чији фундаментални домен има позитивну запремину скуп $\mathbb{Z}^{d+1}/\Lambda$ може идентификовати са целобројним тачкама у фундаменталном домену. Број елемената $\mathbb{Z}^{d+1}/\Lambda$ једнак је детерминанти матрице чије колоне су вектори $\widetilde{v}_i$. Према томе,

$$N_\Lambda = |\mathbb{Z}^{d+1}/\Lambda| = \mathrm{Vol}(\Delta_A)d!. \tag{5.1}$$

За ово тврђење, читалац се упућује на [Na1, глава 6, одељак 1].

Лема 5.2.1. [CG, лема 3.1] Нека је $A \subset \mathbb{Z}^d$ коначан скуп такав да $A-A$ генерише $\mathbb{Z}^d$, и чији конвексни омотач је d-симплекс са теменима $v_1, \ldots, v_{d+1}$. Ако је (α, M) минимални елемент од $\mathcal{S}_\pi$, тада је

$$M \leqslant N_\Lambda - 1.$$

Доказ. Без умањења општости, може се претпоставити да је 0 теме Δ_A, на пример $v_{d+1} = 0$. Пошто је (α, M) минимални елемент скупа $\mathcal{S}_\pi$, важи да је $\alpha = a_1 + \cdots + a_M$ за неке $a_i \in A$. Довољно је доказати да су суме

$$a_1, a_1 + a_2, a_1 + a_2 + a_3, \ldots, a_1 + \cdots + a_M$$

различите модуло Λ, јер је број ненула класа модуло Λ једнак $\mathrm{Vol}(\Delta_A)d! - 1$ по (5.1).

Нека су $a_1 + \cdots + a_n$ и $a_1 + \cdots + a_m$ конгруентни модуло Λ за неке природне бројеве $1 \leqslant m < n \leqslant M$. Тада је $a_{m+1} + \cdots + a_n \in \Lambda$. Пошто a_i припадају Δ_{Λ^+}, и Δ_{Λ^+} је конвексно, то сума $a_{m+1} + \cdots + a_n$ припада скупу $\Delta_{\Lambda^+} \cap \Lambda = \Lambda^+$. Према томе, постоје $k_i \in \mathbb{N}_0$ такви да је

$$a_{m+1} + \cdots + a_n = \sum_{i=1}^{d} k_i v_i.$$

Такође, свако a_j се може записати у барицентричним координатама, пошто се налазе у симплексу Δ_A: $a_j = \sum_{i=1}^{d} \lambda_{i,j} v_i$, при чему су $\lambda_{i,j} \geqslant 0$ и $\sum_{i=1}^{d} \lambda_{i,j} \leqslant 1$. Одавде,

$$a_{m+1} + \cdots + a_n = \sum_{i=1}^{d} \left(\sum_{j=m+1}^{n} \lambda_{i,j} \right) v_i = \sum_{i=1}^{d} k_i v_i.$$

Пошто су ненула темена Δ_A линеарно независна, важи да је

$$\sum_{i=1}^{d} k_i = \sum_{j=m+1}^{n} \sum_{i=1}^{d} \lambda_{i,j} \leqslant \sum_{j=m+1}^{n} 1 = n - m.$$

Међутим, ово је у контрадикцији са претпоставком да је (α, M) минимални елемент $\mathcal{S}_\pi$. Наиме, нека је $\beta = \alpha - (a_{m+1} + \cdots + a_n)$. Тада је

$$(\alpha, M) - (\beta, M - (n-m)) = \left(\sum_{i=1}^{d} k_i v_i, n - m \right) \in \Lambda^+,$$

јер је $\sum_{i=1}^{d} k_i \leqslant n-m$ и $(0,\ldots,0)$ је теме Δ_A. □

Лема 5.2.2. Нека су $v_1,\ldots,v_{d+1} \in \mathbb{Z}^d$ вектори који генеришу $\mathbb{Z}^d$ за које је $\det(\widetilde{v}_1,\ldots,\widetilde{v}_{d+1}) \neq 0$. Даље, нека је $w \in \mathbb{Z}^d$ вектор такав да је $\widetilde{w} = a_1\widetilde{v}_1 + \cdots + a_{d+1}\widetilde{v}_{d+1}$ за ненегативне реалне коефицијенте a_i за које је $a_1+\cdots+a_{d+1}=1$. Тада су коефицијенти a_i рационални бројеви.

Доказ. Пошто су $\widetilde{v}_1,\ldots,\widetilde{v}_{d+1},\widetilde{w}$ вектори са целобројним коефицијентима, и $\det(\widetilde{v}_1,\ldots,\widetilde{v}_{d+1}) \neq 0$, по Крамеровом правилу коефицијенти a_i морају бити рационални бројеви. □

У овом одељку ће бити нађено горње и доње ограничење за $|hA|$, када је $A \subset \mathbb{Z}^d$ скуп са $d+3$ елемената.

5.3 Пример

У следећем примеру ће бити показано да за разлику од случаја када A има $d+2$ елемената, ако A има $d+3$ елемената, мера скупа A није довољна да се одреди величина hA. У два случаја ће бити описан поступак, а у осталим примерима се ради на аналоган начин.

Пример 5.3.1.

1. Нека је $A_1 = \{0,1,2,8\}$. Лако се види да за довољно велико h, скуп hA се састоји од свих целих бројева од 0 до $8h$ осим бројева $8h-1 = 8(h-1)+7, 8h-2 = 8(h-1)+6, 8h-3 = 8(h-1)+5, 8h-4 = 8(h-1)+4, 8h-5 = 8(h-1)+3, 8h-9 = 8(h-2)+7, 8h-10 = 8(h-2)+6, 8h-11 = 8(h-2)+5, 8h-17 = 8(h-3)+7$. Према томе, $|hA_1| = 8h+1-9 = 8h-8$.
2. Нека је $A_2 = \{0,1,3,8\}$. Слично као у претходном примеру, $|hA_2| = 8h-6$.
3. За $A_3 = \{0,1,4,8\}$, важи $|hA_3| = 8h-8$ за довољно велико h.
4. За $A_4 = \{0,1,5,8\}$, важи $|hA_4| = 8h-4$ за довољно велико h.

   Наиме, скуп hA_4 за довољно велики природни број h садржи све целе бројеве између 0 и $8h$, осим бројева $8h-1$, $8h-2$, $8h-4$, $8h-5$ и $8h-12$. На пример, $8h-3 = (h-1)8+5$, $8h-6 = (h-2)8+5+5$, $8h-10 = (h-2)8+5+1$, $8h-9 = (h-3)8+5+5+5$, $8h-13 = (h-3)8+5+5+1$.
5. За $A_5 = \{0,1,6,8\}$, важи $|hA_5| = 8h-2$ за довољно велико h.
6. За $A_6 = \{0,1,7,8\}$, важи $|hA_6| = 8h+1$ за довољно велико h.

Скупови $A_1, \ldots, A_6$ имају по 4 елемента, и имају исти конвексни омотач, али су величине $|hA_1|, \ldots, |hA_6|$ међусобно различите. Одавде се види да број елемената скупа $|hA|$ не зависи само од запремине конвексног омотача скупа A када A има $d+3$ елемента.

5.4 Доказ теореме 5.1.1

Подсећања ради, уводе се следеће ознаке:

- $\Lambda := \mathrm{span}_{\mathbb{Z}}(\widetilde{v}_1, \ldots, \widetilde{v}_{d+1})$,
- $\Lambda^+ := \mathrm{span}_{\mathbb{N}}(\widetilde{v}_1, \ldots, \widetilde{v}_{d+1})$,
- $\Lambda^+_{(\mathbf{0},1)} := \mathrm{span}_{\mathbb{N}}((\mathbf{0},1), \widetilde{v}_1, \ldots, \widetilde{v}_{d+1})$,
- $N_\Lambda :=$ Број тачака са целобројним координатама у фундаменталном домену за Λ,

Нека је $\mathcal{C}_A$ конус над скупом A. Он је једнак

$$\bigcup_{m=0}^{\infty} \left((mw, m) + \Lambda^+_{(0,1)} \right).$$

Међутим, вектор $(w,1)$ је коначног реда у $\mathbb{Z}^{d+1}/\Lambda$. Може се показати да вектор $o_w(w,1)$ припада Λ^+. Наиме, вектор w припада унутрашњости симплекса Δ_A, па $(w,1)$ припада граници симплекса одређеног теменима $\widetilde{v}_1, \ldots, \widetilde{v}_{d+1}, (\mathbf{0},0)$. Према томе, постоје барицентричне координате $0 \leqslant, \mu_1, \ldots, \mu_{d+1} \leqslant 1$ такве да је $\sum_{i=1}^{d+1} \mu_i \widetilde{v}_i = (w,1)$ и $\sum_{i=1}^{d+1} \mu_i = 1$. По леми 5.2.2, коефицијенти μ_i морају бити рационални бројеви, за које се може узети да је $\mu_i = \frac{a_i}{q_i}$, при чему је $0 \leqslant a_i \leqslant q_i$ и $(a_i, q_i) = 1$. Ред o_w је тада једнак НЗС$(q_1, \ldots, q_{d+1})$. Пошто су коефицијенти $o_w \frac{a_i}{q_i}$ ненегативни цели бројеви, $o_w(w,1) \in \Lambda^+$. Према томе,

$$\mathcal{C}_A = \bigcup_{m=0}^{o_w - 1} \left((mw, m) + \Lambda^+_{(0,1)} \right).$$

Унија не мора бити дисјунктна. По теореми 3.1.3, $\Lambda^+_{(0,1)}(t) = \frac{1 - t^{\mathrm{vol}(\Delta_A) d!}}{(1-t)^{d+2}}$. Ако је $\mathcal{B}_A(t)$ генераторни ред

$$\mathcal{B}_A(t) = \sum_{m=0}^{o_w - 1} t^m \Lambda^+_{(0,1)}(t) = \sum_{m=0}^{o_w - 1} t^m \left(1 - t^{\mathrm{vol}(\Delta_A) d!}\right) \sum_{h \geqslant 0} \binom{h+d+1}{h} t^h = \sum_{h \geqslant 0} b_h t^h,$$

тада за генераторни ред $\mathcal{C}_A(t) = \sum_{h \geqslant 0} |hA| t^h$ важи $|hA| \leqslant b_h$. Ово даје горње ограничење

$$|hA| \leqslant$$

$$\leqslant \begin{cases} \sum\limits_{m=0}^{h} \binom{m+d+1}{m}, & h \leqslant o_w - 1 \\ \sum\limits_{m=0}^{o_w-1} \binom{h+d+1-m}{h-m}, & o_w \leqslant h \leqslant N_\Lambda - 1 \\ \sum\limits_{m=0}^{o_w-1} \binom{h+d+1-m}{h-m} - \sum\limits_{m=0}^{h-N_\Lambda} \binom{m+d+1}{m}, & N_\Lambda \leqslant h \leqslant N_\Lambda + o_w - 1 \\ \sum\limits_{m=0}^{o_w-1} \binom{h+d+1-m}{h-m} - \sum\limits_{m=0}^{o_w-1} \binom{h-N_\Lambda+d+1-m}{h-N_\Lambda-m}, & h \geqslant N_\Lambda + o_w. \end{cases}$$

Глава 6

Елиптичке криве и конгруентни бројеви

6.1 Конгруентни бројеви

Дефиниција 6.1.1. Природан број n је *конгруентан* ако постоји правоугли троугао са три странице рационалне дужине чија површина је једнака n.

Из дефиниције се може закључити да је $n \in \mathbb{N}$ конгруентан број ако постоје рационални бројеви a, b и c који задовољавају следећи систем једначина:

$$a^2 + b^2 = c^2, \tag{6.1}$$

$$\frac{ab}{2} = n. \tag{6.2}$$

Ако су (a, b, c) дужине страница правоуглог троугла површине n, тада су (ad, bd, cd) дужине страница правоуглог троугла површине nd^2. Према томе, природан број n ће бити конгруентан ако и само ако постоје природни бројеви a, b, c и d за које правоугли троугао чије су странице дужине (a, b, c) има површину nd^2.

Нека је сада n конгруентан број (за њега постоје рационални бројеви a, b и c такви да важе једнакости (6.1) и (6.2)), и нека је $A = (c/2)^2$. Када се дода једначина (6.2) помножена са 4 једначини (6.1) (односно када се од (6.1) одузме једначина (6.2) помножена са 4), добија се

$$\begin{aligned} a^2 \pm 2ab + b^2 &= c^2 \pm 4n, \\ \left(\frac{a \pm b}{2}\right)^2 &= \left(\frac{c}{2}\right)^2 \pm n, \\ \left(\frac{a \pm b}{2}\right)^2 &= A \pm n. \end{aligned}$$

Другим речима, за сваки конгруентни број постоје три рационална броја $A-n$, A и $A+n$ који су потпуни квадрати, и суседни су у аритметичкој прогресији. Штавише постоји 1-1 кореспонденција између скупова

$$\{(a,b,c) \in \mathbb{Q}^3 \,:\, a^2+b^2=c^2,\, ab/2=n\} \text{ и } \{(r,s,t) \in \mathbb{Q}^3 \,:\, s^2-r^2=n,\, t^2-s^2=n\}$$

одређена са

$$(a,b,c) \mapsto ((b-a)/2, c/2, (b+a)/2) \text{ и } (r,s,t) \mapsto (t-r, t+r, 2s),$$

због чега су конгруентни бројеви добили такво име.

Пример 6.1.2. Број 6 је конгруентан број, јер је 6 површина правоуглог троугла са дужинама страница $(3,4,5)$.

Пример 6.1.3. Број 210 је конгруентан број, јер је 210 површина правоуглог троугла са дужинама страница $(35,12,37)$, као и правоуглог троугла са дужинама страница $(21,20,29)$.

Ферма је нашао следећи посебан пример неконгруентног броја:

Теорема 6.1.4. Број 1 није конгруентан.

Као последица Теореме 6.1.4, квадрати рационалних бројева не могу бити конгруентни бројеви. Нека су сада p_i прости бројеви конгруентни са i модуло 8. Примери конгруентних бројева су:

- Бројеви облика $2p_3$ (Ово се може видети у [Hee]).
- Прости бројеви p_5 ([St]).
- Прости бројеви p_7 и бројеви облика $2p_7$ ([St]).
- Бројеви облика $2p_3p_5$ и $2p_5p_7$ ([Mo]).
- Бројеви облика $2p_1p_3$ када је $\left(\frac{p_1}{p_3}\right) = -1$ ([Mo]).
- Бројеви облика $2p_1p_7$ када је $\left(\frac{p_1}{p_7}\right) = -1$ ([Mo]).

