

Congruences of twisted L-values

What am I doing at the moment

David Kurniadi Angdinata

University College London

Thursday, 19 October 2023

Overview

Notation:

- ▶ N is an integer
- ▶ p and q are odd primes such that $p \nmid N$ (and $p \equiv 1 \pmod{q}$)
- ▶ E is an elliptic curve over \mathbb{Q} of conductor N (with analytic rank zero)
- ▶ χ is a Dirichlet character of conductor p and order q

Outline:

- ▶ Twisted L-values
- ▶ Modular symbols
- ▶ Arithmetic consequences
- ▶ Asymptotic distribution

The L-function of E

Recall that the **L-function of E** is given by

$$L(E, s) := \prod_p \frac{1}{\det(1 - p^{-s} \cdot \phi_p \mid \rho_{E, \ell}^{I_p})},$$

where $\phi_p \in G_{\mathbb{Q}}$ is an arithmetic Frobenius and $\rho_{E, \ell} : G_{\mathbb{Q}} \rightarrow \text{Aut}(T_{\ell}(E))$ is the representation of the ℓ -adic Tate module $T_{\ell}(E)$ for some $\ell \neq p$.

Conjecture (Birch–Swinnerton-Dyer)

The order of vanishing of $L(E, s)$ at $s = 1$ is $\text{rk}(E)$, and

$$\lim_{s \rightarrow 1} \frac{L(E, s)}{(s - 1)^{\text{rk}(E)}} \cdot \frac{1}{\Omega(E)} = \frac{\text{Reg}(E) \cdot \text{Tam}(E) \cdot \#\text{III}(E)}{\#\text{tor}(E)^2}.$$

When $\text{rk}(E) = 0$, the LHS is the **algebraic L-value of E** , given by

$$\mathcal{L}(E) := L(E, 1) \cdot \frac{1}{\Omega(E)}.$$

The L-function of E/K

Let K/\mathbb{Q} be finite Galois. The **L-function of E/K** is given by

$$L(E/K, s) := \prod_{\mathfrak{p}} \frac{1}{\det(1 - \text{Nm}(\mathfrak{p})^{-s} \cdot \phi_{\mathfrak{p}} \mid \rho_{E/K, \ell}^{I_{\mathfrak{p}}})}.$$

Conjecture (Birch–Swinnerton-Dyer)

The order of vanishing of $L(E/K, s)$ at $s = 1$ is $\text{rk}(E/K)$, and

$$\lim_{s \rightarrow 1} \frac{L(E/K, s)}{(s - 1)^{\text{rk}(E/K)}} \cdot \frac{\sqrt{\Delta(K)}}{\Omega(E/K)} = \frac{\text{Reg}(E/K) \cdot \text{Tam}(E/K) \cdot \#\text{III}(E/K)}{\#\text{tor}(E/K)^2}.$$

On the other hand, Artin formalism gives a factorisation

$$L(E/K, s) = \prod_{\rho: \text{Gal}(K/\mathbb{Q}) \rightarrow \mathbb{C}^{\times}} L(E, \rho, s)^{\dim(\rho)}.$$

Twisted L-functions of E

Let $K = \mathbb{Q}(\zeta_p)$. Then

$$\left\{ \begin{array}{l} \text{Artin representations} \\ \text{Gal}(K/\mathbb{Q}) \rightarrow \mathbb{C}^\times \end{array} \right\} \quad \xleftrightarrow{\sim} \quad \left\{ \begin{array}{l} \text{Dirichlet characters} \\ (\mathbb{Z}/p\mathbb{Z})^\times \rightarrow \mathbb{C}^\times \end{array} \right\}.$$

The **L-function of E twisted by χ** is given by

$$L(E, \chi, s) := \prod_p \frac{1}{\det(1 - p^{-s} \cdot \phi_p \mid (\rho_{E,\ell} \otimes \rho_\chi)^{I_p})}.$$

More concretely,

$$L(E, s) = \sum_{n \in \mathbb{N}} \frac{a_n}{n^s} \quad \xrightarrow{\chi} \quad L(E, \chi, s) = \sum_{n \in \mathbb{N}} \frac{a_n \chi(n)}{n^s}.$$

Conjecture (Deligne–Gross)

The order of vanishing of $L(E, \chi, s)$ at $s = 1$ is $\langle \chi, E(K)_\mathbb{C} \rangle$.

