Canad. J. Math. 2025, pp. 1–25
http://dx.doi.org/10.4153/S0008414X25101065

On L-values of elliptic curves twisted by cubic Dirichlet characters

David Kurniadi Angdinata

Abstract. Given an elliptic curve E over $\mathbb{Q}$ of analytic rank zero, its L-function can be twisted by an even primitive Dirichlet character χ of order q, and in many cases its associated special L-value $\mathscr{L}(E,\chi)$ is known to be integral after normalizing by certain periods. This article determines the precise value of $\mathscr{L}(E,\chi)$ in terms of Birch–Swinnerton-Dyer invariants when $q = 3$, classifies their asymptotic densities modulo 3 by fixing E and varying χ, and presents a lower bound on the 3-adic valuation of $\mathscr{L}(E,1)$, all of which arise from a congruence of modular symbols. These results also explain some phenomena observed by Dokchitser–Evans–Wiersema and by Kisilevsky–Nam.

1 Introduction

The Birch–Swinnerton-Dyer conjecture relates the Hasse–Weil L-function $L(E,s)$ of an elliptic curve E over $\mathbb{Q}$ to certain algebraic invariants that encode important global arithmetic information of E [34]. Over a finite extension K of $\mathbb{Q}$, Artin's formalism for L-functions says that the Hasse–Weil L-function $L(E/K,s)$ of E base changed to K decomposes into a finite product of certain twisted L-functions $L(E,\chi,s)$, ranging over all Artin representations χ that factor through K, so that the behavior of $L(E/K,s)$ is completely governed by $L(E,\chi,s)$. The algebraic and analytic properties of these twisted L-functions are studied extensively in the literature, and they are the subject of many important open problems in the arithmetic of elliptic curves, most notably equivariant refinements of the Birch–Swinnerton-Dyer conjecture [5].

The special value $L^*(E,\chi,1)$ of $L(E,\chi,s)$ at $s = 1$ can be normalized by certain factors to get a *modified twisted L-value* $\mathscr{L}(E,\chi)$ that is conjectured to have nice algebraic properties. When $\chi = 1$ is the trivial representation, $\mathscr{L}(E,\chi)$ is simply given by the special value of $L(E,s)$ at $s = 1$ divided by the real period $\Omega(E)$. When χ is a nontrivial even Dirichlet character of prime conductor p, this is given by

$$\mathscr{L}(E,\chi) \coloneqq \frac{L^*(E,\chi,1)p}{\tau(\chi)\Omega(E)},$$

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

Received by the editors December 11, 2024; revised April 24, 2025; accepted April 28, 2025.
Published online on Cambridge Core June 20, 2025.
This work was supported by the Engineering and Physical Sciences Research Council [EP/S021590/1], the EPSRC Centre for Doctoral Training in Geometry and Number Theory (The London School of Geometry and Number Theory), University College London.
AMS subject classification: **11G05, 11G40.**
Keywords: L-values, elliptic curves, Dirichlet characters.

Classically, Birch and Swinnerton-Dyer conjectured that $\mathscr{L}(E,1) = \mathrm{BSD}(E)$, where $\mathrm{BSD}(E)$ is the *Birch–Swinnerton-Dyer quotient*

$$\mathrm{BSD}(E) \coloneqq \frac{\mathrm{Tam}(E)\#\text{Ш}(E)\,\mathrm{Reg}(E)}{\#\,\mathrm{tor}(E)^2},$$

where $\mathrm{Tam}(E)$, $\text{Ш}(E)$, and $\mathrm{Reg}(E)$ is the Tamagawa number, the Tate–Shafarevich group, and the elliptic regulator respectively. In contrast, there seems to be a barrier in formulating an analogous conjecture for $\mathscr{L}(E,\chi)$ when χ is nontrivial, with concrete examples of arithmetically identical elliptic curves with modified twisted L-values that differ by a unit [12, Section 4]. Having such a formula would present nontrivial consequences for the arithmetic of E/K, such as predictions for the non triviality of Tate–Shafarevich groups and the existence of points of infinite order, which are intractable with classical techniques for Selmer groups [12, Section 3].

Prominent existing techniques to study the ℓ-primary parts of Selmer groups, such as via the Iwasawa main conjectures, only gives a description of the ideal I generated by $\mathscr{L}(E,\chi)$, rather than its actual value. In a recent paper to understand a refinement of the classical Birch–Swinnerton-Dyer conjecture, Burns–Castillo determined I in terms of arithmetic invariants of E in certain relative K-groups [5, Proposition 7.3]. More concretely, Dokchitser–Evans–Wiersema expressed the norm of I in terms of $\mathrm{BSD}(E)$ and its base-changed quotient $\mathrm{BSD}(E/K)$, where K is the number field cut out by χ [12, Theorem 38], but the actual value of $\mathscr{L}(E,\chi)$ remains elusive.

This article completely determines the actual value of $\mathscr{L}(E,\chi)$ for cubic Dirichlet characters of prime conductor, under fairly generic assumptions on the Manin constants $c_0(E)$ and $c_1(E)$, culminating in the following result proven in Section 5.

Theorem 1.1 (Corollary 5.2) *Let E be an elliptic curve over $\mathbb{Q}$ of conductor N such that $L(E,1) \neq 0$. Let χ be a cubic Dirichlet character of odd prime conductor $p \nmid N$ such that $3 \nmid c_0(E)\,\mathrm{BSD}(E)\#E(\mathbb{F}_p)$. Assume further that $c_1(E) = 1$ and that the Birch–Swinnerton-Dyer conjecture holds over number fields. Then*

$$\mathscr{L}(E,\chi) = u\overline{\chi(N)}B,$$

where the positive rational number $B \in \mathbb{Q}^\times$ is the positive square root of the positive rational square $\mathrm{BSD}(E/K)/\mathrm{BSD}(E) \in (\mathbb{Q}^\times)^2$, and the sign $u = \pm 1$ is such that

$$u \equiv -\#E(\mathbb{F}_p)\,\mathrm{BSD}(E)B^{-1} \mod 3.$$

On the analytic side of things, in a paper on an analog of the Brauer–Siegel theorem for elliptic curves over cyclic extensions, Kisilevsky–Nam observed some patterns in the asymptotic distribution of $\mathscr{L}(E,\chi)$ [18, Section 7]. They considered six elliptic curves E and five positive integers q, and numerically computed the norms of $\mathscr{L}(E,\chi)$ for primitive Dirichlet characters χ of conductor p and order q, ranging over the thirty pairs of (E,q) and millions of positive integers p. For each pair of (E,q), they added a normalization factor to $\mathscr{L}(E,\chi)$ to obtain a real L-value $\mathscr{L}^+(E,\chi)$, and empirically determined the greatest common divisor $\gcd_{E,q}$ of the norms of $\mathscr{L}^+(E,\chi)$ by varying over all p. Upon dividing these norms by $\gcd_{E,q}$, they observed that these integers have unexpected biases when reduced modulo q.

This article completely predicts these biases for cubic Dirichlet characters of prime conductor, again under fairly generic assumptions, for three of the six elliptic curves they considered. The following result is proven under slightly relaxed assumptions in Section 7, where the normalization for $\mathscr{L}^+(E,\chi)$ is also defined.

Theorem 1.2 (Proposition 7.7) *Let E be an elliptic curve over $\mathbb{Q}$ of conductor N and minimal discriminant $\Delta = \pm N^n$ for some $n \in \mathbb{N}$, such that E has no rational 3-isogeny and that $3 \nmid nc_0(E)\operatorname{gcd}_{E,3}$. Let χ be a cubic Dirichlet character of odd prime conductor $p \nmid N$. Then*

$$\frac{\mathscr{L}^+(E,\chi)}{\operatorname{gcd}_{E,3}} \equiv \begin{cases} 0 \mod 3 & \text{if } \#E(\mathbb{F}_p) \equiv 0 \mod 3, \\ 2 \mod 3 & \text{if } \#E(\mathbb{F}_p) \equiv 1 \mod 3, \text{ and} \\ & p \text{ splits completely in the 3-division field of } E, \\ 1 \mod 3 & \text{otherwise.} \end{cases}$$

To put things in a more structured perspective, these biases can be quantified asymptotically by considering the natural densities of $\mathscr{L}(E,\chi)$ when reduced modulo q. More precisely, let $X_{E,q}^{<n}$ be the set of Dirichlet characters of odd order $q > 1$ and odd prime conductor $p < n$ such that p does not divide the conductor of E. Now define the *residual densities* $\delta_{E,q}$ of $\mathscr{L}(E,\chi)$ to be the natural densities of $\mathscr{L}(E,\chi)$ modulo $(1-\zeta_q)$. In other words, this is the value

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

if such a limit exists. It turns out that such a limit always exists, and its value for any $\lambda \in \mathbb{F}_q$ only depends on $\operatorname{BSD}(E)$, the torsion subgroup $\operatorname{tor}(E)$, and the mod-q^2 Galois image $\operatorname{im}(\overline{\rho_{E,q^2}})$. The following result classifies the possible residual densities for cubic Dirichlet characters, namely the ordered triples

$$\delta_{E,3} \coloneqq (\delta_{E,3}(0), \delta_{E,3}(1), \delta_{E,3}(2)).$$

Theorem 1.3 (Theorem 6.4) *Let E be an elliptic curve over $\mathbb{Q}$ such that $L(E,1) \neq 0$ and that $3 \nmid c_0(E)$. Assume further that the Birch–Swinnerton-Dyer conjecture holds. Then $\delta_{E,3}$ only depends on $\operatorname{BSD}(E)$ and on $\operatorname{im}(\overline{\rho_{E,9}})$, and can only be one of*

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

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

In particular, $\delta_{E,3}$ can be determined as follows.

- *If $\operatorname{ord}_3(\operatorname{BSD}(E)) = 0$ and $3 \nmid \#\operatorname{tor}(E)$, then $\delta_{E,3}$ is given by the table in Section A.1.*
- *If $\operatorname{ord}_3(\operatorname{BSD}(E)) = -1$, then $\delta_{E,3}$ is given by the table in Section A.2.*
- *Otherwise, $\delta_{E,3} = (1,0,0)$.*

Note that the aforementioned normalization factors are not present here, so that the resulting residual densities will be different from that of Kisilevsky–Nam. Section 6 proves this result and outlines the general procedure for higher order characters.

This classification builds upon the independent result that $\mathrm{ord}_3(\mathrm{BSD}(E)) \geq -1$. In a seminal paper quantifying the cancellations between $\mathrm{tor}(E)$ and $\mathrm{Tam}(E)$, Lorenzini proved that if a prime $\ell > 3$ is such that $\ell \mid \#\,\mathrm{tor}(E)$, then $\ell \mid \mathrm{Tam}(E)$ with finitely many explicit exceptions [20, Proposition 1.1]. In particular, when E has analytic rank zero, the denominator $\#\,\mathrm{tor}(E)^2$ of the rational number $\mathrm{BSD}(E)$ necessarily shares a factor with $\mathrm{Tam}(E)$ in its numerator, so that $\mathrm{ord}_\ell(\mathrm{BSD}(E)) \geq -1$ for any prime $\ell > 3$. On the other hand, he noted that there are explicit families with $\#\,\mathrm{tor}(E) = 3$ without any cancellation [20, Lemma 2.26], another family of which was given by Barrios–Roy [1, Corollary 5.1]. Subsequently, Melistas showed that these cancellations may instead occur between $\mathrm{tor}(E)$ and $\text{Ш}(E)$ in the numerator of $\mathrm{BSD}(E)$, and hence $\mathrm{ord}_3(\mathrm{BSD}(E)) \geq -1$, except possibly for certain reduction types [23, Theorem 1.4]. He then observed that there are again explicit exceptions, and in all these exceptions $c_0(E) = 3$ [23, Example 3.8], but did not explain this coincidence. The following result gives a lower bound for the odd part of the denominator of $\mathrm{BSD}(E)$.

Theorem 1.4 (Theorem 4.4) *Let E be an elliptic curve over $\mathbb{Q}$ such that $L(E,1) \neq 0$. Let ℓ be an odd prime such that $\ell \nmid c_0(E)$. Assume further that the Birch–Swinnerton-Dyer conjecture holds. If $\ell \mid \#\,\mathrm{tor}(E)$, then $\ell \mid \mathrm{Tam}(E)\#\text{Ш}(E)$. In particular,* $\mathrm{ord}_\ell(\mathrm{BSD}(E)) \geq -1$.

Section 4 states this result in terms of $\mathscr{L}(E,1)$ and proves it in slightly larger generality. Note that this is related to the Gross–Zagier conjecture for $\#\,\mathrm{tor}(E) = 3$ proven by Byeon–Kim–Yhee [9, Theorem 1.2], but their divisibility result holds over imaginary quadratic fields with a Heegner point of infinite order. In particular, the local computations here are a subset of their local Tamagawa number computations, but the global divisibility argument here uses the integrality of $\mathscr{L}(E,1)$ instead.

The methods in this article rely on the key fact that $\mathscr{L}(E,\chi) \in \mathbb{Z}[\zeta_q]$ for nontrivial primitive Dirichlet characters χ of order q, which was proven by Wiersema–Wuthrich under some mild hypotheses by expressing $\mathscr{L}(E,\chi)$ in terms of Manin's modular symbols [33, Theorem 2]. Parts of their argument can be adapted to obtain an explicit congruence between $\mathscr{L}(E,\chi)$ and $\mathscr{L}(E,1)$ modulo the prime $(1-\zeta_q)$ in $\mathbb{Z}[\zeta_q]$ above q. After establishing notational conventions in Section 2, some background on Manin's modular symbols will be provided in Section 3 to obtain this congruence. The remaining sections will be devoted to proving the four aforementioned results, with an appendix consisting of a list of mod-3 and 3-adic Galois images.

2 Background and conventions

This section establishes some relevant background on Galois representations and L-functions of elliptic curves and Dirichlet characters, as well as some notational conventions that might be deemed less standard in the literature.