Примери неконгруентних бројева су:

- Прости бројеви p_1, који се могу записати као $p_1 = a^2 + 4b^2$ (a и b су цели бројеви) и за које важи $\left(\frac{a+2b}{p_1}\right) = -1$ ([B]).
- Бројеви облика $2p$, где је p прост број конгруентан 9 модуло 16 ([B]).
- Прости бројеви p_3 ([Ge]).
- Бројеви облика $2p_5$ ([Ge]).
- Бројеви облика p_3q_3, где су p_3 и q_3 два различита проста броја конгруентна 3 модуло 8 ([Ge]).
- Бројеви облика $2p_5q_5$, где су p_5 и q_5 два различита проста броја конгруентна 5 модуло 8 ([Ge]).

Нека је $A_n = \left\{(a,b,c) \in \mathbb{Q}^3 \,:\, a^2 + b^2 = c^2,\ \frac{ab}{2} = n\right\}$ скуп уређених тројки рационалних бројева који задовољавају систем једначина (6.1) и (6.2). Може се видети да је A_n пресек две површи са $\mathbb{Q}^3$:

$$A_n = \left\{(a,b,c) \in \mathbb{R}^3 \,:\, a^2 + b^2 = c^2\right\} \cap \left\{(a,b,c) \in \mathbb{R}^3 \,:\, \frac{ab}{2} = n\right\} \cap \mathbb{Q}^3.$$

Према томе, природно је очекивати да је A_n заправо скуп тачака са рационалним координатама на некој кривој. Заиста, важи следећа теорема:

Теорема 6.1.5. Пресликавање $\psi : A_n \to \{(x,y) \in (\mathbb{Q}^\times)^2 \,:\, y^2 = x^3 - n^2x\}$ дефинисано са

$$\psi(a,b,c) = \left(\frac{bn}{c-a}, \frac{2n^2}{c-a}\right)$$

је бијекција чији инверз је дефинисан са

$$\phi(x,y) = \left(\frac{x^2-n^2}{y}, \frac{2nx}{y}, \frac{x^2+n^2}{y}\right).$$

Доказ. Заменом $c = t + a$ добија се да је $b^2 = t^2 + 2ta$. Уврштавањем $a = \frac{2n}{b}$ и множењем са b добија се

$$b^3 = t^2b + 4tn,$$

одакле је

$$\left(\frac{bn}{t}\right)^3 = \frac{bn^3}{t} + \frac{4n^4}{t^2},$$

а ово се може преуредити у

$$\left(\frac{2n^2}{t}\right)^2 = \left(\frac{bn}{t}\right)^3 - n^2\left(\frac{bn}{t}\right).$$

У супротном смеру се лако провери да се $(x, y) = \psi(a, b, c)$ за $(a, b, c) \in A_n$ пресликавањем ϕ слика натраг у (a, b, c), па је ϕ инверз пресликавања ψ. □

6.2 Елиптичке криве

У овом одељку ће бити дат кратак увод у елиптичке криве. За детаљнији опис елиптичких кривих, читалац се упућује на [Si, глава 3].

Дефиниција 6.2.1. *Елиптичка крива* је глатка, пројективна, алгебарска крива рода 1, са истакнутом (односно базном) тачком O. Елиптичка крива E је *дефинисана над пољем* K (што се записује са E/K), ако је E дефинисана над K као алгебарски варијетет, и $O \in E(K)$. (За поље K, $E(K)$ је скуп свих тачака на кривој E са координатама у пољу K.) *Идеал од* E је скуп

$$I(E) := \{f \in \overline{K}[X_1, X_2] \,:\, f(P) = 0, \text{ за свако } P \in E\}.$$

Ако је $I(E/K) = I(E) \cap K[X_1, X_2]$, тада се дефинише *афини координатни прстен од* E/K са

$$K[E] := \frac{K[X_1, X_2]}{I(E/K)}.$$

Поље разломака прстена $K[E]$ се обележава са $K(E)$, и зове се *функцијско поље од* V/K. На сличан начин се дефинишу $\overline{K}[E]$ и $\overline{K}(E)$.

Свака елиптичка крива E/K је изоморфна глаткој кривој C у пројективном простору $\mathbb{P}^2$ која је дата једначином у хомогеним координатама X и Y:

$$C : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6,$$

где су $a_1, a_2, a_3, a_4, a_6 \in K$, и базна тачка се слика у тачку $[0, 1, 0]$. Ако поље K није карактеристике 2 или 3, тада крива може да се представи као скуп решења кубне једначине (у нехомогеним координатама x и y) следећег облика

$$E : y^2 = x^3 + ax + b,$$

где су a и b цели бројеви.

На елиптичкој кривој E се може дефинисати операција, на следећи начин:

Дефиниција 6.2.2. За елиптичку криву $E \subset \mathbb{P}^2$, нека су $P, Q \in E$, нека је $L \subset \mathbb{P}^2$ права која пролази кроз P и Q (ако је $P = Q$, онда се узима права L тангентна на E у P), и нека је R трећа тачка пресека. Нека је затим L' права која пролази кроз R и O. Тада се дефинише $P \oplus Q$ као трећа тачка пресека E и L'.

Може се показати да је E Абелова група у односу на ову операцију са неутралом O (базном тачком). Додатно, скуп $E(K)$ је и једна подгрупа групе E. Од посебног интереса ће бити тачке реда највише 2 криве E са рационалним координатама. Скуп таквих тачака се обележава са $E(\mathbb{Q})[2]$. Нека је сада E елиптичка крива задата једначином

$$y^2 = x^3 + Ax + B.$$

Ако је $P \in E(\mathbb{Q})[2]$, тада је $P + P = O$, тј. постоји права L тангентна на E у P паралелна y-оси. Ово се дешава ако и само ако је $y = 0$. У посебном случају, ако је $E_n : y^2 = x^3 - n^2 x$, тада је

$$E_n(\mathbb{Q})[2] = \{O, (0,0), (n,0), (-n,0)\}. \tag{6.3}$$

У теореми 6.1.5 је показано да постоји бијекција уређених тројки рационалних бројева који су дужине страница правоуглог троугла површине n, и тачака $(x, y) \in E_n(\mathbb{Q})$ са $x, y \neq 0$. По (6.3), ниједна тачка реда 2 не одговара некој тројци (a, b, c). Према томе, ако је $E_n(\mathbb{Q}) = E_n(\mathbb{Q})[2]$, тада n не може бити конгруентан број.

Важи Мордел-Вејлова теорема: ако је K бројевно поље, и E/K елиптичка крива, тада је $E(K)$ коначно генерисана Абелова група. Другим речима, постоји ненегативан цео број r такав да је $E(K) \cong E_{\text{tors}}(K) \times \mathbb{Z}^r$, где је $E_{\text{tors}}(K)$ торзиона подгрупа од $E(K)$ (скуп свих тачака коначног реда у $E(K)$). Пошто је $E(K)$ коначно генерисана Абелова група, $E_{\text{tors}}(K)$ мора бити коначна група.

6.3 Галоаова кохомологија

Пре следећег одељка, биће уведен појам Галоаове кохомологије. Нека је K савршено поље, нека је $\overline{K}$ алгебарско затворење поља K, и нека је $G_{\overline{K}/K}$ Галоаова група поља $\overline{K}$ над K. Група $G_{\overline{K}/K}$ је инверзни лимес група $G_{L/K}$ када L пролази кроз сва коначна Галоаова раширења поља K. Према томе, $G_{\overline{K}/K}$ је профинитна група, па има топологију чија база отворених скупова се састоји од колекције нормалних подгрупа са коначним индексом у $G_{\overline{K}/K}$.

Дефиниција 6.3.1. Дискретан $G_{\overline{K}/K}$-модул је Абелова група M на коју $G_{\overline{K}/K}$ дејствује, при чему је дејство непрекидно за профинитну топологију на $G_{\overline{K}/K}$

и дискретну топологију на M. Другим речима, за свако $m \in M$, стабилизатор елемента m

$$\{\sigma \in G_{\overline{K}/K} \,:\, m^\sigma = m\},$$

је подгрупа коначног индекса у $G_{\overline{K}/K}$.

Дефиниција 6.3.2. Нулта кохомолошка подгрупа $G_{\overline{K}/K}$-модула M је група $G_{\overline{K}/K}$ инваријантних елемената у M

$$M^{G_{\overline{K}/K}} = H^0(G_{\overline{K}/K}, M) = \{m \in M \,:\, m^\sigma = m \text{ за свако } \sigma \in G_{\overline{K}/K}\}.$$

Дефиниција 6.3.3. Нека је M један $G_{\overline{K}/K}$-модул. Група непрекидних 1-коциклова из $G_{\overline{K}/K}$ у M је

$$Z^1_{\text{cont}}(G_{\overline{K}/K}, M) = \{\xi : G_{\overline{K}/K} \to M \,:\, \xi \text{ непрекидно и } \xi(\sigma\tau) = \xi(\sigma)^\tau \xi(\tau)\}.$$

Група 1-кограница из $G_{\overline{K}/K}$ у M је

$$B^1(G_{\overline{K}/K}, M) = \{\xi : G_{\overline{K}/K} \to M : (\exists m \in M)(\forall \sigma \in G_{\overline{K}/K})\xi(\sigma) = m^\sigma - m\}.$$

Пошто M има дискретну топологију, сваки елемент $B^1(G_{\overline{K}/K}, M)$ је непрекидно пресликавање. Прва кохомолошка група $G_{\overline{K}/K}$-модула M је

$$H^1(G_{\overline{K}/K}, M) = \frac{Z^1_{\text{cont}}(G_{\overline{K}/K}, M)}{B^1(G_{\overline{K}/K}, M)}.$$

Тврђење 6.3.4. [Si] Нека је

$$0 \longrightarrow P \xrightarrow{\phi} M \xrightarrow{\psi} N \longrightarrow 0$$

тачан низ $G_{\overline{K}/K}$-модула. Тада постоји хомоморфизам кохомолошких група $\delta : H^0(G_{\overline{K}/K}, N) \to H^1(G_{\overline{K}/K}, P)$ такав да је следећи низ тачан:

$$0 \longrightarrow H^0(G_{\overline{K}/K}, P) \longrightarrow H^0(G_{\overline{K}/K}, M) \longrightarrow H^0(G_{\overline{K}/K}, N) \xrightarrow{\delta}$$

$$\xrightarrow{\delta} H^1(G_{\overline{K}/K}, P) \longrightarrow H^1(G_{\overline{K}/K}, M) \longrightarrow H^1(G_{\overline{K}/K}, N).$$

6.4 Селмерова и Тејт-Шафаревичева група

Дефиниција 6.4.1. *Изогенија* ϕ између елиптичких кривих E и E' је морфизам варијетета $\phi : E \to E'$ за који важи $\phi(O) = O$.

Може се показати да изогенија $\phi : E_1 \to E_2$ између елиптичких кривих индукује инјекцију функцијских поља

$$\phi^* : \overline{K}(E_2) \to \overline{K}(E_1)$$

Дефиниција 6.4.2. *Степен изогеније* ϕ је степен коначног раширења $\overline{K}(E_1)/\phi^*(\overline{K}(E_2))$, и обележава се са $\deg \phi$.

Прецизније о изогенијама се може наћи у [Si, глава 3, одељак 4].

За цео број m, изогенија множења са $[m]$ на елиптичкој кривој E је $[m](P) = P + \cdots + P$ (елемент P сабран m пута са самим собом). За елиптичке криве E_1 и E_2 и сваку неконстантну изогенију $\phi : E_1 \to E_2$ степена m постоји јединствена изогенија $\widehat{\phi} : E_2 \to E_1$ степена m таква да је $\phi \circ \widehat{\phi} = [m]$ на E_2 и $\widehat{\phi} \circ \phi = [m]$ на E_1. Изогенија $\widehat{\phi}$ је тзв. дуал изогеније ϕ.

Дефиниција 6.4.3. *Хомогени простор* елиптичке криве E/K је глатка крива C/K дефинисана над пољем K заједно са транзитивним дејством алгебарске групе E на C. Другим речима, хомоген простор елиптичке криве E/K је пар (C, μ), при чему је C/K глатка крива дефинисана над K, и $\mu : C \times E \to C$ је морфизам варијетета дефинисан над K са следећим својствима:

1. За сваку тачку $p \in C$ важи $\mu(p, O) = p$.
2. За све тачке $P, Q \in E$ и $p \in C$ важи $\mu(\mu(p, P), Q) = \mu(p, P + Q)$.
3. За све тачке $p, q \in C$ постоји јединствена тачка $P \in E$ таква да је $\mu(p, P) = q$.

Два хомогена простора C/K и C'/K елиптичке криве E/K су еквивалентна ако постоји изоморфизам хомогених простора C и C' који се слаже са дејством алгебарске групе E. Колекција свих класа еквиваленције хомогених простора елиптичке криве E/K се обележава са $WC(E/K)$. Постоји бијекција скупова $WC(E/K) \to H^1(G_{\overline{K}/K}; E)$, што оправдава назив скупа $WC(E/K)$: Вејл-Шателе група за елиптичку криву E/K. Вејл-Шателе група је интересантна, јер говори нешто о хомогеним просторима. Наиме, хомогени простор C/K припада тривијалној класи у $C(E/K)$ ако и само ако је скуп $C(K)$ непразан. Према томе, једно

важно диофантовско питање је поистовећено са проверавањем да ли је хомогени простор тривијалан.

