ŠIAULIŲ UNIVERSITETAS
REGIONŲ PLĖTROS INSTITUTAS

Daina Baravykienė
(Matematikos studijų programa, valstybinis kodas: 621G10006)

Elipsinių kreivių L funkcijų išvestinės diskretusis universalumas

Magistro darbas

Magistro darbo vadovė
doc. dr. V.Garbaliauskienė

Šiauliai
2020

TURINYS

ĮVADAS

Elipsinės kreivės yra svarbūs algebrinės geometrijos ir apskritai matematikos objektai. Jų teorija yra gana sudėtinga ir apraizgyta daugelio hipotezių. Universalumo tyrimo pradžia susijusi su Rymano (Riemann) dzeta funkcijos augimu kritinėje juostoje. Informacija apie Rymano dzeta funkcijos augimą svarbi daugelio skaičių teorijos problemų nagrinėjimui. Rymano dzeta funkcijos tyrimai paskatino ištisų dzeta funkcijų klasių atsiradimą, viliantis, kad platesnis požiūris padės suprasti pačios Rymano dzeta funkcijos savybes.

Bendriausia prasme pavadinimas dzeta funkcija reiškia funkciją, kurioje nors srityje išreiškiamą Dirichlė (Dirichlet) eilute. Kitaip tariant, visas dzeta funkcijas galima suskirstyti į dvi klases: dzeta funkcijos su Oilerio (Euler) sandauga ir be jos. Dzeta funkcijos su Oilerio sandauga paprastai vadinamos L funkcijomis. Taikymuose yra svarbu žinoti dzeta funkcijų asimptotines savybes. Jas galima charakterizuoti įvairiais įverčiais, vidurkių asimptotika. Praėjusio amžiaus trečiame dešimtmetyje H. Boras (Bohr) ir B. Jesenas (Jessen) pasiūlė dzeta funkcijų asimptotinio elgesio reguliarumą charakterizuoti ribinėmis teoremomis, kurios yra artimos šiuolaikinėms ribinėms teoremoms silpnojo tikimybinių matų konvergavimo prasme. Tokias teoremas galima įrodyti dzeta funkcijoms kompleksinėje plokštumoje, analizinių, meromorfinių ir net tolydžiųjų funkcijų erdvėse. Dzeta funkcijų universalumas reiškia, kad jų postūmiai norimu tikslumu tolygiai kompaktinėse aibėse aproksimuoja bet kokią analizinę funkciją.

Tegu E elipsinė kreivė virš racionaliųjų skaičių kūno duota Vejerštraso (Weierstrass) lygtimi

$$y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Z}.$$

Pažymėkime $\Delta = -16(4a^3 + 27b^2)$ kreivės E diskriminantą ir tarkime, kad $\Delta \neq 0$. Tada kubinio trinario x^3+ax+b šaknys yra skirtingos, ir kreivė E yra nesinguliarioji. Pavyzdžiui, nesinguliariosios elipsinės kreivės yra $y^2 = x^3 - x$ ir $y^2 = x^3 + x$; singuliariosios – $y^2 = x^3$ ir $y^2 = x^3 + x^2$ [12].

Kiekvienam pirminiam p, pažymėkime $\nu(p)$, lyginio

$$y^2 \equiv x^3 + ax + b \ (\mathrm{mod} p)$$

sprendinių skaičių. Tegu $\lambda(p) = p - \nu(p)$, o $s = \sigma + it$ – kompleksinis kintamasis. Tada kreivės E L funkcija apibrėžiama Oilerio sandauga

$$L_E(s) = \prod_{p|\Delta} \left(1 - \frac{\lambda(p)}{p^s}\right)^{-1} \prod_{p\nmid\Delta} \left(1 - \frac{\lambda(p)}{p^s} + \frac{1}{p^{2s-1}}\right)^{-1}.$$

Remiantis Hasės (Hasse) įverčiu

$$|\lambda(p)| < 2\sqrt{p},$$

begalinė sandauga, apibrėžianti funkciją $L_E(s)$, konverguoja absoliučiai ir tolygiai pusplokštumės $D_a = \left\{s \in \mathbb{C} : \sigma > \frac{3}{2}\right\}$ kompaktiniuose poaibiuose ir apibrėžia analizinę nelygią nuliui funkciją.

Šioje srityje $L_E(s)$ gali būti išreikšta Dirichlė eilute

$$L_E(s) = \sum_{m=1}^{\infty} \frac{\lambda(m)}{m^s},$$

čia $\lambda(m)$ yra multiplikatyvioji funkcija.

Funkcijos $L_E(s)$ analizinis pratęsimas glaudžiai susijęs su tam tikrų modulinių formų L funkcijomis. Funkcijos $L_E(s)$ analizinės savybės sutampa su svorio 2 naujųjų formų L funkcijų savybėmis.

Glaustai aptarkime universalumo savybę. Universalumas – įdomi dzeta ir L funkcijų savybė. Šią savybę 1975 m. Rymano dzeta funkcijai $\zeta(s)$, $s = \sigma + it$, apibrėžtai pusplokštumėje $\sigma > 1$ formule

$$\zeta(s) = \sum_{m=1}^{\infty} \frac{1}{m^s}$$

ir analiziškai pratęsiamai į visą kompleksinę plokštumą, išskyrus $s = 1$, kuriame funkcija turi paprastą polių su reziduumu 1, įrodė S. M. Voroninas (Voronin) [10].

