THE FUNCTIONAL INDEPENDENCE OF THE POWERS OF *L*-FUNCTIONS OF ELLIPTIC CURVES

Sigita Čepukaitė[1], Virginija Garbaliauskienė[1, 2], Antanas Garbaliauskas[2]
[1] *Šiauliai University*
[2] *Šiauliai College*

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 wattled 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.

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

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

We assume that the cubic $x^3 + ax + b$ has not a multiple root. 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. For example, the non-singular curves are $y^2 = x^3 - x$ and $y^2 = x^3 + x$, and the singular elliptic curves are $y^2 = x^3$ and $y^2 = x^3 + x^2$.

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

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

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

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

In view of the Hasse estimate

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

the infinite product for $L_E(s)$ converges absolutely and uniformly on compact subsets of the half-plane $D_a = \left\{s \in C : \sigma > \frac{3}{2}\right\}$, and defines there an analytic function with no zeros. The function $L_E(s)$ also can be written in the form of Dirichlet series

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

where

$$\lambda(m) = \prod_{p^\alpha \| m} \lambda(p^\alpha),$$

and $p^\alpha \| m$ means that $p^\alpha \mid m$ but $\not{p}^{\alpha} \mid m$, and the series also converges absolutely in D_a.

Analytic properties of the function $L_E(s)$

Analytic continuation of the function $L_E(s)$ and its universality is closely related to those of *L*-function of certain modular forms. Therefore, we start with some facts from the theory of modular forms.

Denote by $SL(2, \mathbf{Z})$ the full modular group, i. e.

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

Furthermore, for a positive integer *q*, define

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

Then $\Gamma_0(q)$ is a subgroup of $SL(2, \mathbf{Z})$, and it is called Hecke's or congruence subgroup $\mathrm{mod}\, q$.

Now let

$$U = \left\{ z \in \mathbf{C} : z = x + iy, \; i = \sqrt{-1}, \; y > 0 \right\}$$

be the upper half-plane together with ∞. The rational numbers and ∞ are called cusps. Let $F(s)$ be a holomorphic on *U* function, and suppose that, for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbf{Z})$, the functional equation

$$F\left(\frac{az + b}{cz + d}\right) = (cz + d)^\kappa F(z) \qquad (1)$$

with some even positive integer κ is satisfied. Then

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

is the Fourier series expansion of $F(z)$ at infinity. The function $F(z)$ is called holomorphic at infinity if $c(m)=0$ for $m<0$, and vanishing at infinity if $c(m)=0$ for $m\leq 0$. Moreover, $F(z)$ is called holomorphic and vanishing at other cusps if the function

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

is holomorphic and vanishing at infinity for all $\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in SL(2,\mathbf{Z})$, respectively. If $F(z)$ is holomorphic at the cusps, then it is called a modular form of weight κ. In this case, the Fourier series expansion at infinity of $F(z)$ is

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

If the modular form $F(z)$ of weight κ vanishes at the cusps, then it is called a cusp form of weight κ, and

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

is its Fourier series expansion at infinity. If equation (1) is satisfied for all $\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in\Gamma_0(q)$, then the cusp form $F(z)$ is called a cusp form of weight κ and level *q*.

The Ramanujan cusp form

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

is a classical example of cusp forms for $SL(2,\mathbf{Z})$. Its weight is 12, and $\tau(m)$ is called the Ramanujan function. The function $\tau(m)$ is multiplicative.

Denote by $S_\kappa(\Gamma_0(q))$ the space of all cusp forms of weight κ and level q. An element *F* of $S_\kappa(\Gamma_0(q))$ is called a Hecke's eigenform if *F* is an eigenfunction for all Hecke operators

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

If $q_1 \mid q$, then an element *F* of $S_\kappa(\Gamma_0(q_1))$ can be also an element of $S_\kappa(\Gamma_0(q))$. An element of $S_\kappa(\Gamma_0(q))$ is called a newform if it is a Hecke eigenform and if it is not a cusp form of level less than *q*. Let $F(s)$ be a cusp form of weight κ with the Fourier series expansion (2). Then the function

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

is called the *L*-function of the cusp form $F(z)$. The series for $L(s,F)$ converges absolutely for

$$\sigma>\frac{\kappa+1}{2},$$

moreover, $L(s,F)$ is analytically continuable to an entire function.

Now we will state the principal properties of the function $L_E(s)$. For long time, these properties were known as the conjectures.

Conjecture A (H. Hasse). The function $L_E(s)$ is analytically continuable 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, $\eta=\pm1$ is the root number, and $\Gamma(s)$, as usual, denotes the Euler gamma-function.

