L-values of elliptic curves twisted by cubic characters

David Ang

Wednesday, 24 April 2024

1 Motivational background

Let E be an elliptic curve over $\mathbb{Q}$. Associated to E is its Hasse-Weil L-function

$$\mathrm{L}(E,s) \coloneqq \prod_p \frac{1}{\det\bigl(1 - p^{-s} \cdot \mathrm{Fr}_p^{-1} \mid \bigl(\rho_{E,q}^\vee\bigr)^p\bigr)},$$

where Fr_p is an arithmetic Frobenius at a prime p, and $\rho_{E,q}$ is the q-adic representation associated to the q-adic Tate module of E for any prime $q \ne p$. The algebraic and analytic properties of these L-functions are studied extensively in the literature, and they are the subject of many problems in the arithmetic of elliptic curves. Most notably, the Birch–Swinnerton-Dyer conjecture says that the order of vanishing r of $\mathrm{L}(E,s)$ at $s = 1$ is precisely the Mordell-Weil rank $\mathrm{rk}(E)$, and its leading term is given by

$$\lim_{s\to 1} \frac{\mathrm{L}(E,s)}{(s-1)^r} \cdot \frac{1}{\Omega(E)} = \frac{\mathrm{Tam}(E) \cdot \#\text{Ш}(E) \cdot \mathrm{Reg}(E)}{\#\mathrm{tor}(E)^2},$$

where $\Omega(E)$ denotes the real period, $\mathrm{Tam}(E)$ denotes the Tamagawa number, $\text{Ш}(E)$ denotes the Tate–Shafarevich group, $\mathrm{Reg}(E)$ denotes the elliptic regulator, and $\mathrm{tor}(E)$ denotes the torsion subgroup. As Tate once said, this remarkable conjecture relates the behaviour of a function $\mathrm{L}(E,s)$ at a point where it is not at present known to be defined, to the order of a group $\text{Ш}(E)$ which is not known to be finite. Since then, the modularity theorem of Taylor–Wiles shows that $\mathrm{L}(E,s)$ admits analytic continuation to the entire complex plane, and $\text{Ш}(E)$ is now known to be finite for $r \le 1$ thanks to the works of Gross–Zagier and Kolyvagin. For the sake of convenience, call the left hand side the algebraic L-value of E, denoting it by $\mathcal{L}(E)$, and call the right hand side the Birch–Swinnerton-Dyer quotient of E, denoting it by $\mathrm{BSD}(E)$.

When E is base changed to a finite Galois extension K of $\mathbb{Q}$, analogous quantities $\mathrm{L}(E/K,s)$, $\mathrm{rk}(E/K)$, $\Omega(E/K)$, $\mathrm{Tam}(E/K)$, $\text{Ш}(E/K)$, $\mathrm{Reg}(E/K)$, and $\mathrm{tor}(E/K)$ can be defined to formulate a generalisation of the conjecture over K. However, the modularity theorem has yet to be extended to elliptic curves beyond specific number fields, so the conjectural equality remains ill-defined in general. On the other hand, Artin's formalism for L-functions says that $\mathrm{L}(E/K,s)$ decomposes into a product of twisted L-functions

$$\mathrm{L}(E,\rho,s) \coloneqq \prod_p \frac{1}{\det\bigl(1 - p^{-s} \cdot \mathrm{Fr}_p^{-1} \mid \bigl(\rho_{E,q}^\vee \otimes \rho^\vee\bigr)^p\bigr)},$$

over all irreducible Artin representations ρ that factor through K, so the behaviour of $\mathrm{L}(E/K,s)$ is completely governed by $\mathrm{L}(E,\rho,s)$. These twisted L-functions can in turn be analytically continued to the entire complex plane by expressing them as Rankin-Selberg convolutions of $\mathrm{L}(E,s)$, so the validity of the conjecture can be asked at the level of twisted L-functions. For instance, the Deligne–Gross conjecture states that the order of vanishing of $\mathrm{L}(E,\rho,s)$ at $s = 1$ is precisely the multiplicity of ρ in the Artin representation associated to $E(K)$. Analogous to the classical leading term conjecture that $\mathcal{L}(E) = \mathrm{BSD}(E)$, the twisted leading term conjecture would be a statement about a twisted algebraic L-value $\mathcal{L}(E,\rho)$ of E. For the sake of simplicity, when K is a cyclotomic extension of $\mathbb{Q}$, the corresponding twisted algebraic L-value is given by