For a primitive nth root of unity ζ_n, the ring of integers of the cyclotomic field $\mathbb{Q}(\zeta_n)$ will be denoted $\mathbb{Z}[\zeta_n]$, and denote its norm map by $\mathrm{Nm}_n : \mathbb{Q}(\zeta_n) \to \mathbb{Q}$. The ring of integers of its maximal totally real subfield $\mathbb{Q}(\zeta_n)^+$ will be denoted $\mathbb{Z}[\zeta_n]^+$, and denote its norm map by $\mathrm{Nm}_n^+ : \mathbb{Q}(\zeta_n)^+ \to \mathbb{Q}$. The isomorphism in class field theory from the unit group $(\mathbb{Z}/n)^\times$ of $\mathbb{Z}$ modulo n to the cyclotomic Galois group

$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ will be given by $a \mapsto (\zeta_n \mapsto \zeta_n^a)$, which identifies Dirichlet characters of modulus n with Artin representations that factor through $\mathbb{Q}(\zeta_n)$.

Denote the two-dimensional special, general, and projective linear group functors by SL_2, GL_2, and PGL_2. For a matrix M in such a matrix group, its trace will be denoted $\mathrm{tr}(M)$ and its determinant will be denoted $\det(M)$. For a prime ℓ, the conjugacy classes of $\mathrm{SL}_2(\mathbb{Z}/\ell)$ can be grouped by their traces as follows [3, Table 1.1 and Exercise 1.4].

- There are three conjugacy classes of trace 2 represented by $\left(\begin{smallmatrix} 1 & z \\ 0 & 1 \end{smallmatrix}\right)$ for $z \in \mathbb{F}_\ell$, one for each of the three Legendre symbols $\left(\frac{z}{\ell}\right) \in \{0, \pm 1\}$, each of which has cardinality equal to $((\ell^2-1)/2)^{|\left(\frac{z}{\ell}\right)|}$ and has elements of order equal to $\ell^{|\left(\frac{z}{\ell}\right)|}$.
- There are three conjugacy classes of trace $\ell - 2$ represented by $\left(\begin{smallmatrix} -1 & z \\ 0 & -1 \end{smallmatrix}\right)$ for $z \in \mathbb{F}_\ell$, one for each of the three Legendre symbols $\left(\frac{z}{\ell}\right) \in \{0, \pm 1\}$, each of which has cardinality equal to $((\ell^2-1)/2)^{|\left(\frac{z}{\ell}\right)|}$ and has elements of order equal to $2\ell^{|\left(\frac{z}{\ell}\right)|}$.
- There are $(\ell-3)/2$ conjugacy classes of trace $x + x^{-1}$ represented by $\left(\begin{smallmatrix} x & 0 \\ 0 & x^{-1} \end{smallmatrix}\right)$ for $x \in \mathbb{F}_\ell^\times \backslash \{\pm 1\}$, one for each unordered pair $\{x^{\pm 1}\}$, each of which has cardinality equal to $\ell(\ell+1)$ and has elements of order equal to the order of x.
- There are $(\ell-1)/2$ conjugacy classes of trace $\xi + \xi^\ell$ represented by

  $$\begin{pmatrix} \frac{1}{2}(\xi + \xi^\ell) & \frac{\zeta}{2}(\xi - \xi^\ell) \\ \frac{1}{2\zeta}(\xi - \xi^\ell) & \frac{1}{2}(\xi + \xi^\ell) \end{pmatrix}, \qquad \xi \in (\mathbb{F}_{\ell^2}^\times / \mathbb{F}_\ell^\times) \backslash \{\pm 1\},$$

  where ζ is a fixed element of $\mathbb{F}_{\ell^2}^\times$ satisfying $\zeta + \zeta^\ell = 0$, one for each pair $\{\xi^{\pm 1}\}$, each of which has cardinality $\ell(\ell-1)$ and elements of order equal to the order of ξ.

This will be useful for Theorem 4.4 and Proposition 6.1.

Throughout, an *elliptic curve* will always refer to an elliptic curve E over $\mathbb{Q}$ of conductor N, and any explicit example of an elliptic curve will be given by its Cremona label [11, Table 1]. For a prime ℓ, the ℓ-adic Galois representation associated with the ℓ-adic Tate module of E is denoted $\rho_{E,\ell}$, and its ℓ-adic Galois image $\mathrm{im}(\rho_{E,\ell})$ will be given by its Rouse–Sutherland–Zureick-Brown label as a subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ up to conjugacy [25, Section 2.4]. For any $n \in \mathbb{N}$, the projection of $\rho_{E,\ell}$ onto $\mathrm{GL}_2(\mathbb{Z}/\ell^n)$ is denoted $\overline{\rho_{E,\ell^n}}$, and its mod-$\ell^n$ Galois image $\mathrm{im}(\overline{\rho_{E,\ell^n}})$ will be given by its Sutherland label as a subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell^n)$ up to conjugacy [31, Section 6.4]. Note that if Fr_v is an arithmetic Frobenius at a prime $v \neq \ell$, then its trace is given by

$$\mathrm{tr}(\rho_{E,\ell}(\mathrm{Fr}_v)) = a_v(E) \coloneqq 1 + v - \#E(\mathbb{F}_v).$$

Let ω_E denote a global invariant differential on a minimal Weierstrass equation of E. Let $X_0(N)$ denote the modular curve associated with the Hecke congruence subgroup $\Gamma_0(N)$ of $\mathrm{SL}_2(\mathbb{Z})$, and let $S_2(N)$ denote the space of weight two cusp forms of level $\Gamma_0(N)$. By the modularity theorem, there is a surjective morphism $\phi_E : X_0(N) \twoheadrightarrow E$ of minimal degree and an eigenform $f_E \in S_2(N)$ with Fourier coefficients $a_v(E)$ for each prime $v \nmid N$. These constructions define two differentials on $X_0(N)$, namely $2\pi i f_E(z)\,\mathrm{d}z$ and the pullback $\phi_E^*\omega_E$ of ω_E by f_E, which are related by

$$\phi_E^*\omega_E = \pm c_0(E) 2\pi i f_E(z)\,\mathrm{d}z,$$

where $c_0(E)$ is a positive integer called the Manin constant [13, Proposition 2].

It is conjectured that $c_0(E) = 1$ when E is $\Gamma_0(N)$-optimal in its isogeny class, which was recently proven for semistable E [10, Theorem 1.2], but it is possible that $c_0(E) \neq 1$ in general. Nevertheless, every modular parameterization by $X_0(N)$ factors through a parameterization by the modular curve $X_1(N)$ associated with the congruence subgroup $\Gamma_1(N)$ of $\mathrm{SL}_2(\mathbb{Z})$ [30, Theorem 1.9]. An analogous construction using $X_1(N)$ yields the Manin constant $c_1(E)$, with the following important conjecture.

Conjecture 2.1 (Stevens) *Let E be an elliptic curve. Then $c_1(E) = 1$.*

For a complex Galois representation ρ, its local Euler factor at a prime v is given by

$$L_v(\rho, T) \coloneqq \det\left(1 - T\,\mathrm{Fr}_v^{-1} \,\middle|\, \rho^{I_v}\right),$$

where ρ^{I_v} is the subrepresentation of ρ invariant under the inertia subgroup I_v at v. The L-function $L(E, s)$ of E is then defined to be the infinite Euler product of $L_v(\rho_{E,\ell}^\vee, v^{-s})^{-1}$ over all primes v, where $\rho_{E,\ell}^\vee$ is the dual of the complex Galois representation associated with $\rho_{E,\ell} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ for some prime $\ell \neq v$. The modularity theorem says that $L(E, s)$ is the Hecke L-function of f_E, so that its order of vanishing at $s = 1$, and hence its leading term $L^*(E, 1)$, are both well-defined.

The Birch–Swinnerton-Dyer conjecture predicts this order of vanishing and its leading term in terms of arithmetic invariants as follows. Let $\mathrm{tor}(E)$ and $\mathrm{rk}(E)$ denote the torsion subgroup and the rank of the Mordell–Weil group $E(\mathbb{Q})$ respectively. Let $\Omega(E)$ denote the real period given by $\int_{E(\mathbb{R})} \omega_E$, with orientation chosen such that $\Omega(E) > 0$. Let $\mathrm{Tam}(E)$ denote the Tamagawa number, given as the product of local Tamagawa numbers $\mathrm{Tam}_v(E)$ over all primes v. Let $\mathrm{Reg}(E)$ denote the elliptic regulator defined in terms of the Néron–Tate pairing $\langle P, Q\rangle = \frac{1}{2}h_E(P + Q) - \frac{1}{2}h_E(P) - \frac{1}{2}h_E(Q)$, where h_E is the canonical height on E. Finally, let $Ш(E)$ denote the Tate–Shafarevich group, which is implicitly assumed to be finite in this article.

Conjecture 2.2 (Birch–Swinnerton-Dyer) *Let E be an elliptic curve. Then the order of vanishing of $L(E, s)$ at $s = 1$ is equal to $\mathrm{rk}(E)$, and its leading term satisfies*

$$\frac{L^*(E,1)}{\Omega(E)} = \frac{\mathrm{Tam}(E)\#Ш(E)\,\mathrm{Reg}(E)}{\#\,\mathrm{tor}(E)^2}.$$

Here, the left hand side is the *modified L-value* of E, which will be denoted $\mathscr{L}(E)$, and the right hand side is the *Birch–Swinnerton-Dyer quotient* of E, which will be denoted $\mathrm{BSD}(E)$. For the base change E/K of E to an extension K of $\mathbb{Q}$, there are analogous quantities $\mathscr{L}(E/K)$ and $\mathrm{BSD}(E/K)$ [12, Section 1.5]. If $\mathrm{ord}_\ell : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ denotes the ℓ-adic valuation for some prime ℓ, the conjecture that $\mathrm{ord}_\ell(\mathscr{L}(E)) = \mathrm{ord}_\ell(\mathrm{BSD}(E))$ is called the ℓ-part of the Birch–Swinnerton-Dyer conjecture.

Remark 2.3 Thanks to the Gross–Zagier formula [15, Theorem 7.3] and Kolyvagin's Euler system [19, Corollary 2], the rank conjecture and the finiteness of $Ш(E)$ are known when $L(E, 1) \neq 0$. In this setting, $\mathrm{BSD}(E)$ is clearly rational since $\mathrm{Reg}(E) = 1$, and the later Proposition 3.3 will show that $\mathscr{L}(E)$ is also rational. On the other hand, the leading term conjecture is not known even in this setting, but substantial progress has been made toward $\mathrm{ord}_\ell(\mathscr{L}(E)) = \mathrm{ord}_\ell(\mathrm{BSD}(E))$ as a consequence of the Iwasawa main conjectures for GL_2, starting with the work of Skinner–Urban [29, Theorem 2]. This is summarized in a survey by Burungale–Skinner–Tian [7, Section 3.3], but note that there is very recent progress in the supersingular case by Burungale–Skinner–Tian–Wan [8, Theorem 1.5], as well as in the ordinary case by Keller–Yin [17, Theorem C] and by Burungale–Castella–Skinner [6, Corollary 1.3.1]. For the purposes of this article, only the case $\ell = 3$ will be used in assumptions.

Throughout, a *character* will always refer to a nontrivial even primitive Dirichlet character χ of order $q > 1$ and prime conductor $p \nmid N$, which automatically means that $\chi(-1) = 1$ and $p \equiv 1 \bmod q$. The L-function $L(E, \chi, s)$ of E twisted by χ is defined to be the Euler product of $L_v(\rho_{E,\ell}^\vee \otimes \overline{\chi}, v^{-s})^{-1}$ over all primes v, so that in particular $\mathscr{L}(E, 1) = \mathscr{L}(E)$. The modularity theorem says that $L(E, \chi, s)$ is the Hecke L-function of f_E twisted by χ [28, Theorem 3.66], so that its order of vanishing at $s = 1$, and hence its leading term $L^*(E, \chi, 1)$, are again well-defined. When $L(E, \chi, 1) \neq 0$, Kato showed that $\mathrm{rk}(E) = \mathrm{rk}(E/K)$ and $Ш(E/K)$ is finite [16, Corollary 14.3]. The analogous *modified twisted L-value* is given by

$$\mathscr{L}(E, \chi) := \frac{L^*(E, \chi, 1)p}{\tau(\chi)\Omega(E)},$$

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

Remark 2.4 The definitions of L-values and Birch–Swinnerton-Dyer invariants in this section agree with those by Wiersema–Wuthrich [33, Section 7] and those by Dokchitser–Evans–Wiersema [12, Section 1.5] whenever $L(E, \chi, 1) \neq 0$, except for one notable difference for twisted L-functions due to the choice of normalization coming from class field theory. In this article, the Dirichlet series of $L(E, \chi, s)$ is $\sum_{n=1}^{\infty} \chi(n) a_n(E) n^{-s}$, and $\mathscr{L}(E, \chi)$ is defined in terms of $L(E, \chi, s)$. Wiersema–Wuthrich gives two definitions for twisted L-functions, namely an automorphic one that agrees with $L(E, \chi, s)$, and a motivic one that coincides with $L(E, \overline{\chi}, s)$ instead of $L(E, \chi, s)$. However, their modified twisted L-value is defined using the motivic definition, so that it coincides with $\mathscr{L}(E, \overline{\chi})$ instead of $\mathscr{L}(E, \chi)$. Dokchitser–Evans–Wiersema follows the motivic convention, so that their twisted L-functions and modified twisted L-values coincide with $L(E, \overline{\chi}, s)$ and $\mathscr{L}(E, \overline{\chi})$ respectively.

3 Modular symbols

This section recalls some classical facts on modular symbols. Most arguments here are well-known since the time of Manin [22], with some recent results by Wiersema–Wuthrich [33], but they are provided here for reference. Nevertheless, the main tool is the congruence in Corollary 3.7. Note that similar congruences were explored by Fearnley–Kisilevsky–Kuwata [14, Theorem 3.5], and are essentially equivalent to the equivariant Tamagawa number conjecture as shown by Bley [2, Section 2].

