DISCRETE UNIVERSALITY THEOREM FOR *L*-FUNCTIONS OF ELLIPTIC CURVES

Jurgita Čeponienė, Virginija Garbaliauskienė, Antanas Garbaliauskas
Šiauliai University, Šiauliai College

Introduction

Let **N, Z, Q** and **C** denote the sets of all positive integers, integers, rational and complex numbers, respectively. Consider an elliptic curve E given by the Weierstrass equation $y^2 = x^3 + ax+b$, $a, b \in \mathbf{Z}$. Suppose that the discriminant $\Delta = -16(4a^3 + 27b^2)$ of the curve E is non-zero; then E is non-singular.

For each prime p, denote by $v(p)$ the number of solutions of the congruence $y^2 = x^3 + ax+b(\mathrm{mod}\,p)$. Denote $\lambda(p) = p - v(p)$ H. Hasse proved that $|\lambda(p)| \leq 2\sqrt{p}$. For the investigations into value-distribution of the numbers $\lambda(p)$ H. Hasse and H. Weil introduced the L-function attached to the curve E. Let $s = \sigma + it$ be a complex variable. Then the L-function of the elliptic curve E is defined, for $\sigma > 3/2$, by

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

The Hasse conjecture on analytic continuation and the functional equation of $L_E(s)$ becomes true after proving the Shimura-Taniyama-Weil conjecture [1]. Therefore, the function $L_E(s)$ is analytically continuable to entire function and satisfies the following functional equation

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

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

In [6] the universality of the function $L_E(s)$ was obtained. Let $\{A\}$ denote the Lebesgue measure of the set $A \subset \mathbf{R}$. Then we have following assertion [6].

Theorem 1. *Suppose that E is a non-singular elliptic curve over the field of rational numbers. Let K be a compact subset of the strip* $D = \{s \in \mathbf{C} : 1 < \sigma < 3/2\}$ *withconnectedcomplement, and let* $f(s)$ *be a continuous non-vanishing function on K, which is analytic in the interior of K. Then for every* $\varepsilon > 0$,

$$\liminf_{T\to\infty} \frac{1}{T} meas\left\{\tau \in [0,T] : \sup_{s\in K}\left|L_E(s+i\tau) - f(s)\right| < \varepsilon\right\} > 0.$$

In [2] the assertion of Theorem 1 was extended to powers $L_E^k(s)$, $k \in \mathbf{N}$. If $L_E(s) \neq 0$ on D, then the function $L_E^{-k}(s)$, $k \in \mathbf{N}$ is also universal in the above sense.

Note that the universality of the Riemann zeta-function was discovered by S. M. Voronin [10]. Later A. Reich, S. M. Gonek, B. Bagchi, K. Matsumoto, J. Steuding, Y. Mishou, H. Bauer, A. Laurinčikas, R. Garunkštis and others obtained the universality of other classical zeta-functions and of some classes of Dirichlet series. The Linnik-Ibragimov conjecture asserts that all functions given by Dirichlet series, analytically continuable to the left absolute convergence half-plane and satisfying some growth conditions, are universal.

Our ***aim*** here is to obtain the discrete universality for the function $L_E(s)$. Let $N \in \mathbf{N}$,

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

where in the place of dots a condition satisfied by m is to be written. In discrete theorems instead of the translations $L_E(s+i\tau)$, $\tau \in [0,T]$, the translations $L_E(s+imh)$, $m = 0,1,\ldots,N$, where $h > 0$ is a fixed number, are considered.

Theorem 2. *Suppose that* $\exp\{2\pi k/h\}$ *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* $\varepsilon > 0$,

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

Theorem 2 shows that the set $\{m,\ m = 0,1,\ldots\}$ such that $L_E(s+imh)$ approximates a given analytic function is sufficiently rich: it has a positive lower density. Since by Hermite-Lindemann theorem $\exp\{a\}$ is irrational with an algebraic number $a \neq 0$, we can take, for example, $h = 2\pi$. On the other hand, Theorems 1 and 2 are non-effective in the sense that it is impossible to indicate τ or m with approximation properties.

Consequently we suppose that $\exp\{2\pi k / h\}$, $k \in \mathbf{Z} \setminus \{0\}$ is an irrational number.