A teorema. *Tegu $0 < r < \frac{1}{4}$, o $f(s)$ yra tolydi nelygi nuliui funkcija skritulyje $|s| \le r$, kuri yra analizinė skritulio viduje. Tada kiekvienam $\varepsilon > 0$ egzistuoja realusis skaičius $\tau = \tau(\varepsilon)$, toks, kad*

$$\max_{|s|\le r} \left| \zeta\left(s + \frac{3}{4} + i\tau\right) - f(s) \right| < \varepsilon.$$

Vėliau S. M. Gonekas (Gonek), A. Reichas (Reich), B. Bagči (Bagchi), A. Laurinčikas, K. Matsumoto, R. Garunkštis, J. Štaudingas (Steuding), V. Švarcas (Schwarz), H. Mišu (Mishou), R. Kačinskaitė, R. Šleževičienė, J. Ignatavičiūtė, J. Genys, H. Nagoši (Nagoshi) ir kiti apibendrino ir pagerino Voronino teoremą. Jie įrodė, kad duotąją analizinę funkciją $f(s)$ galima tolygiai aproksimuoti $\zeta(s)$ funkcijos postūmiais bendresnėje srityje negu skritulys. Voronino teoremą Rymano dzeta funkcijai įrodė A. Laurinčikas [8].

Pažymėkime meas$\{A\}$ mačios aibės $A \subset \mathbb{R}$ Lebego matą. Kai $T > 0$, tegu

$$\nu_T(...) = \frac{1}{T}\text{meas}\left\{\tau \in [0,T] : ...\right\},$$

čia vietoj daugtaškio įrašomos sąlygos, kurias tenkina τ. $\mathbb{C}$ žymime kompleksinę plokštumą.

B teorema. *Tegu K yra juostos $D = \{s \in \mathbb{C} : \frac{1}{2} < \sigma < 1\}$ kompaktinis poaibis su jungiamuoju papildiniu, $f(s)$ yra tolydi nelygi nuliui funkcija poaibyje K, kuri yra analizinė K viduje. Tada kiekvienam $\varepsilon > 0$,*

$$\liminf_{T\to\infty} \nu_T\left(\sup_{s\in K}|\zeta(s+i\tau) - f(s)| < \varepsilon\right) > 0.$$

Pastaroji teorema rodo, kad egzistuoja be galo daug postūmių $\zeta(s + i\tau)$, kurie aproksimuoja duotąją analizinę funkciją $f(s)$. Aibė tokių τ turi teigiamą apatinį tankį, tačiau nėra žinoma nė viena konkreti τ reikšmė. Ta prasme ši teorema nėra efektyvi.

Kaip ir dauguma klasikinių dzeta ir L funkcijų, taip ir mūsų nagrinėjama elipsinių kreivių L funkcija, yra universali Voronino prasme. Liniko-Ibragimovo hipotezė sako, kad visos funkcijos tam tikroje pusplokštumėje duotos Dirichlė eilute, analiziškai pratęsiamos į kairę nuo absoliutaus konvergavimo pusplokštumės ir tenkinančios tam tikras didėjimo sąlygas, yra universalios Voronino prasme.

Tegul sritis $D = \{s \in \mathbb{C} : 1 < \sigma < \frac{3}{2}\}$. Pirmąją universalumo teoremą elipsinių kreivių L funkcijai įrodė A. Laurinčikas ir V. Garbaliauskienė.

C teorema ([4]). *Tarkime, kad E yra nesinguliari elipsinė kreivė virš racionaliųjų skaičių kūno. Tegu K yra juostos D kompaktinis poaibis su jungiuoju papildiniu, $f(s)$ yra tolydi nelygi nuliui funkcija poaibyje K, kuri yra analizinė K viduje. Tada kiekvienam $\varepsilon > 0$,*

$$\liminf_{T\to\infty} \nu_T\left(\sup_{s\in K}|L_E(s+i\tau) - f(s)| < \varepsilon\right) > 0,$$

t.y. egzistuoja be galo daug postūmių $L_E(s+i\tau)$, kurie aproksimuoja duotąją analizinę funkciją $f(s)$: aibė tokių τ turi teigiamą apatinį tankį.

2006 m. įrodytas elipsinių kreivių L funkcijų išvestinės tolydus universalumas.

D teorema([6]). *Tarkime, kad E yra nesinguliari elipsinė kreivė virš racionaliųjų skaičių kūno. Tegu K yra juostos D kompaktinis poaibis su jungiuoju papildiniu, $f(s)$ yra tolydi funkcija poaibyje K, kuri yra analizinė K viduje. Tada kiekvienam $\varepsilon > 0$,*

$$\liminf_{T\to\infty} \nu_T \left(\sup_{s\in K} |L'_E(s+i\tau) - f(s)| < \varepsilon \right) > 0.$$

Šioje teoremoje, skirtingai negu B ir C teoremose, funkcija $f(s)$ gali būti nykstamoji.

Suformuluotos universalumo teoremos yra tolydaus tipo: postūmio menamoji dalis τ kinta tolydžiai intervale $[0, T]$. Be šio tipo teoremų egzistuoja universalumo teoremų diskretus atvejis. Pirmieji Rymano dzeta funkcijos diskretųjį universalumą nagrinėjo S.M. Voroninas (1979) ir B. Bagči (1981).