Let $N \in \mathbb{N}$. The congruence subgroup $\Gamma_0(N)$ of $\mathrm{SL}_2(\mathbb{Z})$ acts on the extended upper half plane $\mathscr{H}$ of $\mathbb{C}$ by fractional linear transformations, and a smooth path between two points in the same $\Gamma_0(N)$-orbit projects onto a closed path in the quotient $X_0(N) = \mathscr{H}/\Gamma_0(N)$, which defines an integral homology class $\gamma \in H_1(X_0(N), \mathbb{Z})$. This is independent of the smooth path chosen because $\mathscr{H}$ is simply connected, and any integral homology class $\gamma \in H_1(X_0(N), \mathbb{Z})$ arises in such a way. On the other hand, any cusp form $f \in S_2(N)$ induces a differential $2\pi i f(z)\,\mathrm{d}z$ on $X_0(N)$, and integrating this over the closed path γ gives a complex number $\int_\gamma 2\pi i f(z)\,\mathrm{d}z$ called a *modular symbol*. A general definition for paths with arbitrary endpoints is given by Manin [22, Section 1.2], but for the purposes of this article, it suffices to consider the modular symbol associated with the path from 0 to cusps $c \in \mathbb{Q} \cup \{\infty\}$. When c is rational with denominator coprime to N, the image of any smooth path between 0 and c is closed [22, Proposition 2.2], so that it makes sense to write the modular symbol

$$\mu_f(c) := \int_0^c 2\pi i f(z)\,\mathrm{d}z.$$

The key example for f will be the normalized cuspidal eigenform $f_E \in S_2(N)$ associated with an elliptic curve E of conductor N. In this case, it turns out that $\mathscr{L}(E)$, as well as $\mathscr{L}(E, \chi)$ for any character χ of conductor coprime to N, can be written as sums of $\mu_E(c) := \mu_{f_E}(c)$ for some $c \in \mathbb{Q}$. Furthermore, the terms in these sums can be paired up in a way that guarantees integrality, using the following trick.

Lemma 3.1 *Let $c \in \mathbb{Q}$ with denominator coprime to some $N \in \mathbb{N}$. If $f \in S_2(N)$, then*

$$\mu_f(c) + \mu_f(1-c) = 2\Re(\mu_f(c)).$$

In particular, if E is an elliptic curve, then $\mu_E(c) + \mu_E(1-c)$ is an integer multiple of $c_0(E)^{-1}\Omega(E)$.

Proof This is essentially identical to the proof by Wiersema–Wuthrich [33, Lemma 4], but the argument is repeated here for reference. Note that $\mu_f(1-c) - \mu_f(-c)$ is the integral of $2\pi i f(z)$ along the closed path between $-c$ and $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right) \cdot (-c)$, which is zero [22, Proposition 1.4], so that $\mu_f(1-c) = \mu_f(-c)$. The change of variables $z \mapsto -\overline{z}$ then transforms $\mu_f(-c)$ into $\overline{\mu_f(c)}$, and the first statement follows. Now by definition, $c_0(E)\mu_E(c)$ lies in the lattice of modular symbols generated by smooth paths in $H_1(E(\mathbb{C}), \mathbb{Z})$, whose real parts lie in $\frac{1}{2}\Omega(E)\mathbb{Z}$. The second statement then follows from the first statement with $f = f_E$. ■

Remark 3.2 When c is rational with denominator coprime to N, this definition of $\mu_E(c)$ coincides with the modular symbol denoted $\mu(c)$ by Wiersema–Wuthrich [33, Section 2], since their least residue denoted α would vanish.

For this exact reason, the modular symbols $\mu_E(c)$ can be normalized to be integers. More precisely, for an elliptic curve E of conductor N with normalized cuspidal eigenform $f_E \in S_2(N)$, define the normalized modular symbol

$$\mu_E^+(c) := \frac{c_0(E)}{\Omega(E)}(\mu_E(c) + \mu_E(1-c)),$$

which is now an integer. The integrality of $\mathscr{L}(E)$ is now a formal consequence of the action of Hecke operators on the space of modular symbols.

Proposition 3.3 *Let E be an elliptic curve of conductor N. Let v be an odd prime such that $v \nmid N$. Then*

$$c_0(E)\mathscr{L}(E)\#E(\mathbb{F}_v) = \sum_{a=1}^{\lfloor \frac{v-1}{2} \rfloor} \mu_E^+(a/v).$$

In particular, both sides lie in $\mathbb{Z}$.

Proof The first statement is precisely the action of Hecke operators on the space of modular symbols [22, Theorem 4.2] up to a factor of $c_0(E)^{-1}\Omega(E)$. Integrality of both sides then follows immediately from Lemma 3.1 and the first statement. ■

Remark 3.4 The assumption that $v \nmid N$ is crucial, and removing this may cause integrality to fail, such as for the elliptic curve 11a1 where $c_0(E) = 1$ and $\mathscr{L}(E) = \frac{1}{5}$, but $\#E(\mathbb{F}_{11}) = 11$.

The same argument can be adapted for $\mathscr{L}(E,\chi)$ using Birch's formula.

Proposition 3.5 *Let E be an elliptic curve of conductor N. Let χ be a character of order q and odd prime conductor $p \nmid N$. Then*

$$c_0(E)\mathscr{L}(E,\chi) = \sum_{a=1}^{\lfloor \frac{p-1}{2} \rfloor} \overline{\chi(a)}\mu_E^+(a/p).$$

In particular, both sides lie in $\mathbb{Z}[\zeta_q]$. Furthermore, if $c_1(E) = 1$, then $\mathscr{L}(E,\chi) \in \mathbb{Z}[\zeta_q]$.

Proof This is identical to the proof by Wiersema–Wuthrich [33, Proposition 7], noting that the automorphic and motivic definitions of $\mathscr{L}(E,\chi)$ agree under the assumption that $p \nmid N$ [33, Lemma 18]. Integrality of both sides then follows immediately from Lemma 3.1 and the first statement. The final statement is an analogous argument with $c_1(E)$ also given by Wiersema–Wuthrich [33, Proposition 8]. ■

Remark 3.6 The assumption that $p \nmid N$ can be weakened slightly to $p^2 \nmid N$ for the first two statements [33, Proposition 7]. However, removing this completely may cause integrality to fail, such as for the elliptic curve 50b1 satisfying $c_0(E) = 1$ and the unique quadratic character of conductor 5, where $\mathscr{L}(E,\chi) = \frac{1}{3}$.

Now observe that the right hand sides of Propositions 3.3 and 3.5 are highly similar. More precisely, since $\overline{\chi(a)} \equiv 1 \bmod (1-\zeta_q)$ except when $\ell \mid a$, the right hand sides are congruent modulo $(1-\zeta_q)$. This is summarized in the following result, which will be the main tool behind much of the rest of the article.

Corollary 3.7 *Let E be an elliptic curve of conductor N. Let χ be a character of order q and odd prime conductor $p \nmid N$. Then*

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

Furthermore, if $q \nmid c_0(E)$, then

$$\mathscr{L}(E,\chi) \equiv -\mathscr{L}(E)\#E(\mathbb{F}_p) \mod (1-\zeta_q),$$

where the denominators of both sides are inverted modulo $(1-\zeta_q)$.

Remark 3.8 Without considering the factor of $c_0(E)$, both integrality results and the congruence easily fail in trivial ways, but the assumption that $q \nmid c_0(E)$ is a relatively mild one, since $c_0(E) \neq 1$ seems to be relatively rare.

Remark 3.9 Modified twisted L-values $\mathscr{L}(E,\chi)$ are Galois equivariant as predicted by Deligne's period conjecture [4, Theorem 2.7], in the sense that $\mathscr{L}(E,\sigma\circ\chi) = \sigma(\mathscr{L}(E,\chi))$ for any $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$. With this property, $\mathscr{L}(E)$ can be expressed in terms of the sum of $\mathscr{L}(E,\chi)$ for all characters χ of a given conductor and order. For instance, when χ is a cubic character of conductor p,

$$1 + \chi(a) + \overline{\chi(a)} = \begin{cases} 1 & \text{if } a \text{ is not a unit in } \mathbb{F}_p, \\ 3 & \text{if } a \text{ is the cube of a unit in } \mathbb{F}_p, \\ 0 & \text{otherwise,} \end{cases}$$

so that the identities in Propositions 3.3 and 3.5 combine to yield

$$c_0(E)\mathscr{L}(E,\chi) + c_0(E)\mathscr{L}(E,\overline{\chi}) + c_0(E)\mathscr{L}(E)\#E(\mathbb{F}_p) = 3\sum_a \mu_E^+(a/p),$$

where the sum runs over the cubic residues a in $\mathbb{F}_p$ such that $1 \leq a \leq \lfloor \frac{p-1}{2} \rfloor$. By Galois equivariance, the first two terms combine to $2c_0(E)\mathfrak{R}(\mathscr{L}(E,\chi))$, so that this expresses $\mathfrak{R}(\mathscr{L}(E,\chi))$ in terms of $\mathscr{L}(E)$ up to a few error terms consisting of modular symbols. By reducing modulo 3, this recovers the congruence in Corollary 3.7, but also shows that the congruence would not a priori hold modulo 9, unless the modular symbols $\mu_E^+(a/p)$ for each cubic residue a in $\mathbb{F}_p$ sum to a multiple of 3.

4 Denominators of L-values

This section proves a few results on the ℓ-adic valuations of denominators of modified L-values, where ℓ is an odd prime, which may be of independent interest. Since $c_0(E)\mathscr{L}(E)\#E(\mathbb{F}_v)$ is integral, the ℓ-adic valuation of the rational number $c_0(E)\mathscr{L}(E)$ can be bounded from below by the ℓ-adic valuation of $\#E(\mathbb{F}_v)$, which is in turn controlled by $\mathrm{tor}(E)$ in the denominator of $\mathrm{BSD}(E)$. When $\ell \neq 3$, assuming the ℓ-part of the Birch–Swinnerton-Dyer conjecture, such a lower bound follows from Lorenzini's result that $\mathrm{ord}_\ell(\#\,\mathrm{tor}(E)) \leq \mathrm{ord}_\ell(\mathrm{Tam}(E))$ with finitely many exceptions [20, Proposition 1.1], but the case $\ell = 3$ requires more work.

Lemma 4.1 *Let E be an elliptic curve without complex multiplication such that $E(\mathbb{Q})$ has a point of order 3 and that $3 \nmid \mathrm{Tam}(E)$. Then $\mathrm{im}(\overline{\rho_{E,3}})$ is the full Borel subgroup.*

Proof By the assumption that E has a point of order 3, E is isomorphic either to the elliptic curve given by $y^2 + cy = x^3$ for some cube-free $c \in \mathbb{N}$, which has complex multiplication by $\mathbb{Z}[\zeta_3]$, or to the elliptic curve $E_{1,\pm b/a}$ given by

$$y^2 + xy \pm \frac{b}{a}y = x^3,$$

for some coprime $a, b \in \mathbb{N}$ [1, Proposition 2.4]. If $3 \nmid \mathrm{ord}_v(a)$ for some prime v, then $3 \mid \mathrm{Tam}_v(E_{1,\pm b/a})$ [1, Theorem 3.5], which contradicts the assumption that $3 \nmid \mathrm{Tam}(E)$, so that $a = d^3$ for some $d \in \mathbb{N}$ coprime to b. The change of variables

$(x, y) \mapsto (x/d^2, y/d^3)$ yields an isomorphism from $E_{1,\pm b/a}$ to the elliptic curve $E_{d,\pm b}$ given by

$$y^2 + dxy \pm by = x^3,$$

which is now a minimal model and has discriminant $\Delta = \pm b^3(d^3 - 27b)$. Now let v be a prime such that $v \mid b$, so that $v \mid \Delta$ and $\operatorname{ord}_v(d^3 - 27b) = 0$ by coprimality. By step 2 of Tate's algorithm, since $T^2 + dT$ splits in $\mathbb{F}_v$, the elliptic curve $E_{d,\pm b}$ has Kodaira symbol $\mathbf{I}_{\operatorname{ord}_v(\Delta)}$ with split mutiplicative reduction at v, so that

$$\operatorname{Tam}_v(E) = \operatorname{Tam}_v(E_{d,\pm b}) = \operatorname{ord}_v(\Delta) = 3\operatorname{ord}_v(b),$$

which contradicts the assumption that $3 \nmid \operatorname{Tam}(E)$. This forces $b = 1$, but the j-invariant of $E_{d,\pm b} = E_{d,\pm 1}$ computes to be

$$\frac{d^3(d^3 \mp 24)^3}{\pm d^3 - 27} = 27\frac{\left(\frac{27}{\pm d^3-27} + 1\right)\left(\frac{27}{\pm d^3-27} + 9\right)^3}{\left(\frac{27}{\pm d^3-27}\right)^3},$$

which implies that $\operatorname{im}(\overline{\rho_{E,3}})$ is the Borel subgroup 3B.1.1 [35, Theorem 1.2]. ■

Assuming just one direction of the 3-part of the Birch–Swinnerton-Dyer conjecture, a clean divisibility result for $\operatorname{BSD}(E)$ can be derived from the integrality of $c_0(E)\mathscr{L}(E)\#E(\mathbb{F}_v)$ via a case-by-case analysis on $\operatorname{im}(\rho_{E,3})$.

Proposition 4.2 *Let E be an elliptic curve of conductor N such that $L(E, 1) \neq 0$ and that* $\operatorname{tor}(E) \cong \mathbb{Z}/3$. *Assume further that* $\operatorname{ord}_3(\mathscr{L}(E)) \leq \operatorname{ord}_3(\operatorname{BSD}(E))$. *Then* $3 \mid c_0(E)\operatorname{Tam}(E)\#\text{Ш}(E)$. *In particular, if* $3 \nmid c_0(E)$, *then* $\operatorname{ord}_3(\operatorname{BSD}(E)) \geq -1$.

