

# L-values of elliptic curves twisted by cubic characters

David Kurniadi Angdinata

August 13, 2024

## 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  $\chi$  of order  $q$ , and in many cases its associated central modified L-value  $\mathcal{L}(E, \chi)$  is known to be integral. This paper derives some arithmetic consequences from a congruence between  $\mathcal{L}(E, 1)$  and  $\mathcal{L}(E, \chi)$  arising from this integrality, with an emphasis on cubic characters  $\chi$ . These include  $q$ -adic valuations of the denominator of  $\mathcal{L}(E, 1)$ , determination of  $\mathcal{L}(E, \chi)$  in terms of Birch–Swinnerton-Dyer invariants, and asymptotic densities of  $\mathcal{L}(E, \chi)$  modulo  $q$  by varying  $\chi$ .

## Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
<b>2</b>	<b>Background and conventions</b>	<b>4</b>
<b>3</b>	<b>Modular symbols</b>	<b>6</b>
<b>4</b>	<b>Denominators of L-values</b>	<b>8</b>
<b>5</b>	<b>Units of twisted L-values</b>	<b>10</b>
<b>6</b>	<b>Residual densities of twisted L-values</b>	<b>12</b>
<b>7</b>	<b>Twisted L-values of Kisilevsky–Nam</b>	<b>14</b>
<b>A</b>	<b>Tables of Galois images</b>	<b>16</b>

## 1 Introduction

The Hasse–Weil L-function  $L(E, s)$  of an elliptic curve  $E$  over  $\mathbb{Q}$  can be twisted by a primitive Dirichlet character  $\chi$  to get a twisted L-function  $L(E, \chi, s)$ . The algebraic and analytic properties of these L-functions are studied extensively in the literature, and they are the subject of many problems in the arithmetic of elliptic curves. When  $E$  is base changed to a cyclotomic extension  $K$  of  $\mathbb{Q}$ , Artin’s formalism for L-functions says that  $L(E/K, s)$  decomposes into a product of  $L(E, \chi, s)$  over all Dirichlet characters  $\chi$  that factor through  $K$ , so the behaviour of  $L(E/K, s)$  is completely governed by  $L(E, \chi, s)$ .

The special value of  $L(E, \chi, s)$  at  $s = 1$  can be normalised by periods to get an modified twisted L-value  $\mathcal{L}(E, \chi)$  (see Section 2). Classically, the Birch–Swinnerton-Dyer conjecture relates  $\mathcal{L}(E, 1)$  to certain algebraic invariants that encode important global arithmetic information of  $E$ . In contrast, there seems to be a barrier in formulating the analogous refined conjecture for  $\mathcal{L}(E, \chi)$  when  $\chi$  is non-trivial, with concrete examples of arithmetically identical elliptic curves with twisted L-values that differ by a unit [DEW21, Section 4]. Having such a formula would present non-trivial 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 seem to be intractable with classical techniques for Selmer groups [DEW21, Section 3].

Prominent existing techniques to study the  $\ell$ -primary parts of Selmer groups, such as via the main conjecture of Iwasawa theory, only gives a description of the ideal  $I$  generated by  $\mathcal{L}(E, \chi)$ , rather than its actual value. For instance, 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 [BC21, Proposition 7.3]. More concretely, Dokchitser–Evans–Wiersema expressed its norm in terms of the positive square roots of the Birch–Swinnerton-Dyer quotients  $\text{BSD}(E)$  and  $\text{BSD}(E/K)$  (see Section 2), where  $K$  is the number field cut out by  $\chi$  [DEW21, Theorem 38].

This paper completely determines the actual value of  $\mathcal{L}(E, \chi)$  for cubic Dirichlet characters of prime conductor, under fairly generic assumptions on the Manin constants  $c_0(E)$  and  $c_1(E)$ . The following result is proven in Section 5, where the phenomena observed by Dokchitser–Evans–Wiersema is also explained.

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

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

where the sign  $u = \pm 1$  is such that

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

On the analytic side, in their paper on an analogue of the Brauer–Siegel theorem for elliptic curves over cyclic extensions, Kisilevsky–Nam observed some patterns in the asymptotic distribution of  $\mathcal{L}(E, \chi)$  [KN22, Section 7]. They considered six elliptic curves  $E$  and five positive integers  $q$ , and numerically computed the norms of  $\mathcal{L}(E, \chi)$  for primitive Dirichlet characters  $\chi$  of conductor  $p$  and order  $q$ , where  $(E, q)$  ranges over the thirty pairs and  $p$  ranges over millions of positive integers. For each pair  $(E, q)$ , they added a normalisation factor to  $\mathcal{L}(E, \chi)$  to obtain a real value  $\mathcal{L}^+(E, \chi)$ , and empirically determined the greatest common divisor  $\text{gcd}_{E,q}$  of the norms of  $\mathcal{L}^+(E, \chi)$  by varying over all  $p$ . Upon dividing these norms by  $\text{gcd}_{E,q}$  to get an integer  $\tilde{\mathcal{L}}^+(E, \chi)$ , they observed that these integers have unexpected biases when reduced modulo  $q$ .

This paper 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 in Section 7 under slightly relaxed assumptions, where the normalisation for  $\mathcal{L}^+(E, \chi)$  is also defined.

**Theorem 1.2** (Proposition 7.5). *Let  $E$  be an elliptic curve over  $\mathbb{Q}$  of conductor  $N$  and discriminant  $\Delta = \pm N^n$  for some  $3 \nmid n$  with no rational 3-isogeny, such that  $3 \nmid c_0(E)$  and  $3 \nmid \text{gcd}_{E,3}$ , and let  $\chi$  be a cubic Dirichlet character of odd prime conductor  $p \nmid N$ . Then*

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

To put things in better perspective, these biases can be quantified asymptotically by considering the natural densities of  $\mathcal{L}(E, \chi)$  when reduced modulo  $q$ . More precisely, let  $X_{E,q}^{\leq n}$  be the set of Dirichlet characters of order  $q$  and odd prime conductor less than  $n$  that does not divide the conductor of  $E$ . Now define the residual densities  $\delta_{E,q}$  of  $\mathcal{L}(E, \chi)$  to be the natural densities of  $\mathcal{L}(E, \chi)$  modulo  $(1 - \zeta_q)$ , or in other words

$$\delta_{E,q}(\lambda) := \lim_{n \rightarrow \infty} \frac{\#\{\chi \in X_{E,q}^{\leq n} \mid \mathcal{L}(E, \chi) \equiv \lambda \pmod{(1 - \zeta_q)}\}}{\#X_{E,q}^{\leq n}}, \quad \lambda \in \mathbb{F}_q.$$

It turns out that such a limit always exists, and its value for any  $\lambda \in \mathbb{F}_q$  only depends on  $\text{BSD}(E)$ , the torsion subgroup  $\text{tor}(E)$ , and the mod-9 Galois image  $\text{im}(\overline{\rho}_{E,9})$ . The following result classifies the possible ordered triples  $(\delta_{E,3}(0), \delta_{E,3}(1), \delta_{E,3}(2))$  of residual densities for cubic Dirichlet characters.