A twisted BSD-type formula

Is there a conjectural leading term?

When $\text{rk}(E) = 0$, the **algebraic L-value of E twisted by χ** is given by

$$\mathcal{L}(E, \chi) := L(E, \chi, 1) \cdot \frac{p}{\tau(\chi) \cdot \Omega(E)},$$

where $\tau(\chi)$ is the Gauss sum of χ .

Example (Dokchitser–Evans–Wiersema)

Let E_1 and E_2 be given by 307a1 and 307c1, and let χ be the quintic character of conductor 11 given by $\chi(2) = \zeta_5$. Then $\Delta(E_i) = -307$, and

$$\text{Reg}(E_i/K) = \text{Tam}(E_i/K) = \text{III}(E_i/K) = \text{tor}(E_i/K) = 1,$$

for all $K \subseteq \mathbb{Q}(\zeta_{11})^+$. However

$$\mathcal{L}(E_1, \chi) = 1, \quad \mathcal{L}(E_2, \chi) = \zeta_5(\zeta_5 + \zeta_5^2 + \zeta_5^3)^2.$$

Varying the character

Fix E and q . As p varies, how does $\mathcal{L}(E, \chi)$ vary?

Example

Let E be given by 67a1, and let $q = 3$.

| p | 7 | 13 | 19 | 31 | 37 | 43 | 61 | 73 | 79 |
|------------------------|------------|------------|------------|--------------|------------|-------------|------------|-------------|----|
| $\mathcal{L}(E, \chi)$ | $2\zeta_3$ | $3\zeta_3$ | $-\zeta_3$ | $-27\zeta_3$ | $3\zeta_3$ | $-4\zeta_3$ | $-\zeta_3$ | $-3\zeta_3$ | 8 |
| $\zeta_3 \mapsto 1$ | 2 | 3 | -1 | -27 | 3 | -4 | -1 | -3 | 8 |
| $\#E(\mathbb{F}_p)$ | 10 | 12 | 13 | 42 | 39 | 46 | 64 | 81 | 88 |
| sum | 12 | 15 | 12 | 15 | 42 | 42 | 63 | 78 | 96 |

| p | 97 | 103 | 109 | 127 | 139 | 151 | 157 | 163 |
|------------------------|-----|------------|--------------|-------------|-------------|-----|-----|--------------|
| $\mathcal{L}(E, \chi)$ | -17 | $3\zeta_3$ | $-90\zeta_3$ | $74\zeta_3$ | $23\zeta_3$ | -2 | 16 | $-43\zeta_3$ |
| $\zeta_3 \mapsto 1$ | -17 | 3 | -90 | 74 | 23 | -2 | 16 | -43 |
| $\#E(\mathbb{F}_p)$ | 98 | 120 | 108 | 121 | 118 | 149 | 149 | 145 |
| sum | 81 | 123 | 18 | 195 | 141 | 147 | 165 | 102 |

The modularity theorem

Write L-values of E as L-values of modular forms.

Recall that the **Hecke L-function** of a cusp form $f \in S_k(\Gamma)$ is given by

$$L(f, s) := -\frac{(-z)^{s-1}}{\Gamma(s)} \int_0^\infty (2\pi i)^s f(z) dz.$$

Theorem (Carayol, Eichler, Shimura, BCDT, Edixhoven)

There is a finite surjective morphism $\phi_E : X_0(N) \rightarrow E$ defined over \mathbb{Q} , and a cuspidal eigenform $f_E \in S_2(\Gamma_0(N))$, such that

- ▶ the Hecke operator T_p has eigenvalue $a_p(E)$,
- ▶ the Hecke L-function of f_E is $L(E, s)$, and
- ▶ the pullback of ω_E under ϕ_E is a positive multiple of $2\pi i f_E(z) dz$.