A discrete limit theorem in the space of analytic functions for $L_E(s)$

For the proof of Theorem 2 we need a discrete limit theorem in the sense of the weak convergence of probability measures in the space of analytic functions for the function $L_E(s)$. Theorems of such a kind were obtained in [3] for the Matsumoto zeta-function that was introduced in [7]. The Matsumoto zeta-function $\varphi(s)$ is defined by

$$\varphi(s) = \prod_{m=1}^{\infty} A_m^{-1}(p_m^{-s}), \text{ where } A_m(x) = \prod_{j=1}^{g(m)} \left(1 - a_m^{(j)} x^{f(j,m)}\right)$$

is a polynomial of degree $f(1, m) + ... + f(g(m),m)$, $g(m) \in \mathbf{N}$, $a_m^{(j)} \in \mathbf{C}$, $f(j,m) \in \mathbf{N}$, $j = 1, ..., g(m)$, and p_m denotes the mth prime number. If

$$g(m) \le c_1 p_m^{\alpha}, \quad \left|a_m^{(j)}\right| \le c_2 p_m^{\beta} \tag{1}$$

with some positive constants c_1, c_2 and non-negative α and β, then the infinity product for $\varphi(s)$ converges absolutely in the half-plane $\sigma > \alpha + \beta + 1$, and defines there an analytic function with no zeros. Suppose that the function $\varphi(s)$ is analytically continuable to the region $D_1 = \{s \in \mathbf{C} : \sigma > \rho\}$ where $\alpha + \beta + \frac{1}{2} \le \rho < \alpha + \beta + 1$, and, for $\sigma > \rho$,

$$\varphi(\sigma + it) = B\,|t|^{c_3}, \; c^3 \ge 0; \tag{2}$$

and

$$\int_0^T |\varphi(\sigma + it)|^2 \, dt = BT, \; T \to \infty. \tag{3}$$

Here and in the sequel B denotes a quantity bounded by a constant.

Let G be a region on the complex plane, and let $H(D)$ stand for the space of analytic (on G) functions equipped with the topology of uniform convergence on compacta. To state a limit theorem in the space $H(D_1)$ for the function $\varphi(s)$ we need the following topological structure. Let for all $m \in \mathbf{N}$, $\gamma_{p_m} = \gamma = \{s \in \mathbf{C} : |s| = 1\}$, and $\Omega = \prod_{m=1}^{\infty} \gamma_{p_m}$.

With product topology and pointwise multiplication Ω is a topological Abelian group. Denoting by $\mathcal{B}(S)$ the class of Borel sets the space S, we have that the probability Haar measure m_H on $(\Omega, \mathcal{B}(\Omega))$ exists, and this leads to a probability space $(\Omega, \mathcal{B}(\Omega), m_H)$. Let $\omega(p_m)$ be the projection of $\omega \in \Omega$ to the coordinate space γ_{p_m}, and on the probability space $(\Omega, \mathcal{B}(\Omega)\, m_H)$ define an $H(D_1)$ valued random element $\varphi(s, \omega)$ by

$$\varphi(s, \omega) = \prod_{m=1}^{\infty} \prod_{j=1}^{g(m)} \left(1 - \frac{\omega^{f(j,m)}(p_m) a_m^{(j)}}{p_m^{s f(j,m)}}\right)^{-1}.$$

Let P_ξ stand for the distribution of a random element ξ.

Lemma 3. *Suppose conditions* (1) – (3) *are satisfied. Then the probability*

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

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

Proof. The lemma is a particular case of the theorem from [4], where a limit theorem in the space of meromorphic functions for the function $\varphi(s)$ was proved.

Let $V > 0$ and $D_V = \{s \in \mathbf{C} : 1 < \sigma < 3/2, |t| < V\}$. Later we will use a more convenient notation $\Omega = \prod_p \gamma_p$, and $\omega(p)$. On the probability space $(\Omega, \mathcal{B}(\Omega)\, m_H)$ define an $H(D_V)$ – valued random element $L_E(s, \omega)$ by

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

Lemma 4. *The probability measure*

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

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

Proof. Clearly, for $\sigma > 3/2$,

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

where $\lambda(p) = \alpha(p) + \beta(p)$, and $|\alpha(p)| \le \sqrt{p}$, $|\beta(p)| \le \sqrt{p}$. Therefore, (1) is valid with $\alpha = 0$ and $\beta = 1/2$. Moreover, $L_E(s)$ is an entire function and satisfies (2). From the validity of the Shimura-Taniyama-Weil conjecture and [8] we have that (3) is satisfied, too. Consequently, in view of Lemma 3 the probability measure

$$\mu_N(L_E(s + imh) \in A), \; A \in \mathcal{B}(H(\hat{D})),$$

$\hat{D} = \{s \in \mathbf{C} : \sigma > 1\}$, converges weakly to the distribution of the random element $L_E(s,\omega)$, $s \in \hat{D}$. Since the function $F : H(\hat{D}) \to H_1(D_V)$ given by the formula $F(f) = f|_{s \in D_V}$, $f \in H(\hat{D})$, is continuous, hence the lemma follows.

The support of the measure P_{L_E}

Let P be a probability measure on $(S, \mathcal{B}(S))$, where S is a separable metric space. We recall that the support of P is a minimal closed set $S_P \subset S$ such that for every neighbourhood G of each $x \in S_P$ we have $P(G) > 0$. Let

$$S_V = \{g \in H(D_V) : g(s) \neq 0 \ \text{ or } g(s) \equiv 0\}$$

Lemma 5. *The support of the measure* P_{L_E} *is the set* S_V.