Proof The final statement follows from the first statement, so it suffices to prove the latter. Assume that $3 \nmid c_0(E)$. By Proposition 3.3 and the assumptions,

$$\operatorname{ord}_3\left(\frac{\operatorname{Tam}(E)\#\text{Ш}(E)}{9}\#E(\mathbb{F}_v)\right) \geq \operatorname{ord}_3(\mathscr{L}(E)\#E(\mathbb{F}_v)) \geq 0,$$

so it suffices to find an odd prime $v \nmid N$ such that $\#E(\mathbb{F}_v) \equiv 3 \bmod 9$. By Chebotarev's density theorem, this reduces to finding a matrix $M \in \operatorname{im}(\overline{\rho_{E,9}})$ such that $1 + \det(M) - \operatorname{tr}(M) = 3$. By inspecting the table in Section A.2, such matrices exist for all $\operatorname{im}(\rho_{E,3})$ except for the two 3-adic Galois images 9.72.0.1 and 9.72.0.5, so these two cases have to be handled separately. If $\operatorname{im}(\rho_{E,3})$ is 9.72.0.1, then $\operatorname{im}(\overline{\rho_{E,3}})$ is 3Cs.1.1 and not 3B.1.1, so Lemma 4.1 implies that $3 \mid \operatorname{Tam}(E)$. Otherwise $\operatorname{im}(\rho_{E,3})$ is 9.72.0.5, then $\operatorname{im}(\overline{\rho_{E,9}})$ fixes a subspace of the group of 9-torsion points of E, so that $E(\mathbb{Q}) \cong \mathbb{Z}/9$, which contradicts the assumption that $E(\mathbb{Q}) \cong \mathbb{Z}/3$. ■

Remark 4.3 The conclusion of Proposition 4.2 was already observed by Melistas [23, Example 3.8], where the elliptic curves 27a3, 27a4, and 54a3 all have $E(\mathbb{Q}) \cong \mathbb{Z}/3$ and $\operatorname{Tam}(E)\#\text{Ш}(E) = 1$ but $c_0(E) = 3$. By the work of Lorenzini, it is generally expected that the factors in $\operatorname{Tam}(E)$ would cancel $\#\operatorname{tor}(E)$, but in this case it is necessary to consider $\#\text{Ш}(E)$ as well, such as in the elliptic curve 1638j3 where $E(\mathbb{Q}) \cong \mathbb{Z}/3$ and $c_0(E)\operatorname{Tam}(E) = 1$ but $\#\text{Ш}(E) = 9$. Note that the statement is false for $\operatorname{tor}(E) \cong \mathbb{Z}/3$ but $\operatorname{rk}(E) > 0$, such as for the elliptic curve 91b1 where $c_0(E)\operatorname{Tam}(E)\#\text{Ш}(E) = 1$.

A lower bound on the ℓ-adic valuation of $c_0(E)\mathscr{L}(E)$ then follows for any odd prime ℓ, assuming the ℓ-part of the Birch–Swinnerton-Dyer conjecture, but when E has no rational ℓ-isogeny the bound is unconditional by simple group theory.

Theorem 4.4 *Let E be an elliptic curve of conductor N such that* $L(E,1) \neq 0$. *Let* ℓ *be an odd prime.*

(1) *If E has no rational* ℓ*-isogeny, then* $\operatorname{ord}_\ell(c_0(E)\mathscr{L}(E)) \geq 0$.
(2) *Assume further that* $\operatorname{ord}_\ell(\mathscr{L}(E)) = \operatorname{ord}_\ell(\operatorname{BSD}(E))$. *Then* $\operatorname{ord}_\ell(c_0(E)\mathscr{L}(E)) \geq -1$.

Proof For the first statement, by Proposition 3.3, it suffices to find an odd prime $v \nmid N$ such that $\ell \nmid \#E(\mathbb{F}_v)$. By Chebotarev's density theorem, this reduces to finding a matrix $M \in \operatorname{im}(\overline{\rho_{E,\ell}})$ such that $\operatorname{tr}(M) \neq 1 + \det(M)$. Suppose otherwise that $\operatorname{tr}(M) = 1 + \det(M)$ for all matrices $M \in \operatorname{im}(\overline{\rho_{E,\ell}})$, so that in particular $\operatorname{tr}(M) = 2$ for all matrices $M \in \operatorname{im}(\overline{\rho_{E,\ell}}) \cap \operatorname{SL}_2(\mathbb{Z}/\ell)$. In this case, by inspecting the orders of elements in each conjugacy class of $\operatorname{SL}_2(\mathbb{Z}/\ell)$ as in Section 2, it is clear that $\operatorname{im}(\overline{\rho_{E,\ell}}) \cap \operatorname{SL}_2(\mathbb{Z}/\ell)$ is necessarily an ℓ-group, so that in particular $\ell \mid \#\operatorname{im}(\overline{\rho_{E,\ell}})$. Then either $\operatorname{im}(\overline{\rho_{E,\ell}})$ is contained in a Borel subgroup of $\operatorname{GL}_2(\mathbb{Z}/\ell)$ or $\operatorname{im}(\overline{\rho_{E,\ell}})$ contains $\operatorname{SL}_2(\mathbb{Z}/\ell)$ [26, Proposition 15]. The former contradicts the assumption that E has no rational ℓ-isogeny, and the latter is impossible by comparing orders.

For the second statement, the assumption that $\operatorname{ord}_\ell(\mathscr{L}(E)) = \operatorname{ord}_\ell(\operatorname{BSD}(E))$ reduces the statement to proving that $\operatorname{ord}_\ell(c_0(E)\operatorname{BSD}(E)) \geq -1$. By Mazur's torsion theorem, since ℓ is odd, it suffices to consider $\operatorname{tor}(E)$ being one of the eight subgroups

$$\mathbb{Z}/3,\ \mathbb{Z}/5,\ \mathbb{Z}/6,\ \mathbb{Z}/7,\ \mathbb{Z}/9,\ \mathbb{Z}/10,\ \mathbb{Z}/12,\ \mathbb{Z}/2 \oplus \mathbb{Z}/6,$$

If $E(\mathbb{Q}) \ncong \mathbb{Z}/3$, then a case-by-case analysis of Lorenzini's classification yields $\operatorname{ord}_\ell(\operatorname{Tam}(E)) \geq \operatorname{ord}_\ell(\#\operatorname{tor}(E))$ except for the elliptic curve 11a3 with $\ell = 5$, and the elliptic curves 14a4 and 14a6 with $\ell = 3$ [20, Proposition 1.1], but these exceptions all have $\operatorname{ord}_\ell(c_0(E)) = 1$ and $\operatorname{ord}_\ell(\operatorname{BSD}(E)) = -2$, so that in particular $\operatorname{ord}_\ell(c_0(E))\operatorname{BSD}(E)) \geq -1$. If $E(\mathbb{Q}) \cong \mathbb{Z}/3$, then Proposition 4.2 implies that

$$\operatorname{ord}_3(c_0(E)\operatorname{BSD}(E)) = \operatorname{ord}_3(c_0(E)\operatorname{Tam}(E)\#\text{Ш}(E)) - 2 \geq -1,$$

as required. ■

Remark 4.5 The assumption on the ℓ-part of the Birch–Swinnerton-Dyer conjecture in the second statement can be slightly weakened, by only requiring that $\operatorname{ord}_\ell(\mathscr{L}(E)) \geq \operatorname{ord}_\ell(\operatorname{BSD}(E))$ for all E, except for when $\operatorname{im}(\rho_{E,3})$ is 9.72.0.1, where the assumption $\operatorname{ord}_\ell(\mathscr{L}(E)) \leq \operatorname{ord}_\ell(\operatorname{BSD}(E))$ is also needed to proceed with the argument in Proposition 4.2. In fact, it might also be provable without appealing to the conjecture at all, by finding a matrix $M \in \operatorname{im}(\rho_{E,\ell})$ such that $1 + \det(M) - \operatorname{tr}(M) \equiv \ell \mod \ell^2$ along the same lines as the proof of Proposition 4.2. In general, this would need a case-by-case analysis of $\operatorname{im}(\rho_{E,\ell})$ for when E has no rational ℓ-isogeny for $\ell > 3$, whose classification remains incomplete at present.

The following is another easy result on the ℓ-adic valuation of $\mathscr{L}(E)\#E(\mathbb{F}_v)$. The factors arising from the denominator of the rational number $\mathscr{L}(E)\#E(\mathbb{F}_v)$ could a priori cancel the factors appearing in $c_0(E)$, but the congruence of L-values says that this should not happen, assuming Stevens's conjecture that $c_1(E) = 1$.

Proposition 4.6 *Let E be an elliptic curve of conductor N such that $L(E,1) \neq 0$. Let v and ℓ be odd primes such that $v \nmid N$ and that $v \equiv 1 \bmod \ell$. Assume further that $c_1(E) = 1$. Then $\ell \nmid c_0(E)\mathscr{L}(E)\#E(\mathbb{F}_v)$ if and only if $\ell \nmid c_0(E)$ and* $\operatorname{ord}_\ell(\mathscr{L}(E)\#E(\mathbb{F}_v)) = 0$.

Proof Assume that $\ell \nmid c_0(E)\mathscr{L}(E)\#E(\mathbb{F}_v)$ but $\ell \mid c_0(E)$. By the assumption that $c_1(E) = 1$, Proposition 3.5 says that $\mathscr{L}(E,\chi) \in \mathbb{Z}[\zeta_\ell]$ for any character χ of conductor v and order ℓ, so that $c_0(E)\mathscr{L}(E,\chi) \equiv 0 \bmod (1-\zeta_\ell)$, which contradicts $\ell \nmid c_0(E)\mathscr{L}(E)\#E(\mathbb{F}_v)$ by Corollary 3.7. Thus $\ell \nmid c_0(E)$, so that $\operatorname{ord}_\ell(\mathscr{L}(E)\#E(\mathbb{F}_v)) = 0$ also follows, while the converse is immediate noting that $\mathscr{L}(E) \neq 0$. ■

Remark 4.7 Assuming Stevens's conjecture, Proposition 4.6 yields an immediate proof that $\mathscr{L}(E)\#E(\mathbb{F}_v)$ is integral at ℓ if $\operatorname{ord}_\ell(c_0(E)) \leq 1$. This condition seems to hold for all elliptic curves in the LMFDB [32], but a proof remains elusive. On the other hand, assuming the ℓ-part of the Birch–Swinnerton-Dyer conjecture, there might be a direct proof that $\mathscr{L}(E)\#E(\mathbb{F}_v)$ is integral at ℓ, by arguing that $1 + \det(M) - \operatorname{tr}(M)$ cancels $\#\operatorname{tor}(E)^2$ for every matrix M lying in every possible $\operatorname{im}(\rho_{E,\ell})$.

5 Units of twisted L-values

Under the standard arithmetic conjectures, Dokchitser–Evans–Wiersema computed the norm of $\mathscr{L}(E,\chi)$ in terms of $\operatorname{BSD}(E)$ and $\operatorname{BSD}(E/K)$, where K is the degree q subfield of $\mathbb{Q}(\zeta_p)$ cut out by the kernel of χ [12, Theorem 38]. Some of their main results can be summarized in the notation of this article as follows.

Proposition 5.1 *Let E be an elliptic curve of conductor N such that $L(E,1) \neq 0$. Let χ be a character of odd prime conductor $p \nmid N$ and odd prime order $q \nmid c_0(E)\operatorname{BSD}(E)\#E(\mathbb{F}_p)$. Assume further that $c_1(E) = 1$, and that $\mathscr{L}(E) = \operatorname{BSD}(E)$ and $\mathscr{L}(E/K) = \operatorname{BSD}(E/K)$.*

1. *The cyclotomic integer $\mathscr{L}(E,\chi) \in \mathbb{Z}[\zeta_q]$ has norm*
$$\operatorname{Nm}_q(\mathscr{L}(E,\chi)) = \pm\frac{\operatorname{BSD}(E/K)}{\operatorname{BSD}(E)},$$
and it generates an ideal that is invariant under complex conjugation.
2. *The real cyclotomic integer $\mathscr{L}(E,\chi)\zeta \in \mathbb{Z}[\zeta_q]^+$ has norm*
$$\operatorname{Nm}_q^+(\mathscr{L}(E,\chi)\zeta) = \pm B,$$
where the positive rational number $B \in \mathbb{Q}^\times$ is the positive square root of the positive rational square $\operatorname{BSD}(E/K)/\operatorname{BSD}(E) \in (\mathbb{Q}^\times)^2$, and $\zeta \coloneqq \chi(N)^{(q-1)/2}$.

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

Proof By Proposition 4.6, under the arithmetic conjectures, the assumption that $q \nmid c_0(E)\operatorname{BSD}(E)\#E(\mathbb{F}_p)$ reduces to $q \nmid c_0(E)$ and $\operatorname{ord}_q(\mathscr{L}(E)\#E(\mathbb{F}_p)) = 0$. In particular $L(E,1) \neq 0$, and moreover $\operatorname{ord}_q(\mathscr{L}(E,\chi)) = 0$ by Corollary 3.7, so that $L(E,\chi,1) \neq 0$ as well. This verifies the assumptions of a result by Dokchitser–Evans–Wiersema [12, Theorem 13(5)–Theorem 13(12)], and is a restatement. ■

In ideal-theoretic language, Proposition 5.1.1 predicts that the ideal I of $\mathbb{Z}[\zeta_q]$ generated by $\mathscr{L}(E,\chi)$ has norm equal to the nonzero positive rational number

$\mathrm{BSD}(E/K)/\mathrm{BSD}(E)$, and Proposition 5.1.2 says that this rational number is the square of a positive rational number B equal to the norm of the ideal of $\mathbb{Z}[\zeta_q]^+$ generated $\mathscr{L}(E,\chi)\zeta$. Thus there are only finitely many possibilities for the prime ideal factorization of I, and the fact that I is invariant under complex conjugation narrows down the possibilities further. The precise ideal factorization can then be recovered from the $\mathrm{Gal}(K/\mathbb{Q})$-module structure of $Ш(E/K)$ [5, Remark 7.4], such as in the case of $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/5$ explored by Maistret–Shukla [21, Theorem 1.4].

Assuming that I has been computed as an ideal of $\mathbb{Z}[\zeta_q]$, any generator of I is only equal to the actual value of $\mathscr{L}(E,\chi)$ up to a unit $u \in \mathbb{Z}[\zeta_q]$. Proposition 5.1.2 refines this prediction slightly by adding a condition on the norm of $\mathscr{L}(E,\chi)\zeta$, which determines the actual value of $\mathscr{L}(E,\chi)$ up to a unit $u \in \mathbb{Z}[\zeta_q]^+$. In the special case of $q = 3$, this is still ambiguous up to a sign, since the units of $\mathbb{Z}[\zeta_3]^+ = \mathbb{Z}$ are ± 1. Corollary 3.7 comes into the picture by pinning down the sign in terms of $\#E(\mathbb{F}_p)$.