**Theorem 1.3** (Theorem 6.4). *Let  $E$  be an elliptic curve over  $\mathbb{Q}$  such that  $3 \nmid c_0(E)$  and  $L(E, 1) \neq 0$ . Assume that the Birch–Swinnerton-Dyer conjecture holds. Then the ordered triple  $(\delta_{E,3}(0), \delta_{E,3}(1), \delta_{E,3}(2))$  only depends on  $\text{BSD}(E)$  and on  $\text{im}(\overline{\rho_{E,9}})$ , and can only be one of*

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

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

*In particular, the ordered triple  $(\delta_{E,3}(0), \delta_{E,3}(1), \delta_{E,3}(2))$  can be precisely determined as follows.*

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

Note that the aforementioned normalisation factors for twisted L-values are not present here, so the resulting ordered triples of 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 fact that  $\text{ord}_3(\text{BSD}(E)) \geq -1$ , which might be interesting as a standalone result. In a seminal paper quantifying the cancellations between  $\text{tor}(E)$  and the Tamagawa product  $\text{Tam}(E)$ , Lorenzini proved that if  $\ell \mid \#\text{tor}(E)$  for some prime  $\ell > 3$ , then  $\ell \mid \text{Tam}(E)$  with finitely many explicit exceptions [Lor11, Proposition 1.1]. In particular, when  $E$  has analytic rank zero, the denominator  $\#\text{tor}(E)^2$  of the rational number  $\text{BSD}(E)$  necessarily shares a factor with  $\text{Tam}(E)$  in its numerator, so  $\text{ord}_\ell(\text{BSD}(E)) \geq -1$  for any prime  $\ell > 3$ . On the other hand, he noted that there are explicit families with  $\#\text{tor}(E) = 3$  without any cancellation [Lor11, Lemma 2.26], another family of which was given by Barrios–Roy [BR22, Corollary 5.1]. Subsequently, Melistas showed that these cancellations may instead occur between  $\text{tor}(E)$  and the Tate–Shafarevich group  $\text{III}(E)$  in the numerator of  $\text{BSD}(E)$ , and hence  $\text{ord}_3(\text{BSD}(E)) \geq -1$ , except possibly for certain reduction types [Mel23, Theorem 1.4]. He then observed that there are again explicit exceptions, and in all these exceptions  $c_0(E) = 3$  [Mel23, Example 3.8], but did not explain this coincidence. The following result gives a lower bound for the odd part of the denominator of Birch–Swinnerton-Dyer quotients for elliptic curves with analytic rank zero.

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

Section 4 states this result in terms of  $\mathcal{L}(E, 1)$  and proves it in slightly larger generality. It is worth noting that this is related to the Gross–Zagier conjecture for  $\#\text{tor}(E) = 3$  proven by Byeon–Kim–Yhee [BKY19, 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  $\mathcal{L}(E, 1)$  instead.

The methods in this paper rely on the fact that  $\mathcal{L}(E, \chi) \in \mathbb{Z}[\zeta_q]$  for non-trivial primitive Dirichlet characters  $\chi$  of order  $q$ , which was proven by Wiersema–Wuthrich under some mild hypotheses by expressing  $\mathcal{L}(E, \chi)$  in terms of Manin’s modular symbols [WW22, Theorem 2]. Parts of their argument can be adapted to obtain an explicit congruence between  $\mathcal{L}(E, \chi)$  and  $\mathcal{L}(E, 1)$  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.

## Acknowledgements

I thank Vladimir Dokchitser for suggesting the problem and guidance throughout. I thank Harry Spencer and an anonymous reviewer for feedback on a prior draft. I thank Peiran Wu and Jacob Fjeld Grevstad for assistance on some of the group theory arguments. 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.

## 2 Background and conventions

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

For a primitive  $n$ -th root of unity  $\zeta_n$ , the ring of integers of the cyclotomic field  $\mathbb{Q}(\zeta_n)$  will be denoted  $\mathbb{Z}[\zeta_n]$ , and denote the associated norm map by  $\text{Nm}_n : \mathbb{Q}(\zeta_n) \rightarrow \mathbb{Q}$ . The ring of integers of its maximal totally real subfield  $\mathbb{Q}(\zeta_n)^+$  will be denoted  $\mathbb{Z}[\zeta_n]^+$ , and denote the associated norm map by  $\text{Nm}_n^+ : \mathbb{Q}(\zeta_n)^+ \rightarrow \mathbb{Q}$ . The isomorphism  $(\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\sim} \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$  from class field theory 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 special linear group, the general linear group, and the projective linear group respectively by

$$\text{SL}(n) := \text{SL}_2(\mathbb{Z}/n\mathbb{Z}), \quad \text{GL}(n) := \text{GL}_2(\mathbb{Z}/n\mathbb{Z}), \quad \text{PGL}(n) := \text{PGL}_2(\mathbb{Z}/n\mathbb{Z}).$$

For a matrix  $M$  in such a matrix group, its trace will be denoted  $\text{tr}(M)$  and its determinant will be denoted  $\det(M)$ . For a prime  $\ell$ , the following table groups the conjugacy classes of  $\text{SL}(\ell)$  by trace [Bon11, Table 1.1 and Exercise 1.4], which will be useful for Theorem 4.4 and Proposition 6.1.

Representative	Number of classes	Order	Cardinality	Trace
$\begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix},$ $z \in \mathbb{F}_\ell$	one for each symbol $\left(\frac{z}{\ell}\right)$ , for a total of 3 classes	$\ell^{ \left(\frac{z}{\ell}\right) }$	$\left(\frac{\ell^2-1}{2}\right)^{ \left(\frac{z}{\ell}\right) }$	2
$\begin{pmatrix} -1 & z \\ 0 & -1 \end{pmatrix},$ $z \in \mathbb{F}_\ell$	one for each symbol $\left(\frac{z}{\ell}\right)$ , for a total of 3 classes	$2q^{ \left(\frac{z}{\ell}\right) }$	$\left(\frac{\ell^2-1}{2}\right)^{ \left(\frac{z}{\ell}\right) }$	$\ell - 2$
$\begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix},$ $x \in \mathbb{F}_\ell^\times \setminus \{\pm 1\}$	one for each pair $\{x, x^{-1}\}$ , for a total of $\frac{\ell-3}{2}$ classes	order of $x$	$\ell(\ell + 1)$	$x + x^{-1}$
$\begin{pmatrix} \frac{1}{2}(\xi + \xi^\ell) & \frac{\zeta}{2}(\xi - \xi^\ell) \\ \frac{1}{2\zeta}(\xi - \xi^\ell) & \frac{1}{2}(\xi + \xi^\ell) \end{pmatrix},$ $\xi \in (\mathbb{F}_{\ell^2}^\times / \mathbb{F}_\ell^\times) \setminus \{\pm 1\}$	one for each pair $\{\xi, \xi^{-1}\}$ , for a total of $\frac{\ell-1}{2}$ classes	order of $\xi$	$\ell(\ell - 1)$	$\xi + \xi^\ell$