Diskretaus universalumo atveju postūmio menamoji dalis įgyja reikšmes iš aritmetinės progresijos. Tegu $N \in \mathbb{N}$ ir

$$\mu_N(...) = \frac{1}{N+1} \sharp \{0 \le m \le N : ...\},$$

čia vietoj daugtaškių įrašomos sąlygos, kurias tenkina m, o $h > 0$ yra fiksuotas skaičius. Tarkime, kad skaičius h yra pasirenkamas taip, kad $\exp\left\{\frac{2\pi k}{h}\right\}$ yra iracionalusis skaičius visiems $k \in \mathbb{Z} \setminus \{0\}$.

Elipsinių kreivių L funkcijų diskretųjį universalumą įrodė V. Garbaliauskienė ir A. Laurinčikas (2005).

E teorema ([5]). *Tarkime, kad $\exp\left\{\frac{2\pi k}{h}\right\}$ yra iracionalusis skaičius visiems $k \in \mathbb{Z} \setminus \{0\}$. Tegu K juostos D kompaktinis poaibis su jungiuoju papildiniu, $f(s)$ yra tolydi nelygi nuliui funkcija poaibyje K, kuri yra analizinė K viduje. Tada kiekvienam $\varepsilon > 0$,*

$$\liminf_{T\to\infty} \mu_N \left(\sup_{s\in K} |L_E(s+imh) - f(s)| < \varepsilon \right) > 0.$$

Šioje teoremoje matome, jog aibė $\{m : m = 0, 1, ...\}$ tokia, kad postūmiai $L_E(s+imh)$ aproksimuoja duotąją analizinę funkciją, yra pakankamai gausi: turi teigiamą apatinį tankį.

Kadangi $h > 0$ yra fiksuotas skaičius, pasirenkamas taip, kad $\exp\left\{\frac{2\pi k}{h}\right\}$ būtų iracionalusis skaičius visiems $k \in \mathbb{Z} \setminus \{0\}$, tai, pavyzdžiui, $h = \pi$ arba $h = 2\pi$, nes, pagal Hermite-Lindemano teoremą, e^{α} yra iracionalusis, kai

$\alpha \neq 0$ - algebrinis skaičius. Kompleksinis skaičius a vadinamas algebriniu, jei a yra lygties

$$a_n x^n + ... + a_1 x + a_0 = 0$$

su racionaliaisiais koeficientais a_i, $i = 0, ..., n$, šaknis.

Magistro darbo tikslas - įrodyti elipsinių kreivių L funkcijų išvestinės diskretųjį universalumą.

1 teorema. *Tarkime, kad* $\exp\left\{\frac{2\pi k}{h}\right\}$ *yra iracionalusis skaičius visiems* $k \in \mathbb{Z} \setminus \{0\}$. *Tegu* K *juostos* D *kompaktinis poaibis su jungiuoju papildiniu,* $f(s)$ *yra tolydi nelygi nuliui funkcija poaibyje* K, *kuri yra analizinė* K *viduje. Tada kiekvienam* $\varepsilon > 0$,

$$\liminf_{T\to\infty} \mu_N \left(\sup_{s\in K} |L'_E(s + imh) - f(s)| < \varepsilon \right) > 0.$$

Teoremos įrodymas remiasi diskrečiomis ribinėmis teoremomis analizinių funkcijų erdvėje, eilučių aibių tankiu (tirštumu) analiznių funkcijų erdvėje ir Mergeliano (Mergelyan) teorema.

1. ELIPSINIŲ KREIVIŲ L FUNKCIJŲ ANALIZINĖS SAVYBĖS

Suformuluokime funkcijos $L_E(s)$ analizines savybes. Pažymėkime $SL(2,\mathbb{Z})$ pilnąją modulinę grupę, t.y.

$$SL(2,\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in \mathbb{Z}, ad-bc=1 \right\}.$$

Be to, teigiamam sveikajam q apibrėžkime

$$\Gamma_0(q) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z}) : c \equiv 0 (\mathrm{mod} q) \right\}.$$

Čia $\Gamma_0(q)$ yra modulinės grupės $SL(2,\mathbb{Z})$ pogrupis, vadinamas Hekės (Hecke) pogrupiu [7].

Tegu $U = \{z \in \mathbb{C} : z = x+iy, \quad y>0\}$ viršutinė pusplokštumė kartu su ∞. Racionalieji skaičiai ir ∞ vadinami paraboliniais taškais. Tegu $F(z)$ yra analizinė pusplokštumėje U funkcija ir visiems $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z})$ tenkinama funkcinė lygtis

$$F\left(\frac{az+b}{cz+d}\right) = (cz+d)^{\varkappa} F(z) \tag{1.1}$$

su kai kuriuo lyginiu sveikuoju teigiamu $\varkappa$. Tada begalybėje $F(z)$ turi skleidinį Furjė (Fourier) eilute

$$F(z) = \sum_{m=-\infty}^{\infty} c(m) \mathrm{e}^{2\pi i m z}.$$

Funkcija $F(z)$ vadinama analizine begalybėje, jei $c(m)=0$, kai $m<0$, ir nykstamąja begalybėje, jei $c(m)=0$, kai $m \le 0$. Be to, $F(z)$ yra analizinė ir nykstamoji paraboliniuose taškuose, jei funkcija

$$(cz+d)^{-\varkappa} F\left(\frac{az+b}{cz+d}\right)$$

yra analizinė ir nykstamoji begalybėje visiems $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z})$. Jei $F(z)$ yra analizinė paraboliniuose taškuose, tai ji yra svorio $\varkappa$ modulinė forma. Šiuo atveju $F(z)$ turi tokį Furjė eilutės skleidinį begalybėje:

$$F(z) = \sum_{m=0}^{\infty} c(m) \mathrm{e}^{2\pi i m z}.$$

Jei svorio $\varkappa$ modulinė forma $F(z)$ yra nykstanti paraboliniuose taškuose, tai ji yra svorio $\varkappa$ parabolinė forma, ir jos Furjė eilutės skleidinys begalybėje yra

$$F(z) = \sum_{m=1}^{\infty} c(m)\mathrm{e}^{2\pi imz}.$$

Jei visos matricos $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(q)$ tenkina (1.1) lygtį, parabolinė forma $F(z)$ yra svorio $\varkappa$ ir lygmens q parabolinė forma.

Ramanudžano (Ramanujan) parabolinė forma

$$\Delta(z) = \mathrm{e}^{2\pi imz} \prod_{m=1}^{\infty} \left(1 - \mathrm{e}^{2\pi imz}\right)^{24} = \sum_{m=1}^{\infty} \tau(m)\mathrm{e}^{2\pi imz}$$

yra klasikinis parabolinės formos pilnosios modulinės grupės $SL(2,\mathbb{Z})$ atžvilgiu pavyzdys. Čia svoris $\varkappa$ yra 12,

$$\tau(p^{k+1}) = \tau(p)\tau(p^k) - p^{11}\tau(p^{k-1})$$

yra Ramanudžano funkcija. Funkcija $\tau(m)$ yra multiplikatyvioji [7].

Pažymėkime $S_\varkappa(\Gamma_0(q))$ visų svorio $\varkappa$ ir lygmens q parabolinių formų erdvę. Elementas F iš $S_\varkappa(\Gamma_0(q))$ yra Hekės tikrinė forma, jei F yra visų Hekės operatorių tikrinė funkcija

$$(T(m)f)(z) = m^{\varkappa-1} \sum_{\substack{0<d|m \\ ad=m}} d^{-\varkappa} f\left(\frac{az+b}{d}\right).$$

Jei $q_1|q$, tada elementas F iš $S_\varkappa(\Gamma_0(q_1))$ taip pat gali būti elementu iš $S_\varkappa(\Gamma_0(q))$. Elementas iš $S_\varkappa(\Gamma_0(q))$ yra naujoji forma, jei jis yra Hekės tikrinė forma ir nėra parabolinė forma su lygmeniu mažesniu kaip q.

Suformuluokime pagrindines elipsinių kreivių L funkcijų savybes.

1. Funkcija $L_E(s)$ analiziškai pratęsiama į visą kompleksinę plokštumą (yra sveikoji funkcija) ir tenkina funkcinę lygtį

$$\left(\frac{\sqrt{q}}{2\pi}\right)^s \Gamma(s)L_E(s) = \eta\left(\frac{\sqrt{q}}{2\pi}\right)^{2-s} \Gamma(2-s)L_E(2-s),$$

čia q – teigiamas sveikasis skaičius, sudarytas iš determinanto Δ pirminių daugiklių, $\eta = \pm 1$, o $\Gamma(s)$ yra Oilerio gama funkcija.

2. Furjė eilutė

$$F(z) = \sum_{m=1}^{\infty} \lambda(m) \mathrm{e}^{2\pi i m z}$$

yra svorio 2 naujoji forma kurio nors Hekės pogrupio $\Gamma_0(q)$ atžvilgiu.

Pirmieji šias savybes, kurios ilgą laiką buvo žinomos kaip hipotezės, įrodė R. Teiloras (Taylor) ir A. Vailsas (Wiles) [9] pusiau stabilioms elipsinėms kreivėms. Tai buvo panaudota paskutiniam Ferma (Fermat) problemos įrodymui.

2001 m. hipotezes pilnai įrodė C. Brioilis (Breuil), B. Konradas (Conrad), F. Daimondas (Diamond) ir R. Teiloras [2]. Taigi, funkcijos $L_E(s)$ analizinės savybės sutampa su svorio 2 naujųjų formų L funkcijų savybėmis.

2. DISKREČIOJI RIBINĖ TEOREMA FUNKCIJAI $L'_E(s)$

Pagrindinės teoremos įrodymas remiasi diskrečia ribine teorema tikimybinio mato silpnojo konvergavimo prasme analizinių funkcijų erdvėje. Pažymėkime $H(D)$ analizinių srityje D funkcijų erdvę su tolygaus konvergavimo kompaktuose topologija, $\mathcal{B}(S)$ – metrinės erdvės S Borelio (Borel) aibių klasę. Tegu $\gamma = \{s \in \mathbb{C} : |s| = 1\}$ yra vienetinis apskritimas kompleksinėje plokštumoje $\mathbb{C}$ ir begaliniamatis toras

$$\Omega = \prod_p \gamma_p,$$

čia $\gamma_p = \gamma$ kiekvienam pirminiam p. Remiantis Tichonovo (Tichonov) teorema, su sandaugos topologija ir pataškine daugyba begaliniamatis toras Ω yra kompaktinė tolopoginė Abelio (Abelian) grupė. Todėl erdvėje $(\Omega, \mathcal{B}(\Omega))$ egzistuoja tikimybinis Haro (Haar) matas m_H. Taip gauname tikimybinę erdvę $(\Omega, \mathcal{B}(\Omega), m_H)$. Pažymėkime $\omega(p)$ elemento $\omega \in \Omega$ projekciją koordinatinėje erdvėje γ_p. Čia $\{\omega(p) : p \text{ pirminis}\}$ yra nepriklausomų atsitiktinių dydžių, apibrėžtų tikimybinėje erdvėje $(\Omega, \mathcal{B}(\Omega), m_H)$, seka.

