

**Наставно-научном већу
Математичког факултета
Универзитета у Београду**

На 393. седници Наставно-научног већа Математичког факултета одржаној 20. маја 2022. године у Београду одређени смо за преглед и оцену рукописа

**Статистика Селмерових група у фамилији елиптичких кривих
придружених конгруентним бројевима**

који је предат као докторска дисертација кандидата Илије Врећице. Након прегледа рукописа који је Илија Врећица предао комисији, подносимо Наставно-научном већу следећи

ИЗВЕШТАЈ

1. Биографија кандидата

Илија Врећица је 2010. године уписао основне студије на Математичком факултету, смер Теоријска математика и примене. Дипломирао је 2014. године са просечном оценом 9.80. Исте године је уписао Мастер студије на Математичком факултету, које је завршио 2015. године са просеком 10.00, одбравивши мастер рад „Аритметичка статистика кубичних и кватрничних форми” под менторством проф. др Горана Ђанковића. Од 2015. године је студент докторских студија на Математичком факултету, студијски програм Математика.

2. Списак научних радова:

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, IF 2018: 0.566, M22.
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, IF 2020: 0.674, M23.
3. **I. Vrećica**, *Joint distribution for the Selmer ranks of the congruent number curves*, Czechoslovak Mathematical Journal, vol. 70 (2020), issue 1, pp. 105-119, DOI: 10.21136/CMJ.2019.0171-18, IF 2020: 0.338, M23.

Препринт

4. **I. Vrećica**, *A result on the size of iterated sumsets in \mathbb{Z}^d* , arXiv:2109.04377v2, на рецензији

3. Учесћа у летњим школама и научним скуповима:

1. Hausdorff Summer School: *L-functions, Open problems and current methods*, Hausdorff Center for Mathematics, University of Bonn, Germany, 2018
2. Hausdorff Summer School: *The Circle method: Entering its Second Century*, Hausdorff Center for Mathematics, University of Bonn, Germany, 2021
3. Hausdorff Summer School: *Polynomial methods*, Hausdorff Center for Mathematics, University of Bonn, Germany, 2021
4. Building bridges 5th EU/US Summer school and Workshop on Automorphic Forms and Related Topics, Univerzitet u Sarajevu, Bosna i Hercegovina, avgust 2022.

4. Предмет дисертације

Први предмет проучавања у дисертацији је скуп збирова у \mathbb{Z}^d . Ако је G адитивна група, и ако су $A, B \subset G$ подскупови, тада је *скуп збирова* елемената скупова A и B дефинисан са $A + B := \{a + b \in G : a \in A, b \in B\}$. Посебно, за природан број n се дефинише $nA = \{a_1 + \dots + a_n \in G : a_1, \dots, a_n \in A\}$. Скупови збирова у разним групама или прстенима су један од основних објеката проучавања у *адитивној комбинаторици*.

Један од полазних резултата у овој дисертацији је резултат А. Хованског *The Newton polytope, the Hilbert polynomial and sums of finite sets*, из 1992. године, у коме је показано да за сваки коначан скуп $A \subset \mathbb{Z}^d$ постоје полином $p_A(X) \in \mathbb{Q}[X]$ и природан број n_A такви да је $|nA| = p_A(n)$ за сваки природан број $n \geq n_A$. Међутим, рад није дао никакву процену за величину n_A , нити је дао пуно информација о полиному p_A , што је мотивисало даља истраживања скупова збирова у Абеловим групама \mathbb{Z}^d . Иако је теорема доказана на више различитих начина након 1990. године, константа n_A је одређена само у посебним случајевима, када је $A \subset \mathbb{Z}$, или када $A \subset \mathbb{Z}^d$ има $d + 2$ елемената и $A - A$ генерише \mathbb{Z}^d . У општем случају, постоје само процене. Један од главних резултата ове дисертације је одређивање полинома p_A и константе n_A када $A \subset \mathbb{Z}^d$ има $d + 2$ елемента и никојих $d + 1$ елемента скупа A није садржано у некој хиперравни. Такође је нађено горње ограничење за $|hA|$ када $A \subset \mathbb{Z}^d$ има $d + 3$ елемента и симплицијални конвексни омотач.

Други предмет проучавања у дисертацији су Селмерове групе $\text{Sel}^\phi(E_n/\mathbb{Q})$ и $\text{Sel}^{\hat{\phi}}(E_n/\mathbb{Q})$ везане за одређене изогеније ϕ и $\hat{\phi}$ на елиптичкој кривој $E_n : y^2 = x^3 - n^2x$. Оне су уско везане за диофантовски проблем одређивања *конгруентних бројева*. У дисертацији се приказује веза између Селмерових група, теорије графова и конгруентних бројева коју је први пут показао К. Фенг у раду *Non-congruent numbers, odd graphs and the Birch-Swinnerton-Dyer conjecture*. Наиме, природан број n је конгруентан ако и само ако је

збир рангова $s^\phi(n)$ и $s^{\hat{\phi}}(n)$ Селмерових група $\text{Sel}^\phi(E_n/\mathbb{Q})$ и $\text{Sel}^{\hat{\phi}}(E_n/\mathbb{Q})$ различит од нуле. Додатно, елементи Селмерових група $\text{Sel}^\phi(E_n/\mathbb{Q})$ и $\text{Sel}^{\hat{\phi}}(E_n/\mathbb{Q})$ су приказани као парне партиције одређених графова, при чему скупови темена и ивица тих графова зависе од простих фактора природног броја n и Лежандрових симбола између њих.