Here,  $\zeta$  is a fixed element of  $\mathbb{F}_{\ell^2}^\times$  satisfying  $\zeta + \zeta^\ell = 0$ , and  $\left(\frac{z}{\ell}\right)$  is the Legendre symbol modulo  $\ell$  given by

$$\left(\frac{z}{\ell}\right) := \begin{cases} 1 & \text{if } z \text{ is a quadratic residue modulo } \ell \\ 0 & \text{if } \ell \mid z \\ -1 & \text{if } z \text{ is a quadratic nonresidue modulo } \ell \end{cases}.$$

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 [Cre92, Table 1]. For a prime  $\ell$ , the  $\mathbb{Z}_\ell$ -representation associated to the  $\ell$ -adic Tate module of  $E$  is denoted  $\rho_{E,\ell}$ , and its  $\ell$ -adic Galois image  $\text{im}(\rho_{E,\ell})$  will be given by its Rouse–Sutherland–Zureick–Brown label as a subgroup of  $\text{GL}_2(\mathbb{Z}_\ell)$  up to conjugacy [RSZB22, Section 2.4]. For any  $n \in \mathbb{N}$ , the projection of  $\rho_{E,\ell}$  onto  $\text{GL}(\ell^n)$  is denoted  $\overline{\rho_{E,\ell^n}}$ , and its mod- $\ell^n$  Galois image  $\text{im}(\overline{\rho_{E,\ell^n}})$  will be given by its Sutherland label as a subgroup of  $\text{GL}(\ell^n)$  up to conjugacy [Sut16, Section 6.4]. Note that if  $\text{Fr}_v$  is an arithmetic Frobenius at a prime  $v \neq \ell$ , then

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

Let  $\omega_E$  denote a global invariant differential on a minimal Weierstrass equation of  $E$ . Let  $X_0(N)$  denote the modular curve associated to the congruence subgroup  $\Gamma_0(N)$ , 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  $\phi_E : X_0(N) \rightarrow E$  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 define two differentials on  $X_0(N)$ , namely  $2\pi i f_E(z) dz$  and the pullback  $\phi_E^* \omega_E$ , which are related by

$$\phi_E^* \omega_E = \pm c_0(E) 2\pi i f_E(z) dz,$$

where  $c_0(E)$  is a positive integer called the Manin constant [Edi91, Proposition 2].

When  $E$  is  $\Gamma_0(N)$ -optimal in its isogeny class, it is conjectured that  $c_0(E) = 1$ , and this was recently proven for semistable  $E$  [Č18, Theorem 1.2], but it is certainly possible that  $c_0(E) \neq 1$  in general. Nevertheless, every modular parameterisation by  $X_0(N)$  factors through a modular parameterisation by the modular curve  $X_1(N)$  associated to the congruence subgroup  $\Gamma_1(N)$  [Ste89, Theorem 1.9], and an analogous construction using  $X_1(N)$  yields the Manin constant  $c_1(E)$  with the following conjecture.

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

The L-function  $L(E, s)$  of  $E$  is defined to be the 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 representation associated to  $\rho_{E,\ell}$  for some prime number  $\ell \neq v$ . Here, for a complex representation  $\rho$ , the local Euler factors are given by  $L_v(\rho, T) := \det(1 - T \cdot \text{Fr}_v^{-1} | \rho^{I_v})$ , where  $\rho^{I_v}$  is the subrepresentation of  $\rho$  fixed by the inertia subgroup  $I_v$  at  $v$ . The modularity theorem says that  $L(E, s)$  is the Hecke L-function of  $f_E$ , so its order of vanishing at  $s = 1$  is well-defined.

The Birch–Swinnerton-Dyer conjecture predicts this order of vanishing and its leading term in terms of arithmetic invariants as follows. Let  $\text{tor}(E)$  and  $\text{rk}(E)$  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  $\text{Tam}(E)$  denote the Tamagawa product of local Tamagawa numbers  $\text{Tam}_v(E)$  at each prime  $v$ . Let  $\text{Reg}(E)$  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  $\text{III}(E)$  denote the Tate–Shafarevich group, which is implicitly assumed to be finite in this paper.

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

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

Here, the left hand side is the modified L-value of  $E$ , which will be denoted  $\mathcal{L}(E)$ , and the right hand side is the Birch–Swinnerton-Dyer quotient of  $E$ , which will be denoted  $\text{BSD}(E)$ . By the combined works of Gross–Zagier [GZ86, Theorem 7.3] and Kolyvagin [Kol88, Corollary 2], it is known that  $L(E, 1) \neq 0$  implies that  $\text{rk}(E) = 0$  and  $\text{III}(E)$  is finite. In this setting,  $\text{BSD}(E)$  is clearly rational since  $\text{Reg}(E) = 1$ , and Proposition 3.3 shows that  $\mathcal{L}(E)$  is also rational. If  $\text{ord}_\ell : \mathbb{Q} \rightarrow \mathbb{Z} \cup \{\infty\}$  denotes the  $\ell$ -adic valuation for some prime  $\ell$ , the conjecture that  $\text{ord}_\ell(\mathcal{L}(E)) = \text{ord}_\ell(\text{BSD}(E))$  is called the  $\ell$ -part of the Birch–Swinnerton-Dyer conjecture. For the base change  $E/K$  of  $E$  to an extension  $K$  of  $\mathbb{Q}$ , the analogous quantities  $\mathcal{L}(E/K)$  and  $\text{BSD}(E/K)$  can be defined as in the paper by Dokchitser–Evans–Wiersema [DEW21, Section 1.5].

Throughout, a **character** will always refer to a non-trivial even primitive Dirichlet character  $\chi$  of prime conductor  $p \nmid N$  and order  $q > 1$ , which automatically means that  $\chi(-1) = 1$  and  $p \equiv 1 \pmod{q}$ . The L-function  $L(E, \chi, s)$  of  $E$  twisted by  $\chi$  is defined to be the Euler product of  $L_v(\rho_{E,\ell}^\vee \otimes \bar{\chi}, v^{-s})^{-1}$  over all primes  $v$ , so that in particular  $\mathcal{L}(E, 1) = \mathcal{L}(E)$ . The modularity theorem says that  $L(E, \chi, s)$  is the Hecke L-function of a weight two cusp form of level  $\Gamma_0(N)$  twisted by  $\chi$  [Shi71, Theorem 3.66], so its order of vanishing  $r$  at  $s = 1$  is again well-defined. When  $L(E, \chi, 1) \neq 0$ , Kato showed that  $\text{rk}(E) = \text{rk}(E/K)$  and  $\text{III}(E/K)$  is finite [Kat04, Corollary 14.3]. The analogous modified twisted L-value is given by

$$\mathcal{L}(E, \chi) := \lim_{s \rightarrow 1} \frac{L(E, \chi, s)}{(s-1)^r} \cdot \frac{p}{\tau(\chi) \Omega(E)},$$

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

**Remark 2.3.** The definitions of L-values and Birch–Swinnerton-Dyer invariants in this section agree with those in Wiersema–Wuthrich [WW22, Section 7] and those in Dokchitser–Evans–Wiersema [DEW21, Section 1.5] whenever  $L(E, \chi, 1) \neq 0$ , except for one notable difference for twisted L-functions due to the choice of normalisation in class field theory. In this paper, the Dirichlet series of  $L(E, \chi, s)$  is  $\sum_{n=1}^{\infty} \chi(n) a_n(E) n^{-s}$ , and  $\mathcal{L}(E, \chi)$  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  $L(E, \bar{\chi}, s)$  instead of  $L(E, \chi, s)$ . However, their modified twisted L-value is defined using the motivic definition, so it coincides with  $\mathcal{L}(E, \bar{\chi})$  instead of  $\mathcal{L}(E, \chi)$ . Dokchitser–Evans–Wiersema follows the motivic convention, so their twisted L-functions and modified twisted L-values coincide with  $L(E, \bar{\chi}, s)$  and  $\mathcal{L}(E, \bar{\chi})$  respectively.