Tegul juosta $D = \{s \in \mathbb{C} : 1 < \sigma < \frac{3}{2}\}$. Tikimybinėje erdvėje $(\Omega, \mathcal{B}(\Omega), m_H)$ apibrėžiame $H(D)$ reikšmį atsitiktinį elementą $L'_E(s, \omega)$ formule

$$L'_E(s,\omega) = \prod_{p\nmid\Delta}\left(1 - \frac{\lambda(p)\omega(p)}{p^s} + \frac{\omega^2(p)}{p^{2s-1}}\right)^{-1} \prod_{p|\Delta}\left(1 - \frac{\lambda(p)\omega(p)}{p^s}\right)^{-1} \times$$

$$\Big(-\sum_{p\nmid\Delta}\left(\frac{\lambda(p)\omega(p)\log p}{p^s} - \frac{2\omega^2(p)\log p}{p^{2s-1}}\right)\left(1 - \frac{\lambda(p)\omega(p)}{p^s} + \frac{\omega^2(p)}{p^{2s-1}}\right)^{-1} -$$

$$-\sum_{p|\Delta}\frac{\lambda(p)\omega(p)\log p}{p^s}\left(1 - \frac{\lambda(p)\omega(p)}{p^s}\right)^{-1}\Big).$$

Pažymėkime $P_{L'_E}(A)$ atsitiktinio elemento $L'_E(s, \omega)$ skirstinį

$$P_{L'_E}(A) = m_H(\omega \in \Omega : L'_E(s,\omega) \in A), \quad A \in \mathcal{B}(H(D)).$$

Aptarsime tikimybinio mato

$$P_N(A) \stackrel{def}{=} \frac{1}{N+1}\sharp\{0 \le m \le N : L'_E(s + imh) \in A\}, \quad A \in \mathcal{B}(H(D))$$

silpnąjį konvergavimą.

2.1 teorema. *Tarkime, kad* $\exp\{\frac{2\pi k}{h}\}$ *yra iracionalusis skaičius visiems* $k \in \mathbb{Z}\backslash\{0\}$. *Tada tikimybinis matas* P_N *silpnai konverguoja į atsitiktinio elemento* $L_E'(s,\omega)$ *skirstinį, kai* $N \to \infty$.

Įrodymas. Apibrėžkime tikimybinį matą

$$Q_N(A) = \frac{1}{N+1}\sharp\{0 \le m \le N : L_E(s+imh) \in A\}, \quad A \in \mathcal{B}(H(D)).$$

V. Garbaliauskienė ir Laurinčikas [4] įrodė, kad tikimybinis matas Q_N silpnai konverguoja į $H(D)$ reikšmio atsitiktinio elemento

$$L_E(s,\omega) = \prod_{p\nmid\Delta}\left(1 - \frac{\lambda(p)\omega(p)}{p^s} + \frac{\omega^2(p)}{p^{2s-1}}\right)^{-1} \prod_{p|\Delta}\left(1 - \frac{\lambda(p)\omega(p)}{p^s}\right)^{-1}$$

skirstinį Q_{L_E}, kai $N \to \infty$.

Tolydi funkcija $u : H(D) \to H(D)$ apibrėžiama formule

$$u(g(s)) = g'(s), \quad g(s) \in H(D).$$

Mato Q_N silpnasis konvergavimas ir 5.1 teorema iš [1] rodo, kad tikimybinis matas P_N silpnai konverguoja į $Q_{L_E}u^{-1}$, kai $N \to \infty$. Kadangi $Q_{L_E}u^{-1}$ yra atsitiktinio elemento $L_E'(s,\omega)$ skirstinys, teorema įrodyta.

3. ATSITIKTINIO ELEMENTO $L'_E(s,\omega)$ ATRAMA

Erdvė $H(D)$ yra separabili. Todėl atsitiktinio elemento $L'_E(s,\omega)$ skirstinio $P_{L'_E}$ atrama yra minimali uždara aibė $S_{P_{L'_E}} \subseteq H(D)$ tokia, kad $P_{L'_E}(S_{P_{L'_E}}) = 1$.

Norėdami įrodyti pagrindinę teoremą, turime žinoti mato P_{L_E} atramą. Pirmiausia apibrėškime atsitiktinio elemento $L'_E(s,\omega)$ atramą. Tegu

$$S = \{g \in H(D) : g(s) \neq 0 \text{ arba } g(s) \equiv 0\}.$$

3.1 lema. *Atsitiktinio elemento $L_E(s,\omega)$ atrama yra aibė S.*

Lemos įrodymą galima rasti V. Garbaliauskienės ir A. Laurinčiko darbe [4], 5 lema. Pateiksime erdvės $H(D)$ metrikos su tolygaus konvergavimo kompaktuose topologija apibrėžimą. Yra žinoma [3], kad juostos D kompaktiniuose poaibiuose egzistuoja seka $\{K_m : m \in \mathbb{N}\}$, tokia, kad

$$D = \bigcup_{m=1}^{\infty} K_m,$$

$K_m \subset K_{m+1}$, $m \in \mathbb{N}$, ir kiekvienam juostos D kompaktui K egzistuoja m, su kuriuo $K \subseteq K_m$.