Corollary 5.2 *Let E be an elliptic curve of conductor N such that $L(E,1) \neq 0$. Let χ be a cubic character of odd prime conductor $p \nmid N$ such that $3 \nmid c_0(E)\,\mathrm{BSD}(E)\#E(\mathbb{F}_p)$. Assume further that $c_1(E) = 1$, and that $\mathscr{L}(E) = \mathrm{BSD}(E)$ and $\mathscr{L}(E/K) = \mathrm{BSD}(E/K)$. Then*

$$\mathscr{L}(E,\chi) = u\overline{\chi(N)}B,$$

where the positive rational number $B \in \mathbb{Q}^\times$ is the positive square root of the positive rational square $\mathrm{BSD}(E/K)/\mathrm{BSD}(E) \in (\mathbb{Q}^\times)^2$, and the sign $u = \pm 1$ is such that

$$u \equiv -\#E(\mathbb{F}_p)\,\mathrm{BSD}(E)B^{-1} \mod 3.$$

This follows immediately from Corollary 3.7 and Proposition 5.1. Corollary 5.2 clarifies much of the phenomena observed by Dokchitser–Evans–Wiersema [12, Example 45], where they gave many pairs of examples of arithmetically similar elliptic curves E_1 and E_2 with $\mathscr{L}(E_1,\chi) \neq \mathscr{L}(E_2,\chi)$ for a few cubic characters χ, in the sense that $\mathscr{L}(E_1,\chi) \neq \mathscr{L}(E_2,\chi)$ precisely because $\#E_1(\mathbb{F}_p) \not\equiv \#E_2(\mathbb{F}_p) \bmod 3$.

Example 5.3 Let E_1 and E_2 be the elliptic curves 1356d1 and 1356f1, and let χ be the cubic character of conductor 7 given by $\chi(3) = \zeta_3^2$. Then $c_0(E_i) = \mathrm{BSD}(E_i) = \mathrm{BSD}(E_i/K) = 1$ for $i \in \{1,2\}$, so Proposition 5.1 implies that $\mathscr{L}(E_i,\chi) = \pm\overline{\chi(1356)} = \pm\zeta_3^2$, but it was a priori unclear why $\mathscr{L}(E_1,\chi) = \zeta_3^2$ and $\mathscr{L}(E_2,\chi) = -\zeta_3^2$. Corollary 5.2 explains this by requiring that this sign agrees with $-\#E_i(\mathbb{F}_7)$ modulo 3, and in this case $\#E_1(\mathbb{F}_7) = 11$ and $\#E_2(\mathbb{F}_7) = 7$, which are distinct modulo 3. They provided other examples satisfying $c_0(E) = \mathrm{BSD}(E) = \mathrm{BSD}(E/K) = 1$ with different $\mathscr{L}(E,\chi)$ for a few different cubic characters χ, and they can all be explained similarly. The values of $\mathscr{L}(E,\chi)$ for the above character are tabulated as follows.

E	1356d1	1356f1	3264r1	3264s1
$\mathscr{L}(E,\chi)$	ζ_3^2	$-\zeta_3^2$	$-\zeta_3^2$	ζ_3^2
$\#E(\mathbb{F}_7)$	11	7	10	8

E	3540a1	3540b1	4800i1	4800bj1	4800bm1
$\mathscr{L}(E,\chi)$	$-\zeta_3^2$	ζ_3^2	$-\zeta_3^2$	$-\zeta_3^2$	ζ_3^2
$\#E(\mathbb{F}_7)$	7	11	7	7	11

When $q > 3$ but $\mathrm{BSD}(E) = \mathrm{BSD}(E/K)$, Proposition 5.1 says that $\mathscr{L}(E,\chi)$ is a unit in $\mathbb{Z}[\zeta_q]$, and Corollary 3.7 places a congruence on this unit in terms of $\#E(\mathbb{F}_p)$.

Corollary 5.4 *Let E be an elliptic curve of conductor N such that $L(E,1) \neq 0$. Let χ be a character of odd prime conductor $p \nmid N$ and odd prime order $q \nmid c_0(E)\,\mathrm{BSD}(E)\#E(\mathbb{F}_p)$ such that $\mathrm{BSD}(E) = \mathrm{BSD}(E/K)$. Assume further that $c_1(E) = 1$, and that $\mathscr{L}(E) = \mathrm{BSD}(E)$ and $\mathscr{L}(E/K) = \mathrm{BSD}(E/K)$. Then $\mathscr{L}(E,\chi) = u$ for some unit $u \in \mathbb{Z}[\zeta_q]$ such that $u \equiv -\#E(\mathbb{F}_p)\,\mathrm{BSD}(E) \bmod (1-\zeta_q)$.*

Again, this follows immediately from Corollary 3.7 and Proposition 5.1. Corollary 5.4 explains the remaining phenomena observed by Dokchitser–Evans–Wiersema [12, Example 44], where they gave many pairs of examples of arithmetically trivial elliptic curves E_1 and E_2 with $\mathscr{L}(E_1,\chi) \neq \mathscr{L}(E_2,\chi)$ for quintic characters χ, in the sense that $\mathscr{L}(E_1,\chi) \neq \mathscr{L}(E_2,\chi)$ precisely because $\#E_1(\mathbb{F}_p) \not\equiv \#E_2(\mathbb{F}_p) \bmod 5$.

Example 5.5 Let E_1 and E_2 be the elliptic curves 307a1 and 307c1, and let χ be the quintic character of conductor 11 given by $\chi(2) = \zeta_5$. Then $c_0(E_i) = \mathrm{BSD}(E_i) = \mathrm{BSD}(E_i/K) = 1$ for $i \in \{1,2\}$, so Proposition 5.1 implies that $\mathscr{L}(E_i,\chi)$ is a unit, but it was a priori unclear why $\mathscr{L}(E_1,\chi) = 1$ and $\mathscr{L}(E_2,\chi) = \zeta_5 u^2$, where $u := 1 + \zeta_5^4$. Corollary 5.4 explains this by requiring that $\mathscr{L}(E_i,\chi) \equiv -\#E_i(\mathbb{F}_{11}) \bmod (1-\zeta_5)$, and in this case $\#E_1(\mathbb{F}_{11}) = 9$ and $\#E_2(\mathbb{F}_{11}) = 16$, which are distinct modulo 5. They provided other examples satisfying $c_0(E) = \mathrm{BSD}(E) = \mathrm{BSD}(E/K) = 1$ with different $\mathscr{L}(E,\chi)$ for this character, and they can all be explained similarly as follows.

E	307a1	307c1	432g1	432h1	714b1	714h1
$\mathscr{L}(E,\chi)$	1	$\zeta_5 u^2$	u^2	$-\zeta_5 u^{-1}$	1	$-\zeta_5^4 u^3$
$\#E(\mathbb{F}_{11})$	9	16	16	8	9	13

E	1187a1	1187b1	1216g1	1216k1
$\mathscr{L}(E,\chi)$	$\zeta_5^2 u^{-1}$	$\zeta_5 u^{-3}$	$-\zeta_5^3 u^2$	$\zeta_5^4 u^{-1}$
$\#E(\mathbb{F}_{11})$	17	8	9	7

When $q > 3$ and $\mathrm{BSD}(E) \neq \mathrm{BSD}(E/K)$, it is awkward to rephrase Proposition 5.1 to apply Corollary 3.7, but it can be illustrated with an example [12, Example 46].

Example 5.6 Let E_1 and E_2 be the elliptic curves 291d1 and 139a1, and let χ be the quintic character of conductor 31 given by $\chi(3) = \zeta_5^3$. Then $c_0(E_i) = \mathrm{BSD}(E_i) = 1$, but

$\mathrm{BSD}(E_i/K) = 11^2$ for $i \in \{1, 2\}$, so Proposition 5.1 implies that $\mathscr{L}(E_i, \chi)$ generates an ideal of norm 11^2 that is invariant under complex conjugation. By considering the primes above 11^2 in $\mathbb{Z}[\zeta_5]$, there are only two such ideals, generated by $\lambda_1 := 3\zeta_5^3 + \zeta_5^2 + 3\zeta_5 \equiv 2 \bmod (1 - \zeta_5)$ and $\lambda_2 := \zeta_5^3 + 3\zeta_5 + 3 \equiv 2 \bmod (1 - \zeta_5)$, and in fact $(\mathscr{L}(E_i, \chi)) = (\lambda_i)$. Assuming this fact, Corollary 3.7 then predicts that $\mathscr{L}(E_i, \chi) = u_i\lambda_i$ for some units $u_i \in \mathbb{Z}[\zeta_5]$ such that $2u_i \equiv -\#E_i(\mathbb{F}_{31}) \bmod (1 - \zeta_5)$, and in this case $\#E_1(\mathbb{F}_{31}) = 33 \equiv 3 \bmod 5$ and $\#E_1(\mathbb{F}_{31}) = 23 \equiv 3 \bmod 5$, so that $u_i \equiv 1 \bmod (1 - \zeta_5)$. In fact, $u_1 = \zeta_5^4$ and $u_2 = \zeta_5^2 - \zeta_5 + 1$.

Remark 5.7 As this example highlights, in general it is possible for $\mathscr{L}(E_1, \chi) \equiv \mathscr{L}(E_2, \chi) \bmod (1 - \zeta_q)$ but $\mathscr{L}(E_1, \chi) \neq \mathscr{L}(E_2, \chi)$, even when $c_0(E_i) = \mathrm{BSD}(E_i) = 1$, so that a general Birch–Swinnerton-Dyer formula for $\mathscr{L}(E, \chi)$ remains unlikely even with the factor of $\#E(\mathbb{F}_p)$. There are also examples for when E_i have the same conductor and minimal discriminant, and furthermore $\mathrm{BSD}(E_i/K) = 1$, such as for the elliptic curves 544b1 and 544f1 and the quintic character χ of conductor 11 given by $\chi(2) = \zeta_5$, where $\mathscr{L}(E_1, \chi) = -\zeta_5^3 - \zeta_5$ and $\mathscr{L}(E_2, \chi) = -2\zeta_5^3 - 3\zeta_5^2 - 2\zeta_5$. This is the pair of elliptic curves with the smallest conductor satisfying the aforementioned properties but with $\mathscr{L}(E_1, \chi) \neq \mathscr{L}(E_2, \chi)$, but other examples do seem to be rare.

6 Residual densities of twisted L-values

For a fixed elliptic curve E of conductor N, a natural problem is to determine the asymptotic distribution of $\mathscr{L}(E, \chi)$, as χ varies over characters of some fixed prime order q but of arbitrarily high odd prime conductor $p \nmid N$. However, for each such p, there are $q - 1$ characters χ of conductor p and order q, giving rise to $q - 1$ conjugates of $\mathscr{L}(E, \chi)$, so that 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 $\mathscr{L}(E, \chi)$ modulo $(1 - \zeta_q)$ is independent of the choice of χ for each p, so that a simpler problem would be to determine the asymptotic distribution of these residue classes instead. As in the introduction, let $X_{E,q}^{<n}$ be the set of characters of odd order q and odd prime conductor $p < n$ not dividing N. Define the *residual densities* $\delta_{E,q}$ of $\mathscr{L}(E, \chi)$ to be the natural densities of $\mathscr{L}(E, \chi)$ modulo $(1 - \zeta_q)$. In other words, this is the value

$$\delta_{E,q}(\lambda) := \lim_{n \to \infty} \frac{\#\left\{\chi \in X_{E,q}^{<n} \;\middle|\; \mathscr{L}(E, \chi) \equiv \lambda \mod (1 - \zeta_q)\right\}}{\#X_{E,q}^{<n}}, \qquad \lambda \in \mathbb{F}_q,$$

if such a limit exists. Note that as these residue classes only depend on p rather than χ, the set $X_{E,q}^{<n}$ can be replaced with the set of equivalence classes of characters in $X_{E,q}^{<n}$, where two characters are equivalent if they have the same conductor. When $q \nmid c_0(E)$, this can be computed for each $\lambda \in \mathbb{F}_q$ using Corollary 3.7, with the only subtlety being the possible cancellations between $\mathscr{L}(E)$ and $\#E(\mathbb{F}_p)$. In the generic scenario when $\mathrm{im}(\overline{\rho_{E,q}})$ is maximal, there is a clean description in terms of Legendre symbols.

Proposition 6.1 *Let E be an elliptic curve such that $L(E, 1) \neq 0$. Let q be an odd prime such that $q \nmid c_0(E)$.*

(1) *If* $\operatorname{ord}_q(\mathscr{L}(E)) > 0$*, then* $\delta_{E,q}(0) = 1$ *and* $\delta_{E,q}(\lambda) = 0$ *for any* $\lambda \in \mathbb{F}_q^\times$.

(2) *If* $\operatorname{ord}_q(\mathscr{L}(E)) \leq 0$*, then set* $m := 1 - \operatorname{ord}_q(\mathscr{L}(E))$ *and*

$$G_{E,q^m} := \left\{M \in \operatorname{im}(\overline{\rho_{E,q^m}}) \,\middle|\, \det(M) \equiv 1 \mod q\right\}.$$

Then for any $\lambda \in \mathbb{F}_q$,

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

In particular, if $\operatorname{ord}_q(\mathscr{L}(E)) \leq 0$ *and* $\overline{\rho_{E,q}}$ *is surjective, then compute the Legendre symbols*

$$\varepsilon_{E,q}(\lambda) := \left(\frac{\lambda\mathscr{L}(E)^{-1}}{q}\right)\left(\frac{\lambda\mathscr{L}(E)^{-1} + 4}{q}\right).$$

Then for any $\lambda \in \mathbb{F}_q$,

$$\delta_{E,q}(\lambda) = \begin{cases} \frac{1}{q-1} & \textit{if } \varepsilon_{E,q}(\lambda) = 1, \\ \frac{q}{q^2-1} & \textit{if } \varepsilon_{E,q}(\lambda) = 0, \\ \frac{1}{q+1} & \textit{if } \varepsilon_{E,q}(\lambda) = -1. \end{cases}$$

Proof By Corollary 3.7, $\delta_{E,q}(\lambda)$ is just the natural density of $-\mathscr{L}(E)\#E(\mathbb{F}_p) \equiv \lambda \mod q$. If $\operatorname{ord}_q(\mathscr{L}(E)) > 0$, then only $\lambda = 0$ gives a nonzero natural density. Otherwise $\operatorname{ord}_q(\mathscr{L}(E)) \leq 0$, then this is equivalent to $1 + p - a_p(E) \equiv -\lambda\mathscr{L}(E)^{-1} \mod q^m$, noting that $\mathscr{L}(E)^{-1}$ is well-defined and nonzero modulo q^m by definition. By Chebotarev's density theorem, this occurs with the proportion of matrices $M \in G_{E,q}$ with $\det(M) = p$ and $\operatorname{tr}(M) = a_p(E)$, so that the second statement follows. If $\overline{\rho_{E,q}}$ is surjective, then Theorem 4.4.1 yields $m = 1$, so that $\delta_{E,q}(\lambda)$ is the proportion of matrices $M \in \mathrm{SL}_2(\mathbb{Z}/q)$ such that $\operatorname{tr}(M) \equiv 2 - \lambda\mathscr{L}(E)^{-1} \mod q$. The final statement then follows by $\#\,\mathrm{SL}_2(\mathbb{Z}/q) = (q-1)q(q+1)$ and by inspecting the possible traces in $\mathrm{SL}_2(\mathbb{Z}/q)$ as in Section 2, noting that $\operatorname{tr}(M) = x + x^{-1}$ for some $x \in \mathbb{F}_q \backslash \{\pm 1\}$ precisely when $x^2 - 4$ is a quadratic residue modulo q. ■

Remark 6.2 Without the assumption that $q \nmid c_0(E)$, the same argument can be used to compute the residual density of $c_0(E)\mathscr{L}(E,\chi)$ instead, by adding a factor of $c_0(E)$ to every instance of $\mathscr{L}(E)$ in the statement and proof of Proposition 6.1. However, Proposition 3.5 predicts that $\mathscr{L}(E,\chi) \in \mathbb{Z}[\zeta_q]$ under Stevens's conjecture, so that both sides of the congruence are divisible by q and the statement becomes vacuous.