### 3 Modular symbols

This section recalls some classical facts on modular symbols. Most of the arguments here are well-known since the time of Manin [Man72], with a few recent integrality results by Wiersema–Wuthrich [WW22], 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 [FKK12, Theorem 3.5], and is essentially equivalent to the equivariant Tamagawa number conjecture as shown by Bley [Ble13, Section 2].

Let  $N \in \mathbb{N}$ . The congruence subgroup  $\Gamma_0(N)$  acts on the extended upper half plane  $\mathcal{H}$  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  $X_0(N) = \mathcal{H}/\Gamma_0(N)$ , which defines an integral homology class  $\gamma \in H_1(X_0(N), \mathbb{Z})$ . This is independent of the smooth path chosen because  $\mathcal{H}$  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  $2\pi i f(z) dz$  on  $X_0(N)$ , and integrating this over the closed path  $\gamma$  gives a complex number  $\int_\gamma 2\pi i f(z) dz$  called a **modular symbol**. A general definition for paths with arbitrary endpoints is given by Manin [Man72, Section 1.2], but for the purposes of this paper, it suffices to consider the modular symbol associated to the path from 0 to cusps  $c \in \mathbb{Q} \cup \{\infty\}$ . When the denominator of  $c \in \mathbb{Q}$  is coprime to  $N$ , the image of any smooth path between 0 and  $c$  is closed [Man72, Proposition 2.2], so it makes sense to write

$$\mu_f(c) := \int_0^c 2\pi i f(z) dz \in \mathbb{C}.$$

The key example for  $f$  will be the normalised cuspidal eigenform  $f_E \in S_2(N)$  associated to an elliptic curve  $E$  of conductor  $N$ . In this case, it turns out that  $\mathcal{L}(E)$ , as well as  $\mathcal{L}(E, \chi)$  for any character  $\chi$  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  $N \in \mathbb{N}$ , and let  $f \in S_2(N)$ . 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 similar to the proof in Wiersema–Wuthrich [WW22, 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 smooth path between  $-c$  and  $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot (-c)$ , which is zero [Man72, Proposition 1.4], so  $\mu_f(1-c) = \mu_f(-c)$ . The change of variables  $z \mapsto -\bar{z}$  then transforms  $\mu_f(-c)$  into  $\overline{\mu_f(c)}$ , so 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  $\frac{1}{2} \Omega(E) \cdot \mathbb{Z}$ . The second statement then follows from the first statement.  $\square$

**Remark 3.2.** When the denominator of  $c \in \mathbb{Q}$  is coprime to  $N$ , these modular symbols  $\mu_E(c)$  coincide precisely with the modular symbols  $\mu(c)$  defined in Wiersema–Wuthrich [WW22, Section 2].

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

$$\mu_E^\pm(c) := \frac{c_0(E)}{\Omega(E)} (\mu_E(c) + \mu_E(1-c)) \in \mathbb{Z}.$$

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

**Proposition 3.3.** *Let  $E$  be an elliptic curve of conductor  $N$  not divisible by an odd prime  $v$ . Then*

$$c_0(E) \mathcal{L}(E) \# E(\mathbb{F}_v) = \sum_{a=1}^{\lfloor \frac{v-1}{2} \rfloor} \mu_E^\pm\left(\frac{a}{v}\right).$$

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

*Proof.* The first statement is precisely the Hecke action [Man72, Theorem 4.2] up to a factor of  $c_0(E)^{-1} \Omega(E)$ . Integrality then follows immediately from Lemma 3.1 and the first statement.  $\square$

**Remark 3.4.** The assumption that  $v \nmid N$  is crucial. Removing this may cause integrality to fail, such as for the elliptic curve 11a1 where  $c_0(E) = 1$  and  $\mathcal{L}(E) = \frac{1}{5}$ , but  $a_{11}(E) = 1$  and  $\sigma_1(11) = 12$ .

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

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

$$c_0(E) \mathcal{L}(E, \chi) = \sum_{a=1}^{\lfloor \frac{p-1}{2} \rfloor} \overline{\chi(a)} \mu_E^{\pm}\left(\frac{a}{p}\right).$$

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

*Proof.* This is identical to the proof in Wiersema–Wuthrich [WW22, Proposition 7], noting that the automorphic and motivic definitions of  $\mathcal{L}(E, \chi)$  agree under the assumption that  $p \nmid N$  [WW22, Lemma 18]. Integrality then follows immediately from Lemma 3.1 and the first statement. The final statement is an analogous argument with  $c_1(E)$  also given in Wiersema–Wuthrich [WW22, Proposition 8].  $\square$

**Remark 3.6.** The assumption that  $p \nmid N$  can be weakened slightly to  $p^2 \nmid N$  for the first two statements [WW22, Proposition 7]. Removing this 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  $\mathcal{L}(E, \chi) = \frac{1}{3}$ .

Observe that the right hand sides of Proposition 3.3 and Proposition 3.5 are highly similar. More precisely, since  $\overline{\chi(a)} \equiv 1 \pmod{(1 - \zeta_q)}$  except when  $\ell \mid a$ , the right hand sides are congruent modulo  $(1 - \zeta_q)$ .

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

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

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

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

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

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

**Remark 3.9.** Modified twisted L-values  $\mathcal{L}(E, \chi)$  satisfy Deligne's period conjecture [BD07, Theorem 2.7], so in particular they are Galois equivariant, in the sense that  $\mathcal{L}(E, \sigma \circ \chi) = \sigma(\mathcal{L}(E, \chi))$  for any  $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$ . With this property,  $\mathcal{L}(E)$  can be expressed in terms of the sum of  $\mathcal{L}(E, \chi)$  for all characters  $\chi$  of a given conductor and order. For instance, when  $\chi$  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 the identities in Proposition 3.3 and Proposition 3.5 combine to yield

$$c_0(E) \mathcal{L}(E, \chi) + c_0(E) \mathcal{L}(E, \bar{\chi}) + c_0(E) \mathcal{L}(E) \#E(\mathbb{F}_p) = 3 \sum_a \mu_E^{\pm}\left(\frac{a}{p}\right),$$

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  $2c_0(E) \Re(\mathcal{L}(E, \chi))$ , so this expresses  $\Re(\mathcal{L}(E, \chi))$  in terms of  $\mathcal{L}(E)$  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 extraneous modular symbols  $\mu_E^{\pm}\left(\frac{a}{p}\right)$  for each cubic residue  $a$  in  $\mathbb{F}_3$  sum to a multiple of 3.

