L-functions of Dirichlet twists of elliptic curves: computations and congruences

PhD viva examination

David Kurniadi Angdinata

University College London

Monday, 1 December 2025

Notation

Let K be a global field.

For each place $v \in \Upsilon_K$,

- let q_v be the size of its residue field,
- let I_v be its inertia group, and
- let φ_v be a choice of geometric Frobenius.

For a λ-adic representation ρ of K,

- let $\mathfrak{a}(\rho)$ be its global Artin conductor,
- let $\epsilon(\rho)$ be its global epsilon factor, and
- let $W(\rho)$ be its global root number.

Examples of λ-adic representations of K will include

- the ℓ-adic cohomology $\rho_{A,\ell}^{\vee}$ of an abelian variety A,
- the ℓ-adic Tate module $\rho_{E,\ell}$ of an elliptic curve E,
- an Artin representation ϱ, and
- a primitive Dirichlet character χ.

Classical L-functions

The **L-function** of an abelian variety A over K is the complex function

$$L(A, s) := \prod_{v \in \Upsilon_K} \frac{1}{L_v(A, s)},$$

where for each place $v \in \Upsilon_K$, the **local Euler factor** of A is given by

$$L_v(A, s) := \det(1 - (\rho_{A,\ell}^\vee)^{I_v}(\varphi_v) \cdot q_v^{-s}),$$

for some prime $\ell \nmid q_v$.

Conjecture (Birch–Swinnerton-Dyer (BSD))

Assume that $L(A, s)$ has meromorphic continuation at $s = 1$. Then its order of vanishing at $s = 1$ is $\mathrm{rk}(A)$, and its leading term is

$$L^*(A, 1) = \frac{\Omega(A) \cdot \mathrm{Reg}(A) \cdot \# Ш(A) \cdot \mathrm{Tam}(A)}{\mu_K \cdot \# \operatorname{tor}(A) \cdot \# \operatorname{tor}(A^\vee)}.$$

Twisted L-functions

Over a finite Galois extension K' of K, Artin's formalism gives

$$L(A/K', s) = \prod_{\varrho} L(A, \varrho, s),$$

where ϱ runs over Artin representations of K that factor through K' and $L(A, \varrho, s)$ are certain **twisted L-functions** of A.

One may ask a variety of theoretical and computational questions.

- Are there algebraic or integral versions of $L^*(A, \varrho, 1)$?
- Can $L^*(A, \varrho, 1)$ be expressed in terms of BSD invariants?
- Does $L^*(A, \varrho, 1)$ have a predictable asymptotic distribution?
- Can $L^*(A, \varrho, 1)$ be computed numerically or algorithmically?
- Is $L^*(A, \varrho, 1)$ directly related to $L^*(A, 1)$?

I provide partial answers when $A = E$ is an elliptic curve and $\varrho = \chi$ is a primitive Dirichlet character over the global fields $K = \mathbb{Q}$ and $K = \mathbb{F}_q(t)$.

Algebraic L-values

When $K = \mathbb{Q}$, the **algebraic L-value** of A twisted by ϱ is defined by

$$\mathscr{L}(A, \varrho) := \frac{L^*(A, \varrho, 1) \cdot \sqrt{\mathfrak{a}(\varrho)}^{\dim(A)}}{W(\varrho)^{\dim(A)} \cdot \Omega_+(A)^{\dim(\varrho^{\varsigma=+})} \cdot \Omega_-(A)^{\dim(\varrho^{\varsigma=-})}},$$

where ς is a lift of complex conjugation in $G_{\mathbb{Q}}$, and denote

$$\mathscr{L}(A) := \mathscr{L}(A, 1).$$

If $A = E$ and $\varrho = \chi$, then

$$\mathscr{L}(E, \chi) = \frac{L^*(E, \chi, 1) \cdot \mathfrak{a}(\chi)}{\mathfrak{g}(\chi) \cdot \Omega_{\chi(-1)}(E)},$$

where $\mathfrak{g}(\chi)$ is the Gauss sum of χ, and

$$\mathscr{L}(E) = \frac{L^*(E, 1)}{\Omega(E)}.$$

Formal L-functions

When $K = \mathbb{F}_q(C)$, rationality gives

$$L(A, \varrho, s) = \frac{P_1(\rho_{A,\ell}^\vee \otimes \varrho, q^{-s})}{P_0(\rho_{A,\ell}^\vee \otimes \varrho, q^{-s}) \cdot P_2(\rho_{A,\ell}^\vee \otimes \varrho, q^{-s})},$$

where there are canonical $\overline{\mathbb{Q}_\ell}$-representations $H^n(\rho)$ such that

$$P_n(\rho, T) := \det(1 - T \cdot H^n(\rho)(\varphi_q)) \in \overline{\mathbb{Q}}[T].$$