$H^1(G_{\overline{K}/K}; E)$ је прва Галоаова кохомолошка група $G_{\overline{K}/K}$ модула E (Више о Галоаовим кохомологијама у 6.3). Ако се за G модул M са $H^0(G; M)$ обележи скуп свих G инваријантних елемената, тада сваки кратак тачан низ $G_{\overline{K}/K}$ модула $0 \to P \to M \to N \to 0$ индукује тачан низ

$$0 \longrightarrow H^0(G_{\overline{K}/K}; P) \longrightarrow H^0(G_{\overline{K}/K}; M) \longrightarrow H^0(G_{\overline{K}/K}; N) \xrightarrow{\delta}$$

$$\xrightarrow{\delta} H^1(G_{\overline{K}/K}; P) \longrightarrow H^1(G_{\overline{K}/K}; M) \longrightarrow H^1(G_{\overline{K}/K}; N).$$

Нека је сада $\phi : E \to E'$ ненула изогенија елиптичких кривих дефинисаних над K, са језгром $E[\phi]$. Тада је следећи низ тачан:

$$0 \longrightarrow E[\phi] \longrightarrow E \xrightarrow{\phi} E' \longrightarrow 0.$$

Када се узме Галоаова кохомологија $H^1(G_{\overline{K}/K}; \cdot)$, добија се дуги тачан низ

$$0 \longrightarrow E(K)[\phi] \longrightarrow E(K) \xrightarrow{\phi} E'(K) \xrightarrow{\delta}$$

$$\xrightarrow{\delta} H^1(G_{\overline{K}/K}; E[\phi]) \longrightarrow H^1(G_{\overline{K}/K}; E) \xrightarrow{\phi} H^1(G_{\overline{K}/K}; E');$$

а одавде се добија кратак тачан низ

$$0 \longrightarrow E'(K)/\phi(E(K)) \xrightarrow{\delta} H^1(G_{\overline{K}/K}; E[\phi]) \longrightarrow H^1(G_{\overline{K}/K}; E)[\phi] \longrightarrow 0.$$

Група $H^1(G_{\overline{K}/K}; E)$ се може поистоветити са $WC(E/K)$. Нека је сада M_K скуп свих нееквивалентних апсолутних вредности на K. За свако $v \in M_K$ се фиксира екстензија од v на K, која одређује утапање поља $K \subset K_v$, и декомпозициону групу $G_v \subset G_{\overline{K}/K}$. Пошто G_v дејствује на $E(K_v)$ и $E'(K_v)$, истим аргументом се добијају тачни низови

$$0 \longrightarrow E'(K_v)/\phi(E(K_v)) \xrightarrow{\delta} H^1(G_v; E[\phi]) \longrightarrow H^1(G_v; E)[\phi] \longrightarrow 0.$$

Инклузије $G_v \subset G_{\overline{K}/K}$ и $E(K) \subset E(K_v)$ индукују рестрикције на кохомолошким групама, због чега је следећи дијаграм комутативан:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E'(K)/\phi(E(K)) & \xrightarrow{\delta} & H^1(G_{\overline{K}/K}; E[\phi]) & \longrightarrow & WC(E/K)[\phi] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \prod_{v \in M_K} E'(K_v)/\phi(E(K_v)) & \xrightarrow{\delta} & \prod_{v \in M_K} H^1(G_v; E[\phi]) & \longrightarrow & \prod_{v \in M_K} WC(E/K_v)[\phi] & \longrightarrow & 0.
\end{array}$$

Један од главних циљева теорије елиптичких кривих је налажење слике количника $E'(K)/\phi(E(K))$ у групи $H^1(G_{\overline{K}/K}; E[\phi])$, што је еквивалентно са налажењем језгра пресликвања

$$H^1(G_{\overline{K}/K}; E[\phi]) \longrightarrow WC(E/K)[\phi].$$

Ово је еквивалентно са проверавањем да ли одређени хомогени простори садрже рационалну K тачку. Овај проблем је тежак над глобалним пољима. Једна олакшица је што се проблем може посматрати над локалним пољима. Наиме, на аналоган начин као за глобална поља, проблем налажења локалног језгра

$$\mathrm{Ker}\left(H^1(G_v; E[\phi]) \longrightarrow WC(E/K_v)[\phi]\right)$$

се своди на налажење K_v рационалне тачке на одређеним хомогеним просторима. Као важан помоћни алат за налажење језгара, корисна је следећа дефиниција:

Дефиниција 6.4.4. Нека је $\phi : E/K \to E'/K$ изогенија елиптичких кривих. Тада је *ϕ-Селмерова група* E/K подгрупа од $H^1(G_{\overline{K}/K}; E[\phi])$ дефинисана са

$$\mathrm{Sel}^{\phi}(E/K) = \mathrm{Ker}\left(H^1(G_{\overline{K}/K}; E[\phi]) \longrightarrow \prod_{v \in M_K} WC(E/K_v)\right),$$

док је *Тејт-Шафаревичева група* дефинисана са

$$Ш(E/K) = \mathrm{Ker}\left(WC(E/K) \longrightarrow \prod_{v \in M_K} WC(E/K_v)\right).$$

Тејт-Шафаревичева група може да се види као група класа еквиваленције хомогених простора за E/K чији хомогени простори садрже K_v рационалну тачку за свако $v \in M_K$. За групе дефинисане у дефиницији 6.4.4 важи следеће:

Теорема 6.4.5. [Si, глава 10, одељак 4, теорема 4.2] Нека је $\phi : E/K \to E'/K$ изогенија елиптичких кривих дефинисаних над K. Тада важи:

1. Постоји тачан низ

$$0 \longrightarrow E'(K) = \phi(E(K)) \longrightarrow \mathrm{Sel}^{\phi}(E/K) \longrightarrow Ш(E/K)[\phi] \longrightarrow 0.$$

2. Група $\mathrm{Sel}^{\phi}(E/K)$ је коначна.

Тврђење 6.4.6. [Si] Нека су $E/\mathbb{Q}$ и $E'/\mathbb{Q}$ елиптичке криве дате једначинама

$$E : y^2 = x^3 + ax^2 + bx \text{ и } E' : y^2 = x^3 - 2ax^2 + (a^2 - 4b)x$$

за $a, b \in \mathbb{Z}$, и нека је

$$\phi : E \to E',\ \phi(x,y) = \left(\frac{y^2}{x^2}, \frac{y(b-x^2)}{x^2}\right)$$

изогенија степена два чије језгро је $E[\phi] = \{O, (0,0)\}$. Нека је

$$S = \{\infty\} \cup \{\text{прости фактори } 2b(a^2-4b)\}.$$

Даље, нека је M подгрупа од $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ генерисана са -1 и простим факторима $2b(a^2-4b)$. За свако $d \in M$ дефинисани су хомогени простори $C_d/\mathbb{Q}$ и $C'_d/\mathbb{Q}$ за $E/\mathbb{Q}$ и $E'/\mathbb{Q}$ следећим једначинама

$$C_d : dw^2 = d^2t^4 - 2adt^2z^2 + (a^2-4b)z^4,$$

$$C'_d : dw^2 = d^2t^4 + adt^2z^2 + bz^4,$$

за $(w,t,z) \in \mathbb{Q}^3$. Тада је

$$\mathrm{Sel}^\phi(E/\mathbb{Q}) \cong \{d \in M \,:\, C_d(\mathbb{Q}_v) \neq \emptyset \text{ за свако } v \in S\},$$

$$\mathrm{Sel}^{\widehat{\phi}}(E/\mathbb{Q}) \cong \{d \in M \,:\, C'_d(\mathbb{Q}_v) \neq \emptyset \text{ за свако } v \in S\},$$

где се са $C_d(\mathbb{Q}_v) \neq \emptyset$ подразумева да постоји нетривијално решење $(w,t,z) \in \mathbb{Q}_v^3 \setminus \{(0,0,0)\}$ једначине C_d у $\mathbb{Q}_v$.

6.5 L-функција на елиптичкој кривој

Нека је $E/\mathbb{Q}$ елиптичка крива дефинисана једначином $y^2 = x^3 + ax + b$, где су $a, b \in \mathbb{Z}$. Ако је

$$a_p := \frac{p - |\{(x,y) \in \mathbb{F}_p \,:\, y^2 = x^3 + ax + b\}|}{2\sqrt{p}},$$

тада се дефинише Хасе-Вејлова L-функција помоћу Ојлеровог производа:

$$L_E(s) := \prod_p \frac{1}{1 - a_p p^{-s} + p^{-2s}},$$

при чему Ојлеров производ апсолутно конвергира за $\mathrm{Re}(s) > 1$. Из Шимура-Танијама хипотезе (коју су доказали Е. Вајлс и Р. Тејлор) следи да се Хасе-Вејлова L-функција може аналитички проширити на целу комплексну раван.

Следећа хипотеза је позната као Бирч-Свинертон-Дајер хипотеза, тј. БСД хипотеза. У следећем одељку ће бити приказана веза између БСД хипотезе и конгруентних бројева.

Хипотеза 1. [BSD] Нека је $E/\mathbb{Q}$ елиптичка крива. Тада важи

1. $L_E(s)$ има нулу у $s=1$ чији ред је једнак рангу $r = \text{rank}E(\mathbb{Q})$.
2. Постоји лимес
$$\lim_{s\to 1} \frac{L_E(s)}{(s-1)^r} = A|Ш(E/\mathbb{Q})|,$$
где је A тачно одређена ненула константа.

Прецизнији опис константе A није предмет ове дисертације, нити се употребљава у њој. Дефиниција константе A се може наћи у [Si, Додатак C, хипотеза 16.5]. Познато је да се L функција L_E елиптичке криве дефинисане над пољем $\mathbb{Q}$ може аналитички проширити на целу комплексну раван. Међутим, и даље се не зна да ли је $|Ш(E/\mathbb{Q})|$ коначно. У случају елиптичке криве $E_n : y^2 = x^3 - n^2x$ дефинисане над $\mathbb{Q}$ за природан број n, ако је $L_{E_n}(1) \neq 0$, други део БСД хипотезе постаје
$$L_{E_n}(1)/B = |Ш(E_n/\mathbb{Q})|, \tag{6.4}$$
за ненула константу B. У радовима [Ru1] и [Ru2] је показано да из $L_{E_n}(1) \neq 0$ следи да је група $Ш(E_n/\mathbb{Q})$ коначног реда, и да су непарни делови обе стране у (6.4) једнаки. Хипотеза 1 има битну улогу у проучавању конгруентних бројева. Наиме, позната је следећа хипотеза

Хипотеза 2. [ACK] Ако је природан број n конгруентан са $5, 6$ или 7 модуло 8, тада је n конгруентан број.

Опште је познато да је $L_{E_n}(1) = 0$ када је n конгруентно са $5, 6$ или 7 модуло 8 (ово се може видети у [Ko, глава 2, тврђење 12]). Ако важи хипотеза 1, тада је $\text{rank}E_n(\mathbb{Q}) \neq 0$ када је n конгруентно са $5, 6$ или 7 модуло 8. По теореми 6.1.5 постоје рационални бројеви a, b, c такви да је $a^2 + b^2 = c^2$ и $ab/2 = n$, па је n конгруентан број. Према томе, из хипотезе 1 следи хипотеза 2.

Хипотеза 1 има још једну везу са конгруентним бројевима: Нека су

$$\begin{aligned}
A_n &= \left|\{(x,y,z) \in \mathbb{Z}^3 \,:\, n = 2x^2 + y^2 + 32z^2\}\right|, \\
B_n &= \left|\{(x,y,z) \in \mathbb{Z}^3 \,:\, n = 2x^2 + y^2 + 8z^2\}\right|, \\
C_n &= \left|\{(x,y,z) \in \mathbb{Z}^3 \,:\, n = 8x^2 + 2y^2 + 64z^2\}\right|, \\
D_n &= \left|\{(x,y,z) \in \mathbb{Z}^3 \,:\, n = 8x^2 + 2y^2 + 16z^2\}\right|.
\end{aligned}$$

У раду [T] је показано безусловно да за непарне конгруентне бројеве n важи да је $2A_n = B_n$, док за парне конгруентне бројеве важи да је $2C_n = D_n$. Са друге стране, ако за непаран број n важи $2A_n = B_n$ (односно ако за паран број n важи $2C_n = D_n$), може се показати да је тада n конгруентан број, али једино уз помоћ хипотезе 1.

Глава 7

Теорија графова и Селмерове групе

7.1 Селмерове групе и графови

У овој глави ће бити приказан резултат из рада [F]. То је један од првих радова у коме је приказана веза између Селмерових група и теорије графова. Такође ће бити приказана веза између графова и БСД хипотезе.

Пре тога, биће уведени основни појмови везани за графове.

Дефиниција 7.1.1. *Граф* је уређени пар $G = (V, E)$, где је V непразан скуп, а E је подскуп скупа $\{(x, y) \mid x, y \in V\}$. Елементи V су *темена* графа G, а елементи E су *ивице* графа G. Ако за свако $(x, y) \in E$ важи да $(y, x) \in E$, тада је граф G *неусмерен*, и ивицу (x, y) обележавамо са $\overline{xy}$. У супротном, G је *усмерен* граф, и ако је $(x, y) \in E$, а $(y, x) \notin E$, тада ивицу (x, y) обележавамо са $\overrightarrow{xy}$. *Степен темена* v је број ивица које полазе из v, и обележава се са $\deg v$.

Дефиниција 7.1.2. *Матрица суседства графа* G са $V = \{v_1, \ldots, v_n\}$ је $A(G) = [a_{i,j}]_{1 \leqslant i,j \leqslant n}$, где су коефицијенти $a_{i,j}$ дефинисани са

$$a_{i,j} = \begin{cases} 1, & \text{ако } (v_i, v_j) \in E, \\ 0, & \text{иначе.} \end{cases}$$

Дефиниција 7.1.3. *Лапласова матрица графа* G је

$$M(G) = \operatorname{diag}(\deg v_1, \ldots, \deg v_n) - A(G).$$

Напомена 2. Може се видети да је у Лапласовој матрици неког графа збир свих колона једнак нула колони. Према томе, ако се из матрице избаци нпр. последња колона, тада ранг матрице остеје непромењен.

Дефиниција 7.1.4. Партиција $V = V_1 \cup V_2$ графа $G = (V, E)$ је *непарна* ако постоји теме $v \in V_1$ такво да је $|\{\overrightarrow{vw} : w \in V_2\}|$ непарно, или постоји теме $v \in V_2$ такво да је $|\{\overrightarrow{vw} : w \in V_1\}|$ непарно. Иначе је партиција *парна*. *Граф* G *је непаран* ако је свака нетривијална партиција непарна.