## 4 Denominators of L-values

This section proves a few results on the  $\ell$ -adic valuations of denominators of modified L-values, where  $\ell$  is an odd prime, which may be of independent interest. Since  $c_0(E) \mathcal{L}(E) \#E(\mathbb{F}_v) \in \mathbb{Z}$ , the  $\ell$ -adic valuation of  $c_0(E) \mathcal{L}(E) \in \mathbb{Q}$  can be bounded from below by the  $\ell$ -adic valuation of  $\#E(\mathbb{F}_v)$ , which is in turn controlled by  $\text{tor}(E)$  in the denominator of  $\text{BSD}(E)$ . When  $\ell \neq 3$ , under the  $\ell$ -part of the Birch–Swinnerton-Dyer conjecture, such a lower bound follows from Lorenzini’s result that  $\text{ord}_\ell(\# \text{tor}(E)) \leq \text{ord}_\ell(\text{Tam}(E))$  with finitely many exceptions [Lor11, 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 but  $3 \nmid \text{Tam}(E)$ . Then  $\text{im}(\overline{\rho_{E,3}})$  is the full Borel subgroup.*

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

$$E_{1,\pm b/a} : y^2 + xy \pm \frac{b}{a}y = x^3,$$

for some coprime  $a, b \in \mathbb{N}$  [BR22, Proposition 2.4]. If  $3 \nmid \text{ord}_v(a)$  for some prime  $v$ , then  $3 \mid \text{Tam}_v(E_{1,\pm b/a})$  [BR22, Theorem 3.5]. This contradicts the assumption that  $3 \nmid \text{Tam}(E)$ , so  $a = d^3$  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

$$E_{d,\pm b} : y^2 + dxy \pm by = x^3,$$

which has discriminant  $\Delta = \pm b^3(d^3 - 27b)$ . Now let  $v \mid b$ , so that  $v \mid \Delta$  and  $\text{ord}_v(d^3 - 27b) = 0$  by coprimality. By step 2 of Tate’s algorithm, since  $T^2 + dT$  splits in  $\mathbb{F}_v$ ,  $E_{d,\pm b}$  has Kodaira symbol  $\mathbf{I}_{\text{ord}_v(\Delta)}$  and has split multiplicative reduction at  $v$ , so  $\text{Tam}_v(E_{d,\pm b}) = \text{ord}_v(\Delta) = 3 \text{ord}_v(b)$ . This forces  $b = 1$  by the assumption that  $3 \nmid \text{Tam}(E)$ , so the  $j$ -invariant of  $E_{d,\pm b} = E_{d,\pm 1}$  is given by

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

which implies that  $\text{im}(\overline{\rho_{E,3}})$  is the Borel subgroup 3B.1.1 [Zyw15, Theorem 1.2].  $\square$

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

**Proposition 4.2.** *Let  $E$  be an elliptic curve of conductor  $N$  such that  $L(E, 1) \neq 0$  and  $\text{tor}(E) \cong \mathbb{Z}/3\mathbb{Z}$ . Assume that  $\text{ord}_3(\mathcal{L}(E)) \leq \text{ord}_3(\text{BSD}(E))$ . Then  $3 \mid c_0(E) \text{Tam}(E) \# \text{III}(E)$ .*

*Proof.* Assume that  $3 \nmid c_0(E)$ . By Proposition 3.3 and the assumptions, for an odd prime  $v$ ,

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

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

**Remark 4.3.** The conclusion of Proposition 4.2 was already observed by Melistas [Mel23, Example 3.8], where the elliptic curves 27a3, 27a4, and 54a3 all have  $E(\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$  and  $\text{Tam}(E) \# \text{III}(E) = 1$  but  $c_0(E) = 3$ . By the work of Lorenzini, it is generally expected that the factors in  $\text{Tam}(E)$  would cancel  $\# \text{tor}(E)$ , but in this case it is necessary to consider  $\# \text{III}(E)$  as well, such as in the elliptic curve 1638j3 where  $E(\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$  and  $c_0(E) \text{Tam}(E) = 1$  but  $\# \text{III}(E) = 9$ . Note also that the statement is false for  $\text{tor}(E) \cong \mathbb{Z}/3\mathbb{Z}$  but  $\text{rk}(E) > 0$ , such as for the elliptic curve 91b1 where  $c_0(E) \text{Tam}(E) \# \text{III}(E) = 1$ .



A lower bound on the  $\ell$ -adic valuation of  $c_0(E)\mathcal{L}(E)$  then follows under the  $\ell$ -part of the Birch–Swinnerton-Dyer conjecture, but when  $E$  has no rational  $\ell$ -isogeny the bound can be made unconditional.

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

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

*Proof.* For the first statement, by Proposition 3.3, it suffices to find an odd prime  $v \nmid N$  such that  $\ell \nmid \#E(\mathbb{F}_v)$ , so by Chebotarev’s density theorem this reduces to finding a matrix  $M \in \text{im}(\overline{\rho_{E,\ell}})$  such that  $\text{tr}(M) \neq 1 + \det(M)$ . Suppose otherwise that  $\text{tr}(M) = 1 + \det(M)$  for all  $M \in \text{im}(\overline{\rho_{E,\ell}})$ , so in particular  $\text{tr}(M) = 2$  for all  $M \in \text{im}(\overline{\rho_{E,\ell}}) \cap \text{SL}(\ell)$ . In this case, by inspecting the order in each conjugacy class of  $\text{SL}(\ell)$ ,  $\text{im}(\overline{\rho_{E,\ell}}) \cap \text{SL}(\ell)$  is necessarily a  $\ell$ -group, so in particular  $\ell \mid \#\text{im}(\overline{\rho_{E,\ell}})$ . Then either  $\text{im}(\overline{\rho_{E,\ell}})$  is contained in a Borel subgroup of  $\text{GL}(\ell)$  or  $\text{im}(\overline{\rho_{E,\ell}})$  contains  $\text{SL}(\ell)$  [Ser72, Proposition 15]. The former contradicts the assumption that  $E$  has no rational  $\ell$ -isogeny, and the latter is impossible by comparing orders.

For the second statement, the assumption on the  $\ell$ -adic valuations reduces the statement to proving that  $\text{ord}_\ell(c_0(E)\text{BSD}(E)) \geq -1$ . By Mazur’s torsion theorem, it suffices to consider  $\text{tor}(E)$  being one of

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

since  $\ell$  is odd. If  $E(\mathbb{Q}) \not\cong \mathbb{Z}/3\mathbb{Z}$ , then a case-by-case analysis of  $\ell$  yields  $\text{ord}_\ell(\text{Tam}(E)) \geq \text{ord}_\ell(\#\text{tor}(E))$  except for the elliptic curve 11a3 with  $\ell = 5$ , and the elliptic curves 14a4 and 14a6 with  $\ell = 3$  [Lor11, Proposition 1.1], but these exceptions all have  $\text{ord}_\ell(c_0(E)) = 1$  and  $\text{ord}_\ell(\text{BSD}(E)) = -2$ . If  $E(\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$ , then Proposition 4.2 implies that  $\text{ord}_3(\text{BSD}(E)) = \text{ord}_3(c_0(E)\text{Tam}(E)\#\text{III}(E)) - 2 \geq -1$ .  $\square$

**Remark 4.5.** The assumption on the  $\ell$ -part of the Birch–Swinnerton-Dyer conjecture in the second statement can be slightly weakened, by only requiring that  $\text{ord}_\ell(\mathcal{L}(E)) \geq \text{ord}_\ell(\text{BSD}(E))$  for all  $E$ , except for when  $\text{im}(\rho_{E,3})$  is 9.72.0.1, where the assumption  $\text{ord}_\ell(\mathcal{L}(E)) \leq \text{ord}_\ell(\text{BSD}(E))$  is also needed to proceed with the argument in Proposition 4.2. Currently this remains an open problem in general even for  $\ell = 3$ , although substantial progress has been made recently by Keller-Yin when  $\text{im}(\overline{\rho_{E,\ell}})$  is small [KY24, Theorem C] and by Burungale–Castella–Skinner when  $\text{im}(\overline{\rho_{E,\ell}})$  is large [BCS24, Corollary 1.3.1].