$$\mathcal{L}(E,\chi) \coloneqq \lim_{s\to 1} \frac{\mathrm{L}(E,\chi,s)}{(s-1)^r} \cdot \frac{p}{\tau(\chi)\,\Omega(E)},$$

where $\tau(\chi)$ is the Gauss sum of the primitive Dirichlet character χ associated to K. When E is semistable Γ_0-optimal of conductor N and χ has prime conductor $p \nmid N$ and order $q > 1$, it is known that $\mathcal{L}(E,\chi) \in \mathbb{Z}[\zeta_q]$.

2 Known results

Unfortunately, there seems to be a barrier to formulating a twisted leading term conjecture for $\mathcal{L}(E,\chi)$, even assuming classical leading term conjectures over general number fields. Dokchitser–Evans–Wiersema gave many explicit pairs of examples of elliptic curves E_1 and E_2 over $\mathbb{Q}$, with $\mathcal{L}(E_1,\chi) \neq \mathcal{L}(E_2,\chi)$ for some fixed Dirichlet character χ, but are arithmetically identical over the number field K cut out by χ.

Example (DEW21, Example 45)**.** Let E_1 and E_2 be the elliptic curves given by the Cremona labels 1356d1 and 1356f1 respectively, and let χ be the cubic character of conductor 7 such that $\chi(3) = \zeta_3^2$. Then $\mathrm{BSD}(E_i) = \mathrm{BSD}\big(E_i/K\big) = 1$ for $i = 1,2$, but $\mathcal{L}(E_1,\chi) = \zeta_3^2$ and $\mathcal{L}(E_2,\chi) = -\zeta_3^2$.

This phenomenon can be partially explained with the assumption of standard arithmetic conjectures. For instance, under Stevens's Manin constant conjecture and the leading term conjectures over $\mathbb{Q}$ and over K, Dokchitser–Evans–Wiersema expressed the norm of $\mathcal{L}(E,\chi)$ in terms of Birch–Swinnerton-Dyer quotients.

Theorem (DEW21, Theorem 38)**.** *Let E be a semistable Γ_0-optimal elliptic curve over $\mathbb{Q}$ of conductor N, let χ be a primitive Dirichlet character of odd prime conductor $p \nmid N$ and odd prime order $q \nmid \mathrm{BSD}(E)\,\#E\big(\mathbb{F}_p\big)$, and let $\zeta \coloneqq \chi(N)^{(q-1)/2}$. Then $\mathcal{L}(E,\chi)\cdot\zeta \in \mathbb{Z}[\zeta_q]^+$, and has norm*

$$\mathrm{Nm}_{\mathbb{Q}}^{\mathbb{Q}(\zeta_q)^+}\big(\mathcal{L}(E,\chi)\cdot\zeta\big) = \sqrt{\frac{\mathrm{BSD}(E/K)}{\mathrm{BSD}(E)}}.$$

In particular, if $\mathrm{BSD}(E) = \mathrm{BSD}(E/K)$, then there is a unit $u \in \mathbb{Z}[\zeta_q]^+$ such that $\mathcal{L}(E,\chi) = u\cdot\zeta^{-1}$.

In the relevant case of $\mathrm{BSD}(E) = \mathrm{BSD}(E/K)$, this predicts the ideal of $\mathbb{Q}(\zeta_q)^+$ generated by $\mathcal{L}(E,\chi)$, but not the precise value of $\mathcal{L}(E,\chi)$. Note that in general, the exact prime ideal factorisation of $\mathcal{L}(E,\chi)$ can be recovered from the $\mathrm{Gal}(K/\mathbb{Q})$-module structure of $\text{Ш}(E/K)$ under stronger Iwasawa-theoretic assumptions.