Нека су сада $E_n : y^2 = x^3 - n^2x$ и $E'_n : y^2 = x^3 + 4n^2x$ елиптичке криве дефинисане над $\mathbb{Q}$, и нека је $\phi : E_n \to E'_n$ изогенија степена 2 задата са

$$\phi(x, y) = \left(\frac{y^2}{x^2}, \frac{y(-n^2 - x^2)}{x^2}\right).$$

Тада постоје тачни низови

$$0 \to \frac{E'_n(\mathbb{Q})[\phi]}{\phi(E_n(\mathbb{Q})[2])} \to \frac{E'_n(\mathbb{Q})}{\phi(E_n(\mathbb{Q}))} \xrightarrow{\widehat{\phi}} \frac{E_n(\mathbb{Q})}{2E_n(\mathbb{Q})} \to \frac{E_n(\mathbb{Q})}{\widehat{\phi}(E'_n(\mathbb{Q}))} \to 0 \tag{7.1}$$

$$0 \to \frac{E'_n(\mathbb{Q})}{\phi(E_n(\mathbb{Q}))} \to \mathrm{Sel}^{\phi}(E_n) \xrightarrow{f} Ш(E_n)[\phi] \to 0 \tag{7.2}$$

$$0 \to \frac{E_n(\mathbb{Q})}{\widehat{\phi}(E'_n(\mathbb{Q}))} \to \mathrm{Sel}^{\widehat{\phi}}(E'_n) \xrightarrow{\widehat{f}} Ш(E'_n)[\widehat{\phi}] \to 0 \tag{7.3}$$

$$0 \to Ш(E_n)[\phi] \to Ш(E_n)[2] \xrightarrow{\widehat{\phi}} Ш(E'_n)[\widehat{\phi}] \to 0, \tag{7.4}$$

где је $\widehat{\phi}$ дуал ϕ. Нека је сада M подгрупа од $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ генерисана са -1 и простим факторима $2n$, и нека је $S = \{\infty\} \cup \{\text{прости фактори } 2n\}$. Када се примени тврђење 6.4.6 на криве E_n и E'_n, добија се

$$\mathrm{Sel}^{\phi}(E_n) \cong \{d \in M : C_d(\mathbb{Q}_v) \neq \emptyset \text{ за свако } v \in S\}.$$

$$\mathrm{Sel}^{\widehat{\phi}}(E_n) \cong \{d \in M : C'_d(\mathbb{Q}_v) \neq \emptyset \text{ за свако } v \in S\},$$

где су

$$C_d : dw^2 = d^2t^4 + 4n^2z^4,$$
$$C'_d : dw^2 = d^2t^4 - n^2z^4.$$

хомогени простори елиптичких кривих E_n и E'_n. Језгра пресликавања f и $\widehat{f}$ у (7.2) и (7.3) су

$$\mathrm{Ker} f = \{d \in M \,:\, C_d(\mathbb{Q}) \neq \emptyset\},\ \mathrm{Ker}\widehat{f} = \{d \in M \,:\, C'_d(\mathbb{Q}) \neq \emptyset\}, \tag{7.5}$$

одакле се види да $1 \in \mathrm{Ker} f$ и $\pm 1, \pm n \in \mathrm{Ker}\widehat{f}$. Према томе

$$\begin{aligned} 2 + \mathrm{rank} E_n(\mathbb{Q}) &= \dim_{\mathbb{F}_2} \mathrm{Ker} f + \dim_{\mathbb{F}_2} \mathrm{Ker}\widehat{f} \\ &= \dim_{\mathbb{F}_2} \mathrm{Sel}^{\phi}(E_n) - \dim_{\mathbb{F}_2} Ш(E_n)[\phi] \\ &+ \dim_{\mathbb{F}_2} \mathrm{Sel}^{\widehat{\phi}}(E'_n) - \dim_{\mathbb{F}_2} Ш(E'_n)[\widehat{\phi}]. \end{aligned}$$

Дакле, $\mathrm{rank} E_n(\mathbb{Q}) = 0$ ако и само ако је $\mathrm{Ker} f = \{1\}$ и $\mathrm{Ker}\widehat{f} = \{\pm 1, \pm n\}$. Посебно, ако је $\mathrm{Sel}^{\phi}(E_n) = \{1\}$ и $\mathrm{Sel}^{\widehat{\phi}}(E'_n) = \{\pm 1, \pm n\}$, тада је $\mathrm{rank} E_n(\mathbb{Q}) = 0$ и $Ш(E_n)[\phi] = Ш(E'_n)[\widehat{\phi}] = \{1\}$. Помоћу (7.4) се додатно добија да је $Ш(E_n)[2] = \{1\}$, одакле је ред групе $Ш(E_n)$ непаран.

Постоји граф чија непарност даје информацију о Селмеровој групи. Граф се конструише на следећи начин: за природан број n конструише се граф $G(n)$ чији је скуп темена једнак скупу простих фактора n, и скуп ивица је $\{\overrightarrow{p_i p_j} : \left(\frac{p_j}{p_i}\right) = -1\}$, где је $\left(\frac{p}{q}\right)$ Лежандров симбол (узима се да је $\left(\frac{n}{2}\right) = 1$ за непарне целе бројеве n).

Теорема 7.1.5. [F] У следећа два случаја је $\mathrm{Sel}^{\phi}(E_n) = \{1\}$ и $\mathrm{Sel}^{\widehat{\phi}}(E_n) = \{\pm 1, \pm n\}$:

1. $n = p_1 \dots p_t$ $(t \geqslant 1)$, где су $p_1, \dots, p_t$ различити прости фактори броја n за које је $p_1 \equiv 3 \pmod 8$ и $p_i \equiv 1 \pmod 8$, $2 \leqslant i \leqslant t$, и $G(n)$ је непаран граф.
2. $n = 2p_1 \dots p_t$ $(t \geqslant 1)$, где су $p_1, \dots, p_t$ различити прости фактори броја n за које је $p_1 \equiv 5 \pmod 8$ и $p_i \equiv 1 \pmod 8$, $2 \leqslant i \leqslant t$, и $G(n/2)$ је непаран граф.

Доказ.

1. Граф $G(n)$ је неусмерен по Гаусовом закону реципроцитета. Такође, ако је $G(n)$ непарно, тада и $G(2n)$ непарно. Нека су

$$M = \langle -1, 2, p_1, \dots, p_t \rangle \subset \mathbb{Q}^{\times}/(\mathbb{Q}^{\times})^2,\ S = \{\infty, 2, p_1, \dots, p_t\},$$

$$C_d : dw^2 = d^2t^4 + 4n^2z^4,\ C'_d : dw^2 = d^2t^4 - n^2z^4.$$

Потребно је показати следеће:

а) За свако $d \in M \setminus \{1\}$ постоји $v \in S$ за које је $C_d(\mathbb{Q}_v) = \emptyset$.

б) За свако $d \in M \setminus \{\pm 1, \pm n\}$ постоји $v \in S$ за које је $C'_d(\mathbb{Q}_v) = \emptyset$.

а) Нека је $V = \{2, p_1, \ldots, p_t\}$. За $d < 0$ је $C_d(\mathbb{Q}_\infty) = \emptyset$. Довољно је размотрити случај када је $d = \prod_{p \in V_1} p$ за свако $V_1 \subset V$, $V_1 \neq \emptyset$. Ако је $V_1 \neq V$, тада је V_1 и $V_2 = V \setminus V_1$ нетривијална партиција од V. Пошто је $G(2n)$ непаран граф, тада или постоји $q \in V_1$ за које је $\left(\frac{2n/d}{q}\right) = -1$, или постоји $p \in V_2$ за које је $\left(\frac{d}{p}\right) = -1$.

Сада треба показати да је $C_d(\mathbb{Q}_p) = C_d(\mathbb{Q}_q) = \emptyset$. Нека је $(w, t, z) \neq (0, 0, 0)$ нетривијално решење једначине C_d у $\mathbb{Q}_p$. За $w = dw'$, крива C_d има облик

$$C_d : dw'^2 = t^4 + (2n/d)^2 z^4.$$

За свако $l \in \mathbb{Z}$, тројка $(w'p^{2l}, tp^l, zp^l)$ је такође решење C_d. Према томе, може се претпоставити да су $w', t, z \in \mathbb{Z}_p$ и да је $v_p(w') = v_p(t) = 0$, где је v_p експоненцијална валуација на $\mathbb{Q}_p$ нормализована са $v_p(p) = 1$. Пошто $p \nmid d$ и $p \mid \frac{2n}{d}$, то је $dw'^2 \equiv t^4$ модуло p. Ово је немогуће, јер је $\left(\frac{d}{p}\right) = -1$. Према томе, $C_d(\mathbb{Q}_p) = \emptyset$.

Са друге стране, $q \neq 2$, пошто је $\left(\frac{m}{2}\right) = 1$ за све непарне целе бројеве m. Ако је $q = p_1 \equiv 3 \pmod 8$, тада једначина C_d даје $t^4 \equiv -(2n/d)^2 z^4 \pmod q$, јер $q \mid d$ и $q \nmid \frac{2n}{d}$. Ово је немогуће, јер је претпостављено да је $\left(\frac{-1}{q}\right) = -1$. Ако је $q = p_i \equiv 1$ модуло 8 за неко $i \geqslant 2$, тада је

$$\left(\frac{-1}{p}\right)_4 = 1 \text{ и } \left(\frac{2n/d}{q}\right) = \left(\frac{-(2n/d)^2}{q}\right)_4 = 1,$$

што је у супротности са претпоставком да је $\left(\frac{2n/d}{q}\right) = -1$ (за цео број n и прост број p који не дели n, симбол $\left(\frac{n}{p}\right)_4$ је једнак 1 ако постоји цео број x такав да је $x^4 \equiv n$ модуло p). Према томе, $C_d(\mathbb{Q}_q) = \emptyset$. Нека је сада $V_1 = V$, тј. $d = 2n$. Крива C_{2n} је одређена једначином

$$C_{2n} : 2nw'^2 = t^4 + z^4.$$

Међутим, редукцијом модуло p_1 се добија да је $C_{2n}(\mathbb{Q}_{p_1}) = \emptyset$. Дакле, $\mathrm{Sel}^\phi(E_n) = \{1\}$.

б) Нека је сада $V = \{p_1, \ldots, p_t\}$. Пошто $\pm 1, \pm n$ припадају $\mathrm{Sel}^{\widehat{\phi}}(E'_n)$ и $C'_2(\mathbb{Q}_2) = \emptyset$, треба показати да $d \notin \mathrm{Sel}^{\widehat{\phi}}(E'_n)$ за свако $1 < d < n$ које дели n. Нека је сада $d = \prod_{p \in V_1} p$, где је V_1 подскуп од V за који је $1 \leqslant |V_1| < t$. Пошто је $G(n)$ непаран граф, или постоји $q \mid d$ такво да је $\left(\frac{n/d}{q}\right) = -1$, или постоји $p \mid n/d$ такво да је $\left(\frac{d}{p}\right) = -1$. Како је $G(n)$ неусмерен, непаран граф, постоје бар два проста фактора n са својством p или q. Према томе, може се претпоставити да је $p \neq p_1$.

Нека једначина

$$C'_d : dw^2 = d^2t^4 - n^2z^4$$

има нетривијално решење $(w,t,z) \neq (0,0,0)$ у $\mathbb{Q}_p$. Може се претпоставити да је $\min\{v_p(w), v_p(t), v_p(z)\} = 0$. Ако је $v_p(w) \geqslant 1$, тада је $v_p(t) \geqslant 1$. Нека су $w = \frac{n}{d}w'$ и $t = \frac{n}{d}t'$. Тада C'_d има једначину

$$C'_d : dw'^2 = n^2t'^4 - d^2z^4,$$

одакле је $\left(\frac{\pm d}{p}\right) = 1$, што је у контрадикцији са $\left(\frac{d}{p}\right) = -1$. Према томе, $C'_d(\mathbb{Q}_p) = \emptyset$, па је $\mathrm{Sel}^{\widehat{\phi}}(E'_n) = \{\pm 1, \pm n\}$.

2. Ако је d позитиван паран број такав да $d \mid n$, тада је $C_d(\mathbb{Q}_2) = C'_d(\mathbb{Q}_2) = \emptyset$, па $d \notin \mathrm{Sel}^{\phi}(E_n)$ и $d \notin \mathrm{Sel}^{\widehat{\phi}}(E'_n)$ за такве d. Пошто је $G(n/2)$ неусмерен, непаран граф, може се показати да $d \notin \mathrm{Sel}^{\phi}(E_n)$ за свако $d \mid n/2$, $1 < d \leqslant n/2$, и да $d \notin \mathrm{Sel}^{\widehat{\phi}}(E'_n)$ за свако $d \mid n/2$, $1 < d \leqslant n/2$ на исти начин као у доказу дела 1. Према томе, $\mathrm{Sel}^{\phi}(E_n) = \{1\}$ и $\mathrm{Sel}^{\widehat{\phi}}(E'_n) = \{\pm 1, \pm n\}$. □

7.2 БСД хипотеза и графови

По БСД хипотези, ако је $L_{E_n}(1) \neq 0$, тада је $L_{E_n}(1) = A|\text{Ш}(E_n)|$, где је A ненула константа.