**Remark 4.6.** The second statement might also be provable without appealing to the  $\ell$ -part of the Birch–Swinnerton-Dyer conjecture when  $\ell > 3$ , by finding a matrix  $M \in \text{im}(\rho_{E,\ell})$  such that  $1 + \det(M) - \text{tr}(M) \equiv \ell \pmod{\ell^2}$  along the same lines as the proof of Proposition 4.2. In general, this would need a case-by-case analysis of  $\text{im}(\rho_{E,\ell})$  for when  $E$  has no rational  $\ell$ -isogeny, which remains open.

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

**Proposition 4.7.** *Let  $E$  be an elliptic curve of conductor  $N$  such that  $L(E, 1) \neq 0$ , and let  $v \nmid N$  and  $\ell$  be odd primes such that  $v \equiv 1 \pmod{\ell}$ . Assume that  $c_1(E) = 1$ . Then*

$$\ell \nmid c_0(E)\mathcal{L}(E)\#E(\mathbb{F}_v) \iff \ell \nmid c_0(E) \text{ and } \text{ord}_\ell(\mathcal{L}(E)\#E(\mathbb{F}_v)) = 0.$$

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

**Remark 4.8.** Assuming Stevens’s conjecture, Proposition 4.7 yields an immediate proof that  $\mathcal{L}(E)\#E(\mathbb{F}_v)$  is integral at  $\ell$  if  $\text{ord}_\ell(c_0(E)) \leq 1$ . This condition seems to hold for all elliptic curves in the LMFDB [Col], but a proof remains elusive. On the other hand, assuming the  $\ell$ -part of the Birch–Swinnerton-Dyer conjecture, there might be a direct proof that  $\mathcal{L}(E)\#E(\mathbb{F}_v)$  is integral at  $\ell$ , by arguing that  $1 + \det(M) - \text{tr}(M)$  cancels  $\#\text{tor}(E)^2$  for every matrix  $M$  lying in every possible  $\text{im}(\rho_{E,\ell})$ . Again, this will be omitted here.

## 5 Units of twisted L-values

Under standard arithmetic conjectures, Dokchitser–Evans–Wiersema computed the norm of  $\mathcal{L}(E, \chi)$  in terms of  $\text{BSD}(E)$  and  $\text{BSD}(E/K)$ , where  $K$  is the degree  $q$  subfield of  $\mathbb{Q}(\zeta_p)$  cut out by the kernel of  $\chi$  [DEW21, Theorem 38]. Some of their results can be summarised in the notation of this paper as follows.

**Proposition 5.1.** *Let  $E$  be an elliptic curve of conductor  $N$  such that  $L(E, 1) \neq 0$ , and let  $\chi$  be a character of odd prime conductor  $p \nmid N$  and odd prime order  $q \nmid c_0(E) \text{BSD}(E) \#E(\mathbb{F}_p)$ . Assume that  $c_1(E) = 1$ , and that  $\mathcal{L}(E) = \text{BSD}(E)$  and  $\mathcal{L}(E/K) = \text{BSD}(E/K)$ . Furthermore, set  $\zeta := \chi(N)^{(q-1)/2}$ .*

1. *The ideal generated by  $\mathcal{L}(E, \chi) \in \mathbb{Z}[\zeta_q]$  is invariant under complex conjugation and has norm*

$$\text{Nm}_q(\mathcal{L}(E, \chi)) = \pm \frac{\text{BSD}(E/K)}{\text{BSD}(E)}.$$

2. *The product  $\mathcal{L}(E, \chi) \cdot \zeta \in \mathbb{Z}[\zeta_q]^+$  has norm*

$$\text{Nm}_q^+(\mathcal{L}(E, \chi) \cdot \zeta) = \pm \sqrt{\frac{\text{BSD}(E/K)}{\text{BSD}(E)}}.$$

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

*Proof.* By Proposition 4.7, under the arithmetic conjectures, the assumption that  $q \nmid c_0(E) \text{BSD}(E) \#E(\mathbb{F}_p)$  reduces to  $q \nmid c_0(E)$  and  $\text{ord}_q(\mathcal{L}(E) \#E(\mathbb{F}_p)) = 0$ . In particular  $L(E, 1) \neq 0$ , and moreover  $\text{ord}_q(\mathcal{L}(E, \chi)) = 0$  by Corollary 3.7, so  $L(E, \chi, 1) \neq 0$  as well. This verifies the assumptions of a result by Dokchitser–Evans–Wiersema [DEW21, Theorem 13(5) to Theorem 13(12)], and is a restatement of it.  $\square$

In other words, Proposition 5.1.1 predicts that the ideal  $I$  of  $\mathbb{Z}[\zeta_q]$  generated by  $\mathcal{L}(E, \chi)$  has norm equal to the rational number  $\text{BSD}(E/K) / \text{BSD}(E)$ , and Proposition 5.1.2 says that  $\text{BSD}(E/K) / \text{BSD}(E)$  is necessarily the square of a rational number whose positive square root is equal to the norm of  $\mathcal{L}(E, \chi) \cdot \zeta$ . Thus there are only finitely many possibilities for the prime factorisation of  $I$ , and the fact that  $I$  is invariant under complex conjugation narrows down the possibilities further. The precise ideal factorisation can then be recovered from the  $\text{Gal}(K/\mathbb{Q})$ -module structure of  $\text{III}(E/K)$  [BC21, Remark 7.4].

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  $\mathcal{L}(E, \chi)$  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  $\mathcal{L}(E, \chi) \cdot \zeta$ , which determines the actual value of  $\mathcal{L}(E, \chi)$  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  $\pm 1$ . 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  $L(E, 1) \neq 0$ , and let  $\chi$  be a cubic character of odd prime conductor  $p \nmid N$  such that  $3 \nmid c_0(E) \text{BSD}(E) \#E(\mathbb{F}_p)$ . Assume that  $c_1(E) = 1$ , and that  $\mathcal{L}(E) = \text{BSD}(E)$  and  $\mathcal{L}(E/K) = \text{BSD}(E/K)$ . Then*

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

*where the sign  $u = \pm 1$  is such that*

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

This follows immediately from Corollary 3.7 and Proposition 5.1. Corollary 5.2 clarifies much of the phenomena observed by Dokchitser–Evans–Wiersema [DEW21, Example 45], where they gave many pairs of examples of arithmetically similar elliptic curves  $E_1$  and  $E_2$  with  $\mathcal{L}(E_1, \chi) \neq \mathcal{L}(E_2, \chi)$  for a few cubic characters  $\chi$ , in the sense that  $\mathcal{L}(E_1, \chi) \neq \mathcal{L}(E_2, \chi)$  precisely because  $\#E_1(\mathbb{F}_p) \not\equiv \#E_2(\mathbb{F}_p) \pmod{3}$ .