Define the **formal L-function** of A twisted by ϱ by

$$\mathcal{L}(A, \varrho, T) := \frac{P_1(\rho_{A,\ell}^\vee \otimes \varrho, T)}{P_0(\rho_{A,\ell}^\vee \otimes \varrho, T) \cdot P_2(\rho_{A,\ell}^\vee \otimes \varrho, T)},$$

so that $L(A, \varrho, s) = \mathcal{L}(A, \varrho, q^{-s})$, and denote

$$\mathcal{L}(A, T) := \mathcal{L}(A, 1, T).$$

Algebraicity of L-functions

Assuming an appropriate automorphic correspondence for E over $\mathbb{Q}^{\chi}$, a local argument shows that $\mathscr{L}(E,\varrho)$ is the algebraic version of $L^*(E,\varrho,1)$.

Theorem (Theorem 4.2 of Bouganis–Dokchitser 2007)

Let $K=\mathbb{Q}$. *If* $(\mathfrak{a}(E),\mathfrak{a}(\chi))=1$, *then*

- $\mathscr{L}(E,\chi)\in\mathbb{Q}(\chi)$, *and*
- $\mathscr{L}(E,\chi)^{\varsigma}=\mathscr{L}(E,\varsigma\circ\chi)$ *for all* $\varsigma\in G_{\mathbb{Q}}$.

They deduced this from the corresponding result for Rankin–Selberg convolutions of certain parallel weight primitive Hilbert modular forms.

A similar local argument works for $\mathcal{L}(E,\chi,T)$ without assumptions.

Theorem (Theorem 5.7 of thesis)

Let $K=\mathbb{F}_q(C)$. *Then*

- $\mathcal{L}(E,\chi,T)\in\mathbb{Q}(\chi)(T)$, *and*
- $\mathcal{L}(E,\chi,T)^{\varsigma}=\mathcal{L}(E,\varsigma\circ\chi,T)$ *for all* $\varsigma\in G_{\mathbb{Q}}$.

Integrality of L-functions

Under assumptions on the Manin constant $\mathfrak{c}_0(E)$, Wiersema–Wuthrich 2022 proved that $\mathscr{L}(E, \chi)$ is integral in many cases, by formally manipulating its expression as period sums of modular symbols.

Theorem (Proposition 3.8 of thesis)

Let $K = \mathbb{Q}$. If χ has prime order $\ell \nmid \mathfrak{c}_0(E)$ and $(\mathfrak{a}(E), \mathfrak{a}(\chi)) = 1$, then

- $\mathscr{L}(E, \chi) \in \mathbb{Z}_\ell[\zeta_\ell]$, *and*
- $\mathscr{L}(E) \cdot \#E(\mathbb{F}_v) \in \mathbb{Z}_\ell$ *for any odd prime $v \nmid \mathfrak{a}(E)$.*

A similar result holds for $\mathcal{L}(E, \chi, T)$ when E and χ are generic.

Theorem (Proposition 5.10 of thesis)

Let $K = \mathbb{F}_q(C)$. If χ is separable geometric and $(\mathfrak{a}(E), \mathfrak{a}(\chi)) = 1$, then

- $\mathcal{L}(E, \chi, T) \in \mathbb{Q}(\chi)[T]$, *and*
- $\mathcal{L}(E, T) \in \mathbb{Q}[T]$ *if E is non-constant.*

Congruences of L-functions

When χ has prime order ℓ, a bit of further work gives a congruence with $\mathscr{L}(E)$ or $\mathcal{L}(E, T)$ modulo the prime $(1 - \zeta_\ell)$ of $\mathbb{Z}[\zeta_\ell]$ above ℓ.

Theorem (Corollary 3.9 of thesis)

Let $K = \mathbb{Q}$. If $\ell \nmid \mathfrak{c}_0(E) \cdot \mathfrak{a}(\chi)$ and $(\mathfrak{a}(E), \mathfrak{a}(\chi)) = 1$, then

$$\mathscr{L}(E, \chi) \equiv \mathscr{L}(E) \cdot \prod_{v \mid \mathfrak{a}(\chi)} (-L_v(E, 1)) \mod (1 - \zeta_\ell).$$

Theorem (Theorem 5.12 of thesis)

Let $K = \mathbb{F}_q(t)$. If E is non-constant and χ is separable geometric, and furthermore $(\mathfrak{a}(E), \mathfrak{a}(\chi)) = 1$, then

$$\mathcal{L}(E, \chi, T) \equiv \mathcal{L}(E, T) \cdot \prod_{v \mid \mathfrak{a}(\chi)} \mathcal{L}_v(E, T) \mod (1 - \zeta_\ell).$$

Ideals of L-values

The ideal of $\mathbb{Z}[\chi]$ generated by $\mathscr{L}(E,\chi)$ and $\mathcal{L}(E,\chi,q^{-1})$ can be expressed in terms of χ-isotypic components of $\mathrm{Reg}(E)$ and $Ш(E)$.

