THE UNIVERSALITY OF DEGREES OF *L*-FUNCTIONS OF ELLIPTIC CURVES

Martynas Latakas, Virginija Garbaliauskienė, Antanas Garbaliauskas
Šiauliai University, Šiauliai College

Introduction

Let E be an elliptic curve defined by the Weierstrass equation $y^2 = x^3 + ax + b$ with $a, b \in \mathbf{Z}$. The number $\Delta = -16(4a^3 + 27b^2)$ is the discriminant of E. Suppose that $\Delta \neq 0$, i.e. the curve E is non-singular.

For each prime p let us mark by $v(p)$ the number of solutions of the congruence $y^2 \equiv x^3 + ax + b(\bmod p)$,
and let $\lambda(p) = p - v(p)$. Then the result of H. Hasse asserts that $|\lambda(p)| < 2\sqrt{p}$. (1)

H. Hasse and H. Weil attached to the curve E the L-function defined by the following 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 $s = \sigma + it$ is a complex variable. The latter product converges absolutely for $\sigma > \frac{3}{2}$, and in this region $L_E(s)$ can be written as the Dirichlet series

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

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.

Now we shortly discuss L-functions attached to cusp forms. Let

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

be the full modular group, and let q be a positive integer. The subgroup of $SL(2,\mathbf{Z})$

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

is called the Hecke subgroup or congruence subgroup mod$q$. Let κ be an even positive integer, and let $F(z)$ be a holomorphic function in the upper half-plane Im $z > 0$ Then the function $F(z)$ is called a cusp form of weight κ and level q provided that

$$F\left(\frac{az+b}{cz+d}\right) = (cz+d)^\kappa F(z) \text{ for all } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(q),$$ and

provided that $F(z)$ are holomorphic and vanishing at the cusps. In this case $F(z)$ has at ∞ the following Fourier series expansion

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

Denote by $S_\kappa(\Gamma_0(q))$ the space of all cusp forms of weight κ and level q. Let $q_1|q$. Then a function $F(z) \in S_\kappa(\Gamma_0(q_1))$ can also be an element of $S_\kappa(\Gamma_0(q))$. A cusp form $F(z) \in S_\kappa(\Gamma_0(q))$ is called a newform if $F(z)$ is not a cusp form of a level less than q, and if $F(z)$ is an Hecke eigenform, i. e. $F(z)$ is an eigenfunction $T_m F = c(m) F$ of all the Hecke operators T_m, $m = 1, 2, ...$ From this it follows that $c(1) \neq 0$, and we may assume that $F(z)$ is a normalized newform with $c(1) = 1$.

E. Hecke attached to a cusp form $F(z)$ with the Fourier expansion (2) the L-function

$$L(s,F) = \sum_{m=1}^{\infty} \frac{c(m)}{m^s}.$$

The latter Dirichlet series converges absolutely for $\sigma > \frac{\kappa+1}{2}$ and defines there a holomorphic function. Moreover, since $F(z)$ is a newform, $L(s, F)$, for $\sigma > \frac{\kappa+1}{2}$ has the Euler product expansions

$$L(s,F) = \prod_{p|q}\left(1 - \frac{c(p)}{p^s}\right)^{-1} \prod_{p|q}\left(1 - \frac{c(p)}{p^s} + \frac{1}{p^{2s+1-\kappa}}\right)^{-1}.$$

Also, it is well known that $L(s, F)$ is analytically continuable to the entire function and satisfies functional equation

$$\left(\frac{\sqrt{q}}{2\pi}\right)^s \Gamma(s) L(s,F) = \varepsilon(-1)^{\frac{\kappa}{2}} \left(\frac{\sqrt{q}}{2\pi}\right)^{\kappa-s} \Gamma(\kappa-s) L_E(\kappa-s,F),$$

where $\varepsilon = \pm 1$ is the sign of the functional equation corresponding to the eigenvalues ± 1 of the Atkin-Lehner involution $\begin{pmatrix} 0 & -q \\ 1 & 0 \end{pmatrix}$ on $S_\kappa(\Gamma_0(q))$.