Tegul $g_1, g_2 \in H(D)$, tada erdvės $H(D)$ metrika su tolygaus konvergavimo kompaktuose topologija apibrėžiama formule

$$\rho(g_1, g_2) = \sum_{m=1}^{\infty} 2^{-m} \frac{\rho_m(g_1, g_2)}{1 + \rho_m(g_1, g_2)},$$

čia

$$\rho_m(g_1, g_2) = \sup_{s \in K_m} |(g_1(s) - g_2(s))|.$$

Pateikime Mergeliano teoremą apie analizinių funkcijų aproksimavimą daugianariais [11].

3.2 lema. *Tarkime, kad K kompleksinės plokštumos kompaktinė aibė turinti jungųjį papildinį, o funkcija $g(s)$ yra tolydi aibėje K ir analizinė jos viduje. Tuomet su kiekvienu $\varepsilon > 0$ egzistuoja toks daugianaris $p(s)$, kad*

$$\sup_{s \in K} |g(s) - p(s)| < \varepsilon.$$

3.3 teorema. *Atsitiktinio elemento $L'_E(s,\omega)$ atrama yra erdvė $H(D)$.*

Įrodymas. Tegu funkcija $u : S \to H(D)$, apibrėžta formule

$$u(g(s)) = g'(s), \quad g(s) \in S.$$

Iš Koši integralinės formulės gauname, kad funkcija u yra tolydi. Todėl kiekvienai atvirai aibei $G \subset H(D)$ aibė $u^{-1}G$ yra erdvės S atviras poaibis. Parodykime, kad $u^{-1}G$ nėra tuščia aibė.

Tegu $g \in u^{-1}G$. Remdamiesi funkcijos u apibrėžimu, gauname, kad $u(g) \in G$.

Tegu K yra juostos D kompaktinis poaibis su jungiuoju papildiniu. Pagal 3.2 lemą, kompakto K viduje egzistuoja daugianaris $p(s)$, kuris nurodytu tikslumu tolygiai aproksimuoja funkciją $u(g(s))$. Taigi, $p(s) \in G$. Gauname, kad srityje D egzistuoja daugianaris $q(s) \in u^{-1}(p(s))$, be to, $q(s) \neq 0$. Tai parodo, kad aibė $u^{-1}G$ yra netuščia.

4. PAGRINDINĖS TEOREMOS ĮRODYMAS

Pagrindinė magistro darbo teorema:

1 teorema. *Tarkime, kad* $\exp\left\{\frac{2\pi k}{h}\right\}$ *yra iracionalusis skaičius visiems* $k \in \mathbb{Z} \setminus \{0\}$. *Tegu* K *juostos* D *kompaktinis poaibis su jungiuoju papildiniu,* $f(s)$ *yra tolydi funkcija poaibyje* K, *kuri yra analizinė* K *viduje. Tada kiekvienam* $\varepsilon > 0$,

$$\liminf_{N\to\infty} \frac{1}{N+1}\sharp\left\{0 \le m \le N : \sup_{s\in K} |L'_E(s+imh) - f(s)| < \varepsilon\right\} > 0.$$

Įrodymas. Remiantis 2.1 teorema, tikimybinis matas P_N silpnai konverguoja į atsitiktinio elemento $L'(s,\omega)$ skirstinį $P_{L'_E}$, kai $N \to \infty$. Vadinasi, remdamiesi 2.1 teorema iš [1], gauname, kad visoms atviroms aibėms $A \subset H(D)$,

$$\liminf_{N\to\infty} P_N(A) \ge P_{L'_E}(A). \tag{4.1}$$

Pagal 3.2 lemos tvirtinimą, egzistuoja daugianaris $p(s)$ toks, kad

$$\sup_{s\in K} |f(s) - p(s)| < \frac{\varepsilon}{2}. \tag{4.2}$$

Tegul G yra erdvės $H(D)$ atvira aibė, apibrėžta formule

$$G = \{g \in H(D) : \sup_{s\in K} |g(s) - f(s)| < \frac{\varepsilon}{2}\}.$$

Kadangi mato $P_{L'_E}$ atrama, sudaryta iš visų $g \in H(D)$, tokių, kad kiekvienai g aplinkai G teisinga nelygybė $P'_{L_E}(G) > 0$, ir pagal 3.3 teoremos tvirtinimą $p(s) \in S_{P'_{L_E}}$, gauname, kad $P'_{L_E}(G) > 0$. Todėl iš (4.1) nelygybės gauname, kad

$$\liminf_{N\to\infty} \frac{1}{N+1}\left\{0 \le m \le N : \sup_{s\in K} |L'(s+imh) - f(s)| < \frac{\varepsilon}{2}\right\} > 0. \tag{4.3}$$

Nelygybė (4.2) reiškia, kad

$$\left\{0 \le m \le N : \sup_{s\in K} |L'(s+imh) - f(s)| < \varepsilon\right\}$$
$$\supseteq \left\{0 \le m \le N : \sup_{s\in K} |L'(s+imh) - p(s)| < \frac{\varepsilon}{2}\right\}.$$

Šios nelygybės kartu su (4.3) formule parodo, kad

$$\liminf_{N\to\infty} \frac{1}{N+1} \left\{ 0 \le m \le N : \sup_{s\in K} |L'(s+imh) - f(s)| < \varepsilon \right\} > 0.$$

Teorema įrodyta.

