A DISCRETE LIMIT THEOREM FOR *L*-FUNCTIONS OF ELLIPTIC CURVES

Virginija Garbaliauskienė[1], Antanas Garbaliauskas[2]
[1]Šiauliai University, [2]Šiauliai State College
E-mail: virginija.garbaliauskiene@su.lt, a.garbaliauskas@svako.lt

Introduction

Elliptic curves are one of the most important objects in algebraic geometry and, in general, in mathematics. The theory of elliptic curves is rather complicated and enveloped by many conjectures. On the other hand, the elliptic curves have many practical applications, for example, in cryptography, in factoring of positive integers and in primality testing. To study the properties of elliptic curves H. Hasse introduced *L*-functions attached to these curves. The proof of the Fermat last theorem is closely related to *L*-functions of elliptic curves.

Let $E: y^2 = x^3 + ax + b$, $a,b \in \mathbf{Z}$, be an elliptic curve. Suppose that the discriminant $\Delta = -16(4a^3 + 27\,b^3) \neq 0$. In this case an elliptic curve is non-singular.

Let, for a prime p, $v(p)$ be the number of solutions of the congruence $y^2 \equiv x^3 + ax + b \pmod p$, and let $\lambda(p) = p - v(p)$. Let $s = \sigma + it$ be a complex variable. Then the *L*-function of elliptic curves is the Euler product

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

In view of the H. Hasse estimate $|\lambda(p)| \le 2\sqrt{p}$ the infinite product converges absolutely and uniformly on compact subsets of the half-plane $D = \left\{s \in \mathbf{C} : \sigma > \frac{3}{2}\right\}$, and defines there an analytic function with no zeros.

The function $L_E(s)$ also can be written in the form Dirichlet series

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

where $\lambda(m)$ is a multiplicative function, and the series also converges absolutely in D.

H. Hasse conjectured that the function $L_E(s)$ has analytic continuation to an entire function and 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 from prime factors of the discriminant Δ, $\eta = \pm 1$ is the root number, and $\Gamma(s)$, as usual, denotes the Euler gamma-function.

We consider an approximation of analytic functions by translations $L_E(s+imh)$, where $h>0$ is a fixed number. In this cases we suppose that the number h is choosen so that $\exp\left\{\frac{2\pi k}{h}\right\}$ is an irrational number for all $k \in \mathbf{Z}\setminus\{0\}$.

Let, for $N \in \mathbf{N}$,

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

where in place of dots a condition satisfied by m is to be written.

Let $D = \left\{s \in \mathbf{C} : 1 < \sigma < \frac{3}{2}\right\}$.

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

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

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

We recall that a complex number a is called algebraic if a is a root of the equation

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

with rational coefficients a_i, $i = 0,...,n$, and at least one a_i is non-zero. For example, every rational number a is algebraic because it is a root of the equation $x - a = 0$. A complex number a is called transcendental if it is not algebraic number.

Lemma 2. *Let a be an algebraic number, $a \neq 0$. Then the number e^q is transcendental.*

The lemma is the classical Hermite-Lindemann theorem, for the proof, see, for example, [1]. From Lemma 2 it follows that in Theorem 1 we can take, for example, $h = \pi$ or $h = 2\pi$.

The proof of the discrete universality for L-functions of elliptic curves is based on limit theorem in the sense of weak convergence of probability measures in functional spaces.

The discrete limit theorem for $L_E(s)$

The aim of this note is to prove the discrete limit theorem in the space of analytic functions for $L_E(s)$.

For the proof a discrete limit theorem in the sense of the weak convergence of probability measures in the space of analytic functions for the function $L_E(s)$, we will apply a discrete limit theorem for the zeta-function

$$\varphi(s) = \prod_p A_p^{-1}\left(p^{-s}\right),$$

where

$$A_p(s) = \prod_{j=1}^{g(p)}\left(1 - a_p^{(j)} x^{f(j,p)}\right).$$

Suppose that

$$g(p) \le c_1 p^{\alpha}, \quad \left|a_p^{(j)}\right| \le c_2 p^{\beta} \qquad (1)$$

with some positive c_1 and c_2 and non-negative α and β. Then the function $\varphi(s)$ is analytic for $\sigma > \alpha + \beta + 1$. Suppose that the function $\varphi(s)$ is analytically continuable to the region $D_1 = \left\{s \in \mathbf{C} : \sigma > \alpha + \beta + \frac{1}{2}\right\}$ and that in this region the estimates

$$\varphi(\sigma + it) << |t|^a, \quad |t| \ge t_0 > 0, \quad a > 0, \qquad (2)$$

and

$$\int_0^T \left|\varphi(\sigma + it)\right|^2 \mathrm{d}t << T, \quad T \to \infty, \qquad (3)$$

are satisfied. On the probability space $(\Omega, \mathrm{B}(\Omega), m_H)$ define an $H(D_1)$ - valued random element $\varphi(s,\omega)$ by

$$\varphi(s,\omega) = \prod_p \prod_{j=1}^{g(p)} \left(1 - \frac{a^{f(j,p)}(p) a_m^{(j)}}{p^{sf(j,p)}}\right)^{-1},$$

and let P_φ be its distribution.

Lemma 3. *Suppose that $\exp\left\{\frac{2\pi k}{h}\right\}$ is an irrational number for all $k \in \mathbf{Z}\setminus\{0\}$, and that conditions (1)-(3) are satisfied. Then the probability measure*

$$\mu_N(\varphi(s + imh) \in A), \ A \in \mathrm{B}(H(D_1)),$$

converges weakly to the measure P_φ as $N \to \infty$.