From a purely analytic perspective, a natural problem is to determine the asymptotic distribution of $\mathcal{L}(E,\chi)$ as χ varies over primitive Dirichlet characters of some fixed prime order q but arbitrarily high prime conductor $p \nmid N$, for some fixed elliptic curve E of conductor N. However, for each such p, there are $q-1$ primitive Dirichlet characters χ of conductor p and order q, giving rise to $q-1$ conjugates of $\mathcal{L}(E,\chi)$, so a uniform choice of χ for each p has to be made for any meaningful analysis. One solution is to observe that the residue class of $\mathcal{L}(E,\chi)$ modulo $\langle 1-\zeta_q\rangle$ is independent of the choice of χ, so a simpler problem would be to determine the asymptotic distribution of these residue classes instead. Let $X_{E,q}^{<n}$ be the set of equivalence classes of primitive Dirichlet characters of odd order q and odd prime conductor $p \nmid N$ less than n, where two primitive Dirichlet characters in $X_{E,q}^{<n}$ are equivalent if they have the same conductor. Define the residual densities $\delta_{E,q}$ of $\mathcal{L}(E,\chi)$ to be the natural densities of $\mathcal{L}(E,\chi)$ modulo $\langle 1-\zeta_q\rangle$, namely

$$\delta_{E,q}(\lambda) \coloneqq \lim_{n\to\infty} \frac{\#\Big\{\chi \in X_{E,q}^{<n} \;\Big|\; \mathcal{L}(E,\chi) \equiv \lambda \mod \langle 1-\zeta_q\rangle\Big\}}{\#X_{E,q}^{<n}}, \qquad \lambda \in \mathbb{F}_q,$$

if such a limit exists. Fixing six elliptic curves E and five small orders q, Kisilevsky–Nam numerically computed $\delta_{E,q}$ by varying χ over millions of conductors p, and observed inherent biases.

Example (KN22, Section 7)**.** Let E be the elliptic curve given by the Cremona label 11a1. Then

$$\delta_{E,3}(0) \approx \tfrac{3}{8}, \qquad \delta_{E,3}(1) \approx \tfrac{3}{8}, \qquad \delta_{E,3}(2) \approx \tfrac{1}{4}.$$

Note that their actual computational results seemingly give

$$\delta_{E,3}(0) \approx \tfrac{9}{24}, \qquad \delta_{E,3}(1) \approx \tfrac{15}{24}, \qquad \delta_{E,3}(2) \approx \tfrac{1}{24},$$

but this is simply due to a difference in normalisation. Instead of considering the residual density of $\mathcal{L}(E,\chi)$, they computed that of the norms of $\mathcal{L}^+(E,\chi)\,/\,\mathrm{gcd}_{E,q}$, where

$$\mathcal{L}^+(E,\chi) \coloneqq \begin{cases} \mathcal{L}(E,\chi) & \text{if } \chi(N) = 1 \\ \mathcal{L}(E,\chi)\cdot\Big(1+\overline{\chi(N)}\Big) & \text{if } \chi(N) \neq 1 \end{cases},$$

and $\mathrm{gcd}_{E,q}$ is the greatest common divisor of these norms as χ varies, which is determined empirically.

3 New results

I refined the result of Dokchitser–Evans–Wiersema by predicting the precise value of $\mathcal{L}(E,\chi)$ in terms of an abstract generator of the ideal of $\mathbb{Q}(\zeta_q)^+$ generated by $\mathcal{L}(E,\chi)$. When χ is cubic, this can be made explicit.