**Example 5.3.** Let  $E_1$  and  $E_2$  be the elliptic curves 1356d1 and 1356f1 respectively, and let  $\chi$  be the cubic character of conductor 7 such that  $\chi(3) = \zeta_3^2$ . Then  $c_0(E_i) = \text{BSD}(E_i) = \text{BSD}(E_i/K) = 1$  for  $i = 1, 2$ , so Proposition 5.1 implies that  $\mathcal{L}(E_i, \chi) = \pm \chi(1356) = \pm \zeta_3^2$ , but it was a priori unclear why  $\mathcal{L}(E_1, \chi) = \zeta_3^2$  and  $\mathcal{L}(E_2, \chi) = -\zeta_3^2$ . 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 many other examples satisfying  $c_0(E) = \text{BSD}(E) = \text{BSD}(E/K) = 1$  with different  $\mathcal{L}(E, \chi)$  for a few different cubic characters  $\chi$ , and they can all be explained similarly. For reference and comparison, the values of  $\mathcal{L}(E, \chi)$  for the above character and of  $\#E(\mathbb{F}_7)$  are tabulated as follows.

$E$	1356d1	1356f1	3264r1	3264s1	3540a1	3540b1	4800i1	4800bj1	4800bm1
$\mathcal{L}(E, \chi)$	$\zeta_3^2$	$-\zeta_3^2$	$-\zeta_3^2$	$\zeta_3^2$	$-\zeta_3^2$	$\zeta_3^2$	$-\zeta_3^2$	$-\zeta_3^2$	$\zeta_3^2$
$\#E(\mathbb{F}_7)$	11	7	10	8	7	11	7	7	11

When  $q \neq 3$  but  $\text{BSD}(E) = \text{BSD}(E/K)$ , Proposition 5.1 says that  $\mathcal{L}(E, \chi)$  is a unit in  $\mathbb{Z}[\zeta_q]$ , and Corollary 3.7 places an explicit 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  $L(E, 1) \neq 0$ , and let  $\chi$  be a character of odd prime conductor  $p \nmid N$  and odd prime order  $q \nmid c_0(E) \text{BSD}(E) \#E(\mathbb{F}_p)$  such that  $\text{BSD}(E) = \text{BSD}(E/K)$ . Assume that  $c_1(E) = 1$ , and that  $\mathcal{L}(E) = \text{BSD}(E)$  and  $\mathcal{L}(E/K) = \text{BSD}(E/K)$ . Then  $\mathcal{L}(E, \chi) = u$  for some unit  $u \in \mathbb{Z}[\zeta_q]$ , such that  $u \equiv -\#E(\mathbb{F}_p) \text{BSD}(E) \pmod{(1 - \zeta_q)}$ .*

Again, this follows immediately from Corollary 3.7 and Proposition 5.1. Corollary 5.4 partially explains the remaining phenomena observed by Dokchitser–Evans–Wiersema [DEW21, Example 44], where they gave many pairs of examples of arithmetically trivial elliptic curves  $E_1$  and  $E_2$  with  $\mathcal{L}(E_1, \chi) \neq \mathcal{L}(E_2, \chi)$  for quintic characters  $\chi$ , in the sense that  $\mathcal{L}(E_1, \chi) \neq \mathcal{L}(E_2, \chi)$  precisely because  $\#E_1(\mathbb{F}_p) \not\equiv \#E_2(\mathbb{F}_p) \pmod{5}$ .

**Example 5.5.** Let  $E_1$  and  $E_2$  be the elliptic curves 307a1 and 307c1 respectively, and let  $\chi$  be the quintic character of conductor 11 such that  $\chi(2) = \zeta_5$ . Then  $c_0(E_i) = \text{BSD}(E_i) = \text{BSD}(E_i/K) = 1$  for  $i = 1, 2$ , so Proposition 5.1 implies that  $\mathcal{L}(E_i, \chi)$  is a unit, but it was a priori unclear why  $\mathcal{L}(E_1, \chi) = 1$  and  $\mathcal{L}(E_2, \chi) = \zeta_5 u^2$ , where  $u := 1 + \zeta_5^4$ . Corollary 5.4 explains this by requiring that  $\mathcal{L}(E_i, \chi) \equiv -\#E_i(\mathbb{F}_{11}) \pmod{(1 - \zeta_5)}$ , and in this case  $\#E_1(\mathbb{F}_{11}) = 9$  and  $\#E_2(\mathbb{F}_{11}) = 16$ , which are distinct modulo 5.

They provided a few other examples satisfying  $c_0(E) = \text{BSD}(E) = \text{BSD}(E/K) = 1$  with different  $\mathcal{L}(E, \chi)$  for this character, and they can all be explained similarly. For reference and comparison, the values of  $\mathcal{L}(E, \chi)$  for the above character and of  $\#E(\mathbb{F}_{11})$  are tabulated as follows.

$E$	307a1	307c1	432g1	432h1	714b1	714h1	1187a1	1187b1	1216g1	1216k1
$\mathcal{L}(E, \chi)$	1	$\zeta_5 u^2$	$u^2$	$-\zeta_5 u^{-1}$	1	$-\zeta_5^4 u^3$	$\zeta_5^2 u^{-1}$	$\zeta_5 u^{-3}$	$-\zeta_5^3 u^2$	$\zeta_5^4 u^{-1}$
$\#E(\mathbb{F}_{11})$	9	16	16	8	9	13	17	8	9	7

When  $q \neq 3$  and  $\text{BSD}(E) \neq \text{BSD}(E/K)$ , it is slightly awkward to rephrase Proposition 5.1 in a way that is applicable by Corollary 3.7, so it is best illustrated with an example [DEW21, Example 46].

**Example 5.6.** Let  $E_1$  and  $E_2$  be the elliptic curves 291d1 and 139a1 respectively, and let  $\chi$  be the quintic character of conductor 31 such that  $\chi(3) = \zeta_5^3$ . Then  $c_0(E_i) = \text{BSD}(E_i) = 1$ , but  $\text{BSD}(E_i/K) = 11^2$  for  $i = 1, 2$ , so Proposition 5.1 implies that  $\mathcal{L}(E_i, \chi)$  generates an ideal of norm  $11^2$  invariant under complex conjugation. By considering the primes above  $11^2$  in  $\mathbb{Z}[\zeta_5]$ , there are only two such ideals, generated by  $\lambda_1 := 3\zeta_5^3 + \zeta_5^2 + 3\zeta_5 \equiv 2 \pmod{(1 - \zeta_5)}$  and  $\lambda_2 := \zeta_5^3 + 3\zeta_5 + 3 \equiv 2 \pmod{(1 - \zeta_5)}$ , and in fact  $(\mathcal{L}(E_i, \chi)) = (\lambda_i)$ . Assuming this, Corollary 3.7 then predicts that  $\mathcal{L}(E_i, \chi) = u_i \lambda_i$  for some units  $u_i \in \mathbb{Z}[\zeta_5]$  such that  $2u_i \equiv -\#E_i(\mathbb{F}_{31}) \pmod{(1 - \zeta_5)}$ , and in this case  $\#E_1(\mathbb{F}_{31}) = 33 \equiv 3 \pmod{5}$  and  $\#E_2(\mathbb{F}_{31}) = 23 \equiv 3 \pmod{5}$ , so  $u_i \equiv 1 \pmod{(1 - \zeta_5)}$ . In fact,  $u_1 = \zeta_5^4$  and  $u_2 = \zeta_5 - \zeta_5 + 1$ .