Proof. The proof of the lemma is similar to that of Lemma 8 in [6], therefore we will give only a sketch of the proof. Let $a_p \in \gamma$ and $s \in D_V$,

$$g_p(s, a_p) = \begin{cases} -\log\left(1 - \dfrac{\lambda(p) a_p}{p^s} + \dfrac{a_p^2}{p^{2s-1}}\right), & \text{if } p \nmid \Delta, \\ -\log\left(1 - \dfrac{\lambda(p) a_p}{p^s}\right), & \text{if } p \mid \Delta. \end{cases}$$

Then it is proved that the set of all convergent series $\sum_p g_p(s, a_p)$ is dense in $H(D_V)$. For this some properties of functions of exponential type are applied, see, for example, [5].

The sequence $\{\omega(p)\}$ is a sequence of independent random variables defined on the probability space $(\Omega, \mathcal{B}(\Omega)\ m_H)$. The support of each $\omega(p)$ is the unit circle γ. Therefore, $\{g_p(s, \omega(p))\}$ is a sequence of independent $H(D_V)$ – valued random elements, and the support of the random elements $g_p(s, \omega(p))$ is the set

$$\{g \in H(D_V) : g(s) = g_p(s, a) \ \text{ with } |a| = 1\}$$

Hence, in view of Theorem 1.7.10 of [5] the support of the random element

$$\log L_E(s,\omega) = \sum_p g_p(s, \omega(p))$$

is the closure of the set of all convergent series $\sum_p g_p(s, a_p)$ with $a_p \in \gamma$. However, as we have seen above, the later set is dense in $H(D_V)$. Let $h : H(D_V) \to H(D_V)$ be given by the formula $h(g) = \exp\{g\}$, $g \in H(D_V)$. Then clearly, h is a continuous function sending $\log L_E(s,\omega)$ to $L_E(s,\omega)$ and $H(D_V)$ to $S_V \setminus \{0\}$. This shows that the support S_{L_E} of the random element $\log L_E(s,\omega)$ contains the set $S_V \setminus \{0\}$. However, the support is a closed set, therefore in view of the Hurwitz theorem [9] we obtain that $\overline{S_V \setminus \{0\}} = S_V$. Hence $S_V \subseteq S_{L_E}$. On the other hand, $L_E(s,\omega)$ is an almost surely convergent product of non-vanishing factors, and the Hurwitz theorem again shows that $L_E(s,\omega) \in S_V$. Thus, $S_{L_E} \subseteq S_V$, and the lemma is proved.

Proof of the two theorems

Let K be compact subset of the strip D with connected complement, and suppose that $V > 0$ is such that $K \subset D_V$. First let the function $f(s)$ have a non-vanishing analytic continuation to the region D_V. Denote by G the set of functions $g \in H(D_V)$ satisfying

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

The set G is an open one, and Lemma 5 implies that $G \subset S_V$. Now properties of the weak convergence of probability measures and of support together with Lemmas 4 yield

$$\liminf_{T \to \infty} \mu_N\left(L_E(s + imh) \in G\right) \geq P_{L_E}(G) > 0. \tag{4}$$

Now let $f(s)$ satisfy the hypotheses of the two theorems. Then according to the Mergelyan theorem (see, for example, [11]) there exists a polynomial $p(s)$ that has no zeros on K and such that

$$\sup_{s \in K} |f(s) - p(s)| < \frac{\varepsilon}{4}. \tag{5}$$

Similarly, there exists a polynomial $q(s)$ such that

$$\sup_{s \in K} |p(s) - e^{q(s)}| < \frac{\varepsilon}{4}.$$

This and (5) show that

$$\sup_{s \in K} |f(s) - e^{q(s)}| < \frac{\varepsilon}{2}, \tag{6}$$

and $e^{q(s)} \neq 0$. Therefore, by (4)

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

Hence in virtue of (6) the theorem follows.