Theorem (Ang24, Corollary 5.2). *Let E be a semistable Γ_0-optimal elliptic curve over $\mathbb{Q}$ of conductor N, and let χ be a cubic primitive Dirichlet character of odd prime conductor $p \nmid N$ such that $3 \nmid \mathrm{BSD}(E)\,\#E(\mathbb{F}_p)$. Then*

$$\mathcal{L}(E,\chi) = u \cdot \overline{\chi(N)} \sqrt{\frac{\mathrm{BSD}(E/K)}{\mathrm{BSD}(E)}},$$

for some sign $u = \pm 1$, chosen such that

$$u \equiv -\#E(\mathbb{F}_p) \sqrt{\frac{\mathrm{BSD}(E)^3}{\mathrm{BSD}(E/K)}} \mod 3.$$

This clarifies the original example given by Dokchitser–Evans–Wiersema, as well as all of their other cubic examples, in the sense that $\mathcal{L}(E_1,\chi) \neq \mathcal{L}(E_2,\chi)$ precisely because $\#E_1(\mathbb{F}_p) \not\equiv \#E_2(\mathbb{F}_p) \mod 3$.

Example (Ang24, Example 5.3). Let E_1 and E_2 be the elliptic curves given by the Cremona labels 1356d1 and 1356f1 respectively, and let χ be the cubic character of conductor 7 such that $\chi(3) = \zeta_3^2$. Then $\mathcal{L}(E_i,\chi) = u \cdot \zeta_3^2$ for $u \equiv -\#E_i(\mathbb{F}_7) \mod 3$ for $i = 1, 2$, and indeed $\#E_1(\mathbb{F}_7) = 11$ and $\#E_2(\mathbb{F}_7) = 7$.

When χ has order $q > 3$, the same proof only yields a congruence on the unit $u \in \mathbb{Z}[\zeta_q]^+$ modulo q, since the group of units of $\mathbb{Z}[\zeta_q]^+$ is infinite. This does clarify all of the quintic examples given by Dokchitser–Evans–Wiersema with $\mathrm{BSD}(E) = \mathrm{BSD}(E/K)$, in the sense that $\mathcal{L}(E_1,\chi) \neq \mathcal{L}(E_2,\chi)$ precisely because $\#E_1(\mathbb{F}_p) \not\equiv \#E_2(\mathbb{F}_p) \mod 5$. Unfortunately, enforcing the congruence on $\#E(\mathbb{F}_p)$ modulo q remains insufficient to determine the precise value of $\mathcal{L}(E,\chi)$, as the following rare example shows.

Example (Ang24, Remark 5.7). Let E_1 and E_2 be the the elliptic curves given by the Cremona labels 544b1 and 544f1 respectively, and let χ be the quintic character of conductor 11 such that $\chi(2) = \zeta_5$. Then $\mathrm{BSD}(E_i) = \mathrm{BSD}(E_i/K) = 1$, but $\mathcal{L}(E_1,\chi) = -\zeta_5^3 - \zeta_5$ and $\mathcal{L}(E_2,\chi) = -2\zeta_5^3 - 3\zeta_5^2 - 2\zeta_5$.

I also classified the possible residual densities of $\mathcal{L}(E,\chi)$ in terms of the mod-q^m representations $\overline{\rho_{E,q^m}}$.

Theorem (Ang24, Proposition 6.1). *Let E be a semistable Γ_0-optimal elliptic curve over $\mathbb{Q}$ such that $\mathrm{L}(E,1) \neq 0$, and let q be an odd prime. If $\mathrm{ord}_q(\mathrm{BSD}(E)) > 0$, then $\delta_{E,q}(0) = 1$ and $\delta_{E,q}(\lambda) = 0$ for any $\lambda \in \mathbb{F}_q^\times$. Otherwise, for any $\lambda \in \mathbb{F}_q$,*

$$\delta_{E,q}(\lambda) = \frac{\#\left\{M \in G_{E,q^m} \;\middle|\; 1 + \det(M) - \mathrm{tr}(M) \equiv -\lambda \mathrm{BSD}(E)^{-1} \mod q^m\right\}}{\#G_{E,q^m}},$$