By the Shimura-Taniyama conjecture every L-function $L_E(s)$ attached to a non-singular elliptic curve E over the rationals is the L-function attached to certain newform F of weight 2 of some Hecke subgroup. This conjecture as well as the Hasse conjecture on analytic continuation of $L_E(s)$ was partially proved by A Wiles [11], and a full proof was recently given in [2]. Consequently, instead of $L_E(s)$ we may consider the L-functions attached to newforms.

One of the remarkable properties of functions given by Dirichlet series is their universality. This property for the Riemann zeta-function was discovered by S. M. Voronin [9]. Later many authors generalized and improved the Voronin theorem (see survey papers [5], [7]). There exists the Linnik-Ibragimov conjecture that all functions given by Dirichlet series, analytically continuable to the left of the half-plane of absolute convergence, and satisfying some growth conditions, are universal in the Voronin sense. It seems to be that the latter conjecture is very difficult.

In [6] the universality of L-functions attached to newforms was proved, and from this some other properties for $L(s, F)$ were derived. Therefore, we have the following analogue of the Voronin theorem for L-functions of elliptic curve. Let meas $\{A\}$ denote the Lebesque measure of the set $A \subset \mathbf{R}$, and let $T > 0$, $\nu_T(...) = \frac{1}{T}\text{meas}\{\tau \in [0,T]:...\}$, where in place of dots a condition satisfied by τ is to be written. **C** stands for the complex plane.

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* $D = \left\{ s \in \mathbf{C} : 1 < \sigma < \frac{3}{2} \right\}$ *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* $\varepsilon > 0$,

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

Let k be a positive integer. **The aim of this note** is to generalize Theorem 1 for the function $L_E^k(s)$.

Theorem 2. *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 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* ε > 0, *and* $k \in \mathbf{N}$,

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

This theorem shows that there exist many translations $L_E^k(s+i\tau)$ which approximate a given analytic function $f(s)$: the set of τ has a positive lower density.

It turns out that if for $L_E^k(s)$ the analogue of the Riemann hypothesis is valid, then $L_E^{-1}(s)$ is also universal.

Theorem 3. *Suppose that* $L_E(s) \neq 0$ *on D. Then the assertion of Theorem 1 is true for the function* $L_E^{-k}(s)$.

Limit theorems

Let $\mathbf{C}_\infty = \mathbf{C} \cup \{\infty\}$ be the Riemann sphere with spherical metric d defined by the formulae

$$d(s_1,s_2) = \frac{2\,|s_1 - s_2|}{\sqrt{1+|s_1|^2}\sqrt{1+|s_2|^2}},$$

$$d(s_1,\infty) = \frac{2}{\sqrt{1+|s_1|^2}}, \quad d(\infty,\infty) = 0, \; s_1, s_2 \in \mathbf{C}.$$

Let G be a region on **C**, and let $M(G)$denote the space of meromorphic function $g: G \to (\mathbf{C}_\infty, d)$ equipped with the topology of uniform convergence on compacta. In this topology, a sequence $g_n(s) \in M(G)$ converges to a function $g(s) \in M(G)$ if $d(g_n(s)\ g(s)) \to 0$ as $n \to \infty$, uniformly on compact subsets of G. The space $H(G)$ of analytic of G functions is a subspace of $M(G)$.

Let $\gamma = \{s \in \mathbf{C} : |s| = 1\}$ and $\Omega = \prod_p \gamma_p$, where $\gamma_p = \gamma$ for each prime p. With product topology and pointwise multiplication the infinite-dimensional torus Ω is a compact topological Abelian group. Therefore, the probability Haar measure m_H on $(\Omega, \mathcal{B}(\Omega))$ ($\mathcal{B}(S)$ stands for the class of Borel sets of the space S) exists, and we have a probability space $(\Omega, \mathcal{B}(\Omega)\ m_H)$. Let $\omega(p)$ be the projection of $\omega \in \Omega$ to the coordinate space γ_p. Then $\{\omega(p)\}$ is a sequence of independent random variables defined by the probability space $(\Omega, \mathcal{B}(\Omega)\ m_H)$.