Remark 6.3 Under the standard arithmetic conjectures, Proposition 5.1 says that $\mathscr{L}(E,\chi)\zeta \in \mathbb{Z}[\zeta_q]$, so that $\mathrm{Nm}_q^+(\mathscr{L}(E,\chi)\zeta)$ is an integer. Since the norm is multiplicative and $\zeta \equiv 1 \mod (1 - \zeta_q)$, the asymptotic distribution of the residue class of $\mathrm{Nm}_q^+(\mathscr{L}(E,\chi)\zeta)$ modulo q essentially boils down to computing $\delta_{E,q}$.

Assuming the q-part of the Birch–Swinnerton-Dyer conjecture, Theorem 4.4.3 says $\operatorname{ord}_q(\mathrm{BSD}(E)) \geq -1$, so that nontrivial values of $\delta_{E,q}$ are only visible when $\operatorname{ord}_q(\mathrm{BSD}(E)) \in \{0, -1\}$. Once this is determined, computing $\delta_{E,q}$ then reduces to identifying $\operatorname{im}(\overline{\rho_{E,q}})$ or $\operatorname{im}(\overline{\rho_{E,q^2}})$, and then weighing the proportion of matrices with a certain determinant and trace. To illustrate this in action, the next result describes the possible ordered triples $(\delta_{E,3}(0), \delta_{E,3}(1), \delta_{E,3}(2))$ of residual densities, which is only made possible thanks to the classification of 3-adic Galois images by Rouse–Sutherland–Zureick-Brown [25, Corollaries 1.3.1 and 12.3.3]. As in the introduction, these ordered triples will also be denoted $\delta_{E,3}$ for ease of notation.

Theorem 6.4 *Let E be an elliptic curve such that $L(E,1) \neq 0$ and that $3 \nmid c_0(E)$. Assume further that $\operatorname{ord}_3(\mathscr{L}(E)) = \operatorname{ord}_3(\mathrm{BSD}(E))$. Then precisely one of the following holds.*

(1) *If $\operatorname{ord}_3(\mathrm{BSD}(E)) > 0$, then $\delta_{E,3} = (1, 0, 0)$.*
(2) *If $\operatorname{ord}_3(\mathrm{BSD}(E)) = 0$ and $3 \mid \#\operatorname{tor}(E)$, then $\delta_{E,3} = (1, 0, 0)$.*
(3) *If $\operatorname{ord}_3(\mathrm{BSD}(E)) = 0$ and $3 \nmid \#\operatorname{tor}(E)$, then $\delta_{E,3}$ is given by the table in Section A.1.*
(4) *If $\operatorname{ord}_3(\mathrm{BSD}(E)) = -1$, then $\delta_{E,3}$ is given by the table in Section A.2.*

In particular, $\delta_{E,3}$ only depends on $\mathrm{BSD}(E)$ and $\operatorname{im}(\overline{\rho_{E,9}})$, and can only be one of

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

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

Proof The fact that there are only four possibilities is immediate from Theorem 4.4. By Proposition 6.1, the first statement follows immediately under the assumption that $\operatorname{ord}_3(\mathscr{L}(E)) = \operatorname{ord}_3(\mathrm{BSD}(E))$, while the second statement follows from $3 \mid 1 + \det(M) - \operatorname{tr}(M)$ for all matrices $M \in \operatorname{im}(\overline{\rho_{E,3}})$ whenever $3 \mid \#\operatorname{tor}(E)$.

For the third statement, it suffices to consider $G_{E,3} = \operatorname{im}(\overline{\rho_{E,3}}) \cap \mathrm{SL}_2(\mathbb{Z}/3)$, and there are only 5 possibilities for $\operatorname{im}(\overline{\rho_{E,3}})$ when $\overline{\rho_{E,3}}$ is not surjective, as tabulated in the table in Section A.1. If $\overline{\rho_{E,3}}$ is surjective, then $\delta_{E,3}$ is already computed in the final statement in Proposition 6.1, while the other 5 cases are similar but easier computations. For instance, if $\operatorname{im}(\overline{\rho_{E,3}})$ is 3B.1.2, then $G_{E,3}$ is conjugate to the subgroup of unipotent upper triangular matrices in $\mathrm{SL}_2(\mathbb{Z}/3)$. There are 6 matrices in this subgroup, all of which have trace 0, so that $\delta_{E,3} = (1, 0, 0)$. Note that when $\delta_{E,3}(1) \neq \delta_{E,3}(2)$, the nonzero residue of $\mathrm{BSD}(E)$ modulo 3 would swap the values of $\delta_{E,3}(1)$ and $\delta_{E,3}(2)$. For instance, if $\overline{\rho_{E,3}}$ is surjective, then $G_{E,3} = \mathrm{SL}_2(\mathbb{Z}/3)$, and

$$\delta_{E,3} = \begin{cases} \left(\tfrac{3}{8}, \tfrac{1}{4}, \tfrac{3}{8}\right) & \text{if } \mathrm{BSD}(E) \equiv 1 \mod 3, \\ \left(\tfrac{3}{8}, \tfrac{3}{8}, \tfrac{1}{4}\right) & \text{if } \mathrm{BSD}(E) \equiv 2 \mod 3. \end{cases}$$

For the fourth statement, it suffices to consider $G_{E,9}$, and by the classification this is simply the projection onto $\mathrm{GL}_2(\mathbb{Z}/9)$ of 21 different possible $\operatorname{im}(\rho_{E,3})$, as tabulated in the table in Section A.2. For instance, if $\operatorname{im}(\rho_{E,3})$ is 3.8.0.1, then $G_{E,9}$ is the preimage of the subgroup of $\mathrm{SL}_2(\mathbb{Z}/3)$ generated by $\left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 2 \\ 0 & 2 \end{smallmatrix}\right)$under the canonical projection $\mathrm{GL}_2(\mathbb{Z}/9) \twoheadrightarrow \mathrm{GL}_2(\mathbb{Z}/3)$. This preimage in $\mathrm{GL}_2(\mathbb{Z}/9)$ consists of 243 matrices, of which 135 have trace 0 and 54 have trace 1 and 2 each, so that

$$\delta_{E,3} = \left(\tfrac{135}{243}, \tfrac{54}{243}, \tfrac{54}{243}\right) = \left(\tfrac{5}{9}, \tfrac{2}{9}, \tfrac{2}{9}\right).$$

The other 20 cases are similar but easier computations, noting again that the nonzero residue of $3\,\mathrm{BSD}(E)$ modulo 3 would swap the values of $\delta_{E,3}(1)$ and $\delta_{E,3}(2)$ when $\delta_{E,3}(1) \neq \delta_{E,3}(2)$. For instance, if $\operatorname{im}(\rho_{E,3})$ is 27.648.18.1, then

$$\delta_{E,3} = \begin{cases} \left(\frac{1}{3}, 0, \frac{2}{3}\right) & \text{if } 3\,\mathrm{BSD}(E) \equiv 1 \mod 3, \\ \left(\frac{1}{3}, \frac{2}{3}, 0\right) & \text{if } 3\,\mathrm{BSD}(E) \equiv 2 \mod 3. \end{cases}$$

Finally, the final statement follows immediately from the first four. ■

Remark 6.5 The first case happens when $3 \nmid \#\mathrm{tor}(E)$ but $3 \mid \mathrm{Tam}(E)\#\text{Ш}(E)$, such as for the elliptic curve 50b4 where $\mathrm{BSD}(E) = 3$, and the second case happens when $9 \mid \mathrm{Tam}(E)\#\text{Ш}(E)$, such as for the elliptic curve 84a1 where $\mathrm{BSD}(E) = \frac{1}{2}$.

Remark 6.6 If $\mathrm{im}(\overline{\rho_{E,3}})$ is 3Cs.1.1, then a much easier argument to prove that $\delta_{E,3} = (1, 0, 0)$ is to observe that $G_{E,3}$ is trivial, so that $E(\mathbb{F}_p)$ acquires full 3-torsion for any $p \equiv 1 \bmod 3$, and thus $\mathscr{L}(E, \chi) \equiv -\mathrm{BSD}(E)\#E(\mathbb{F}_p) \equiv 0 \bmod 3$ always.

Remark 6.7 Theorem 6.4 can be rephrased to describe the the actual densities of $\mathscr{L}(E, \chi)$ rather than their residual densities, since it describes the densities of the sign u determined in Corollary 5.2, but this will not be explored here.

7 Twisted L-values of Kisilevsky–Nam

The computation of residual densities was originally motivated by patterns in the statistical data by Kisilevsky–Nam [18, Section 7], where they numerically computed millions of modified twisted L-values by fixing the elliptic curve and varying the character. However, they considered an alternative normalization, given by

$$\mathscr{L}^+(E, \chi) := \begin{cases} \mathscr{L}(E, \chi) & \text{if } \chi(N) = 1, \\ \mathscr{L}(E, \chi)(1 + \overline{\chi(N)}) & \text{if } \chi(N) \neq 1, \end{cases}$$

in contrast to the normalization factor ζ given in Proposition 5.1. Under the implicit assumption that $\mathscr{L}(E, \chi) \in \mathbb{Z}[\zeta_q]$, they showed that $\mathscr{L}^+(E, \chi) \in \mathbb{Z}[\zeta_q]^+$ [18, Proposition 2.1], so that $\mathrm{Nm}_q^+(\mathscr{L}^+(E, \chi))$ is an integer. Fixing six elliptic curves E and five small integers q, they varied the character χ of order q over millions of conductors p with an arbitrary choice of χ for each p, empirically determined the greatest common divisor $\gcd_{E,q}$ of all the integers $\mathrm{Nm}_q^+(\mathscr{L}^+(E, \chi))$, and considered the integer

$$\widetilde{\mathscr{L}^+}(E, \chi) := \frac{\mathrm{Nm}_q^+(\mathscr{L}^+(E, \chi))}{\gcd_{E,q}}.$$

Remark 7.1 When q is odd and $L(E, 1) \neq 0$, this definition of $\widetilde{\mathscr{L}^+}(E, \chi)$ coincides with the modified twisted L-value denoted A_χ by Kisilevsky–Nam, since $\chi(N) = -1$ never occurs and the global root number is always 1 [18, Section 2.2]. Their definition of $\mathscr{L}(E, \chi)$ has an extra factor of 2, but this is cancelled out after division by $\gcd_{E,q}$.

Remark 7.2 In the interpretation of Proposition 5.1, the integer $\gcd_{E,q}$ is predicted to arise from contributions by the common divisors of $\mathrm{BSD}(E/K)/\mathrm{BSD}(E)$, ranging over various number fields K of degree q over $\mathbb{Q}$ coming from characters of order q.

As their normalization differs from that in Proposition 5.1 [18, Remark 1], the resulting residual densities are skewed. More precisely, define the set $X_{E,q}^{<n}$ as before, and analogously define the *skewed residual densities* $\widetilde{\delta}_{E,q}$ of $\widetilde{\mathscr{L}^+}(E, \chi)$ to be the natural densities of $\widetilde{\mathscr{L}^+}(E, \chi)$ modulo q. In other words, this is the value

$$\widetilde{\delta}_{E,q}(\lambda) \coloneqq \lim_{n\to\infty} \frac{\#\left\{\chi \in X_{E,q}^{<n} \,\middle|\, \widetilde{\mathscr{L}}^{+}(E,\chi) \equiv \lambda \mod q\right\}}{\#X_{E,q}^{<n}}, \qquad \lambda \in \mathbb{F}_q,$$

if such a limit exists. In the simplest case where $q = 3 \nmid \mathrm{gcd}_{E,3}$,

$$\widetilde{\mathscr{L}}^{+}(E,\chi) \equiv \begin{cases} \mathscr{L}(E,\chi)\,\mathrm{gcd}_{E,3} & \text{if } \chi(N) = 1, \\ 2\mathscr{L}(E,\chi)\,\mathrm{gcd}_{E,3} & \text{if } \chi(N) \neq 1, \end{cases}$$

since there is no norm. This becomes amenable to a computation similar to that of Proposition 6.1 provided that the condition $\chi(N) = 1$ can be controlled. For many elliptic curves, including half of those considered by Kisilevsky–Nam, $\chi(N)$ depends completely on $\#E(\mathbb{F}_p)$ due to a shared action of Frobenius in $\mathrm{GL}_2(\mathbb{Z}/3)$.

Lemma 7.3 *Let E be an elliptic curve of conductor N with no rational 3-isogeny such that the splitting field F of $X^3 - N$ lies in the splitting field K of the 3-division polynomial $\psi_{E,3}$. Let χ be a cubic character of odd prime conductor $p \nmid N$. Then* $\mathrm{im}(\overline{\rho_{E,3}}) = \mathrm{GL}_2(\mathbb{Z}/3)$ *and* $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{PGL}_2(\mathbb{Z}/3)$. *Furthermore, if p does not split completely in K, then* $\#E(\mathbb{F}_p) \equiv 2 \bmod 3$ *if and only if* $\chi(N) = 1$. *Otherwise,* $\#E(\mathbb{F}_p) \not\equiv 2 \bmod 3$ *and* $\chi(N) = 1$.