where $m \coloneqq 1 - \mathrm{ord}_q(\mathrm{BSD}(E))$ and $G_{E,q^m} \coloneqq \left\{M \in \mathrm{im}\overline{\rho_{E,q^m}} \;\middle|\; \det(M) \equiv 1 \mod q\right\}$, and furthermore if $\overline{\rho_{E,q}}$ is surjective, then for any $\lambda \in \mathbb{F}_q$,

$$\delta_{E,q}(\lambda) = \begin{cases} \frac{1}{q-1} & \text{if } \lambda_{E,q} = 1 \\ \frac{q}{q^2-1} & \text{if } \lambda_{E,q} = 0 \\ \frac{1}{q+1} & \text{if } \lambda_{E,q} = -1 \end{cases}, \qquad \lambda_{E,q} \coloneqq \left(\frac{\lambda \mathrm{BSD}(E)^{-1}}{q}\right)\left(\frac{\lambda \mathrm{BSD}(E)^{-1} + 4}{q}\right).$$

When χ is cubic, this can be made very explicit.

Theorem (Ang24, Theorem 6.4). *Let E be a semistable Γ_0-optimal elliptic curve over $\mathbb{Q}$ such that $\mathrm{L}(E,1) \neq 0$. Then there is an explicit algorithm to determine the ordered triple $(\delta_{E,3}(0), \delta_{E,3}(1), \delta_{E,3}(2))$ in terms of only $\mathrm{BSD}(E)$ and $\mathrm{im}\overline{\rho_{E,9}}$. In particular, they can only be one of*

$$(1,0,0)\,,\ \left(\tfrac{3}{8},\tfrac{3}{8},\tfrac{1}{4}\right),\ \left(\tfrac{3}{8},\tfrac{1}{4},\tfrac{3}{8}\right),\ \left(\tfrac{1}{2},\tfrac{1}{2},0\right),\ \left(\tfrac{1}{2},0,\tfrac{1}{2}\right),\ \left(\tfrac{1}{8},\tfrac{3}{4},\tfrac{1}{8}\right),$$

$$\left(\tfrac{1}{8},\tfrac{1}{8},\tfrac{3}{4}\right),\ \left(\tfrac{1}{4},\tfrac{1}{2},\tfrac{1}{4}\right),\ \left(\tfrac{1}{4},\tfrac{1}{4},\tfrac{1}{2}\right),\ \left(\tfrac{5}{9},\tfrac{2}{9},\tfrac{2}{9}\right),\ \left(\tfrac{1}{3},\tfrac{2}{3},0\right),\ \left(\tfrac{1}{3},0,\tfrac{2}{3}\right).$$

This algorithm is in the form of two tables and will be omitted for brevity, but ultimately does recover the predicted residual densities in the six examples of Kisilevsky–Nam.

4 Proof ingredients

The proofs of all of these results crucially rely on the following fundamental congruence.

Theorem (Ang24, Corollary 3.7)**.** *Let E be a semistable Γ_0-optimal elliptic curve of conductor N, and let χ be a primitive Dirichlet character of odd prime conductor $p \nmid N$ and order $q > 1$. Then*

$$\mathcal{L}(E,\chi) \equiv -\mathcal{L}(E)\,\#E(\mathbb{F}_p) \mod \langle 1-\zeta_q \rangle .$$

This is a consequence of writing $\mathrm{L}(E,1)$ and $\mathrm{L}(E,\chi,1)$ as sums of modular symbols

$$\mu_E(q) \coloneqq \int_0^q 2\pi i f(z)\,\mathrm{d}z,$$

where f is the normalised cuspidal eigenform associated to E by the modularity theorem. Specifically, the Hecke action on the space of modular symbols and a modification of Birch's formula respectively give

$$-\mathrm{L}(E,1)\,\#E(\mathbb{F}_p) = \sum_{a=1}^{p-1} \mu_E\left(\tfrac{a}{p}\right), \qquad \mathrm{L}(E,\chi,1) = \frac{\tau(\chi)}{n} \sum_{a=1}^{p-1} \overline{\chi(a)} \mu_E\left(\tfrac{a}{p}\right).$$