Suppose $s \in D$,

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

Then [1] and [4] show that $L_E^k(s,\omega)$ is an $H(D)$-valued random element defined on the probability space $(\Omega, \mathcal{B}(\Omega)\ m_H)$. Denote by $P_{L_E^k}$ the distribution of the random element $L_E^k(s,\omega)$, i. e.,

$$P_{L_E^k}(A) = m_H\left(\omega \in \Omega : L_E^k(s,\omega) \in A\right), \quad A \in \mathcal{B}(H(D)).$$

Lemma 4. *The probability measure*

$$\nu_T\left(L_E^k(s+i\tau) \in A\right), \quad A \in \mathcal{B}(H(D)),$$

converges weakly to $P_{L_E^k}$ *as* $T \to \infty$.

Proof. In view of validity of the Shimura-Taniyama conjecture and Lemma 3 of [6] we have that the probability measure

$$\nu_T\left(L_E(s+i\tau) \in A\right), \quad A \in \mathcal{B}(H(D)),$$

converges weakly to $P_{L_E} = P_{L_E^1}$ as $T \to \infty$. The function $h: H(D) \to H(D)$ defined by the formula $h(f) = f^k$, $f \in H(D)$, is continuous. Therefore, by a property of the weak convergence of probability measures (Theorem 5.1 of [1]) we obtain the lemma.

Now let $V > 0$, and

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

Lemma 5. *The probability measure*

$$P_T(A) \overset{def}{=} \nu_T\left(L_E^k(s+i\tau) \in A\right), \quad A \in \mathcal{B}(H(D_V)),$$

converges weakly to $m_H(L_E^k(s,\omega) \in A)$, $A \in \mathcal{B}(H(D_V))$ *as* $T \to \infty$.

Proof. Since the function defined by coordinate restriction is continuous, the lemma follows from Lemma 4 in the same way as Lemma 4.

Lemma 6. *Suppose that* $L_E(s) \neq 0$ *on D. Then the probability measure*

$$\nu_T\left(L_E^{-k}(s+i\tau) \in A\right), \quad A \in \mathcal{B}(H(D_V)),$$

converges weakly to $m_H(L_E^{-k}(s,\omega) \in A)$, $A \in \mathcal{B}(H(D_V))$ *, as* $T \to \infty$.

Proof. The metric d satisfies the equality

$$d\left(\frac{1}{f_1}, \frac{1}{f_2}\right) = d(f_1, f_2), \quad f_1, f_2 \in H(D_V)$$

Therefore, the function $h: H(D_V) \to M(D_V)$ given by the formula $h(f) = f^{-1}$, $f \in H(D_V)$ is continuous, and the lemma is consequence of its hypothesis and Lemma 5.

A density lemma

Let $a_p \in \gamma$ and $s \in D_V$,

$$g_p(s, a_p) = \begin{cases} \pm k \log\left(1 - \dfrac{\lambda(p) a_p}{p^s} + \dfrac{a_p^2}{p^{2s-1}}\right) & f \quad p|\Delta, \\ \pm k \log\left(1 - \dfrac{\lambda(p) a_p}{p^s}\right) & f \quad p|\Delta. \end{cases}$$

Lemma 7. *The set of all convergent series* $\sum_p g_p(s, a_p)$ *is dense in* $H(D_V)$.

Proof. In [6], Lemma 8, it was proved that the set of all convergent series $\sum_p \hat{g}_p(s, a_p)$ is dense in $H(D_V)$, where

$$g_p(s, a_p) = \begin{cases} -\log\left(1 - \dfrac{c(p) a_p}{p^s} + \dfrac{a_p^2}{p^{2s+1-\kappa}}\right) & f \quad p|q, \\ -\log\left(1 - \dfrac{c(p) a_p}{p^s}\right) & f \quad p|q. \end{cases}$$

and $c(p)$are the coefficients of L-functions attached to newforms of weight κ and level q. Since, by [2], $\hat{g}_p(s, a_p)$ with $\kappa = 2$ differs from $g_p(s, a_p)$ only by a fixed factor $\pm k$, the assertion of the lemma follows from Lemma 8 of [6].