Proof. The lemma is a particular case of the theorem from [2]. In [2] a limit theorem in the space of meromorphic functions for the function $\varphi(s)$ was proved. In this case it was assumed that the function $\varphi(s)$ is meromomorphically continuable to the region D_1 and all its poles in this region are included in a compact set. Then, under the conditions of Lemma 3, it was proved that the probability measure

$$\mu_N(\varphi(s + imh) \in A), \ A \in \mathrm{B}(H(D_1)),$$

converges weakly to the measure P_φ as $N \to \infty$. Here $M(D_1)$ is the space of meromorphic on D_1 functions equipped with the topology of uniform convergence on compacta.

Now let $V > 0$, and

$$D_V = \left\{s \in \mathbf{C} : 1 < \sigma < \frac{3}{2}, \quad |t| < V\right\}.$$

On the probability space $(\Omega, \mathrm{B}(\Omega), m_H)$ define an $H(D_V)$ – valued random element $L_E(s,\omega)$ by

$$L_E(s,\omega) = \prod_{p|\Delta}\left(1 - \frac{\lambda(p)\omega(p)}{p^s} + \frac{\omega^2(p)}{p^{2s-1}}\right)^{-1} \prod_{p|\Delta}\left(1 - \frac{\lambda(p)\omega(p)}{p^s}\right)^{-1}, \quad (4)$$

and let P_{L_E} be its distribution.

Theorem 4. *Suppose that $\exp\left\{\frac{2\pi k}{h}\right\}$ is an irrational number for all $k \in \mathbf{Z}\setminus\{0\}$. Then the probability measure*

$$\mu_N(L_E(s + imh) \in A), \ A \in \mathrm{B}(H(D_V)),$$

converges weakly to the measure P_{L_E} as $N \to \infty$.

Proof. The function $L_E(s)$ is an entire Matsumoto function with $\alpha = \frac{1}{2}$ and $\beta = 0$. Moreover, the conditions of Lemma 3 are satisfied. Therefore,

denoting $\hat{D} = \{s \in \mathbf{C} : \sigma > 1\}$, we have by Lemma 3 that the probability measure

$$\mu_N(L_E(s + imh) \in A), \ A \in \mathsf{B}(H(\hat{D})), \qquad (5)$$

converges weakly to the distribution of the $H(\hat{D})$ – valued random element $L_E(s,\omega)$ defined on the probability space $(\Omega, \mathrm{B}(\Omega), m_H)$ by (2.4) with $s \in \hat{D}$ as $N \to \infty$. Since $D_V \subset \hat{D}$, the function $h : H(\hat{D}) \to H(D_V)$ given by the formula

$$h(f(s)) = f(s)\big|_{s \in D_V}, \ f \in H(\hat{D}),$$

is continuous, therefore the theorem is a consequence of the weak convergence of the probability measure (5) and Theorem 5.1 of [3].

Note that in this case $\exp\left\{\frac{2\pi k}{h}\right\}$ is irrational for all $k \in \mathbf{Z}\backslash\{0\}$, therefore the limit measures in Lemma 3 as well as in Theorem 4 are independent of the number h.

References

1. Golochkin A. I., Nesterenko Yu. V., Shidlovskij A. B., 1995, *Introduction to Number Theory*. Moscow University.
2. Kačinskaitė R., 2002, A discrete limit theorem for the Matsumoto zeta-function in the space of meromorphic functions, *Lith. Math. J.,* Vol. 42, No. 1, p. 37-53.
3. P. Billingsley, 1968, *Convergence of probability measures*, New York: John Wiley.

Summary

A DISCRETE LIMIT THEOREM FOR *L*-FUNCTIONS OF ELLIPTIC CURVES

Virginija Garbaliauskienė, Antanas Garbaliauskas

In the paper, we prove the discrete limit theorem in the sense of the weak convergence of probability measures in the space of analytic on $D_V = \left\{s \in \mathbf{C} : 1 < \sigma < \frac{3}{2}, \ |t| < V\right\}$ functions for L-functions of elliptic curves $L_E(s)$. The main statement of the paper is as follows. Let $h > 0$ be a fixed real number such that $\exp\left\{\frac{2\pi k}{h}\right\}$ is an irrational number for all $k \in \mathbf{Z}\backslash\{0\}$. Then the probability measure $\mu_N(L_E(s + imh) \in A), \ A \in \mathsf{B}(H(D_V)),$ converges weakly to the measure P_{L_E} as $N \to \infty$.

Keywords: *elliptic curve, L-function, limit theorem, weak convergence*.

Santrauka

DISKRETI RIBINĖ TEOREMA ELIPSINIŲ KREIVIŲ *L*-FUNKCIJOMS

Virginija Garbaliauskienė, Antanas Garbaliauskas

Įrodyta diskreti ribinė teorema silpnojo tikimybinių matų konvergavimo prasme analizinių $D_V = \left\{s \in \mathbf{C} : 1 < \sigma < \frac{3}{2}, \ |t| < V\right\}$ srityje funkcijų erdvėje elipsinių kreivių L-funkcijai $L_E(s)$. Pagrindinis straipsnio tvirtinimas: tegul $h > 0$ yra fiksuotas realus skaičius toks, kad $\exp\left\{\frac{2\pi k}{h}\right\}$ būtų iracionalus su $k \in \mathbf{Z}\backslash\{0\}$. Tada tikimybinis matas $\mu_N(L_E(s + imh) \in A), \ A \in \mathsf{B}(H(D_V)),$ silpnai konverguoja į matą P_{L_E}, kai $N \to \infty$.

Prasminiai žodžiai: *elipsinė kreivė, L-funkcija, ribinė teorema, silpnasis konvergavimas.*

Įteikta 2018-11-19
Priimta 2018-11-28