У раду [T] изражена је вредност $L_{E_n}(1)/A$. За непарно n, нека је

$$a(n) = \frac{1}{2} \sum_{\substack{x^2+y^2+2z^2=n \\ 2|y}} \eta_1(x+iy), \tag{7.6}$$

где је η_1 карактер групе $(\mathbb{Z}[i]/(4(1+i)))^\times$ дефинисан са

$$\eta_1(\alpha) = \begin{cases} 1, & \text{за } \alpha = 1, 7, 3+2i, 1+2i \\ -1, & \text{за } \alpha = 3, 5, 7+2i, 5+2i. \end{cases}$$

За $2||n$, нека је

$$b(n/2) = \frac{1}{2} \sum_{\substack{x^2+2y^2+z^2=n/2 \\ 2|z}} \eta_2(x+\sqrt{-2}y) \tag{7.7}$$

где је η_2 карактер групе $\left(\mathbb{Z}[\sqrt{-2}]/(4)\right)^\times$ дефинисан са

$$\eta_2(\alpha) = \eta_2(-\alpha),\ \eta_2(1) = 1,\ \eta_2(1+2\sqrt{-2}) = \eta_2(3+2\sqrt{-2}) = -1.$$

Ако је $\omega(n)$ број различитих простих фактора од n, тада је

$$L_{E_n}(1) = \begin{cases} (a(n)/2^{\omega(n)})^2, & \text{ако } 2 \nmid n, \\ (b(n/2)/2^{\omega(n/2)})^2, & \text{ако } 2||n. \end{cases}$$

Скуп решења једначине $x^2 + y^2 + 2z^2 = n$ је у бијекцији са скупом решења једначине $X^2 + Y^2 + Z^2 = 2n$ за која важи $2 \mid Z$; бијекција је следећег облика:

$$(X, Y, Z) = (x + y, x - y, 2z),\ (x, y, z) = \left(\frac{X+Y}{2}, \frac{X-Y}{2}, \frac{Z}{2}\right).$$

Број решења (X, Y, Z) је $4h(-2n)$, где је $h(-2n)$ класни број поља $\mathbb{Q}(\sqrt{-2n})$. Рубин је показао да су непарни делови $L_{E_n}(1)/A$ и Ш(E_n) једнаки ако је $a(n) \neq 0$ или $b(n/2) \neq 0$ (непарни делови два цела броја су исти ако су њихове просте факторизације исте до на степен двојке). Према томе, треба одредити Силовљеву 2-подгрупу $C^{(2)}_{\mathbb{Q}(\sqrt{-2n})}$ класне групе $C_{\mathbb{Q}(\sqrt{-2n})}$. По Гаусовој теорији рода (чији доказ може да се види у [Ga, глава 5, теорема 305, страна 364]),

$$2 - \operatorname{rank} C_K = \omega(2n) - 1 = \omega(n).$$

У радовима [Re] и [RR] је за сваки природан број n конструисан граф $G(n)$ такав да $2^{\omega(n)}||h(-2n)$ ако и само ако је $G(n)$ непаран граф (за дефиницију непарног графа видети почетак главе 7). Нека је $K = \mathbb{Q}(\sqrt{-D})$ имагинарно квадратно поље са $D \geqslant 2$, класним бројем $h_K = |C_K|$, 2-рангом групе C_K једнаким $r_2 = \dim_{\mathbb{F}_2} C_K/C_K^2$ и дискриминантом $\operatorname{disc}(K) = -D$. Ако је $\omega(n) = t$, тада је по Гаусовој теорији рода $r_2 = t - 1$, па $2^{t-1} \mid h_K$.

Као у доказу теореме 7.1.5, за овакво поље се конструише граф $G(D)$ (на исти начин као граф $G(n)$): скуп темена је једнак скупу простих фактора D, и скуп ивица је $\{\overrightarrow{p_i p_j} : \left(\frac{p_j}{p_i}\right) = -1\}$, где је $\left(\frac{p}{q}\right)$ Лежандров симбол (узима се да је $\left(\frac{n}{2}\right) = 1$ за непарне целе бројеве n). Непарност графа $G(D)$ ће дати информацију о класном броју h_K поља $K = \mathbb{Q}(\sqrt{-D})$.

Теорема 7.2.1. Нека је $K = \mathbb{Q}(\sqrt{-D})$ имагинарно квадратно поље са $D \geqslant 2$, $\operatorname{disc}(K) = -D$, и $\omega(D) = t$. Тада

1. $2^{t-1}||h_K$ ако и само ако је граф $G(D)$ непаран.
2. Ако је $D = 8p_2 \dots p_t$ $(t \geqslant 2)$, $p_2 \equiv \pm 3 \pmod 8$ и $p_i \equiv \pm 1 \pmod 8$ за $i \geqslant 3$, тада $2^{t-1}||h_K$ ако и само ако је $G(D/8)$ непаран граф.

Доказ.

1. Нека су $p_1, \ldots, p_t$ различити прости фактори D. За сваки подскуп $S \subset \{1, \ldots, t\}$ са $1 \leqslant |S| \leqslant t-1$, нека је $Q_S = \prod_{i \in S} p_i$, и нека је Q'_S бесквадратни део D/Q_S. Нека је α_S ознака за произвољни идеал у O_K норме $N(\alpha_S) = Q_S$. Тада скуп
$$\{[\alpha_S] = [\alpha_{\overline{S}}] \,:\, S \subset \{1, \ldots, t\},\, 1 \leqslant |S| \leqslant t-1\}$$
садржи $2^{r_2} - 1 = \frac{1}{2}(2^t - 2)$ класа идеала у C_K реда 2, при чему је $\overline{S} = \{1, \ldots, t\} \setminus S$. У радовима [Re] и [RR] показано је да класа $[\alpha_S]$ припада C_K^2 ако и само ако једначина
$$u^2 Q_S + v^2 Q'_S - w^2 = 0$$
има нетривијално решење $(u, v, w) \neq (0, 0, 0)$. Према томе,
$$\begin{aligned} 2^{t-1} || h_K &\Leftrightarrow [\alpha_S] \notin C_K^2 \text{ за сваки скуп } S \subset \{1, \ldots, t\} \text{ са } 1 \leqslant |S| \leqslant t-1 \\ &\Leftrightarrow \text{за сваки скуп } S \subset \{1, \ldots, t\} \text{ са } 1 \leqslant |S| \leqslant t-1 \text{ или постоји} \\ &\quad \text{прост број } p | Q'_S \text{ такав да је } \left(\frac{Q_S}{p}\right) = -1, \text{ или постоји} \\ &\quad \text{прост број } q | Q_S \text{ такав да је } \left(\frac{Q'_S}{q}\right) = -1 \\ &\Leftrightarrow G(D) \text{ је непаран граф.} \end{aligned}$$

2. Граф $G(D/8)$ је неусмерен по Гаусовом закону реципроцитета, а пошто је $\left(\frac{2}{p_2}\right) = -1$ и $\left(\frac{2}{p_i}\right) = 1$ за $i \geqslant 3$, граф $G(D)$ се може добити од графа $G(D/8)$ тако што се дода теме 2, и веза $\overrightarrow{p_2 2}$ на граф $G(D/8)$. Граф $G(D)$ је непаран ако и само ако је то и $G(D/8)$. □

Нека је сада $N(n; a_1, \ldots, a_n)$ број целобројних решења једначине $n = a_1 x_1^2 + \cdots + a_n x_n^2$ за природне бројеве $a_1, \ldots, a_n$. Тада важи следећа теорема

Теорема 7.2.2. 1. Нека n задовољава прво својство у теореми 7.1.5. Тада крива E_n задовољава БСД хипотезу ако и само ако је $N(n; 1, 64, 2) \equiv 0$ модуло 2^{t+1}.

2. Нека n задовољава друго својство у теореми 7.1.5. Тада крива E_n задовољава БСД хипотезу ако и само ако је $N(n/2; 1, 32, 4) \equiv 0$ модуло 2^{t+1}.

Доказ.

1. По раду [T], вредност L-функције у 1 криве E_n се може изразити као

$$L_{E_n}(1)/A = (a(n)/2^t)^2,$$

где је $a(n)$ дато у (7.6). Пошто је $n \equiv 3$ модуло 8, важи следеће:

$$\begin{aligned} a(n) &= \frac{1}{2} \sum_{x^2+16y^2+2z^2=n} \eta_1(x+4iy) = \frac{1}{2} \sum_{x^2+16y^2+2z^2=n} (-1)^{((x+4y)^2-1)/8} \\ &= \frac{1}{2} \sum_{x^2+16y^2+2z^2=n} (-1)^{(x^2-1)/8+y} \\ &= \frac{1}{2} \left(\sum_{\substack{x^2+16y^2+2z^2=n \\ 2|y}} (-1)^{(x^2-1)/8} - \sum_{\substack{x^2+16y^2+2z^2=n \\ 2\nmid y}} (-1)^{(x^2-1)/8} \right) \\ &= \sum_{x^2+64y^2+2z^2=n} (-1)^{(x^2-1)/8} - \frac{1}{2} \sum_{x^2+16y^2+2z^2=n} (-1)^{(x^2-1)/8}. \end{aligned}$$

Када је $n \equiv 3$ модуло 16, тада је $n \equiv x^2 + 2z^2 \equiv 3$ модуло 16, па је $x^2 \equiv 1$ модуло 16, и $(x^2-1)/8$ је парно. Са друге стране, када је $n \equiv 11$ модуло 16, тада је $n \equiv x^2 + 2 \equiv 11$ модуло 16, па је $x^2 \equiv 9$ модуло 16, и $(x^2-1)/8$ је непарно. Према томе, $a(n)$ је одређено до на знак. Другим речима, важи

$$a(n) = \pm \left(N(n;1,64,2) - \frac{1}{2} N(n;1,16,2) \right).$$

Пошто је $n \equiv 3$ модуло 8, важи

$$\begin{aligned} N(n;1,16,2) &= \left| \{(x,y,z) \in \mathbb{Z}^3 \,:\, x^2+y^2+2z^2 = n, 4 \mid y\} \right| \\ &= 2h(-2n) \\ &\equiv 2^{t+1} \,(\mathrm{mod}\, 2^{t+2}) \text{ по теореми 7.2.1} \end{aligned}$$

Из теореме 7.1.5 се добија да је $\mathrm{rank} E_n(\mathbb{Q}) = 0$ и да је $|Ш(E_n)|$ непарно. Према томе:

$$\begin{aligned} \text{Важи БСД хипотеза} &\Leftrightarrow a(n)/2^t \equiv 1 \,(\mathrm{mod}\, 2) \\ &\Leftrightarrow 2N(n;1,64,2) - N(n;1,16,2) \equiv 2^{t+1} \,(\mathrm{mod}\, 2^{t+2}) \\ &\Leftrightarrow N(n;1,64,2) \equiv 0 \,(\mathrm{mod}\, 2^{t+1}). \end{aligned}$$

2. У овом случају важи

$$L_{E_n}(1)/A = (b(n/2)/2^t)^2,$$

где је $b(n/2)$ дато са (7.7). Ако је $n/2 \equiv 5$ модуло 8, тада је

$$\begin{aligned} b(n/2) &= \frac{1}{2} \sum_{x^2+8y^2+4z^2=n/2} \eta_2(x + 2\sqrt{-2}y) \\ &= \frac{1}{2} \left(N(n/2; 1, 32, 4) - \sum_{\substack{x^2+8y^2+4z^2=n/2 \\ 2 \nmid y}} 1 \right) \\ &= N(n/2; 1, 32, 4) - \frac{1}{2} N(n/2; 1, 8, 4). \end{aligned}$$

Међутим, такође важи

$$\begin{aligned} N(n/2; 1, 8, 4) &= |\{(x, y, z) \in \mathbb{Z}^3 \, : \, x^2 + 2y^2 + z^2 = n, 2 \mid z\} \\ &= 2h(-n) \equiv 2^{t+1} \pmod{2^{t+2}} \text{ по теореми 7.2.1.} \end{aligned}$$

Према томе:

$$\begin{aligned} \text{Важи БСД хипотеза} &\Leftrightarrow b(n/2)/2^t \equiv 1 \pmod 2 \\ &\Leftrightarrow N(n/2; 1, 32, 4) - \frac{1}{2} N(n/2; 1, 8, 4) \equiv 2^t \pmod{2^{t+1}} \\ &\Leftrightarrow N(n/2; 1, 32, 4) \equiv 0 \pmod{2^{t+1}}. \square \end{aligned}$$

Глава 8

Заједничка дистрибуција Селмеровог ранга кривих конгруентног броја

8.1 Увод

Нека је за бесквадратни цели број n

$$E_n : y^2 = x^3 - n^2 x$$

елиптичка крива дефинисана над $\mathbb{Q}$, нека је

$$\phi : E_n \to E'_n$$

изогенија другог степена са кодоменом

$$E'_n : y^2 = x^3 + 4n^2 x$$

дефинисана са

$$\phi(x, y) = (y^2/x^2, y(n^2 - x^2)/x^2),$$

и нека је $\widehat{\phi}$ изогенија дуална ϕ. Даље, нека је број елемената $\mathrm{Sel}^{[2]}(E_n/\mathbb{Q})$ једнак $2^{2+s(n)}$, број елемената $\mathrm{Sel}^{\phi}(E_n/\mathbb{Q})$ једнак $2^{s^{\phi}(n)}$ и број елемената $\mathrm{Sel}^{\widehat{\phi}}(E_n/\mathbb{Q})$ једнак $2^{2+s^{\widehat{\phi}}(n)}$. За ранг $r(n)$ елиптичке криве E_n важе битне неједнакости:

$$r(n) \leqslant s(n),$$

$$r(n) \leqslant s^{\phi}(n) + s^{\widehat{\phi}}(n).$$

Према томе, ако је $s(n) = 0$, или ако је $s^{\phi}(n) + s^{\widehat{\phi}}(n) = 0$, тада је $r(n) = 0$. Ранг $s(n)$ је приступачнији од $r(n)$, због чега је група $\mathrm{Sel}^{[2]}(E_n/\mathbb{Q})$ привукла пажњу (на пример у [FJ], [F], [FX], [HB1], [HB2], [JO]). У раду [Rh] је нађена вероватноћа да за бесквадратан цео број n са m простих фактора важи $(s^{\phi}(n), s^{\widehat{\phi}}(n)) = (0, 0)$.

У овој глави ће бити одређена дистрибуција $(s^{\phi}(n), s^{\widehat{\phi}}(n))$ над непарним, бесквадратним природним бројевима са фиксираним бројем простих фактора. Прецизније, биће доказане следеће две теореме.