IŠVADOS

1. Darbe suformuluotos elipsinių kreivių L funkcijų analizinės savybės, kurios sutampa su svorio 2 naujųjų formų L funkcijų savybėmis.

2. Funkcijai $L'_E(s)$ įrodyta diskreti ribinė teorema tikimybinio mato silpnojo konvergavimo prasme analizinių funkcijų erdvėje, kuria remiasi universalumo įrodymas.

3. Darbe įrodytas elipsinių kreivių L funkcijų išvestinės diskretusis universalumas, t. y., jei $\exp\left\{\frac{2\pi k}{h}\right\}$ yra iracionalusis skaičius visiems $k \in \mathbb{Z} \setminus \{0\}$, o K juostos D kompaktinis poaibis su jungiuoju papildiniu ir $f(s)$ yra tolydi funkcija poaibyje K, kuri yra analizinė K viduje, tai kiekvienam $\varepsilon > 0$ teisinga nelygybė

$$\liminf_{N\to\infty} \frac{1}{N+1} \sharp \left\{ 0 \le m \le N : \sup_{s\in K} |L'_E(s+imh) - f(s)| < \varepsilon \right\} > 0.$$

LITERATŪRA

1. P. Billingsley, *Convergence of probability measures*, New York: John Wiley, 1968.

2. C. Breuil, B. Conrad, F. Diamond, R. Taylor, On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises, *J. Amer. Math. Soc.*, **14** (2001), 843–939.

3. J. B. Conway, *Functions of One Complex Variable*, Springer, New York, 1978.

4. V. Garbaliauskienė, A. Laurinčikas, Some analytic properties for L-functions of elliptic curves, *Proc. Inst. Math. NAN Belarus*, **13** (1)(2005), 75–82.

5. V. Garbaliauskienė, A. Laurinčikas, Universality theorems for L-functions of elliptic curves, *Fizikos ir matematikos fakulteto seminaro darbai*, **8** (2005), 14–25.

6. V. Garbaliauskienė, A. Laurinčikas, The universality of the derivatives of L-functions of elliptic curves, *Analytic and Probabilistic Methods in Number Theory*. Proceedings of the fourth international conference in honour of J. Kubilius, Palanga, Lithuania, 25-29 September. Vilnius: TEV, (2006), p. 24–29.

7. R. Garunkštis, *Modulinių formų įvadas*, TEV, Vilnius, 2007.

8. A. Laurinčikas, *Limit Theorems for the Riemann Zeta-Function*, Kluwer, Dordrecht, 1996.

9. R. Taylor, A. Wiles, Ring-theoretic properties of certain Hecke algebras, *Ann. Math.*, **141** (1995), 3–26.

10. S. M. Voronin, Theorem on the "universality" of the Riemann zeta-function, *Math. USSR Izv.,* **9** (1975), 443–453.

11. J. L. Walsh, Interpolation and Approximation by Rational Functions in the Complex Domain, *Amer. Math. Soc. Collog. Publ.,* **20** (1960).

12. L. C. Washington, *Elliptic curves: number theory and cryptography*, Boca Raton, Florida 2003.

Elipsinių kreivių L funkcijų išvestinės diskretusis universalumas

SANTRAUKA

Tegu E elipsinė kreivė virš racionaliųjų skaičių kūno duota Vejerštraso lygtimi

$$y^2 = ax^3 + bx + c,$$

koeficientai a, b ir c yra sveikieji skaičiai. Tarkime, kad kreivės E diskriminantas $\Delta = -16(4a^3 + 27b^2)$ nelygus nuliui. Tada kreivė E yra nesinguliarioji.

Kiekvienam pirminiam p, pažymėkime $\nu(p)$, lyginio

$$y^2 \equiv x^3 + ax + b \ (\mathrm{mod} p)$$

sprendinių skaičių, ir tegu $\lambda(p) = p - \nu(p)$. Tegu $s = \sigma + it$ – kompleksinis kintamasis. Tada elipsinės kreivės L funkcija apibrėžiama Oilerio sandauga

$$L_E(s) = \prod_{p \nmid \Delta} \left(1 - \frac{\lambda(p)}{p^s} + \frac{1}{p^{2s-1}}\right)^{-1} \prod_{p|\Delta} \left(1 - \frac{\lambda(p)}{p^s}\right)^{-1}.$$

Remiantis Hasės įverčiu

$$|\lambda(p)| < 2\sqrt{p},$$

funkciją $L_E(s)$ apibrėžianti begalinė sandauga konverguoja absoliučiai ir tolygiai pusplokštumės $\sigma > \frac{3}{2}$ kompaktiniuose poaibiuose ir apibrėžia analizinę funkciją. Funkcija $L_E(s)$ analiziškai pratęsiama į visą kompleksinę plokštumą, t. y. yra sveikoji funkcija, ir tenkina funkcinę lygtį

$$\left(\frac{\sqrt{q}}{2\pi}\right)^s \Gamma(s) L_E(s) = \eta \left(\frac{\sqrt{q}}{2\pi}\right)^{2-s} \Gamma(2-s) L_E(2-s),$$

čia q – teigiamas sveikasis skaičius, sudarytas iš determinanto Δ pirminių daugiklių, $\eta = \pm 1$, o $\Gamma(s)$ yra Oilerio gama funkcija.