References

1. Breuil C., Conrad B., Diamond F., Taylor R., 2001, On the modularity of elliptic curves over Q: wild 3-adic exercises. *J. Amer. Math. Soc.* Vol. 14. P. 843–939.
2. Garbaliauskienė V., Laurinčikas A., 2005, Some analytic properties for *L*-functions of elliptic curves. *Proc. Inst. Math. NAN Belarus*. Vol. 13, No. 1. P. 75–82.
3. Kačinskaitė R., 2002, A discrete limit theorem for the Matsumoto zeta-function in the space of meromorphic functions. *Liet. Mat. Rink.* Vol. 42, No. 2.1. P. 46–67 (in Russian).
4. Kačinskaitė R., Laurinčikas A., 2004, On the value distribution of the Matsumoto zeta-function. *Acta Math. Hungar.* Vol. 105, No. 4.1. P. 339–359.
5. Laurinčikas A., 1996, *Limit Theorems for the Riemann Zeta-Function*. Kluwer, Dordrecht.
6. Laurinčikas A., Matsumoto K., Steuding J., 2003, The universality of *L*-functions associated to newforms. *Izv. Math.* Vol. 67. P. 77–90.
7. Matsumoto K., 1990, Value-distribution of zeta-function. Lecture Notes in Math. 1434, *Springer-Verlag*. P. 178–187.
8. Matsumoto K., 1989, A probabilistic study on the value-distribution of Dirichlet series attached to certain cusp forms. *Nagoya Math. J.* Vol. 116. P. 123–138.
9. Titchmarsh E. C., 1939, *The Theory of Functions*. Oxford University Press, Oxford.
10. Voronin S. M., 1975, Theorem on the "universality" of the Riemann zeta-function. *Math. USSR Izv.* Vol. 9. P. 443–453.
11. Walsh J. L., 1960, *Interpolation and Approximation by Rational Functions in the Complex Domain*. Amer. Math. Soc. Collog. Publ. V. 20.

DISCRETE UNIVERSALITY THEOREM FOR *L*-FUNCTIONS OF ELLIPTIC CURVES

Jurgita Čeponienė, Virginija Garbaliauskienė, Antanas Garbaliauskas

Summary

Let E be an elliptic curve over the field of rational numbers Q defined by the Weierstrass equation $y^2 = x^3 + ax+b,$ $a, b \in \mathbf{Z}$. Denote by $\Delta = -16(4a^3 + 27b^2)$ the discriminant of the curve E, and suppose that $\Delta \neq 0$. Then the roots of the cubic $x^3 + ax+b$ are distinct, and the curve E is non-singular. In the paper there is done a research on discrete universality theorems (in Voronin's sense) for L-functions of the curve E defined by Euler product

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

where p is prime number, $\nu(p)$ is the number of solutions of the congruence $y^2 = x^3 + ax+b \pmod p$, $\lambda(p) = p - \nu(p)$, and $s = \sigma + it$ is a complex variable. We use the difference of an arithmetical progression $h > 0$ $h > 0$ such that $\exp\left\{\frac{2\pi k}{h}\right\}$ is irrational for some $k \neq 0$. The proof of the universality for L-functions of elliptic curves is based on discrete limit theorems in the sense of weak convergence of probability measures in functional spaces.

Keywords. Elliptic curve, *L*-function, universality, limit theorem, probability measure, weak convergence.

DISKRETI UNIVERSALUMO TEOREMA ELIPSINIŲ KREIVIŲ *L*-FUNKCIJOMS

Jurgita Čeponienė, Virginija Garbaliauskienė, Antanas Garbaliauskas

Santrauka

Straipsnyje apibrėžiama elipsinė kreivė, su ja susieta elipsinių kreivių *L*-funkcija, išreikšta Oilerio sandauga. Tegul E – elipsinė nesinguliarioji kreivė virš racionaliųjų skaičių kūno, duota Vejetrašo lygtimi $y^2 = x^3 + ax+b,$ $a, b \in \mathbf{Z}$, su diskriminantu $\Delta = -16(4a^3 + 27b^2)$. Kiekvienam pirminiam p pažymėkime $\nu(p)$ lyginio $y^2 = x^3 + ax+b \pmod p$ sprendinių skaičių ir $\lambda(p) = p - \nu(p)$. Elipsinių kreivių *L*-funkcija $L_E(s)$, kur $s = \sigma + it$ yra kompleksinis kintamasis, apibrėžiama Oilerio sandauga

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

Funkcija $L_E(s)$ yra analizinė pusplokštumėje $D = \left\{s \in \mathbf{C} : \sigma > \frac{3}{2}\right\}$ ir analiziškai pratęsiama į visą kompleksinę plokštumą. Elipsinių kreivių L-funkcijų diskretus universalumas remiasi ribinėmis teoremomis tikimybinio mato silpno konvergavimo prasme funkcinėse erdvėse, todėl straipsnyje pirmiausia pateikiama diskreti ribinė teorema, tirštumo bei atramos lemos. Naudojantis šiomis teoremomis įrodoma diskreti universalumo teorema elipsinių kreivių L-funkcijoms, kai visiems $k \in \mathbf{N} \setminus \{0\}$ ir fiksuotam skaičiui $h > 0$, $\exp\left\{\frac{2\pi k}{h}\right\}$ yra iracionalusis skaičius.

Prasminiai žodžiai: elipsinė kreivė, L-funkcija, universalumas, ribinė teorema, tikimybinis matas, silpnas konvergavimas.

Įteikta 2010-09-15