Теорема 8.1.1. [V1] Нека су $m \in \mathbb{N}$, p и q ненегативни цели бројеви, X реалан број већи од 0 и $\alpha(X; p, q, m)$ број бесквадратаних природних бројева $n \leqslant X$ конгруентних са ± 3 модуло 8 и са m простих фактора за које је $(s^{\phi}(n), s^{\widehat{\phi}}(n)) = (p, q)$. Када $X \to \infty$, за $\gamma_{\alpha}(m, p, q) = 2^{(m-q+p-1)(m-q+p)/2+(m-q+p-1)(q-p+1)}$ важи:

1. Ако је $q \geqslant p + 1$, тада је

$$\alpha(X; p, q, m) = \sum_{\substack{t_1+t_2=m-q+p-1 \\ s_1+s_2=q-p+1 \\ t_2+s_1 \equiv 1 \,(\mathrm{mod}\, 2)}} (1 + o(1)) \frac{X(\log\log X)^{m-1}}{\log X} \frac{m}{t_1!t_2!s_1!s_2!} \frac{1}{4^m}$$
$$\times \gamma_{\alpha}(m, p, q) \sum_{k=0}^{m-q-1} \mathrm{sym}(m - q + p - 1, k) E_{m-q+p-1-k,q-p}(m - q - 1 - k),$$

2. Ако је $q = p$, тада је

$$\alpha(X; q, q, m) = \sum_{\substack{t_1+t_2=m-1 \\ s_1+s_2=1 \\ t_2+s_1 \equiv 1 \,(\mathrm{mod}\, 2)}} (1 + o(1)) \frac{X(\log\log X)^{m-1}}{\log X} \frac{m}{t_1!t_2!} \frac{1}{4^m}$$
$$\times \gamma_{\alpha}(m, p, p) \mathrm{sym}(m - 1, m - 1 - q),$$

3. Ако је $p = q + 1$, тада је

$$\alpha(X; q + 1, q, m) = \sum_{\substack{t_1+t_2=m \\ t_2 \equiv 1 \,(\mathrm{mod}\, 2)}} (1 + o(1)) \frac{X(\log\log X)^{m-1}}{\log X} \frac{m}{t_1!t_2!} \frac{1}{4^m}$$
$$\times \gamma_{\alpha}(m, q + 1, q) \mathrm{par}(m, q),$$

4. Ако је $q < p - 1$, $q > m + p - 1$ или $m < q + 1$, тада је

$$\alpha(X; p, q, m) = 0.$$

Теорема 8.1.2. [V1] Нека су $m \in \mathbb{N}$, p и q ненегативни цели бројеви, X реалан број већи од 0 и $\beta(X;p,q,m)$ број бесквадратних природних бројева $n \leqslant X$ конгруентних са ± 1 модуло 8 и са m простих фактора за које је $(s^{\phi}(n), s^{\widehat{\phi}}(n)) = (p,q)$. Када $X \to \infty$, за $\gamma_\beta(m,p,q) := 2^{(m-q+p-2)(m-q+p-1)/2+(m-q+p-2)(q-p+2)}$ важи:

1. Ако је $q \geqslant p$, тада је

$$\begin{aligned}
\beta(X;p,q,m) &= \sum_{\substack{t_1+t_2=m-q+p-2\\ t_2\neq 0\\ s_1+s_2=q-p+2\\ t_2+s_1\equiv 0 \,(\mathrm{mod}\, 2)}} (1+o(1))\frac{X(\log\log X)^{m-1}}{\log X}\frac{m}{t_1!t_2!s_1!s_2!}\frac{1}{4^m}\\
&\times \gamma_\beta(m,p,q)\left\{\sum_{k=0}^{m-q-2}\mathrm{sym}(m-q+p-2,k)E_{m-q+p-3-k,q-p+1}(m-q-2-k)2^{-q}\right.\\
&\left.+\sum_{k=0}^{m-q-3}\mathrm{sym}(m-q+p-2,k)E_{m-q+p-3-k,q-p+1}(m-q-k-2)(1-2^{-q})\right\}+\\
&+\sum_{\substack{s_1+s_2=q-p+2\\ s_1\neq 0\\ s_1\equiv 0 \,(\mathrm{mod}\, 2)}} (1+o(1))\frac{X(\log\log X)^{m-1}}{\log X}\frac{m}{(m-q+p-2)!s_1!s_2!}\frac{1}{4^m}\times\\
&\times \gamma_\beta(m,p,q)\sum_{k=0}^{m-q-2}\mathrm{sym}(m-q+p-2,k)E_{m-q+p-1-k,q-p}(m-q-k-2)+\\
&+(1+o(1))\frac{X(\log\log X)^{m-1}}{\log X}\frac{m}{(m-q+p-2)!(q-p+2)!}\frac{1}{4^m}\times\\
&\times \gamma_\beta(m,p,q)\sum_{k=0}^{m-q-1}\mathrm{sym}(m-q+p-2,k)E_{m-q+p-2-k,q-p+1}(m-q-k-1)
\end{aligned}$$

2. Ако је $q = p-1$, тада је

$$\begin{aligned}
\beta(X;q+1,q,m) &= \sum_{\substack{t_1+t_2=m-1\\ t_2\neq 0\\ s_1+s_2=1\\ t_2+s_1\equiv 0 \,(\mathrm{mod}\, 2)}} (1+o(1))\frac{X(\log\log X)^{m-1}}{\log X}\frac{m}{t_1!t_2!}\frac{1}{4^m}\\
&\times \gamma_\beta(m,p,p-1)\\
&\times \big(\mathrm{sym}(m-2,m-2-q)2^{-q}+\mathrm{sym}(m-2,m-3-q)(1-2^{-q})\big)\\
&+(1+o(1))\frac{X(\log\log X)^{m-1}}{\log X}\frac{m}{4^m}\gamma_\beta(m,p,p-1)\mathrm{sym}(m-1,m-1-q);
\end{aligned}$$

3. Ако је $q = p-2$, тада је

$$\beta(X; q+2, q, m) = \sum_{\substack{t_1+t_2=m \\ t_2\neq 0 \\ t_2\equiv 0 \,(\mathrm{mod}\, 2)}} (1+o(1))\frac{X(\log\log X)^{m-1}}{\log X}\frac{m}{t_1!t_2!}\frac{1}{4^m}$$
$$\times \gamma_\beta(m, p, p-2)$$
$$\times \left(\mathrm{sym}(m-2, m-q-2)2^{-q} + \mathrm{sym}(m-2, m-q-3)(1-2^{-q})\right)$$
$$+ (1+o(1))\frac{X(\log\log X)^{m-1}}{\log X}\frac{1}{(m-1)!}\frac{1}{4^m}\gamma_\beta(m, p, p-2)\mathrm{par}(m, q),$$

4. Ако је $q < p-2$, $q > m-p+2$ или $m < q+1$, тада је

$$\beta(X; p, q, m) = 0.$$

За доказ теорема 8.1.1 и 8.1.2 биће неопходна веза између теорије графова и Селмерових група, број природних бројева n са k простих фактора са одређеном расподелом простих фактора по конгруенцијама модуло 8, као и вероватноћа да матрица фиксне димензије има одређен ранг.

Тврђење 8.1.3. [XZ] Нека је $n = p_1 \dots p_t q_1 \dots q_s$ непаран, бесквадратни природан број, где су p_i прости фактори броја n конгруентни са 1 модуло 4, а q_j прости фактори конгруентни 3 модуло 4. Тада важи

1. Ако је $n \equiv \pm 3$ модуло 8, нека је $G_1 = (V_1, E_1)$ граф дефинисан са

$$V_1 = \{p_1, \dots, p_t, q_1, \dots, q_s\},$$
$$E_1 = \left\{\overline{p_i p_j} \,:\, \left(\frac{p_j}{p_i}\right) = -1,\ 1 \leqslant i \neq j \leqslant t\right\}$$
$$\cup \left\{\overrightarrow{p_i q_r} \,:\, \left(\frac{q_r}{p_i}\right) = -1,\ 1 \leqslant i \leqslant t,\ 1 \leqslant r \leqslant s\right\}.$$

   Ако је $M_1(n)$ Лапласова матрица графа $G_1(n)$, тада су рангови $s^\phi(n) = t - \mathrm{rank}_{\mathbb{F}_2} M_1(n)$ и $s^{\widehat{\phi}}(n) = s - 1 + t - \mathrm{rank}_{\mathbb{F}_2} M_1(n)$.

2. Ако је $n \equiv \pm 1$ модуло 8, нека је $G_2 = (V_2, E_2)$ граф дефинисан са

$$V_2 = \{p_1, \dots, p_t, q_1, \dots, q_s, -1\},$$
$$E_2 = \left\{\overline{p_i p_j} \,:\, \left(\frac{p_j}{p_i}\right) = -1,\ 1 \leqslant i \neq j \leqslant t\right\}$$
$$\cup \left\{\overrightarrow{p_i q_r} \,:\, \left(\frac{q_r}{p_i}\right) = -1,\ 1 \leqslant i \leqslant t,\ 1 \leqslant r \leqslant s\right\}$$
$$\cup \left\{\overrightarrow{(-1)p} \,:\, p \equiv \pm 3 \,(\mathrm{mod}\, 8),\ p \in V_2\right\}.$$

Ако је $M_2(n)$ Лапласова матрица графа $G_2(n)$, тада је $s^{\phi}(n) = t + 1 - \operatorname{rank}_{\mathbb{F}_2} M_2(n)$ и $s^{\widehat{\phi}}(n) = s - 1 + t - \operatorname{rank}_{\mathbb{F}_2} M_2(n)$.

Лема 8.1.4. [Rh] Нека је $\operatorname{par}(t, e)$ вероватноћа да неусмерен граф са t темена има 2^{e+1} парних партиција, где је $0 \leqslant e \leqslant t-1$. Тада је

$$\operatorname{par}(t,e) = 2^{\binom{t-e}{2}-\binom{t}{2}} d(t-1,e) \prod_{j=1}^{\lfloor t-e/2 \rfloor} \left(1 - \left(\frac{1}{2}\right)^{2j-1}\right),$$

где је $d(m,j) = \prod_{i=0}^{j-1}(2^m - 2^i)/(2^j - 2^i)$ и $d(m,0) = 1$.

Лема 8.1.5. [Rh] Нека је G неусмерен граф са t темена, и нека је ρ ранг Лапласове матрице графа G. Тада је број парних партиција графа G једнак $2^{t-\rho}$.

У следећим теоремама ће бити одређен број природних бројева чији прости фактори задовољавају услове неопходне за теореме 8.1.1 и 8.1.2.

Теорема 8.1.6. [Rh] Нека су k и $m > 1$ природни бројеви, X позитиван реалан број, $0 \leqslant a_1, \ldots, a_{\varphi(m)} \leqslant k$ цели бројеви такви да је $a_1 + \cdots + a_{\varphi(m)} = k$. Даље, нека је $\pi_k(X; m; a_1, \ldots, a_{\varphi(m)})$ број бесквадратних целих бојева $n \leqslant X$ са k простих фактора, при чему је тачно a_j од тих фактора конгруентно са r_j модуло m, где су $1 = 1 < r_2 < \cdots < r_{\varphi(m)} < m$ стандардни представници елемената $(\mathbb{Z}/m\mathbb{Z})^{\times}$.

1. Ако је $m = 4$, $t = a_1$, $s = a_2$ и када $X \to \infty$, тада важи:

$$\pi_k(X; 4; t, s) = (1 + o(1)) \frac{k}{t!s!} \frac{1}{2^k} \frac{X(\log\log X)^{k-1}}{\log X}.$$

2. Ако је $m = 8$, $t_1 = a_1$, $s_1 = a_2$, $t_2 = a_3$, $s_2 = a_4$, и када $X \to \infty$, тада важи:

$$\pi_k(X; 8; t_1, t_2, s_1, s_2) = (1 + o(1)) \frac{k}{t_1!t_2!s_1!s_2!} \frac{1}{4^k} \frac{X(\log\log X)^{k-1}}{\log X}.$$

Теорема 8.1.7. [Rh] Нека је k природан број, нека је $\delta = (\delta_1, \ldots, \delta_k)$, при чему $\delta_i \in \{1, 3, 5, 7\}$ за $1 \leqslant i \leqslant k$, и нека су ε_{ij} фиксирани елементи $\{-1, 1\}$, за $1 \leqslant i < j \leqslant k$. Нека је $C_k(X, \delta)$ скуп k-торки $(p_1, \ldots, p_k)$ простих бројева $2 < p_1 < p_2 < \cdots \leqslant X$ за које је $p_1 \ldots p_k \leqslant X$, $p_j \equiv \delta_j$ модуло 8. Тада је број елемената $C_k(X, \delta)$ за које је $\left(\frac{p_i}{p_j}\right) = \varepsilon_{ij}$ са $1 \leqslant i < j \leqslant k$ једнак

$$2^{-\binom{k}{2}}(1 + o(1))|C_k(X, \delta)|.$$

Тврђење 8.1.8. [BM] Нека су $t, s, \rho \geqslant 0$ цели бројеви, нека су $\Pi_n(q) = (1-q)(1-q^2)\dots(1-q^n)$ и $\Pi_0(q) = 1$, и нека је

$$\begin{bmatrix} n \\ k \end{bmatrix}(q) = \frac{\Pi_n(q)}{\Pi_k(q)\Pi_{n-k}(q)}.$$

Ако се вероватноћа да произвољна матрица димензије $t \times s$ са коефицијентима у $\mathbb{F}_2$ има ранг ρ обележи са $E_{t,s}(\rho)$, тада важи:

1. Ако је $s = 0$, $t = 0$ или $\rho > \min\{s, t\}$, тада је

$$E_{t,s}(\rho) = 0.$$

2. Ако је $t \geqslant s$, тада је

$$E_{t,s}(\rho) = 2^{(-s+\rho)(t-\rho)} \begin{bmatrix} s \\ s-\rho \end{bmatrix} \left(\frac{1}{2}\right) \frac{\Pi_t(\frac{1}{2})}{\Pi_{t-\rho}(\frac{1}{2})}.$$

3. Ако је $s \geqslant t$, тада је

$$E_{t,s}(\rho) = 2^{(-t+\rho)(s-\rho)} \begin{bmatrix} t \\ t-\rho \end{bmatrix} \left(\frac{1}{2}\right) \frac{\Pi_s(\frac{1}{2})}{\Pi_{s-\rho}(\frac{1}{2})}.$$

4. Посебно, важи

$$E_{t,t+s}(\rho) = 2^{(-t+\rho)(t+s-\rho)} \begin{bmatrix} t \\ t-\rho \end{bmatrix} \left(\frac{1}{2}\right) \frac{\Pi_{t+s}(\frac{1}{2})}{\Pi_{t+s-\rho}(\frac{1}{2})}.$$

Тврђење 8.1.9. [V1] Број симетричних матрица димензије $n \times n$ са коефицијентима у пољу $\mathbb{F}_2$ ранга ρ је

$$\begin{bmatrix} n \\ n-\rho \end{bmatrix}(2) \cdot \prod_{j=1}^{\lceil \rho/2 \rceil} \left(1 - \left(\frac{1}{2}\right)^{2j-1}\right) 2^{\rho(\rho+1)/2}.$$

Према томе, вероватноћа да произвољна симетрична матрица димензије $n \times n$ са коефицијентима у $\mathbb{F}_2$ има ранг ρ је

$$\mathrm{sym}(n, \rho) := \begin{bmatrix} n \\ n-\rho \end{bmatrix}(2) \cdot \prod_{j=1}^{\lceil \rho/2 \rceil} \left(1 - \left(\frac{1}{2}\right)^{2j-1}\right) 2^{\rho(\rho+1)/2 - n(n+1)/2}.$$

8.2 Доказ теореме 8.1.1

Нека је $n \equiv \pm 3$ модуло 8, и нека је $G_1(n)$ граф дефинисан у тврђењу 8.1.3 са Лапласовом матрицом $M_1(n)$. Да би било $(s^{\phi}(n), s^{\widehat{\phi}}(n)) = (p, q)$, мора да важи следеће: $s^{\phi}(n) = t - \operatorname{rank}_{\mathbb{F}_2} M_1(n) = p$, $s^{\widehat{\phi}}(n) = s - 1 + t - \operatorname{rank}_{\mathbb{F}_2} M_1(n)$. Према томе, мора да важи $s = q - p + 1$, $t = m - s = m - q + p - 1$ и $\operatorname{rank}_{\mathbb{F}_2} M_1(n) = t - p = m - q - 1$. Доказ теореме 8.1.1 је сведен на два дела: налажење вероватноће да матрица $M_1(n)$ има ранг $\rho = m - q - 1$, и налажење вероватноће да природан број $n < X$ са m простих фактора конгруентан са ± 3 модуло 8 има $t = m - 1 + p - 1$ фактора конгруентних 1 модуло 4 и $s = q - p + 1$ фактора конгруентних 3 модуло 4.