The support of the limit measures in Lemmas 5 and 6

The proof of Theorems 2 and 3 based on Lemma 7 and the support of the measure $m_H\left(\omega \in \Omega : L_E^{\pm k}(s,\omega) \in A\right)$, $A \in \mathcal{B}(H(D_V))$. Let $S_V = \{g \in H(D_V) : g(s) \neq 0 \text{ or } g(s) \equiv 0\}$.

Lemma 8. *The support of the measure* $m_H\left(\omega \in \Omega : L_E^{\pm k}(s,\omega) \in A\right)$, $A \in \mathcal{B}(H(D_V))$, *is the set* S_V.

Proof. We have mentioned that $\{\omega(p)\}$is a sequence of independent random variables defined on the probability space $(\Omega, \mathcal{B}(\Omega), m_H)$. Let

$$x_p = x_p(s) = g_p(s, \omega(p)),$$

then $\{x(p)\}$ is a sequence of independent $H(D_V)$-valued random elements. Since the support of each $\omega(p)$ is the unit circle γ, the support of the random elements $x_p(s)$ is the set

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

Therefore, by Theorem 1.7.10 of [3] the support of the random element

$$\log L_E^{\pm k}(s,\omega) = \sum_p x_p(s)$$

is the closure of the set of all convergent series

$$\sum_p g_p(s, a_p), \quad a_p \in \gamma.$$

By Lemma 7 the set of these series is dense in $H(D_V)$. The function $h : H(D_V) \to H(D_V)$ given by the formula $h(g) = \exp\{g\}$, $g \in H(D_V)$, is continuous sending $\log L_E^{\pm k}(s,\omega)$ to $L_E^{\pm k}(s,\omega)$ and $H(D_V)$ to $S_V \setminus \{0\}$. Therefore, the support $S_{L_E^{\pm k}}$ of the random element $\log L_E^{\pm k}(s,\omega)$ contains the set $S_V \setminus \{0\}$. Since the support is a closed set, by the Hurwitz theorem [8] we obtain that $\overline{S_V \setminus \{0\}} = S_V$. This gives

$$S_V \subseteq S_{L_E^{\pm k}}. \tag{3}$$

On the other hand, $L_E^{\pm k}(s,\omega)$ is an almost surely convergent product of non-vanishing factors. Therefore, in virtue of the Hurwitz theorem again we find that $L_E^{\pm k}(s,\omega) \in S_V$. Hence $S_{L_E^{\pm k}} \subseteq S_V$, and this together with (3) implies the lemma.

Proofs of Theorems

Proof of Theorems 2 and 3. Let K be an arbitrary compact subset of D with connected complement. Then, clearly, there exists a number $V > 0$ such that $K \subset D_V$.

First we suppose that the function $f(s)$ in Theorems 2 and 3 has a non-vanishing continuation to D_V, and denote by G the set of functions $g \in H(D_V)$ satisfying the inequality

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

Obviously, G is an open set, and by Lemma 8 we have that $G \subset S_V$. Therefore, properties of the weak convergence of probability measures [1] as well as of the support in view of Lemmas 5 and 6 yield

$$\liminf_{T\to\infty} \nu_T \left(\sup_{s\in K} \left| L_E^{\pm k}(s+i\tau) - f(s) \right| < \varepsilon \right) \geq$$

$$\geq m_H \left(\omega \in \Omega \colon L_E^{\pm k}(s,\omega) \in G \right) > 0. \tag{4}$$