This positive multiple is called the **Manin constant** $c_0(E)$ of E .

Classical modular symbols

A **modular symbol** is a path $\{x, y\} \in \mathcal{H}/\Gamma$, whose **period** is

$$\mu_f(x, y) := \int_x^y 2\pi i f(z) dz,$$

so that $\mu_f(0, \infty) = -L(f, 1)$. For any $x \in \mathbb{Q}$,

$$\mu_f(0, x + \mathbb{Z}) = \mu_f(0, x), \quad \mu_f(0, -x) = \overline{\mu_f(0, x)}.$$

In particular, for any $x \in \mathbb{Q}$,

$$\mu_f(0, x) + \mu_f(0, 1-x) = 2\Re(\mu_f(0, x)).$$

Lemma (Manin)

$$\frac{2\Re(\mu_{f_E}(0, x))}{\Omega(E)} \in \frac{1}{c_0(E)} \mathbb{Z}.$$

L-values as periods

The Hecke operator T_p acts on the space of modular symbols such that

$$-L(E, 1) \cdot \#E(\mathbb{F}_p) = \sum_{n=1}^{p-1} \mu_{f_E}(0, \frac{n}{p}).$$

Dividing by $\Omega(E)$ gives

$$-\mathcal{L}(E) \cdot \#E(\mathbb{F}_p) = \sum_{n=1}^{p-1} \frac{\mu_{f_E}(0, \frac{n}{p})}{\Omega(E)}.$$

Combining the n -th and $(p - n)$ -th terms gives

$$-\mathcal{L}(E) \cdot \#E(\mathbb{F}_p) = \sum_{n=1}^{\frac{p-1}{2}} \frac{2\Re(\mu_{f_E}(0, \frac{n}{p}))}{\Omega(E)}.$$

Multiplying by $c_0(E)$ gives an equality in \mathbb{Z} .

Twisted L-values as periods

Applying the Mellin transform to the Dirichlet series of $f_E \otimes \chi$ yields

$$L(E, \chi, 1) \cdot \frac{p}{\tau(\chi)} = \sum_{n=1}^{p-1} \bar{\chi}(n) \mu_{f_E}(0, \frac{n}{p}).$$

A similar rearrangement gives

$$\mathcal{L}(E, \chi) = \sum_{n=1}^{\frac{p-1}{2}} \bar{\chi}(n) \frac{2\Re(\mu_{f_E}(0, \frac{n}{p}))}{\Omega(E)}.$$

Multiplying by $c_0(E)$ gives an equality in $\mathbb{Z}[\zeta_q]$.

Theorem (Manin)

$$-c_0(E) \cdot \mathcal{L}(E) \cdot \#E(\mathbb{F}_p) \equiv c_0(E) \cdot \mathcal{L}(E, \chi) \pmod{1 - \zeta_q}.$$

Revisiting the example

Example (Dokchitser–Evans–Wiersema)

Let E_1 and E_2 be given by 307a1 and 307c1, and let χ be the quintic character of conductor 11 given by $\chi(2) = \zeta_5$. Then $\Delta(E_i) = -307$, and

$$\text{Reg}(E_i/K) = \text{Tam}(E_i/K) = \text{III}(E_i/K) = \text{tor}(E_i/K) = 1,$$

for all $K \subseteq \mathbb{Q}(\zeta_{11})^+$. However

$$\mathcal{L}(E_1, \chi) = 1, \quad \mathcal{L}(E_2, \chi) = \zeta_5(\zeta_5 + \zeta_5^2 + \zeta_5^3)^2.$$

Now $c_0(E_i) = \mathcal{L}(E_i) = 1$, but

$$\#E_1(\mathbb{F}_{11}) = 9, \quad \#E_2(\mathbb{F}_{11}) = 16,$$

so the congruence says $\mathcal{L}(E_1, \chi) \not\equiv \mathcal{L}(E_2, \chi) \pmod{1 - \zeta_5}$.