Ивице између темена p_i и p_j графа $G_1(n)$ су обостране, док су ивице између темена p_i и q_r усмерене од p_i до q_r. Према томе, матрица $M_1(n)$ је облика

$$M_1(n) = \left[\begin{array}{c|c} \mathrm{A} & \mathrm{B} \\ \hline 0 & 0 \end{array}\right],$$

где је A симетрична матрица димензије $t \times t$, и B је матрица димензије $t \times s$. По напомени 2, ако се избаци последња колона из матрице, ранг ће остати непромењен.

Лема 8.2.1. Вероватноћа да матрица над пољем $\mathbb{F}_2$ облика $[AB]$ има ранг ρ је

$$\sum_{k=0}^{\rho} \operatorname{sym}(t, k) E_{t-k,s}(\rho - k),$$

где је A симетрична матрица димензије $t \times t$, а B матрица димензије $t \times s$ (при чему је $s > 0$).

Доказ. Нека је A ранга k. Тада се могу употребити елементарне трансформације врста и колона да се A трансформише у A^0 (канонску матрицу матрице A), што даје матрицу

$$\left[\begin{array}{c|c|c} E_{k\times k} & 0_{k\times(t-k)} & \\ \hline 0_{(t-k)\times k} & 0_{(t-k)\times(t-k)} & B'_{t\times s} \end{array}\right],$$

где је E јединична матрица, и 0 нула матрица. Коефицијенти у матрици B' ће остати независни и униформно распоређени, пошто је она добијена након примене елементарних трансформација на $[AB]$. Сада се елементарним транс–формација могу анулирати првих k врста матрице B' помоћу јединичне матрице, након чега се добија

$$\left[\begin{array}{c|c|c} E_{k\times k} & 0_{k\times(t-k)} & 0_{k\times s} \\ \hline 0_{(t-k)\times k} & 0_{(t-k)\times(t-k)} & B''_{(t-k)\times s} \end{array}\right].$$

Према томе, вероватноћа да $[AB]$ има ранг ρ је

$$P(\mathrm{rank}_{\mathbb{F}_2}[AB]=\rho)=\sum_{k=0}^{\rho}P(\mathrm{rank}_{\mathbb{F}_2}A=k)P(\mathrm{rank}_{\mathbb{F}_2}B''=\rho-k)$$
$$=\sum_{k=0}^{\rho}\mathrm{sym}(t,k)E_{t-k,s}(\rho-k).\square$$

Пошто је последња колона једнака збиру осталих, у доказу теореме ће бити коришћена горња формула са $s-1$ уместо s. Сада треба посматрати посебне случајеве када је $s=1$ или $s=0$.

1. Ако је $s=1$, када се уклони последња колона, остаће само симетрична матрица A, па вероватноћа да $M_1(n)$ има ранг ρ је

$$\mathrm{sym}(t,\rho).$$

2. Ако је $s=0$, тада је граф $G_1(n)$ неусмерен, па је број парних партиција 2^{e+1} по леми 8.1.5 једнак $2^{t-\rho}$. Дакле, матрица $M_1(n)$ ће имати ранг ρ ако и само ако граф $G_1(n)$ има $2^{t-\rho}$ парних партиција, а вероватноћа да се то деси је по леми 8.1.4 једнака

$$\mathrm{par}(m,t-\rho-1).$$

Напомена 3. У претходној леми је нађена вероватноћа да матрица $M_1(n)$ има ранг ρ. Ако се број таквих матрица помножи са бројем природних бројева n са t простих фактора конгруентних 1 модуло 4 и s простих фактора конгруентних 3 модуло 4, добиће се број природаних бројева $n\leqslant X$ са $m=t+s$ простих фактора који одговарају матрици облика $M_1(n)$ ранга ρ. Међутим, морају се раздвојити случајеви када је $n\equiv\pm3$ модуло 8 и када је $n\equiv\pm1$ модуло 8.

Према томе, треба представити број природних бројева n са t простих фактора конгруентних 1 модуло 4 и s простих фактора конгруентних 3 модуло 4 као збир количина природних бројева n који имају

1. t_1 простих фактора конгруентних 1 модуло 8,
2. t_2 простих фактора конгруентних 5 модуло 8,
3. s_1 простих фактора конгруентних 3 модуло 8,
4. s_2 простих фактора конгруентних 7 модуло 8.

За фиксиране k, s и t важи

$$\pi_k(X;4;t,s) = \sum_{\substack{t_1+t_2=t \\ s_1+s_2=s}} \pi_k(X;8;t_1,s_1,t_2,s_2).$$

Међутим, бројеви n код којих је t_2+s_1 парно су конгруентни ± 1 модуло 8, а када је t_2+s_1 непарно, тада је n конгруентно ± 3 модуло 8. Када се урачунају само сабирци код којих је t_2+s_1 непарно, добија се теорема 8.1.1.

8.3 Доказ теореме 8.1.2

Нека је сада $n \equiv \pm 1$ модуло 8, и нека је $G_2(n)$ граф дефинисан у тврђењу 8.1.3 са Лапласовом матрицом $M_2(n)$. Да би било $(s^{\phi}(n), s^{\widehat{\phi}}(n)) = (p,q)$, мора да важи $s^{\phi}(n) = t+1-\operatorname{rank}_{\mathbb{F}_2} M_2(n) = p$ и $s^{\widehat{\phi}}(n) = s-1+t-\operatorname{rank}_{\mathbb{F}_2} M_2(n)$. Другим речима, треба да важи $s = q-p+2$, $t = m-s = m-q+p-2$ и $\operatorname{rank}_{\mathbb{F}_2} M_2(n) = t+1-p = m-q-1$. Нека су сада t_1, t_2, s_1 и s_2 као у напомени 3. Тада по тврђењу 8.1.3 матрица $M_2(n)$ димензије $(m+1)\times(m+1) = (t+s+1)\times(t+s+1)$ има облик

$$M_2(n) = \left[\begin{array}{c|c|c|c|c} A_1 & A_2 & B_1 & B_2 & 0_{t_1\times 1} \\ \hline A_3 & A_4 & B_3 & B_4 & 0_{t_2\times 1} \\ \hline 0_{s\times t_1} & 0_{s\times t_2} & 0_{s\times s_1} & 0_{s\times s_2} & 0_{s\times 1} \\ \hline 0_{1\times t_1} & 1_{1\times t_2} & 1_{1\times s_1} & 0_{1\times s_2} & * \end{array}\right],$$

при чему су A_1 и A_4 симетричне матрице чије су димензије редом $t_1\times t_1$ и $t_2\times t_2$, матрица A_2 је реда $t_1\times t_2$, матрица $A_3 = A_2^T$, матрице B_1, B_2, B_3 и B_4 су димензија редом $t_1\times s_1$, $t_1\times s_2$, $t_2\times s_1$ и $t_2\times s_2$, и пошто је $n\equiv\pm 1$ модуло 8, коефицијент $*$ је једнак 0. Према томе, пошто је последња колона нула колона, она се може избацити из матрице $M_2(n)$, и ранг ће остати непромењен. Штавише, тако добијена матрица и даље има својство да је збир свих колона једнак нула колони.

Биће посматрана три различита случаја:

1. Ако је $t_2 = s_1 = 0$, тада последња врста има само нуле у себи, па се вероватноћа да матрица има ранг ρ рачуна на исти начин као у доказу теореме 8.1.1:

$$\sum_{k=0}^{\rho} \operatorname{sym}(t,k) E_{t-k,s}(\rho-k).$$

2. Ако је $t_2 = 0$ и $s_1 \neq 0$, тада матрица $M_2(n)$ има следећи облик:

$$\left[\begin{array}{c|c|c} A_1 & B_1 & B_2 \\ \hline 0_{1\times t_1} & 1_{1\times s_1} & 0_{1\times s_2} \end{array}\right].$$

Користећи елементарне трансформације, може се претпоставити да је матрица облика

$$\left[\begin{array}{c|c|c} A_1 & B & u \\ \hline 0_{1\times t_1} & 0_{1\times(s-1)} & 1_{1\times 1} \end{array}\right].$$

Сада се A_1 може елементарним трансформацијама претворити у канонску, и ако је A_1 ранга ρ_1, тада се првих ρ_1 врста у B и u претвори у нула врсте:

$$\left[\begin{array}{c|c|c|c} E_{\rho_1\times\rho_1} & 0 & 0 & 0 \\ \hline 0_{(t-\rho_1)\times\rho_1} & 0 & B' & u' \\ \hline 0_{1\times\rho_1} & 0_{1\times(t-\rho_1)} & 0_{1\times(s-1)} & 1 \end{array}\right].$$

Ако матрица B' димензије $(t-\rho_1)\times(s-1)$ има ранг ρ_2, тада матрица $M_2(n)$ има ранг $\rho_1+\rho_2+1$. Вероватноћа да матрица $M_2(n)$ има ранг ρ је

$$\sum_{\rho_1+\rho_2=\rho-1} \mathrm{sym}(t,\rho_1)E_{t-\rho_1,s-1}(\rho_2).$$

3. Ако је $t_2 \neq 0$, тада се матрица $M_2(n)$ може трансформисати у матрицу облика

$$\left[\begin{array}{c|c|c|c} A_1' & A_2' & B_1' & B_2' \\ \hline A_3' & A_4' & B_3' & B_4' \\ \hline 0_{1\times t_1} & 00\ldots1 & 0_{1\times s_1} & 0_{1\times s_2} \end{array}\right],$$

при чему су A_1' и A_4' симетричне матрице димензија редом $t_1\times t_1$ и $t_2\times t_2$, A_2' је матрица димензије $t_1\times t_2$ таква да је $A_3' = A_2'^T$, и матрице B_1', B_2', B_3' и B_4' су димензија редом $t_1\times s_1$, $t_1\times s_2$, $t_2\times s_1$ и $t_2\times s_2$. Ово се може записати као

$$\left[\begin{array}{c|c|c|c} A_1'' & A_2'' & B_1'' & B_2'' \\ \hline A_3'' & A_4'' & B_3'' & B_4'' \\ \hline 0_{1\times(t-1)} & 1 & 0_{1\times s_1} & 0_{1\times s_2} \end{array}\right],$$

где је A_1'' симетрична матрица димензије $(t-1)\times(t-1)$, A_2'' је димензије $(t-1)\times 1$ таква да је $A_3'' = A_2''^T$ и $A_4'' \in \{0,1\}$. Када се A_1'' трансформише у канонску форму, добија се

$$\left[\begin{array}{c|c|c|c|c} E_{\rho_1\times\rho_1} & 0 & 0 & 0 & 0 \\ \hline 0_{(t-1-\rho_1)\times\rho_1} & 0 & A_2''' & B_1''' & B_2''' \\ \hline 0_{1\times\rho_1} & A_2'''^T & A_4''' & B_3''' & B_4''' \\ \hline 0_{1\times\rho_1} & 0_{1\times(t-1-\rho_1)} & 1 & 0_{1\times s_1} & 0_{1\times s_2} \end{array}\right].$$

Када се уради исто са блоком $\left[\begin{array}{cc} B_1''' & B_2''' \end{array}\right]$, добија се

$$\left[\begin{array}{c|c|c|c|c|c} E_{\rho_1\times\rho_1} & 0 & 0 & 0 & 0 & 0 \\ \hline 0_{\rho_2\times\rho_1} & 0 & 0 & 0 & E & 0 \\ \hline 0_{(t-1-\rho_1-\rho_2)\times\rho_1} & 0 & 0 & u & 0 & 0 \\ \hline 0_{1\times\rho_1} & v & u^T & x & 0 & w \\ \hline 0_{1\times\rho_1} & 0_{1\times\rho_2} & 0_{1\times(t-1-\rho_1-\rho_2)} & 1 & 0_{1\times\rho_2} & 0_{1\times(s-\rho_2)} \end{array}\right]$$

Матрица $M_2(n)$ ће имати ранг $\rho_1+\rho_2+1$ ако су u, v, w нула вектори. Иначе ће ранг бити $\rho_1+\rho_2+2$. Вероватноћа да $M_2(n)$ има ранг ρ је

$$\sum_{\rho_1+\rho_2=\rho-1} \mathrm{sym}(t,\rho_1)E_{t-\rho_1-1,s}(\rho_2)2^{\rho-m}+$$
$$\sum_{\rho_1+\rho_2=\rho-2} \mathrm{sym}(t,\rho_1)E_{t-\rho_1-1,s}(\rho_2)(1-2^{\rho-m}).$$

Пошто се последња колона може уклонити, биће коришћене горње формуле са $s-1$ уместо s.