Theorem (Proposition 7.3 of Burns–Castillo 2024)

Let $K=\mathbb{Q}$. Assume that the refined BSD conjecture holds over K^χ/K. If $(\mathfrak{a}(E),\mathfrak{a}(\chi))=1$, then there is an explicit finite set $S(E,\chi)\subseteq\Upsilon_{\mathbb{Q}(\chi)}$ such that for all $\lambda\in\Upsilon_{\mathbb{Q}(\chi)}\setminus S(E,\chi)$,

$$\mathscr{L}(E,\chi)\cdot\prod_{v|\mathfrak{a}(\chi)}L_v(E,\chi,1)\cdot\mathbb{Z}[\chi]_\lambda=\mathrm{Reg}(E,\chi)\cdot\mathrm{char}(Ш(E,\chi)).$$

Theorem (Theorem 7.12 of Kim–Tan–Trihan–Tsoi 2024)

Let $K=\mathbb{F}_q(C)$. Assume that $Ш(E/K^\chi)$ is finite. Then there is an explicit finite set $S(E,\chi)\subseteq\Upsilon_{\mathbb{Q}(\chi)}$ such that for all $\lambda\in\Upsilon_{\mathbb{Q}(\chi)}\setminus S(E,\chi)$,

$$\mathcal{L}(E,\chi,q^{-1})\cdot\prod_{v|\mathfrak{a}(\chi)}L_v(E,\chi,1)\cdot\mathbb{Z}[\chi]_\lambda=\mathrm{Reg}_\lambda(E,\chi)\cdot\mathrm{char}(Ш_\lambda(E,\chi)).$$

Norms of L-values

When $K = \mathbb{Q}$, Dokchitser–Evans–Wiersema 2021 computed the norm of $\mathscr{L}(E, \chi)$ in terms of $\mathrm{BSD}(E)$ and $\mathrm{BSD}(E/\mathbb{Q}^\chi)$, which are invariants such that the BSD conjecture over $\mathbb{Q}$ and over $\mathbb{Q}^\chi$ respectively read

$$\mathscr{L}(E) = \mathrm{BSD}(E), \qquad \mathscr{L}(E/\mathbb{Q}^\chi) = \mathrm{BSD}(E/\mathbb{Q}^\chi).$$

Theorem (Proposition 3.13 of thesis)

Let $K = \mathbb{Q}$. Assume the Manin constant conjecture $\mathfrak{c}_1(E) = 1$ and the BSD conjecture hold over $\mathbb{Q}$ and over $\mathbb{Q}^\chi$. If $L(E, 1), L(E, \chi, 1) \neq 0$, χ has prime order ℓ, and $(\mathfrak{a}(E), \mathfrak{a}(\chi)) = 1$, then

$$\mathrm{Nm}_{\mathbb{Q}}^{\mathbb{Q}(\zeta_\ell)^+}(\mathscr{L}(E, \chi) \cdot \chi(\mathfrak{a}(E))^{(\ell-1)/2}) = \sqrt{\mathrm{BSD}(E/\mathbb{Q}^\chi)/\,\mathrm{BSD}(E)}.$$

There is an ongoing project led by Maistret and Wiersema as part of Women In Numbers Europe 2025 for the $K = \mathbb{F}_q(C)$ analogue.

Predicting algebraic L-values

Dokchitser–Evans–Wiersema 2021 also gave examples of arithmetically identical elliptic curves E_1 and E_2 such that $\mathscr{L}(E_1, \chi) \neq \mathscr{L}(E_2, \chi)$.

When $\ell = 3$, this difference can be explained by the congruence.