In fact, the congruence clarifies all 30 pairs of examples in the paper.

Insufficiency of congruence

In general, the congruence only serves as a sanity check for the L-value.

Example

Let E_1 and E_2 be given by 182d1 and 460a1, and let χ be the quintic character of conductor 11 given by $\chi(2) = \zeta_5$. Then $\Delta(E_i) < 0$, and

$$\text{Reg}(E_i/K) = \text{Tam}(E_i/K) = \text{III}(E_i/K) = \text{tor}(E_i/K) = 1,$$

for all $K \subseteq \mathbb{Q}(\zeta_{11})^+$. Furthermore $c_0(E_i) = \mathcal{L}(E_i) = 1$, and

$$\#E_1(\mathbb{F}_{11}) = 11, \quad \#E_2(\mathbb{F}_{11}) = 6,$$

so the congruence says $\mathcal{L}(E_1, \chi) \equiv \mathcal{L}(E_2, \chi) \pmod{1 - \zeta_5}$. However

$$\mathcal{L}(E_1, \chi) = -\zeta_5^2, \quad \mathcal{L}(E_2, \chi) = -\zeta_5^3.$$

In certain cases, the congruence can be interpreted as an equality.

Congruence for units

Let $K \subseteq \mathbb{Q}(\zeta_p)$ be the subfield of degree q where χ factors through K/\mathbb{Q} . Assume further that the Birch–Swinnerton-Dyer conjecture holds for E over \mathbb{Q} and over K , and that $c_0(E) = 1$ and $\mathcal{L}(E) \cdot \#E(\mathbb{F}_p) \not\equiv 0 \pmod{q}$.

Theorem (Dokchitser–Evans–Wiersema)

$\mathcal{L}(E, \chi) = \overline{\chi}(N) \cdot \ell$ for some $\ell \in \mathbb{Z}[\zeta_q + \overline{\zeta_q}]$, has norm $\pm \mathcal{B}(E, \chi)$, where

$$\mathcal{B}(E, \chi) := \frac{\text{Tam}(E/K) \cdot \#\text{III}(E/K) \cdot \#\text{tor}(E/K)^{-2}}{\text{Tam}(E/\mathbb{Q}) \cdot \#\text{III}(E/\mathbb{Q}) \cdot \#\text{tor}(E/\mathbb{Q})^{-2}} \in \mathbb{Z},$$

and generates an ideal of $\mathbb{Z}[\zeta_q]$ invariant under complex conjugation.

Corollary

If $\mathcal{B}(E, \chi) = 1$, then $\ell \in \mathbb{Z}[\zeta_q + \overline{\zeta_q}]^\times$, and

$$\ell \equiv -\mathcal{L}(E) \cdot \#E(\mathbb{F}_p) \pmod{2 - (\zeta_q + \overline{\zeta_q})}.$$

If $q = 3$, the congruence determines ℓ exactly.

Congruence for non-units

In general, the ideal generated by $\mathcal{L}(E, \chi)$ has finitely many possibilities.

Example (Dokchitser–Evans–Wiersema)

Let E_1 and E_2 be given by 291d1 and 139a1, and let χ be the quintic character of conductor 31 given by $\chi(3) = \zeta_5^3$. Then $\mathcal{B}(E_i, \chi) = 11^2$, so $\mathcal{L}(E_i, \chi)$ generate ideals of norm 11^2 that are invariant under complex conjugation. There are only two such ideals, generated by

$$\ell_1 := 3\zeta_5^3 + \zeta_5^2 + 3\zeta_5, \quad \ell_2 := \zeta_5^3 + 3\zeta_5 + 3.$$