Magistro darbo tikslas – įrodyti elipsinių kreivių L funkcijų išvestinės diskrečiojo universalumo teoremą.

Darbe įrodomas funkcijos $L'_E(s)$ diskretusis universalumas. Nagrinėjamas analizinės funkcijos aproksimavimas postūmiais $L'_E(s+imh)$, čia kompleksinio kintamojo menamosios dalies postūmiai įgyja reikšmes iš aritmetinės progresijos. $h > 0$ yra fiksuotas skaičius, pasirenkamas taip, kad $\exp\left\{\frac{2\pi k}{h}\right\}$ būtų

iracionalusis skaičius visiems $k \in \mathbb{Z} \setminus \{0\}$.

1 teorema. *Tarkime, kad* $\exp\left\{\frac{2\pi k}{h}\right\}$ *yra iracionalusis skaičius visiems* $k \in \mathbb{Z} \setminus \{0\}$. *Tegu* K *juostos* $D = \{s \in \mathbb{C} : 1 < \sigma < \frac{3}{2}\}$ *kompaktinis poaibis su jungiuoju papildiniu,* $f(s)$ *yra tolydi funkcija poaibyje* K, *kuri yra analizinė* K *viduje. Tada kiekvienam* $\varepsilon > 0$,

$$\liminf_{N\to\infty} \frac{1}{N+1}\sharp\left\{0 \le m \le N : \sup_{s\in K} |L'_E(s+imh) - f(s)| < \varepsilon\right\} > 0.$$

Iš teoremos matyti, kad aibė $\{m : m = 0, 1, ...\}$ tokia, jog postūmiai $L'_E(s+imh)$ aproksimuoja duotąją analizinę funkciją, yra pakankamai gausi: turi teigiamą apatinį tankį.

Elipsinių kreivių L funkcijų išvestinės diskrečiojo universalumo įrodymas remiasi diskrečiąja ribine teorema tikimybinio mato silpnojo konvergavimo prasme analizinių funkcijų erdvėje.

Discrete Universality of the Derivatives of L-functions of Elliptic Curves

SUMMARY

Let E be an elliptic curve over the field of rational numbers given by the Weierstrass equation

$$y^2 = ax^3 + bx + c$$

with integers a, b and c. Suppose that the discriminant $\Delta = -16(4a^3 + 27b^2)$ of the curve E is non-zero. Then the elliptic curve E is non-singular.

For every prime p, denote by $\nu(p)$ the number of solutions of the congruence

$$y^2 \equiv ax^3 + bx + c \,(\mathrm{mod} p),$$

and let $\lambda(p) = p - \nu(p)$. Let $s = \sigma + it$ be a complex variable. Then the L-function of the elliptic curve E is the Euler product

$$L_E(s) = \prod_{p \nmid \Delta} \left(1 - \frac{\lambda(p)}{p^s} + \frac{1}{p^{2s-1}}\right)^{-1} \prod_{p|\Delta} \left(1 - \frac{\lambda(p)}{p^s}\right)^{-1}.$$

In view of the Hasse estimate

$$|\lambda(p)| < 2\sqrt{p}$$

the infinite product converges absolutely and uniformly on compact subsets of the half-plane $\sigma > \frac{3}{2}$, and defines there an analytic function.

The function $L_E(s)$ is analytically continuable to an entire function, and it satisfies the functional equation

$$\left(\frac{\sqrt{q}}{2\pi}\right)^s \Gamma(s) L_E(s) = \eta \left(\frac{\sqrt{q}}{2\pi}\right)^{2-s} \Gamma(2-s) L_E(2-s),$$

where q is a positive integer composed of prime factors of the discriminant Δ, and $\eta = \pm 1$ is the root number, $\Gamma(s)$ denotes the Euler gamma-function.

The aim of this Master's thesis is to prove the discrete universality theorem for the derivatives L-functions of elliptic curves over the field of rational numbers.

In thesis we study the discrete universality of the function $L'_E(s)$. We consider an approximation of analytic functions by translations $L'_E(s+imh)$, where $h > 0$ is a fixed number, the translations of the imaginary part of the complex variable take values from some arithmetical progression. We suppose that the number h is choosen so that $\exp\left\{\frac{2\pi k}{h}\right\}$ is an irrational number

for all $k \in \mathbb{Z} \setminus \{0\}$.

THEOREM 1. *Suppose that* $\exp\left\{\frac{2\pi k}{h}\right\}$ *is an irrational number for all* $k \in \mathbb{Z} \setminus \{0\}$. *Let* K *be a compact subset of the strip* $D = \{s \in \mathbb{C} : 1 < \sigma < \frac{3}{2}\}$ *with connected complement, and let* $f(s)$ *be a continuous function on* K *which is analytic in the interior of* K. *Then, for every* $\varepsilon > 0$,

$$\liminf_{N\to\infty} \frac{1}{N+1}\sharp\left\{0 \le m \le N : \sup_{s\in K} |L'_E(s+imh) - f(s)| < \varepsilon\right\} > 0.$$

Theorem 1 shows that the set $\{m : m = 0, 1, 2, ...\}$ such that $L'_E(s+imh)$ approximates a given analytic function uniformly on compacta is sufficiently wide, it has a positive lower density.

The proof of discrete universality of the derivative L-functions of elliptic curves is based on a limit theorem in the sense of weak convergence of probability measures in the space of analytic functions.