Conjecture B (Shimura-Taniyama-Weil). The Fourier series

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

is a newform of weight 2 for some $\Gamma_0(q)$.

Now Conjectures A and B are proved. First they were proved by R. Taylor and A. Wiles [5] for semistable elliptic curves, and this succeded the proof of the last Fermat problem. We recall that in the semistable case there is no additive reduction but only multiplicative one is.

Recently, Conjectures A and B were proved completely by C. Breuil, B. Conrad, F. Diamond and R. Taylor [1]. Therefore, analytic properties of the function $L_E(s)$ coincide with those of *L*-functions of newforms of weight 2.

Universality theorem of continuous type

The universality is a very interesting property of zeta and *L*-functions. J. Marcinkiewicz was the first who in 1935 used the name of the universality.

The first universality theorem for the Riemann zeta-function $\zeta(s)$ defined, for $\sigma > 1$, by

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

and by analytic continuation elsewhere, was discovered by S. M. Voronin in 1975 [6]. Let $0 < r < \frac{1}{4}$, and let $f(s)$ be a continuous non-vanishing function on the disc $|s| \leq r$ which is analytic in the interior of this disc. Then S. M. Voronin proved that for every ε there exists a real number $\tau = \tau(\varepsilon)$ such that

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

Later, S. M. Gonek, A. Reich, B. Bagchi, A. Laurinčikas, K. Matsumoto, R. Garunkštis, J. Steuding, W. Schwarz, H. Mishou, R. Kačinskaitė, R. Šleževičienė, J. Ignatavičiūtė, J. Genys, H. Nagoshi and others generalized and improved the Voronin theorem. It turns out that a given analytic function $f(s)$ can be approximated by translations of $\zeta(s)$ uniformly on more general sets than a disc. Denote by $\text{meas}\{A\}$ the Lebesgue measure of a measurable set $A \subset \mathbf{R}$, and let, for $T > 0$,

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

where in place of dots a condition satisfied by τ is to be written. Then the last version of the Voronin theorem is contained in the following statement, see, for example, [4]. Let *K* be a compact subset of the strip

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

with connected complement. Let $f(s)$ be a continuous and non-vanishing on *K* function which is analytic in the interior of *K*. Then, for every $\varepsilon > 0$,

$$\liminf_{T \to \infty} \nu_T \left(\sup_{s \in K} \left| \zeta(s + i\tau) - f(s) \right| < \varepsilon \right) > 0. \qquad (3)$$

The later theorem shows that many translations $\zeta(s + i\tau)$ exist which approximate a given analytic function $f(s)$: the set of τ in (3) has a positive lower density.

The majority of classical zeta and *L*-functions are universal in the Voronin sense. The Linnik-Ibragimov conjecture says that all functions in some half-plane given by Dirichlet series, analytically continuable to the left of the absolute convergence half-plane and satisfying some natural growth conditions are universal in the Voronin sense. All recent results on the universality of Dirichlet series support that conjecture.

The aim of this paper is to give a survey on the universality the positive integer powers of *L*-functions of elliptic curves and the functional independence of the function $L_E^k(s)$, $k \in \mathbf{N}$. The universality of *L*-functions of newforms has been proved in [4]. From this the universality of $L_E(s)$ follows. Let $D = \left\{ s \in \mathbf{C} : 1 < \sigma < \frac{3}{2} \right\}$.

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 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 $\varepsilon > 0$,*

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

Theorem 1 can be generalized for powers of $L_E(s)$ as well as the universality theorem of the derivative $L'_E(s)$ can be obtained.

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 $\varepsilon > 0$, and $k \in \mathbf{N}$,*

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

Proof of Theorem 2 is given in [2].

The universality of the derivative $L'_E(s)$ is contained in the following statement.

Theorem 3 [3]. *Let K be a compact subset of the strip D with connected complement, and let $f(s)$ be a continuous function on K which is analytic in the interior of K. Then, for every $\varepsilon > 0$,*

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

Note that, differently from Theorems 3, the function $f(s)$ can be vanishing on *K*.

The functional independence of $L_E^k(s)$

The universality of functions implies their functional independence. Note that the problem of independence of functions comes back to D. Hilbert. S. M. Voronin [7] obtained the functional independence of $\zeta(s)$. Let F_l, $l=0,1,....,n,$ be continuous functions, and let the equality

$$\sum_{l=0}^{n} s^l F_l\left(\zeta(s),\zeta'(s),...,\zeta^{(N-1)}(s)\right)=0$$

be valid identically for *s*. Then $F_l \equiv 0$ for $l=0,1,....,n.$

Functions $L_E^k(s)$ are functional independent too.