In fact, $(\mathcal{L}(E_i, \chi)) = (\ell_i)$ by Burns–Castillo. Furthermore $\mathcal{L}(E_i) = 1$, $\#E_1(\mathbb{F}_{31}) = 33$, and $\#E_2(\mathbb{F}_{31}) = 23$, so the congruence says

$$\mathcal{L}(E_1, \chi) = u_1 \cdot \ell_1, \quad u_1 \cdot (3 + 1 + 3) \equiv -33 \pmod{1 - \zeta_5},$$

$$\mathcal{L}(E_2, \chi) = u_2 \cdot \ell_2, \quad u_2 \cdot (1 + 3 + 3) \equiv -23 \pmod{1 - \zeta_5}.$$

In fact, $u_1 = \zeta_5^4$ and $u_2 = \zeta_5^2 - \zeta_5 + 1$.

Asymptotic distribution

Fix E and q . As p varies, how does $\mathcal{L}(E, \chi)$ modulo $(1 - \zeta_q)$ vary?

The congruence says $\mathcal{L}(E, \chi)$ varies according to $\#E(\mathbb{F}_p)$ modulo q .

On the other hand, by considering $\rho_{E,q}(\phi_p) \in \mathrm{GL}_2(\mathbb{Z}_q)$,

$$\#E(\mathbb{F}_p) = 1 + \det(\rho_{E,q}(\phi_p)) - \mathrm{tr}(\rho_{E,q}(\phi_p)).$$

As $p \equiv 1 \pmod{q}$ varies, $\rho_{E,q}(\phi_p)$ varies over the group

$$G_{E,q^\infty} := \{M \in \mathrm{im}(\rho_{E,q}) : \det(M) \equiv 1 \pmod{q}\}.$$

By Chebotarev, $\rho_{E,q}(\phi_p)$ is asymptotically distributed uniformly in G_{E,q^∞} .

Thus the asymptotic density of $\#E(\mathbb{F}_p) \equiv \ell \pmod{q}$ is the asymptotic density of matrices $M \in G_{E,q^\infty}$ with $1 + \det(M) - \mathrm{tr}(M) \equiv \ell \pmod{q}$.

Maximal Galois image

For most E , suffices to consider $\overline{\rho_{E,q}} : G_{\mathbb{Q}} \rightarrow \text{Aut}(E[q])$ and

$$G_{E,q} := \{M \in \text{im}(\overline{\rho_{E,q}}) : \det(M) = 1\}.$$

Example

Let E be given by 11a1. Then $c_0(E) = 1$ and $\mathcal{L}(E) = \frac{1}{5} \equiv -1 \pmod{3}$, so

$$\mathcal{L}(E, \chi) \equiv \#E(\mathbb{F}_p) \equiv 2 - \text{tr}(\overline{\rho_{E,3}}(\phi_p)) \pmod{1 - \zeta_3}.$$

Now $\overline{\rho_{E,3}}$ is surjective, so $G_{E,3} = \text{SL}_2(\mathbb{F}_3)$. This consists of:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 2 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 2 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 2 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 2 & 0 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 2 & 0 \end{pmatrix} \\ \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 0 & 2 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 2 & 2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 2 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 2 \\ 0 & 2 \end{pmatrix} \\ \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix} \begin{pmatrix} 2 & 2 \\ 2 & 1 \end{pmatrix}$$

Thus $\mathcal{L}(E, \chi) \equiv 0, 1, 2 \pmod{1 - \zeta_3}$ with densities $\frac{9}{24}, \frac{9}{24}, \frac{6}{24}$.