Theorem (Corollary 3.14 of thesis)

Let $K = \mathbb{Q}$. Assume the Manin constant conjecture $\mathfrak{c}_1(E) = 1$ and the BSD conjecture hold over $\mathbb{Q}$ and over $\mathbb{Q}^{\chi}$. If $L(E, 1), L(E, \chi, 1) \neq 0$, χ is cubic, and $(\mathfrak{a}(E), \mathfrak{a}(\chi)) = 1$, then

$$\mathscr{L}(E, \chi) = u \cdot \overline{\chi}(\mathfrak{a}(E)) \cdot \sqrt{\mathrm{BSD}(E/\mathbb{Q}^{\chi}) / \mathrm{BSD}(E)},$$

where $u \in \{\pm 1\}$ is such that

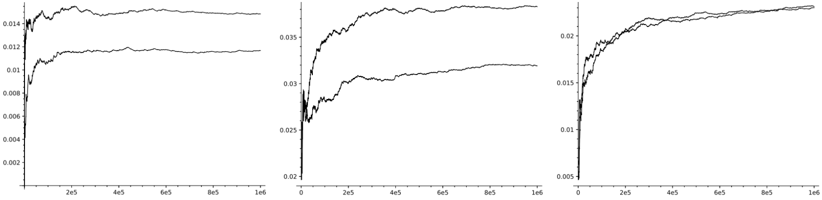
$$u \equiv \frac{\mathrm{BSD}(E) \cdot \prod_{v \mid \mathfrak{a}(\chi)} (-\# E(\mathbb{F}_v))}{\sqrt{\mathrm{BSD}(E/\mathbb{Q}^{\chi}) / \mathrm{BSD}(E)}} \mod 3.$$

Biases of algebraic L-values

Kisilevsky–Nam 2025 observed biases in the distribution of

$$\widetilde{\mathscr{L}}^{+}(E,\chi) := \frac{\mathrm{Nm}_{\mathbb{Q}}^{\mathbb{Q}(\zeta_\ell)^+}\left(\mathscr{L}(E,\chi)\cdot(1+\overline{\chi}(\mathfrak{a}(E)))\right)}{\gcd\left\{\mathrm{Nm}_{\mathbb{Q}}^{\mathbb{Q}(\zeta_\ell)^+}\left(\mathscr{L}(E,\chi)\cdot(1+\overline{\chi}(\mathfrak{a}(E)))\right) : \chi \in \mathcal{X}_\ell^{<N}\right\}},$$

as χ varies over the set $\mathcal{X}_\ell^{<N}$ of primitive Dirichlet characters of $\mathbb{Q}$ of odd prime order $\ell \nmid \mathfrak{c}_0(E)$ and prime $\mathfrak{a}(\chi) < N$ with $N \to \infty$.



(g) $|l| = 7$: Top -7 bottom 7 (h) $|l| = 8$: Top 8 bottom -8 (i) $|l| = 9$: Top -9 bottom 9

FIGURE 50. 11a1: $(\alpha,\beta) = (1,3)$ Ratio (7.11) $x_{6,E}^{(\alpha,\beta)}(X;l)/X^{1/2}\log^2(X)$

Predicting residual L-densities

This distribution can be quantified by computing the **residual L-density** of E modulo an odd prime $\ell \nmid \mathfrak{c}_0(E)$ defined by

$$\mathfrak{d}_{E,\ell}(n) := \lim_{N\to\infty} \frac{\#\{\chi \in \mathcal{X}_\ell^{<N} : \mathscr{L}(E,\chi) \equiv n \mod (1-\zeta_\ell)\}}{\#\mathcal{X}_\ell^{<N}}.$$

Chebotarev's density theorem reduces this to computations in $\mathrm{im}(\rho_{E,\ell})$.

Theorem (Theorem 4.11 of thesis)

Let $K = \mathbb{Q}$. Assume that the BSD conjecture holds over $\mathbb{Q}$. If $L(E,1) \neq 0$, then $\mathfrak{d}_{E,\ell}$ only depends on $\mathrm{ord}_\ell(\mathrm{BSD}(E))$ and on $\mathrm{im}(\overline{\rho}_{E,\ell^2})$.

A similar argument recovers the distribution of Kisilevsky–Nam 2025.

Theorem (Proposition 4.19 of thesis)

Let $K = \mathbb{Q}$. If E has Cremona label 11a1, 15a1, or 17a1, and χ is cubic, then the distribution of $\widetilde{\mathscr{L}}^+(E,\chi)$ can be predicted precisely.

Bounding denominators of L-values

Lorenzini 2011 described the cancellations between $\mathrm{tor}(E)$ and $\mathrm{Tam}(E)$.