Theorem 4. *Let $h_0,...,h_M$ be continuous functions on $\mathbf{C}^n$, $M\in\mathbf{N}_0$, $n\in\mathbf{N}$, $k\in\mathbf{N}$. If*

$$\sum_{m=0}^{M} s^m h_m\left(L_E^k(s),\, kL_E^{k-1}(s)\,L'_E(s),...,(L_E^k(s)^{(n-1)})\right)\equiv 0,$$

then $h_m \equiv 0$ for $m=0,.1,...,M.$

We begin the proof of Theorem 4 with the following statement.

Lemma 5. *Define the mapping $u\colon \mathbf{R}\to\mathbf{C}^n$ by the formula*

$$u(t)=\left(L_E^k(\sigma+it),\, kL_E^{k-1}(\sigma+it)\,L'_E(\sigma+it),...,\right.$$
$$\left. ...,(L_E^k(\sigma+it)^{(n-1)})\right),\quad 1<\sigma<\frac{3}{2}.$$

Then the image of **R** *is dense in C^n.*

Proof. For the proof of the lemma it suffices to check that for each $\varepsilon>0$ and arbitrary complex numbers $a_0,a_1,...,a_{n-1}$ there exists a number $t\in\mathbf{R}$ such that

$$\left|\left(L_E^k(\sigma+it)\right)^{(j)}-a_j\right|<\varepsilon \tag{4}$$

for $j=0,1,...,n-1$.

Consider the polynomial

$$p_n(s)=\frac{a_{n-1}s^{n-1}}{(n-1)!}+\frac{a_{n-2}s^{n-2}}{(n-2)!}+...+\frac{a_0}{0!}.$$

Obviously, $p_n^{(j)}(0)=a_j$, $j=0,1,...,n-1$. We take a fixed number σ_0, $1<\sigma_0<\frac{3}{2}$, and let *K* be a compact subset of the strip *D* with connected complement such that σ_0 is an interior point of *K*. Then Theorem 2 shows that there exists a sequence of real numbers $\{\tau_m\}$, $\lim_{m\to\infty}\tau_m=+\infty$, satisfying

$$\sup_{s\in K}\left|L_E^k(s+i\tau_m)-p_n(s-\sigma_0)\right|<\frac{\varepsilon\delta^n}{2^n n!},$$

where δ is the distance of σ_0 from *K*. Hence, applying the Cauchy integral formula

$$\left(L_E^k(\sigma_0+i\tau_m)\right)^{(j)}-a_j=$$
$$=\frac{j!}{2\pi i}\int_{|s-\sigma_0|=\frac{\delta}{2}}\frac{L_E^k(s+i\tau_m)-p_n(s-\sigma_0)}{\left(s-\sigma_0\right)^{j+1}}ds,$$

we obtain (4).

Lemma 6. *Let h be a continuous function on $\mathbf{C}^n$. Suppose that the equality*

$$h\left(L_E^k(s),\, kL_E^{k-1}(s)\,L'_E(s),...,(L_E^k(s)^{(n-1)})\right)=0 \tag{5}$$

holds identically for s. Then $h\equiv 0$.

Proof. On the contrary, suppose that $h\neq 0$. Then there exists a point $A=(a_0,a_1,a_{n-1})\in\mathbf{C}^n$ such that $h(A)\neq 0$. From the continuity of *h* it follows that there exists a region *G* containing the point *A* and such that

$$\left|h(...)\right|\geq c>0 \tag{6}$$

for all points from *G*. Now let $1<\sigma<\frac{3}{2}$. Then by Lemma 5 we can find values of *s* such that

$$\left(L_E^k(s),\, kL_E^{k-1}(s)\,L'_E(s),...,(L_E^k(s)^{(n-1)})\right)\in G.$$

This together with (6) contradicts (5). Thus, $h\equiv 0.$

Proof of Theorem 4. Without loss of generality we can suppose that $h_0 \not\equiv 0$. Then there exists a bounded region G_0 such that

$$|h_0(...)| \geq c_0 > 0$$

for all points from G_0. Denote by m_0 the greatest integer $\leq M$ such that

$$\sup |h_{m_0}(...)| \neq 0,$$

where the supremum is taken over all points from G_0. Note that if $m_0 = 0$, then the assertion of the theorem is a result of Lemma 6. Therefore, we suppose that $m_0 > 0$. Then we can find a region $G_1 \subset G_0$ such that

$$\inf |h_{m_0}(...)| \geq c_1 > 0, \tag{7}$$

where the infimum is taken over all points from G_1. By the proof of Lemma 5 there exists a sequence $\{\tau_m\}$, $\lim\limits_{m\to\infty} \tau_m = +\infty$, such that

$$\left(L_E^k(\sigma + i\tau_m),\ kL_E^{k-1}(\sigma + i\tau_m)\, L'_E(\sigma + i\tau_m), ..., (L_E^k(\sigma + i\tau_m))^{(n-1)}\right) \in G_1.$$