Остају још два случаја да се испитају: када је $s=1$, и када је $s=0$. Када је $s=1$, морају се размотрити две могућности: $t_2+s_1>0$ и $t_2+s_1=0$. Пошто је $n\equiv\pm1$ модуло 8 (n има паран број фактора конгруентних ±3 модуло 8, па последња врста Лапласове матрице има паран број јединица), ако се уклони последња колона у Лапласовој матрици, последња врста неће бити нула врста. Након елементарних трансформација, добија се

$$\left[\begin{array}{c|c} C_1 & C_2 \\ \hline C_3 & C_4 \\ \hline 0_{1\times(t-1)} & 1 \end{array}\right],$$

где је C_1 симетрична матрица димензије $(t-1)\times(t-1)$, C_2 колона дужине $t-1$ таква да је $C_3=C_2^T$, и $C_4\in\{0,1\}$. Када се C_1 претвори у канонску, добија се

$$\left[\begin{array}{c|c|c} E_{\rho_1\times\rho_1} & 0 & 0 \\ \hline 0_{(t-1-\rho_1)\times\rho_1} & 0 & C_2' \\ \hline 0_{1\times\rho_1} & C_2'^T & C_4 \\ \hline 0_{1\times\rho_1} & 0_{1\times(t-1-\rho_1)} & 1 \end{array}\right],$$

где је ρ_1 ранг матрице C_1. Ако колона C_2' има ненула коефицијенте, ранг матрице $M_2(n)$ је $\rho_1 + 2$, иначе је ранг $\rho_1 + 1$. Дакле, вероватноћа да $M_2(n)$ има ранг ρ је

$$\mathrm{sym}(t-1, \rho-1)2^{\rho-t} + \mathrm{sym}(t-1, \rho-2)(1-2^{\rho-t}).$$

Нека је сада $t_2 + s_1 = 0$. Када се уклони последња колона Лапласове матрице, добија се симетрична матрица, па је вероватноћа да $M_2(n)$ има ранг ρ једнака

$$\mathrm{sym}(t, \rho).$$

Нека је $s = 0$. Тада је $t = m$, и $M_2(n)$ има облик

$$\left[\begin{array}{c|c} F_1 & F_2 \\ \hline 0_{1\times t_1} & 1_{1\times t_2} \end{array}\right].$$

Ако је $t_2 = 0$, тада је $M_2(n)$ Лапласова матрица неусмереног графа са m темена, па је вероватноћа да $M_2(n)$ има ранг ρ једнака

$$\mathrm{par}(m, m-\rho-1).$$

Нека је сада $t_2 > 0$. Матрица $[F_1 F_2]$ је симетрична, и последња колона матрице A је једнака збиру осталих, па то исто важи и за последњу врсту матрице A. Према томе, може се уклонити последња врста (заједно са последњом колоном) матрице $\begin{bmatrix} F_1 & F_2 \end{bmatrix}$. Након елементарних трансформација, добија се

$$\left[\begin{array}{c|c|c} E_{\rho_1\times\rho_1} & 0 & 0 \\ \hline 0_{(m-2-\rho_1)\times\rho_1} & 0 & F_2' \\ \hline 0_{1\times\rho_1} & F_2'^T & F_4 \\ \hline 0_{1\times\rho_1} & 0_{1\times(m-2-\rho_1)} & 1 \end{array}\right].$$

Вероватноћа да $M_2(n)$ има ранг ρ је

$$\mathrm{sym}(m-2, \rho-1)2^{\rho-m+1} + \mathrm{sym}(m-2, \rho-2)(1-2^{\rho-m+1}).$$

Комбиновањем са теоремом 8.1.6 и имајући у виду напомену 3 (само што се сада тражи да је $t_2 + s_1$ парно), добија се теорема 8.1.2.

Литература

[ACK] R. Alter, T. B. Curtz, K. K. Kubota, *Remarks and results on congruent numbers*, Proc. 3rd South Eastern Conf. Combin., Graph Theory and Comput., 1972, Florida Atlantic Univ., Boca Raton, Fla., 1972, 27-35. 41

[B] L. Bastien, *Nombres congruents*, Intermédiaire des Mathématiciens, 22 (1915), 231-232. 33

[BR] M. Beck, S. Robins, *Computing the continuous discretely: Integer-point enumeration in polyhedra*, Springer, New York, 2009. 6

[BSD] B. Birch, P. Swinnerton-Dyer, *Notes on Elliptic Curves (II)*, J. Reine Angew. Math. 165 (218), (1965), 79-108. 41

[BM] R. P. Brent, B. D. McKay, *Determinants and ranks of random matrices over* $\mathbb{Z}_m$, Discrete Math. 66 (1987), 35-49. 58

[CG] M. J. Curran, L. Goldmakher, *Khovanskii's theorem and effective results on sumset structure*, Discrete Analysis, 2021:27, 25 pp , 1, 14, 17, 18, 27

[E] Eugène Ehrhart, *Sur les polyèdres rationnels homothétiques à n dimensions*, C. R. Acad. Sci. Paris, 254:616-618, 1962. 1, 3, 5

[FJ] B. Faulkner, K. James, *A graphical approach to computing Selmer groups of congruent number curves*, The Ramanujan Journal, 14(1), (2007), 107-129 1, 54

[F] K. Feng, *Non-congruent numbers, odd graphs and the Birch-Swinnerton-Dyer conjecture*, Acta Arithmetica, (1996) 71-83 1, 43, 45, 54

[FX] K. Feng, M. Xiong, *On Elliptic Curves* $y^2 = x^3 - n^2x$ *with Rank Zero*, Journal of Number Theory, Vol. 109, Issue 1, Nov. 2004, 1-26. 1, 54

[Ga] C. Gauss, *Disquisitiones Arithmeticae* (Latin), English translation by A. Clarke, revised by W. Waterhouse, 1986 Springer-Verlag reprint of the Yale University Press, New Haven, 1966 edition. 48

[Ge] A. Genocchi, *Sopra tre scritti inediti di Leonardo Pisano pubblicati da B. Boncompagni: Note Analitiche*, Annali di Scienze Matematiche e Fisiche 6 (1855), 161- 185, 218-250, 273-320, 345-362. 33

[GS] A. Granville, G. Shakan, *The Frobenius postage stamp problem, and beyond*, Acta Math. Hungar. 161 (2020), no. 2, pp. 700-718 12, 13

[GSW] A. Granville, G. Shakan, A. Walker, *Effective results on the size and structure of sumsets*, arXiv:2105.09181, 2021, preprint. 12

[GW] A. Granville, A. Walker, *A tight structure theorem for sumsets*, Proceedings of the American Mathematical Society, Volume 149, Number 10, October 2021, Pages 4073-4082 13

[GT] B. Green, T. Tao, *The primes contain arbitrarily long arithmetic progressions*, Annals of Mathematics. 167 (2) (2008), 481-547 10

[HB1] D. R. Heath-Brown, *The size of Selmer groups for the congruent number problem*, Invent. Math. 111 (1993), no.1, 171-195. 1, 54

[HB2] D. R. Heath-Brown, *The size of Selmer groups for the congruent number problem. II.*, Invent. Math. 118 (1994), no. 2, 331-370 1, 54

[Hee] K. Heegner, *Diophantische Analysis und Modulfunktionen*, Mathematische Zeitschrift, 56, (1952), 227-253. 32

[JO] K. James, K. Ono, *Selmer groups of quadratic twists of elliptic curves*, Math. Ann. 314 (1999), no. 1, 1-17. 1, 54

[Kh] A. Khovanskii, *The Newton polytope, the Hilbert polynomial and sums of finite sets*, Funktsional. Anal. i Prilozhen. 26 (1992), no. 4, pp. 57-63, 96. 1, 10

[Ko] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer-Verlag, New York (1993) 41

[L] J. Lee, *Algebraic proof for the geometric structure of sumsets*, Integers 11 (2011), no. 4, pp. 477-486. 13

[Mo] P. Monsky, *Mock Heegner Points and Congruent Numbers*, Mathematische Zeitschrift, 204 (1), (1990), 45-67. 32

[Mu] D. Mumford, *Algebraic Geometry, I, Complex Projective Varieties*, Springer-Verlag, Berlin-Heidelberg-New York (1976). 11

[Na1] M. B. Nathanson, *Additive number theory: Inverse problems and the geometry of sumsets*, Graduate Texts in Mathematics, 165, Springer-Verlag, New York (1996). 15, 27

[Na2] M. B. Nathanson, *Sums of finite sets of integers*, Amer. Math. Monthly 79 (1972), pp. 1010-1012. 13

[NR] M. B. Nathanson, I. Z. Ruzsa, *Polynomial growth of sumsets in abelian semigroups*, J. Théor. Nombres Bordeaux 14 (2002), no. 2, pp. 553-560. 13

[Ne] J. Neukirch, *Algebraic number theory*, Springer, Berlin, 1999. 26

[Re] L. Rédei, *Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper*, J. Reine Angew. Math. 171 (1934), 55-60 48, 49

[RR] L. Rédei, H. Reichardt, *Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers*, J. Reine Angew. Math. 170 (1933), 69-74 48, 49

[Rh] R. C. Rhoades, 2-*selmer groups and the Birch-Swinnerton-Dyer conjecture for the congruent number curves*, Journal of Number Theory 129, no.6 (2009), 1379-1391. Zbl 1245.11078 54, 57

[Ru1] K. Rubin, *Tate-Shafarevich group and L-functions of elliptic curves with complex multiplication*, Invent. Math. 89 (1987), 527-560. 41

[Ru2] K. Rubin, *The main conjecture for imaginary quadratic fields*, Invent. Math. 103 (1991), 25-68. 41

[Sch] T. Schoen, *New bounds in Balog-Szemerdi-Gowers theorem*, Combinatorica, volume 35 (2015), 695-701 10

[Si] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, New York, 1986. 34, 36, 37, 39, 41

[St] N. M. Stephens, *Congruence Properties of Congruent Numbers*, Bulletin of the London Mathematical Society, 7, (1975), 182-184. 32

[Sy] J. J. Sylvester, *Mathematical questions, with their linear solutions*, Educational times, 41 (1884), 21. 13

[T] J.B. Tunnell, *A Classical Diophantine Problem and Modular Forms of Weight* 3/2, Inventiones mathematicae (1983), Volume 72, page 323-334 42, 47, 50

[V1] I. Vrećica, *Joint distribution for the Selmer ranks of the congruent number curves*, Czechoslovak Mathematical Journal, Vol. 70 (2020), No. 1, 105-119 54, 55, 58

[V2] I. Vrećica, *A result on the size of iterated sumsets in* $\mathbb{Z}^d$, https://arxiv.org/abs/2109.04377v2, 2022, preprint 17, 25

[WCC] J. D. Wu, F. J. Chen, Y. G. Chen, *On the structure of the sumsets*, Discrete Math. 311 (2011), no. 6, pp. 408-412. 13

[XZ] M. Xiong, A. Zaharescu, *Selmer groups and Tate-Shafarevich groups for the congruent number problem*, Comment. Math. Helv. 84 (2009), 21-56.

56

Биографија аутора

Илија Вреѓица је рођен 26. октобра 1990. у Београду. Дипломирао је на Математичком факултету 2014. године на смеру Теоријска математика и примене са просечном оценом 9,80. На истом факултету на смеру Теоријска математика и примене 2015. године је завршио мастер студије са просечном оценом 10, и одбранио мастер рад "Аритметичка статистика кубичних и квартичних бинарних форми" (ментор др Горан Ђанковић). Уписао је докторске студије 2015. године на Катедри за алгебру и математичку логику. Има три објављена рада на СЦИ листи:

1. G. Djanković, D. Đokić, N. Lelas, **I. Vrećica**, *On some hybrid power moments of products of generalized quadratic Gauss sums and Kloosterman sums*, Lithuanian Mathematical Journal, Vol. 58, No. 1 (2018), pp. 1-14, ISSN: 0363-1672, DOI: 10.1007/s10986-018-9383-6.

2. D. Đokić, N. Lelas, **I. Vrećica**, *Large values of Dirichlet L-functions over function fields*, International Journal of Number Theory, Vol. 16, No. 5 (2020), pp. 1081-1109, ISSN: 1793-0421, DOI: 10.1142/S1793042120500566.

3. **I. Vrećica**, *Joint distribution for the Selmer ranks of the congruent number curves*, Czechoslovak Mathematical Journal, 70, 1, 105-119, 2020, ISSN: 0011-4642, DOI: 10.21136/CMJ.2019.0171- 18.

Од 2015. године је запослен на Математичком факултету као сарадник у настави, а од 2016. као асистент.

Прилог 1.

Изјава о ауторству

Потписани-а Илија Вретница

број индекса 2001/2015

Изјављујем

да је докторска дисертација под насловом

Статистика Селмерових група у фамилији елиптичких кривих придружених конгруентним бројевима

- резултат сопственог истраживачког рада,
- да предложена дисертација у целини ни у деловима није била предложена за добијање било које дипломе према студијским програмима других високошколских установа,
- да су резултати коректно наведени и
- да нисам кршио/ла ауторска права и користио интелектуалну својину других лица.

Потпис докторанда

У Београду, 17.11.2022.

Илија Вретница

Прилог 2.

Изјава о истоветности штампане и електронске верзије докторског рада

Име и презиме аутора Илија Вретница

Број индекса 2001/2015

Студијски програм Математика

Наслов рада Статистика Селмерових група у фамилији елиптичких кривих придружених конгруентним бројевима

Ментор Горан Ђанковић

Потписани/а Илија Вретница

Изјављујем да је штампана верзија мог докторског рада истоветна електронској верзији коју сам предао/ла за објављивање на порталу **Дигиталног репозиторијума Универзитета у Београду.**

Дозвољавам да се објаве моји лични подаци везани за добијање академског звања доктора наука, као што су име и презиме, година и место рођења и датум одбране рада.

Ови лични подаци могу се објавити на мрежним страницама дигиталне библиотеке, у електронском каталогу и у публикацијама Универзитета у Београду.

Потпис докторанда

У Београду, 17.11.2022.

Илија Вретница

Прилог 3.

Изјава о коришћењу

Овлашћујем Универзитетску библиотеку „Светозар Марковић“ да у Дигитални репозиторијум Универзитета у Београду унесе моју докторску дисертацију под насловом:

Статистика Селморових група у фамилији елиптичких кривих придружених конгруентним бројевима

која је моје ауторско дело.

Дисертацију са свим прилозима предао/ла сам у електронском формату погодном за трајно архивирање.

Моју докторску дисертацију похрањену у Дигитални репозиторијум Универзитета у Београду могу да користе сви који поштују одредбе садржане у одабраном типу лиценце Креативне заједнице (Creative Commons) за коју сам се одлучио/ла.

1. Ауторство

2. Ауторство - некомерцијално

3. Ауторство – некомерцијално – без прераде

4. Ауторство – некомерцијално – делити под истим условима

5. Ауторство – без прераде

6. Ауторство – делити под истим условима

(Молимо да заокружите само једну од шест понуђених лиценци, кратак опис лиценци дат је на полеђини листа).

Потпис докторанда

У Београду, 17.11.2022.

Илија Вретина