Theorem (Proposition 4.5 of thesis)

Let $K = \mathbb{Q}$. If $\ell \nmid 3 \cdot \mathfrak{c}_0(E)$ is an odd prime, then

$$\mathrm{ord}_\ell(\#\,\mathrm{tor}(E)) \leq \mathrm{ord}_\ell(\mathrm{Tam}(E)).$$

The $\ell = 3$ analogue can be deduced from the integrality of $\mathscr{L}(E)$ and the classification of $\mathrm{im}(\rho_{E,3})$ by Rouse–Sutherland–Zureick-Brown 2022.

Theorem (Theorem 4.9 of thesis)

Let $K = \mathbb{Q}$. Assume that the BSD conjecture holds over $\mathbb{Q}$. If $L(E,1) \neq 0$ and $\ell \nmid \mathfrak{c}_0(E)$, then

$$\mathrm{ord}_\ell(\mathscr{L}(E)) = \mathrm{ord}_\ell(\mathrm{BSD}(E)) \geq -1.$$

There is an ongoing project by Melistas and I for the $K = \mathbb{F}_q(t)$ analogue.

Computations of L-values

Much of the previous explorations were only possible thanks to efficient algorithms to compute $\mathscr{L}(E,\chi)$ in computer algebra systems.

Algorithm (Dokchitser 2004)

Computes $L(M,0)$ where M is a motive over a number field.

There are almost no public implementations for global function fields.

Algorithm (Comeau-Lapointe–David–Lalín–Li 2022)

Computes $\mathcal{L}(E,\chi,T)$ where E and χ are defined over $\mathbb{F}_q(t)$.

The proof of the Weil conjectures gives an algorithm for general λ-adic representations, which is used by Maistret and Wiersema in their project.

Algorithm (Algorithm 5.15 of thesis)

Computes $\mathcal{L}(\rho,T)$ where ρ is an almost everywhere unramified λ-adic representation of $\mathbb{F}_q(C)$ (that is pure of weight w and $\rho^\vee \cong \rho^\varsigma \otimes \overline{\mathbb{Q}}(w)$).

Computing formal L-functions

Let ρ be an almost everywhere unramified λ-adic representation of $\mathbb{F}_q(C)$.

Theorem (Proposition 5.13 of thesis)

If $\rho^{G_{\overline{\mathbb{F}_q}(C)}} = 0$, then $\mathcal{L}(\rho, T)$ is a polynomial of degree

$$d := \deg \mathfrak{a}(\rho) + (2g(C) - 2) \dim \rho,$$

where $g(C)$ is the genus of C. Furthermore, if ρ is pure of weight w and $\rho^\vee \cong \rho^\varsigma \otimes \overline{\mathbb{Q}}(w)$, then the functional equation gives $\epsilon(\rho) \in \mathbb{C}^\times$ such that

$$\mathcal{L}(\rho, T) = \epsilon(\rho) \cdot T^d \cdot \mathcal{L}(\rho, (q^{w+1} T)^{-1})^\varsigma.$$

In particular, if $\{c_n\}_{n \in \mathbb{N}}$ denotes the coefficients of $\mathcal{L}(\rho, T)$, then

$$c_n = \begin{cases} 1 & \text{if } n = 1, \\ q^{(w+1)(n-d)} \cdot \epsilon(\rho) \cdot c_{d-n}^\varsigma & \text{if } 0 < n < d, \\ \epsilon(\rho) & \text{if } n = d, \\ 0 & \text{otherwise.} \end{cases}$$

Computing twisted L-functions

There is a refinement of the algorithm for tensor products $\rho \otimes \sigma$.

Theorem (Theorem 2.7 of thesis)

Under the previous assumptions, if $(\mathfrak{a}(\rho), \mathfrak{a}(\sigma)) = 1$*, then*

$$\epsilon(\rho \otimes \sigma) = \frac{\epsilon(\rho)^{\dim \sigma} \cdot \epsilon(\sigma)^{\dim \rho} \cdot \det \sigma(\mathfrak{a}(\rho)) \cdot \det \rho(\mathfrak{a}(\sigma))}{q^{(g(C)-1) \dim \rho \dim \sigma}}.$$

The remainder of the thesis provides explicit examples of $\mathcal{L}(\rho \otimes \sigma, T)$ when ρ and σ arise from elliptic curves or Dirichlet characters.

In particular, the examples use an alternative implementation of Dirichlet characters of $\mathbb{F}_q(t)$ that is more amenable to computation.

Theorem (Theorem 6.6 of thesis)

Let $K = \mathbb{F}_q(t)$*. Then there is a canonical representation of any* $u \in (\mathbb{F}_q[t]/m)^\times$ *that allows for an efficient computation of* $\chi(u)$*.*