This and (7) show that

$$|\, \sigma + i\tau_m\, |^{m_0}\, |\, h_{m_0}\left(L_E^k(\sigma + i\tau_m),\ kL_E^{k-1}(\sigma + i\tau_m)\, L'_E(\sigma + i\tau_m), ...,\ (L_E^k(\sigma + i\tau_m))^{(n-1)}\ |\ \to +\infty\right.$$

as $m \to \infty$. Hence the theorem follows.

References

1. Breuil C., Conrad B., Diamond F., Taylor R., 2001, On the modularity of elliptic curves over $\mathbf{Q}$: 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. Nr. 1. P. 75–82.
3. Garbaliauskienė V., Laurinčikas A., 2007, The universality of the derivatives of *L*-functions of elliptic curves. *Analytic and Probab. Methods in Number Theory, Proceed. the 4th Palanga Confer.* P. 24–29. TEV.
4. Laurinčikas A., 1996, *Limit Theorems for the Riemann Zeta-Function*. Kluwer, Dordrecht.
5. Taylor R., Wiles A., 1995, Ring-theoretic properties of certain Hecke algebras. *Ann. Math.* Vol.141. P. 3–26.
6. Voronin S. M., 1975, Theorem on the "universality" of the Riemann zeta-function. *Math. USSR Izv.* Vol. 9. P. 443–453.
7. Voronin S. M., 1979, Analytic properties of Dirichlet generating functions of arithmetic objects. *Math. Notes*. Vol. 24. P. 966–969.

ELIPSINIŲ KREIVIŲ *L*-FUNKCIJŲ LAIPSNIŲ FUNKCINIS NEPRIKLAUSOMUMAS

Sigita Čepukaitė, Virginija Garbaliauskienė, Antanas Garbaliauskas

Santrauka

Elipsinių kreivių teorija yra gana sudėtinga, skaitlinga hipotezėmis. Kita vertus, elipsinės kreivės turi daug praktinių pritaikymų, pavyzdžiui, kriptografijoje. Straipsnyje apibrėžiama elipsinė kreivė, su ja susieta elipsinių kreivių *L*-funkcija, išreikšta Oilerio sandauga ir Dirichlė eilute, pateikiamos šios funkcijos savybės, t. y. elipsinių kreivių *L*-funkcijos savybės sutampa su svorio 2 modulinių formų analizinėmis savybėmis. Darbe pateikiama tolydaus tipo universalumo teorema, kuri apibendrinama dviem aspektais: nagrinėjamas funkcijos laipsnių ir jos išvestinės universalumas. Su elipsinių kreivių *L*-funkcijų laipsnių universalumu glaudžiai siejami ir elipsinių kreivių *L*-funkcijų laipsnių funkcinis nepriklausomumas, kurio įrodymas ir pateiktas šiame straipsnyje.

Prasminiai žodžiai: elipsinė kreivė, *L*-funkcija, universalumas, funkcinis nepriklausomumas.

THE FUNCTIONAL INDEPENDENCE OF THE POWERS OF *L*-FUNCTIONS OF ELLIPTIC CURVES

Sigita Čepukaitė, Virginija Garbaliauskienė, Antanas Garbaliauskas

Summary

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

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

We assume that the cubic $x^3 + ax + b$ has not a multiple root. 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, a survey on universality theorems (in Voronin's sense) for *L*-functions of the curve *E* defined by Euler product

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

where p is prime number, $\nu(p)$ are the number of solutions of the congruence $y^2 \equiv x^3 + ax + b \,(\mathrm{mod}\, p)$, $\lambda(p) = p - \nu(p),$ and $s = \sigma + it$ be a complex variable. All stated above universality theorems are of continuous type: in them translations of the imaginary part of the complex variable vary continuously in the interval [0, *T*]. The proof of the universality for *L*-functions of elliptic curves is based on limit theorems in the sense of weak convergence of probability measures in functional spaces. The universality theorems can be generalized in two directions: for the positive integer powers of *L*-functions of elliptic curves over the field of rational numbers and their derivatives as well as the functional independence of the function $L_E^k(s)$, $k \in \mathbf{N}$ is given.

Key words: Elliptic curve, *L*-function, universality, functional independence.

Įteikta 2008-09-16