Proof Let L be the extension of K where all points in $E[3]$ are defined. By the assumption that E has no rational 3-isogeny and the classification of $\mathrm{im}(\overline{\rho_{E,3}})$, if $\overline{\rho_{E,3}}$ were not surjective, then $\mathrm{Gal}(L/\mathbb{Q})$ is either 3Nn or 3Ns. Neither of this could occur, since by the assumption that $F \subseteq K$, there are subfield inclusions

$$\mathbb{Q} \subseteq \mathbb{Q}(\zeta_3) \subseteq F \subseteq K \subseteq L.$$

In particular, $\mathrm{Gal}(L/\mathbb{Q})$ surjects onto $\mathrm{Gal}(F/\mathbb{Q}) \cong \mathcal{S}_3$, which forces $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{Z}/3)$. On the other hand, $\mathrm{Gal}(K/\mathbb{Q})$ permutes the roots of the degree 4 polynomial $\psi_{E,3}$, which forces it to be $\mathrm{PGL}_2(\mathbb{Z}/3) \cong \mathcal{S}_4$. Its subgroup $\mathrm{Gal}(K/\mathbb{Q}(\zeta_3)) \cong \mathcal{A}_4$ surjects onto $\mathrm{Gal}(F/\mathbb{Q}(\zeta_3)) \cong \mathbb{Z}/3$, with kernel the unique subgroup $\mathrm{Gal}(K/F) \cong (\mathbb{Z}/2)^2$ of index 4 consisting precisely of all elements of $\mathcal{A}_4$ of order 1 or 2.

Now $\mathrm{Fr}_p \in \mathrm{Gal}(K/\mathbb{Q})$ acts on the residue field of a prime π of F above p by

$$\mathrm{Fr}_p(\zeta_3) \equiv \zeta_3^p \mod \pi, \qquad \mathrm{Fr}_p(\sqrt[3]{N}) \equiv \sqrt[3]{N}^p \mod \pi.$$

Clearly Fr_p fixes ζ_3, so that $\mathrm{Fr}_p \in \mathrm{Gal}(K/\mathbb{Q}(\zeta_3))$. If p does not split completely in K, the condition $\mathrm{Fr}_p \in \mathrm{Gal}(K/F)$ turns out to be equivalent to $\#E(\mathbb{F}_p) \equiv 2 \bmod 3$ and to $\chi(N) = 1$. To see this, on one hand, this means that Fr_p fixes $\sqrt[3]{N}$, or equivalently that $\sqrt[3]{N}^{p-1} \equiv 1 \bmod p$, which is precisely the condition that $\chi(N) = 1$. On the other hand, this also means that $\mathrm{Fr}_p^2 = 1$ in $\mathrm{Gal}(K/\mathbb{Q}(\zeta_3))$, which is equivalent to Fr_p having order exactly 2 in $\mathrm{Gal}(K/\mathbb{Q}(\zeta_3))$. By the Cayley–Hamilton theorem, these are precisely the trace 0 matrices in $\mathrm{PGL}_2(\mathbb{Z}/3)$, or equivalently the trace 0 matrices in $\mathrm{GL}_2(\mathbb{Z}/3)$, which proves the equivalence with $a_p(E) = 0$. Finally, if p splits completely in K, then $\mathrm{Fr}_p = 1$ in $\mathrm{Gal}(K/\mathbb{Q}(\zeta_3))$, and hence $\chi(N) = 1$, but these never have trace 0 in $\mathrm{PGL}_2(\mathbb{Z}/3)$ or in $\mathrm{GL}_2(\mathbb{Z}/3)$, so that $\#E(\mathbb{F}_p) \not\equiv 2 \bmod 3$. ■

Remark 7.4 The first assumption is necessary, evident in the elliptic curve 50b1 with $F \subseteq K$ but $\mathrm{im}(\overline{\rho_{E,3}})$ is 3B, where 7 does not split completely in K but $\#E(\mathbb{F}_7) = 10 \equiv$

1 mod 3 and $\chi(50) = \overline{\chi(50)} = 1$. The second assumption is also necessary, evident in the elliptic curve 21a1 with no rational 3-isogeny but $F \notin K$, where 13 does not split completely in K but $\#E(\mathbb{F}_{13}) = 16 \equiv 1 \bmod 3$ and $\chi(21) = \overline{\chi(21)} = 1$. For the final statement, checking that p splits completely in F but not in K is not sufficient to conclude, such as for the elliptic curve 11a1, where $\#E(\mathbb{F}_{19}) = 20 \equiv 2 \bmod 3$ and $\chi(11) = \overline{\chi(11)} = 1$. If p does split completely in K, then both $\#E(\mathbb{F}_p) \equiv 0 \bmod 3$ and $\#E(\mathbb{F}_p) \equiv 1 \bmod 3$ are possible, such as for the elliptic curve 11a1, where $\#E(\mathbb{F}_{337}) = 360 \equiv 0 \bmod 3$ and $\#E(\mathbb{F}_{193}) = 190 \equiv 1 \bmod 3$.

Remark 7.5 The argument in the proof of Lemma 7.3 only works for cubic characters, as $\mathrm{PGL}_2(\mathbb{Z}/q)$ is almost simple for $q > 3$ and admits few nontrivial surjections.

Remark 7.6 Elliptic curves with minimal discriminant $\Delta = \pm N^n$ for some $n \in \mathbb{N}$ such that $3 \nmid n$ satisfy the assumptions of Lemma 7.3, since $\sqrt[3]{N}$ can then be expressed in terms of $\sqrt[3]{\Delta}$ [26, Section 5.3b]. This condition is in turn satisfied when N is prime, such as for the elliptic curves given by $y^2 = x^3 + ux^2 - 16x$ and $y^2 = x^3 - 2ux^2 + Nx$ studied by Neumann [24, Theorem 5.1] and Setzer [27, Theorem 2] when $N = u^2 + 64$ for some integer u, which occurs infinitely often assuming Bunyakovsky's conjecture.

For these elliptic curves, the residual density of $\widetilde{\mathscr{L}}^+(E,\chi)$ is now easy to compute.

Proposition 7.7 *Let E be an elliptic curve of conductor N with no rational 3-isogeny such that $3 \nmid c_0(E)\,\mathrm{gcd}_{E,3}$ and that the splitting field F of $X^3 - N$ lies in the splitting field K of the 3-division polynomial $\psi_{E,3}$. Let χ be a cubic character of odd prime conductor $p \nmid N$. Then*

$$\widetilde{\mathscr{L}}^+(E,\chi) \equiv \begin{cases} 0 \mod 3 & \textit{if } \#E(\mathbb{F}_p) \equiv 0 \mod 3, \\ 2 \mod 3 & \textit{if } \#E(\mathbb{F}_p) \equiv 1 \mod 3 \textit{ and } p \textit{ splits completely in } K, \\ 1 \mod 3 & \textit{otherwise.} \end{cases}$$

In particular,

$$\widetilde{\delta}_{E,3}(0) = \tfrac{9}{24}, \qquad \widetilde{\delta}_{E,3}(1) = \tfrac{15}{24}, \qquad \widetilde{\delta}_{E,3}(2) = \tfrac{1}{24}.$$

Proof By Corollary 3.7 and the assumption that $3 \nmid c_0(E)\,\mathrm{gcd}_{E,3}$,

$$\widetilde{\mathscr{L}}^+(E,\chi) \equiv \begin{cases} 2\#E(\mathbb{F}_p)\mathscr{L}(E)\,\mathrm{gcd}_{E,3} & \text{if } \chi(N) = 1, \\ \#E(\mathbb{F}_p)\mathscr{L}(E)\,\mathrm{gcd}_{E,3} & \text{if } \chi(N) \neq 1. \end{cases}$$

Clearly $\widetilde{\mathscr{L}}^+(E,\chi) \equiv 0 \mod 3$ when $\#E(\mathbb{F}_p) \equiv 0 \mod 3$. By Lemma 7.3, $\chi(N) = 1$ occurs either when $\#E(\mathbb{F}_p) \equiv 1 \bmod 3$ but p splits completely in K, or when $\#E(\mathbb{F}_p) \equiv 2 \bmod 3$ but p does not split completely in K, the only remaining case being when $\#E(\mathbb{F}_p) \equiv 1 \bmod 3$ and $\chi(N) \neq 1$. The first statement then follows by substituting the residues of $\#E(\mathbb{F}_p)$ modulo 3, and noting that $\mathrm{gcd}_{E,3}$ cancels out the factors in $\mathscr{L}(E)$ by definition. Now the description of the groups in Lemma 7.3 implies that $\#E(\mathbb{F}_p) \equiv \lambda \bmod 3$ occurs with the proportion of matrices $M \in \mathrm{SL}_2(\mathbb{Z}/3)$ with $\mathrm{tr}(M) = 2 - \lambda$, by Chebotarev's density theorem. If p splits completely in K, then $\mathrm{Fr}_p = 1$ in $\mathrm{PGL}_2(\mathbb{Z}/3)$, so that $\mathrm{Fr}_p = \pm 1$ in $\mathrm{GL}_2(\mathbb{Z}/3)$ and in $\mathrm{SL}_2(\mathbb{Z}/3)$, but the condition $\#E(\mathbb{F}_p) \equiv 1 \bmod 3$ forces $\mathrm{Fr}_p = -1$, which has trace 1. The final statement then follows by counting matrices in $\mathrm{SL}_2(\mathbb{Z}/3)$ with given trace. ■

Proposition 7.7 completely explains the numerical data by Kisilevsky–Nam for the elliptic curve 11a1 where $\mathrm{gcd}_{E,3} = 5$ and the elliptic curves 15a1 and 17a1 where $\mathrm{gcd}_{E,3} = 4$, all of which satisfy the assumptions of Proposition 7.7. Unfortunately, the same argument cannot explain the density patterns when $3 \mid \mathrm{gcd}_{E,3}$, such as for the remaining three elliptic curves 14a1, 19a1, and 37b1 considered by Kisilevsky–Nam, since Corollary 3.7 is a priori not valid modulo 9, as noted in Remark 3.9.

A Tables of Galois images

This section tabulates the mod-3 and 3-adic Galois images of elliptic curves E with restricted 3-torsion up to conjugacy, crucially used in Proposition 4.2 and Theorem 6.4. In both tables, the examples of elliptic curves are chosen so that it has the smallest conductor possible satisfying $L(E,1) \neq 0$ and $3 \mid c_0(E)$, but in general there are many elliptic curves with each prescribed mod-3 or 3-adic Galois image.

A.1 Mod-3 Galois images of elliptic curves without 3-torsion

The possible mod-3 Galois images are well-known [35, Theorem 1.2 and Propositions 1.14 and 1.16], and those of elliptic curves without 3-torsion are tabulated as follows. The subgroup labels and generators are taken from Sutherland [31, Section 6.4], and are viewed as elements of $\mathrm{GL}_2(\mathbb{Z}/3)$. The column $G_{E,3}$ lists the elements of $G_{E,3} = \mathrm{im}(\overline{\rho_{E,3}}) \cap \mathrm{SL}_2(\mathbb{Z}/3)$ as defined in Proposition 6.1, so that the residual densities can be read off directly in the column $\delta_{E,3}$ as ordered triples $(\delta_{E,3}(0), \delta_{E,3}(-b), \delta_{E,3}(b))$, where $b \in \mathbb{F}_3$ is the residue of $\mathrm{BSD}(E)$ modulo 3, which is used in Theorem 6.4. The final column E gives examples of elliptic curves E with the given mod-3 Galois image, with $b = 1$ in the first row and $b = 2$ in the second row.

$\mathrm{im}(\overline{\rho_{E,3}})$	$\mathrm{im}(\overline{\rho_{E,3}})$ generators	$G_{E,3}$	$\delta_{E,3}$	E
$\mathrm{GL}_2(\mathbb{Z}/3)$	$\left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 2 & 1 \\ 2 & 0 \end{smallmatrix}\right)$	$\mathrm{SL}_2(\mathbb{Z}/3)$	$\left(\frac{3}{8}, \frac{3}{8}, \frac{1}{4}\right)$	11a2, 11a1
3B.1.2	$\left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right)$	$(1, 0, 0)$	19a2, 14a3
3B	$\left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right),$ $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 2 & 1 \\ 0 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 2 & 2 \\ 0 & 2 \end{smallmatrix}\right)$	$\left(\frac{1}{2}, \frac{1}{2}, 0\right)$	50b3, 50b1
3Cs	$\left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right)$	$\left(\frac{1}{2}, \frac{1}{2}, 0\right)$	304e2, 304b2
3Nn	$\left(\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 2 & 1 \\ 2 & 2 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 1 \\ 1 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 2 \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right),$ $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 2 & 2 \\ 2 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 2 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 \\ 2 & 2 \end{smallmatrix}\right)$	$\left(\frac{1}{8}, \frac{1}{8}, \frac{3}{4}\right)$	704e1, 245b1
3Ns	$\left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 2 \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 2 \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 2 & 0 \end{smallmatrix}\right)$	$\left(\frac{1}{4}, \frac{1}{4}, \frac{1}{2}\right)$	1690d1, 338d1

The remaining two mod-3 Galois images 3B.1.1 and 3Cs.1.1 have 3-torsion, so the residual densities require finer information from their mod-9 Galois images.

A.2 3-adic Galois images of elliptic curves with 3-torsion

The possible 3-adic Galois images have been classified [25, Corollaries 1.3.1 and 12.3.3], and those of elliptic curves with 3-torsion are tabulated as follows. The subgroup labels and generators are taken from Rouse–Sutherland–Zureick-Brown [25, Software Repository], and are viewed as elements of $\mathrm{GL}_2(\mathbb{Z}/3^m)$ if their corresponding 3-adic Galois images are of the form $3^m.i.g.n$. The column $M_{E,3}$ gives matrices $M \in \mathrm{im}(\overline{\rho_{E,9}})$ such that $1 + \det(M) - \mathrm{tr}(M) = 3$, which is used in Proposition 4.2. The column $\#G_{E,9}$ lists the cardinalities of $G_{E,9}$ as defined in Proposition 6.1 for reference, but the residual densities are calculated separately in the column $\delta_{E,3}$ as ordered triples $(\delta_{E,3}(0), \delta_{E,3}(-b), \delta_{E,3}(b))$, where $b \in \mathbb{F}_3$ is the residue of $3\,\mathrm{BSD}(E)$ modulo 3, which is used in Theorem 6.4. The final column E gives examples of elliptic curves E with the given 3-adic Galois image, assuming they exist and are listed in the LMFDB, with $b = 1$ in the first row and $b = 2$ in the second row if it exists.