By Manin's formalism for modular symbols, it turns out that $\mu_E(q) + \mu_E(1-q)$ is an integer multiple of $\Omega(E)$ for any $q \in \mathbb{Q}$, so the modular symbols in both expressions can be paired up and normalised accordingly to give an expression for $-\mathcal{L}(E)\,\#E(\mathbb{F}_p)$ in $\mathbb{Z}$ and an expression for $\mathcal{L}(E,\chi)$ in $\mathbb{Z}[\zeta_q]$. The congruence then follows immediately by comparing both integral expressions, noting that $\overline{\chi(a)} \equiv 1 \mod \langle 1-\zeta_q \rangle$.

This essentially proves the algebraic result, while the analytic results require more work. As the conductor p of χ varies over odd primes congruent to 1 modulo the order q of χ, the congruence says that $\mathcal{L}(E,\chi)$ varies according to $\#E(\mathbb{F}_p) = 1 + \det(\rho_{E,q}(\mathrm{Fr}_p)) - \mathrm{tr}(\rho_{E,q}(\mathrm{Fr}_p))$ modulo q. On the other hand, $\rho_{E,q}(\mathrm{Fr}_p)$ varies over $G_{E,q^\infty} \coloneqq \{ M \in \mathrm{im}\rho_{E,q} \mid \det(M) \equiv 1 \mod q \}$, but Chebotarev's density theorem says that this is asymptotically uniformly distributed. It turns out that it suffices to compute densities in the finite group G_{E,q^m} rather than the infinite group G_{E,q^∞}, and m is bounded above by the following general result.

Theorem (Ang24, Theorem 4.4)**.** *Let E be a semistable Γ_0-optimal elliptic curve over $\mathbb{Q}$ such that $\mathrm{L}(E,1) \neq 0$, and let q be an odd prime. Then $\mathrm{ord}_q(\mathcal{L}(E)) \geq -1$ assuming the Birch–Swinnerton-Dyer conjecture. If E has no rational q-isogeny, then $\mathrm{ord}_q(\mathcal{L}(E)) \geq 0$ unconditionally.*

The proof of this turned out to be quite subtle, involving many cases using a multitude of recent results. Mazur's torsion theorem first reduces this to a finite number of cases depending on $\mathrm{tor}(E)$, and all of which can be dealt with by Lorenzini's theorem on cancellations between torsion and Tamagawa numbers [Lor11, Proposition 1.1], except for when $q = 3$ and $\mathrm{tor}(E) \cong \mathbb{Z}/3\mathbb{Z}$. The proof of this last case follows from an application of Tate's algorithm, the aforementioned integrality of $\mathcal{L}(E)\,\#E(\mathbb{F}_p)$, and a case-by-case analysis on the possible mod-3 and 3-adic Galois images of E classified by Rouse–Sutherland–Zureick-Brown [RSZB22, Corollary 1.3.1 and Corollary 12.3.3]. The analytic results can then be derived by computing the densities of $\rho_{E,3}(\mathrm{Fr}_p)$ in all possible finite groups $G_{E,3}$ and $G_{E,9}$ given by the same classification.

Finally, note that all hypotheses that E is semistable Γ_0-optimal can be weakened by considering Manin constants, which is possible thanks to Česnavičius's theorem on Manin constants [Ces18, Theorem 1.2].

References

Ang24 D Angdinata (2024) L-values of elliptic curves twisted by cubic characters

Ces18 K Česnavičius (2018) The Manin constant in the semistable case

DEW21 V Dokchitser, R Evans, and H Wiersema (2021) On a BSD-type formula for L-values of Artin twists of elliptic curves

KN22 H Kisilevsky and J Nam (2022) Small algebraic central values of twists of elliptic L-functions

Lor11 D Lorenzini (2011) Torsion and Tamagawa numbers

RSZB22 J Rouse, A Sutherland, and D Zureick-Brown (2022) ℓ-adic images of Galois for elliptic curves over $\mathbb{Q}$