Small Galois image

For other E , need to consider $\overline{\rho_{E,q^n}} : G_{\mathbb{Q}} \rightarrow \text{Aut}(E[q^n])$ and

$$G_{E,q^n} := \{M \in \text{im}(\overline{\rho_{E,q^n}}) : \det(M) \equiv 1 \pmod{q}\}.$$

Example

Let E be given by 14a1. Then $c_0(E) = 1$ and $\mathcal{L}(E) = \frac{1}{6}$, so

$$\mathcal{L}(E, \chi) \equiv -\frac{1}{6} \cdot \#E(\mathbb{F}_p) \pmod{1 - \zeta_3}.$$

In other words, $\mathcal{L}(E, \chi) \equiv \ell \pmod{1 - \zeta_3}$ precisely if

$$1 + \det(\overline{\rho_{E,9}}(\phi_p)) - \text{tr}(\overline{\rho_{E,9}}(\phi_p)) \equiv -6\ell \pmod{9}.$$

However, $1 + \det(M) - \text{tr}(M) \equiv 0 \pmod{9}$ for all matrices M in

$$G_{E,9} = \{M \in \text{GL}_2(\mathbb{Z}/9\mathbb{Z}) : M \equiv 1 \pmod{3}\}.$$

Thus $\mathcal{L}(E, \chi) \equiv 0, 1, 2 \pmod{1 - \zeta_3}$ with densities 1, 0, 0.

Large Galois image

For some E , the density of $\#E(\mathbb{F}_p)$ might be visible in G_{E,q^n} .

Example

Let E be given by 20a1. Then $c_0(E) = 1$ and $\mathcal{L}(E) = \frac{1}{6}$, so similarly

$$1 + \det(\overline{\rho_{E,9}}(\phi_p)) - \text{tr}(\overline{\rho_{E,9}}(\phi_p)) \equiv -6\ell \pmod{9}$$

precisely if $\mathcal{L}(E, \chi) \equiv \ell \pmod{1 - \zeta_3}$. Now

$$G_{E,9} = \left\{ M \in \text{GL}_2(\mathbb{Z}/9\mathbb{Z}) : M \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{3} \right\}.$$

There are 135, 54, 54 matrices $M \in G_{E,9}$ such that

$$1 + \det(M) - \text{tr}(M) \equiv -6(0), -6(1), -6(2) \pmod{9}.$$

Thus $\mathcal{L}(E, \chi) \equiv 0, 1, 2 \pmod{1 - \zeta_3}$ with densities $\frac{135}{243}, \frac{54}{243}, \frac{54}{243}$.

The density theorem

Define the **natural density**

$$\delta_{E,q}(\ell) := \lim_{n \rightarrow \infty} \frac{\#\{p \in P_n : c_0(E) \cdot \mathcal{L}(E, \chi) \equiv \ell \pmod{1 - \zeta_q}\}}{\#P_n},$$

where P_n is the set of primes $p \equiv 1 \pmod{q}$ less than n .

Theorem (A.)

Let $c := (c_0(E) \cdot \mathcal{L}(E))^{-1}$, and let $n := \nu_q(c) + 1$. If $n \leq 0$, then $\delta_{E,q}(0) = 1$. Otherwise, c is well-defined and non-zero modulo q^n , and

$$\delta_{E,q}(\ell) = \frac{\#\{M \in G_{E,q^n} : 1 + \det(M) - \text{tr}(M) \equiv -c\ell \pmod{q^n}\}}{\#G_{E,q^n}}.$$

In particular, if $\overline{\rho_{E,q}}$ is surjective, then $n = 1$, and

$$\delta_{E,q}(\ell) = \begin{cases} \frac{1}{q-1} & \text{if } \ell \equiv 1 \pmod{q} \\ \frac{q}{q^2-1} & \\ \frac{1}{q+1} & \end{cases} = \left(\frac{c\ell}{q} \right) \left(\frac{c\ell+4}{q} \right).$$

Current status

Paper is in preparation.

- ▶ Stated congruence for non-trivial even Dirichlet characters of arbitrary conductor and order, but with an error term of periods.
- ▶ Classified natural densities for cubic characters, thanks to classification of 3-adic images by Rouse–Sutherland–Zureick-Brown.
- ▶ Explained some distributions for cubic characters in Kisilevsky–Nam, where the normalisation of $\mathcal{L}(E, \chi)$ depends crucially on $\chi(N)$.