Допринос кандидата је налажење заједничке асимптотске дистрибуције рангова Селмерових група $s^\phi(n)$ и $s^{\hat{\phi}}(n)$ елиптичких кривих E_n помоћу теорије графова.

5. Приказ дисертације

Дисертација има $XI + 69$ страна. Главни део дисертације је подељен на увод и осам глава. Литература се састоји од 43 библиографске јединице.

Дисертација је подељена на два дела. Први део се састоји од глава 1-5, које се дотичу адитивне комбинаторике, док се главе 6-8 баве Селмеровим групама у фамилији елиптичких кривих придружених конгруентним бројевима.

Прва глава садржи увод у Ерхартову теорију, која обухвата пребројавање тачака са целобројним координатама у конвексним политопима $\mathcal{P} \subset \mathbb{Z}^d$ чија темена имају целобројне координате. Уводи се појам конуса над политопом и његове генераторне функције представљене као формални ред. Помоћу конуса и његове генераторне функције показано је да за сваки политоп $\mathcal{P} \subset \mathbb{R}^d$ чија темена имају целобројне координате, и за сваки природан број n постоји полином $\text{ehr}_{\mathcal{P}}(X) \in \mathbb{Z}[X]$ такав да је број тачака са целобројним координатама садржан у скупу $\{nx : x \in \mathcal{P}\}$ једнак $\text{ehr}_{\mathcal{P}}(n)$ за сваки природан број n .

У другој глави се уводи појам (итерираног) скупа збирова. Приказана је теорема Хованског – да за сваки коначан скуп $A \subset \mathbb{Z}^d$ постоје природан број n_A и полином $p_A(X) \in \mathbb{Q}[X]$ степена највише d такав да је број елемената скупа hA једнак $p_A(n)$ за сваки природан број $n \geq n_A$.

Трећа глава садржи тачан опис полинома p_A и константе n_A дефинисаних у другој глави за скупове $A \subset \mathbb{Z}^d$ са $d+2$ елемента такве да скуп $A - A = \{a - b \in \mathbb{Z}^d : a, b \in A\}$ генерише \mathbb{Z}^d . При томе су коришћене методе и алати Ерхартове теорије прилагођени за скупове збирова.

Четврта и пета глава су посвећене оригиналним резултатима кандидата. У четвртој глави је приказан алтернативни начин пребројавања броја елемената hA , када је $A \subset \mathbb{Z}^d$ скуп са $d+2$ елемента, и добија се уопштење резултата из треће главе.

У петој глави су примењене технике из треће главе за одређивање горње границе броја елемената скупа nA када је $A \subset \mathbb{Z}^d$ скуп са $d+3$ елемента и симплицијалним конвексним омотачем. Показано је примерима да величина итерираних скупова збирова hA не може зависити само од величине конвексног омотача скупа A и природног броја n .

Шеста глава садржи увод у појмове конгруентног броја и елиптичких кривих, даје кратак увод у Селмерове групе придружене елиптичким кривама, као и везу између елиптичких кривих и конгруентних бројева. На крају, уводи се појам L -функције $L_E(s)$ елиптичке криве E дефинисане над \mathbb{Q} , и приказана је Birch–Swinnerton-Dyer (БСД) хипотеза. По хипотези, ред нуле L -функције $L_E(s)$ у тачки $s = 1$ једнак је рангу групе

$E(\mathbb{Q})$, због чега би доказ (БСД) хипотезе дао опис конгруентних бројева.

У седмој глави је приказана веза 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. Селмерове групе су даље кодирание тзв. парним партицијама одређеног графа. Затим је показано да елиптичка крива E_n има ранг нула када су рангови Селмерових група минимални.

Осма глава садржи оригинални резултат кандидата. Рангови две Селмерове групе елиптичке криве E_n су изражени преко ранга Лапласове матрице одређеног графа, чији скупови темена и ивица зависе од простих фактора броја n и одређених Лежандрових симбола. Помоћу вероватноће да природан број n има не само одговарајући број простих фактора, већ и фиксирани вредности Лежандрових симбола између њих, као и вероватноће да матрица одређеног облика над пољем \mathbb{F}_2 има дати ранг, кандидат налази дистрибуцију рангова Селмерових група на елиптичким кривама из фамилије E_n .

5. Закључак

Докторска дисертација „*Статистика Селмерових група у фамилији елиптичких кривих придружених конгруентним бројевима*“ проучава два аритметички значајна питања, расподелу ранга Селмерових група једне фамилије елиптичких кривих и кардиналност скупова збирова у \mathbb{Z}^d , методама дискретне математике. Кандидат је дошао до неколико оригиналних резултата у обе наведене тематике. Поред овога, кандидат има коауторске радове и у теорији L -функција и теорији експоненцијалних сума.

Илија Врећица је до сада објавио три рада у часописима са SCI листе, од тога један самосталан. На основу свега наведеног, како су испуњени сви формални услови, предлажемо да се рукопис „*Статистика Селмерових група у фамилији елиптичких кривих придружених конгруентним бројевима*“ **прихвати** као докторска дисертација из математике и да се закаже његова јавна одбрана.

У Београду, 16. новембра 2022. године

Чланови комисије:

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

проф. др Горан Ђанковић, ванредни професор (ментор),
Универзитет у Београду, Математички факултет

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

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

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