Now let for $f(s)$ the hypotheses of Theorems 2 and 3 be satisfied. Then by the Mergelyan's theorem (see [10]) we can find a sequence of polynomials $\{p_n(s)\}$ such that $p_n(s) \to f(s)$, $n \to \infty$, uniformly on K. Then there exists n_0 such that $p_{n_0} \neq 0$ on K, and

$$\sup_{s\in K} |f(s) - p_{n_0}(s)| < \frac{\varepsilon}{4}. \tag{5}$$

Using the well-known properties of polynomials and the Mergelyan's theorem again, we find a polynomial $q(s)$ such that

$$\sup_{s\in K} |p_{n_0}(s) - e^{q(s)}| < \frac{\varepsilon}{4}.$$

Hence and from (5)

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

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

$$\liminf_{T\to\infty} \nu_T \left(\sup_{s\in K} \left| L_E^{\pm k}(s+i\tau) - e^{q(s)} \right| < \frac{\varepsilon}{2} \right) > 0,$$

and this together with (6) proves the theorems.

References

1. Billingsley P., 1968, *Convergence of Probability Measures*. Wiley, New York.
2. 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.
3. Laurinčikas A., 1996, *Limit Theorems for the Riemann Zeta-Function*. Kluwer, Dordrecht.
4. Laurinčikas A., 1998, On the Matsumoto zeta-function. *Acta Arith.* Vol. 84. P. 1–16.
5. Laurinčikas A., 2003, The universality of zeta-functions. *Acta Appl. Math.* Vol. 78. No. 1–3. P. 251–271.
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., 2001. Probabilistic value-distribution theory of zeta-functions. *Sugaku*. Vol. 53. P. 279–296.
8. Titchmarsh E. C., 1939, *The Theory of Functions*. Oxford University Press, Oxford.
9. Voronin S. M., 1975, Theorem on the "universality" of the Riemann zeta-function. *Math. USSR Izv.* Vol. 9. P. 443–453.
10. Walsh J. L., 1960, Interpolation and Approximation by Rational Functions in the Complex Domain. *Amer. Math. Soc. Collog. Publ.* V. 20.
11. Wiles A., 1995, Modular elliptic curves and Fermat's last theorem. *Ann. Math.* Vol. 141. P. 443–551.

THE UNIVERSALITY OF DEGREES OF *L*-FUNCTIONS OF ELLIPTIC CURVES

Martynas Latakas, Virginija Garbaliauskienė, Antanas Garbaliauskas

Summary

Let E be an elliptic non-singular curve over the field of rational numbers **Q** defined by the Weierstrass equation

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

Let us denote by $\Delta = -16(4a^3 + 27b^2)$ the discriminant of the curve E. For each prime p let us mark the number of solutions of congruence $y^2 = x^3 + ax + b (\mathrm{mod}\, p)$ $\nu(p)$ and let $\lambda(p) = p - \nu(p)$. The L-function $L_E(s)$ of elliptic curves, where $s = \sigma + it$ is a complex variable, is 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 $y^2 = x^3 + ax + b (\mathrm{mod}\, p)$, $\lambda(p) = p - \nu(p)$ and

$s = \sigma + it$ is a complex variable. In the paper, a survey on universality theorems (in Voronin's sense) for L-functions and the degrees of L-functions of elliptic curves over the field of rational numbers is given.

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

Keywords: elliptic curve, L-function, universality, limit theorem.

ELIPSINIŲ KREIVIŲ *L*-FUNKCIJŲ LAIPSNIŲ UNIVERSALUMAS

Martynas Latakas, Virginija Garbaliauskienė, Antanas Garbaliauskas

Santrauka

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 $v(p)$ lyginio $y^2 = x^3 + ax + b \pmod p$ sprendinių skaičių ir $\lambda(p) = p - v(p)$. 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, o analizinės savybės sutampa su svorio 2 naujųjų formų savybėmis.

Straipsnyje pateikiama tolydaus tipo ribinė teorema, tirštumo bei atramos lemos ir įrodoma tolydi universalumo teorema elipsinių kreivių L-funkcijos laipsniams $L_E^{\pm k}(s)$, kur $k \in \mathbf{N}$.

Prasminiai žodžiai: elipsinė kreivė, L-funkcija, universalumas, ribinė teorema.

Įteikta 2009-09-02