$\mathrm{im}(\rho_{E,3})$	$\mathrm{im}(\overline{\rho_{E,3}})$	$\mathrm{im}(\rho_{E,3})$ generators	$M_{E,3}$	$\#G_{E,9}$	$\delta_{E,3}$	E
3.8.0.1	3B.1.1	$\left(\begin{smallmatrix}1&2\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2\\0&2\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}4&0\\0&2\end{smallmatrix}\right)$	243	$\left(\frac{5}{9}, \frac{2}{9}, \frac{2}{9}\right)$	20a2, 20a1
3.24.0.1	3Cs.1.1	$\left(\begin{smallmatrix}2&0\\0&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}2&0\\0&4\end{smallmatrix}\right)$	81	$(1, 0, 0)$	26a1, 14a1
9.24.0.1	3B.1.1	$\left(\begin{smallmatrix}7&5\\0&8\end{smallmatrix}\right), \left(\begin{smallmatrix}1&8\\0&4\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}4&0\\0&2\end{smallmatrix}\right)$	81	$(1, 0, 0)$	189c3, 702e3
9.24.0.2	3B.1.1	$\left(\begin{smallmatrix}7&3\\0&8\end{smallmatrix}\right), \left(\begin{smallmatrix}7&2\\6&2\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}4&0\\0&2\end{smallmatrix}\right)$	81	$\left(\frac{1}{3}, \frac{2}{3}, 0\right)$	
9.72.0.1	3Cs.1.1	$\left(\begin{smallmatrix}5&6\\3&1\end{smallmatrix}\right), \left(\begin{smallmatrix}4&6\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}5&0\\0&1\end{smallmatrix}\right)$	N/A	27	$(1, 0, 0)$	54b1
9.72.0.2	3Cs.1.1	$\left(\begin{smallmatrix}8&3\\3&4\end{smallmatrix}\right), \left(\begin{smallmatrix}8&6\\0&4\end{smallmatrix}\right), \left(\begin{smallmatrix}1&3\\0&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}8&0\\0&4\end{smallmatrix}\right)$	27	$(1, 0, 0)$	54a1
9.72.0.3	3Cs.1.1	$\left(\begin{smallmatrix}8&3\\3&4\end{smallmatrix}\right), \left(\begin{smallmatrix}5&0\\0&7\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}2&0\\0&4\end{smallmatrix}\right)$	27	$(1, 0, 0)$	19a1, 7094c1
9.72.0.4	3Cs.1.1	$\left(\begin{smallmatrix}2&3\\6&7\end{smallmatrix}\right), \left(\begin{smallmatrix}1&6\\6&1\end{smallmatrix}\right), \left(\begin{smallmatrix}4&3\\6&4\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}5&0\\0&4\end{smallmatrix}\right)$	27	$(1, 0, 0)$	
9.72.0.5	3B.1.1	$\left(\begin{smallmatrix}1&2\\0&8\end{smallmatrix}\right), \left(\begin{smallmatrix}1&7\\0&4\end{smallmatrix}\right)$	N/A	27	$(1, 0, 0)$	54b3
9.72.0.6	3B.1.1	$\left(\begin{smallmatrix}1&5\\0&8\end{smallmatrix}\right), \left(\begin{smallmatrix}4&1\\0&8\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}4&0\\0&8\end{smallmatrix}\right)$	27	$(1, 0, 0)$	
9.72.0.7	3B.1.1	$\left(\begin{smallmatrix}4&4\\0&5\end{smallmatrix}\right), \left(\begin{smallmatrix}1&0\\0&8\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}4&0\\0&5\end{smallmatrix}\right)$	27	$(1, 0, 0)$	
9.72.0.8	3B.1.1	$\left(\begin{smallmatrix}7&7\\6&4\end{smallmatrix}\right), \left(\begin{smallmatrix}7&7\\6&2\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&2\\3&1\end{smallmatrix}\right)$	27	$\left(\frac{1}{3}, \frac{2}{3}, 0\right)$	
9.72.0.9	3B.1.1	$\left(\begin{smallmatrix}4&2\\3&5\end{smallmatrix}\right), \left(\begin{smallmatrix}1&3\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}7&2\\3&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}4&1\\0&5\end{smallmatrix}\right)$	27	$\left(\frac{1}{3}, \frac{2}{3}, 0\right)$	

$\mathrm{im}(\rho_{E,3})$	$\mathrm{im}(\overline{\rho_{E,3}})$	$\mathrm{im}(\rho_{E,3})$ generators	$M_{E,3}$	$\#G_{E,9}$	$\delta_{E,3}$	E
9.72.0.10	3B.1.1	$\left(\begin{smallmatrix}1&5\\6&5\end{smallmatrix}\right), \left(\begin{smallmatrix}1&0\\0&8\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}4&0\\0&8\end{smallmatrix}\right)$	27	$\left(\frac{1}{3}, \frac{2}{3}, 0\right)$	486c1
27.72.0.1	3B.1.1	$\left(\begin{smallmatrix}7&23\\0&5\end{smallmatrix}\right), \left(\begin{smallmatrix}1&8\\9&16\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}4&0\\0&2\end{smallmatrix}\right)$	81	$(1, 0, 0)$	
27.648.13.25	3B.1.1	$\left(\begin{smallmatrix}16&4\\0&16\end{smallmatrix}\right), \left(\begin{smallmatrix}1&17\\0&26\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}4&0\\0&5\end{smallmatrix}\right)$	27	$(1, 0, 0)$	N/A
27.648.18.1	3B.1.1	$\left(\begin{smallmatrix}16&15\\9&25\end{smallmatrix}\right), \left(\begin{smallmatrix}10&16\\9&17\end{smallmatrix}\right), \left(\begin{smallmatrix}7&22\\6&4\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}4&1\\0&5\end{smallmatrix}\right)$	27	$\left(\frac{1}{3}, \frac{2}{3}, 0\right)$	108a1, 36a1
27.1944.55.31	3Cs.1.1	$\left(\begin{smallmatrix}2&18\\12&25\end{smallmatrix}\right), \left(\begin{smallmatrix}16&18\\21&16\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}5&0\\0&4\end{smallmatrix}\right)$	9	$(1, 0, 0)$	N/A
27.1944.55.37	3Cs.1.1	$\left(\begin{smallmatrix}17&6\\21&10\end{smallmatrix}\right), \left(\begin{smallmatrix}2&3\\3&25\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}5&0\\3&4\end{smallmatrix}\right)$	9	$(1, 0, 0)$	27a1
27.1944.55.43	3B.1.1	$\left(\begin{smallmatrix}19&10\\18&8\end{smallmatrix}\right), \left(\begin{smallmatrix}4&11\\3&16\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}4&4\\0&5\end{smallmatrix}\right)$	9	$\left(\frac{1}{3}, \frac{2}{3}, 0\right)$	243b1
27.1944.55.44	3B.1.1	$\left(\begin{smallmatrix}10&23\\3&13\end{smallmatrix}\right), \left(\begin{smallmatrix}13&13\\0&14\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}4&4\\0&5\end{smallmatrix}\right)$	9	$\left(\frac{1}{3}, \frac{2}{3}, 0\right)$	N/A

Remark A.1 Many of the 3-adic Galois images seemingly do not represent any elliptic curves with $b \neq 0$, in the sense that a search through the LMFDB yields no examples satisfying $L(E, 1) \neq 0$ and $3 \mid c_0(E)$, but current results a priori do not rule out their existence. To rule out examples for a specific 3-adic Galois image, one could consider the explicit family of Weierstrass equations parameterized by the associated modular curve, and then investigate the divisibility of local Tamagawa numbers as in Lemma 4.1, but this will not be explored here. Note that this is the case for the last six 3-adic Galois images arising from elliptic curves with complex multiplication, where their associated modular curves have effectively computable finite sets of rational points.

Acknowledgements I would like to thank Vladimir Dokchitser for suggesting the problem and guidance throughout the project. I would also like to thank Peiran Wu and Jacob Fjeld Grevstad for assistance on some group theory arguments, as well as Harry Spencer and the four anonymous reviewers for feedback on prior drafts.

References

[1] A. Barrios and M. Roy, *Local data of rational elliptic curves with nontrivial torsion*. Pacific J. Math. **318**(2022), no. 1, 1–42.

[2] W. Bley, *The equivariant Tamagawa number conjecture and modular symbols*. Math. Ann. **356**(2013), no. 1, 179–190.

[3] C. Bonnafé, *Representations of* $\mathrm{SL}_2(\mathbb{F}_q)$, volume 13 of Algebra and Applications, Springer-Verlag London, Ltd., London, 2011.

[4] T. Bouganis and V. Dokchitser, *Algebraicity of L-values for elliptic curves in a false Tate curve tower*. Math. Proc. Cambridge Philos. Soc. **142**(2007), no. 2, 193–204.

[5] D. Burns and D. M. Castillo, *On refined conjectures of Birch and Swinnerton-Dyer type for Hasse–Weil–Artin L-series*. Mem. Amer. Math. Soc. **297**(2024), no. 1482, v+156.

[6] A. Burungale, F. Castella, and C. Skinner, *Base change and Iwasawa main conjectures for* GL_2. Preprint, 2025.

[7] A. Burungale, C. Skinner, and Y. Tian, *The Birch and Swinnerton-Dyer conjecture: a brief survey*. In: A. Kechris, N. Makarov, D. Ramakrishnan and X. Zhu (eds.), Nine mathematical

challenges—An elucidation, volume 104 of Proceedings of Symposia in Pure Mathematics, American Mathematical Society, Providence, RI, 2021, pp. 11–29.

[8] A. Burungale, C. Skinner, Y. Tian, and X. Wan, *Zeta elements for elliptic curves and applications*. Preprint, 2024.

[9] D. Byeon, T. Kim, and D. Yhee, *A conjecture of Gross and Zagier: case* $E(\mathbb{Q})_{tor} \cong \mathbb{Z}/3\mathbb{Z}$. Int. J. Number Theory **15**(2019), no. 9, 1793–1800.

[10] K. Česnavičius, *The Manin constant in the semistable case*. Compos. Math. **154**(2018), no. 9, 1889–1920.

[11] J. Cremona, *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, 1992.

[12] V. Dokchitser, R. Evans, and H. Wiersema, *On a BSD-type formula for L-values of Artin twists of elliptic curves*. J. Reine Angew. Math. [Crelle's Journal], **773**(2021), 199–230.

[13] B. Edixhoven, *On the Manin constants of modular elliptic curves*. In: G. van der Geer, F. Oort and J. Steenbrink (eds.), *Arithmetic algebraic geometry (Texel, 1989)*, volume 89 of Progress in Mathematics, Birkhäuser, Boston, MA, 1991, pp. 25–39.

[14] J. Fearnley, H. Kisilevsky, and M. Kuwata, *Vanishing and non-vanishing Dirichlet twists of L-functions of elliptic curves*. J. London Math. Soc. Second Ser. **86**(2012), no. 2, 539–557.

[15] B. Gross and D. Zagier, *Heegner points and derivatives of L-series*. Invent. Math. **84**(1986), no. 2, 225–320.

[16] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms*. Astérisque **295**(2004), 117–290.

[17] T. Keller and M. Yin, *On the anticyclotomic Iwasawa theory of newforms at Eisenstein primes of semistable reduction*. Preprint, 2024.

[18] H. Kisilevsky and J. Nam, *Non-zero central values of Dirichlet twists of elliptic L-functions*. J. Number Theory **266**(2025), 166–194.

[19] V. Kolyvagin, *Finiteness of* $E(\mathbb{Q})$ *and* $Ш(E, \mathbb{Q})$ *for a subclass of Weil curves*. Izv. Akad. Nauk SSSR. Ser. Mat. **52**(1988), no. 3, 522–540.670–671.

[20] D. Lorenzini, *Torsion and Tamagawa numbers. Université de Grenoble*. Ann. Inst. Fourier **61**(2011), no. 5, 1995–2037.

[21] C. Maistret and H. Shukla, *On the factorization of twisted L-values and* 11*-descents over* C_5*-number fields*. Preprint, 2025.

[22] J. I. Manin, *Parabolic points and zeta functions of modular curves*. Izv. Akad. Nauk SSSR. Ser. Mat. **36**(1972), 19–66.

[23] M. Melistas, *A divisibility related to the Birch and Swinnerton-Dyer conjecture*. J. Number Theory **245**(2023), 150–168.

[24] O. Neumann, *Elliptische kurven mit vorgeschriebenem reduktionsverhalten. I*. Math. Nachr. **49**(1971), 107–123.

[25] J. Rouse, A. Sutherland, and D. Zureick-Brown, *ℓ-adic images of Galois for elliptic curves over* $\mathbb{Q}$ *(and an appendix with John Voight)*. Forum Math. Sigma **10**(2022), Paper No. e62.63.

[26] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*. Invent. Math. **15**(1972), no. 4, 259–331.

[27] B. Setzer, *Elliptic curves of prime conductor*. J. London Math. Soc. Second Ser. **10**(1975), 367–378.

[28] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, volume No. 1 of Kanô Memorial Lectures, Publications of the Mathematical Society of Japan, 11, Iwanami Shoten Publishers, Tokyo; Princeton University Press, Princeton, NJ, 1971.

[29] C. Skinner and E. Urban, *The Iwasawa main conjectures for* GL_2. Invent. Math. **195**(2014), no. 1, 1–277.

[30] G. Stevens, *Stickelberger elements and modular parametrizations of elliptic curves*. Invent. Math. **98**(1989), no. 1, 75–106.

[31] A. Sutherland, *Computing images of Galois representations attached to elliptic curves*. Forum Math. Sigma **4**(2016), Paper No. e4. 79.

[32] T. L. Collaboration, *The L-functions and modular forms database*.

[33] H. Wiersema and C. Wuthrich, *Integrality of twisted L-values of elliptic curves*. Doc. Math. **27**(2022), 2041–2066.

[34] A. Wiles, *The Birch and Swinnerton-Dyer conjecture*. In: J. Carlson, A. Jaffe and A. Wiles (eds.), The millennium prize problems. Clay Mathematics Institute, Cambridge, MA, 2006, pp. 31–41.

[35] D. Zywina, *On the possible images of the mod ell representations associated to elliptic curves over Q*. Preprint, 2015.

Department of Mathematics, University College London, London School of Geometry and Number Theory, London, United Kingdom
e-mail: ucahdka@ucl.ac.uk