**Remark 5.7.** As this example highlights, in general it is possible for  $\mathcal{L}(E_1, \chi) \equiv \mathcal{L}(E_2, \chi) \pmod{(1 - \zeta_q)}$  but  $\mathcal{L}(E_1, \chi) \neq \mathcal{L}(E_2, \chi)$ , even when  $c_0(E_i) = \text{BSD}(E_i) = 1$ , so a general Birch–Swinnerton–Dyer formula for  $\mathcal{L}(E, \chi)$  remains unlikely even with  $\#E(\mathbb{F}_p)$ . There are also examples for when  $E_i$  have the same conductor and discriminant, and furthermore  $\text{BSD}(E_i/K) = 1$ , such as for the elliptic curves 544b1 and 544f1 and the quintic character  $\chi$  of conductor 11 given by  $\chi(2) = \zeta_5$ , where  $\mathcal{L}(E_1, \chi) = -\zeta_5^3 - \zeta_5$  and  $\mathcal{L}(E_2, \chi) = -2\zeta_5^3 - 3\zeta_5^2 - 2\zeta_5$ . This is the pair of elliptic curves with the smallest conductor satisfying the aforementioned properties but  $\mathcal{L}(E_1, \chi) \neq \mathcal{L}(E_2, \chi)$ , and other examples do seem to be quite 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  $\mathcal{L}(E, \chi)$  as  $\chi$  varies over characters of some fixed prime order  $q$  but arbitrarily high odd prime conductor  $p \nmid N$ . However, for each such  $p$ , there are  $q - 1$  characters  $\chi$  of conductor  $p$  and order  $q$ , giving rise to  $q - 1$  conjugates of  $\mathcal{L}(E, \chi)$ , so a uniform choice of  $\chi$  for each  $p$  has to be made for any meaningful analysis. One solution is to observe that the residue class of  $\mathcal{L}(E, \chi)$  modulo  $(1 - \zeta_q)$  is independent of the choice of  $\chi$ , so a simpler problem would be to determine the asymptotic distribution of these residue classes instead. As in the introduction, let  $X_{E,q}^{\leq n}$  be the set of equivalence classes of characters of odd order  $q$  and odd prime conductor  $p \nmid N$  less than  $n$ , where two characters in  $X_{E,q}^{\leq n}$  are equivalent if they have the same conductor. Define the residual densities  $\delta_{E,q}$  of  $\mathcal{L}(E, \chi)$  to be the natural densities of  $\mathcal{L}(E, \chi)$  modulo  $(1 - \zeta_q)$ , namely

$$\delta_{E,q}(\lambda) := \lim_{n \rightarrow \infty} \frac{\#\{\chi \in X_{E,q}^{\leq n} \mid \mathcal{L}(E, \chi) \equiv \lambda \pmod{(1 - \zeta_q)}\}}{\#X_{E,q}^{\leq n}}, \quad \lambda \in \mathbb{F}_q,$$

if such a limit exists. When  $q \nmid c_0(E)$ , this can be computed for each  $\lambda \in \mathbb{F}_q$  directly using Corollary 3.7, with the only subtlety being the possible cancellations between  $\mathcal{L}(E)$  and  $\#E(\mathbb{F}_p)$ . In the generic scenario when  $\text{im}(\overline{\rho_{E,q}})$  is maximal, there is a clean description in terms of Legendre symbols.

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

1. *If  $\text{ord}_q(\mathcal{L}(E)) > 0$ , then  $\delta_{E,q}(0) = 1$  and  $\delta_{E,q}(\lambda) = 0$  for any  $\lambda \in \mathbb{F}_q^\times$ .*
2. *If  $\text{ord}_q(\mathcal{L}(E)) \leq 0$ , then set  $m := 1 - \text{ord}_q(\mathcal{L}(E))$  and*

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

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

$$\delta_{E,q}(\lambda) = \frac{\#\left\{ M \in G_{E,q^m} \mid 1 + \det(M) - \text{tr}(M) \equiv -\lambda \mathcal{L}(E)^{-1} \pmod{q^m} \right\}}{\#G_{E,q^m}}.$$

*In particular, if  $\text{ord}_q(\mathcal{L}(E)) \leq 0$  and  $\overline{\rho_{E,q}}$  is surjective, then set*

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

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

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

*Proof.* By Corollary 3.7,  $\delta_{E,q}(\lambda)$  is just the natural density of  $-\mathcal{L}(E) \#E(\mathbb{F}_p) \equiv \lambda \pmod{q}$ . If  $\text{ord}_q(\mathcal{L}(E)) > 0$ , then only  $\lambda = 0$  gives a non-zero natural density, otherwise this is equivalent to  $1 + p - a_p(E) \equiv -\lambda \mathcal{L}(E)^{-1} \pmod{q^m}$ , noting that  $\mathcal{L}(E)^{-1}$  is well-defined and non-zero 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  $\text{tr}(M) = a_p(E)$ , so the second statement follows. If  $\overline{\rho_{E,q}}$  is surjective, then Theorem 4.4.1 yields  $m = 1$ , so  $\delta_{E,q}(\lambda)$  is the proportion of matrices  $M \in \text{SL}(q)$  such that  $\text{tr}(M) \equiv 2 - \lambda \mathcal{L}(E)^{-1} \pmod{q}$ . The final statement then follows by  $\#\text{SL}(q) = (q-1)q(q+1)$  and by inspecting the trace in each conjugacy class of  $\text{SL}(q)$ , noting that  $\text{tr}(M) = x + x^{-1}$  for some  $x \in \mathbb{F}_q \setminus \{\pm 1\}$  precisely when  $x^2 - 4$  is a quadratic residue modulo  $q$ .  $\square$

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

**Remark 6.3.** Under standard arithmetic conjectures, Proposition 5.1 says that  $\mathcal{L}(E, \chi) \cdot \zeta \in \mathbb{Z}[\zeta_q]$ , so  $\text{Nm}_q^+(\mathcal{L}(E, \chi) \cdot \zeta) \in \mathbb{Z}$ . Since the norm is multiplicative and  $\zeta \equiv 1 \pmod{1 - \zeta_q}$ , the asymptotic distribution of the residue class of  $\text{Nm}_q^+(\mathcal{L}(E, \chi) \cdot \zeta)$  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  $\text{ord}_q(\text{BSD}(E)) \geq -1$ , so non-trivial  $\delta_{E,q}$  are only visible when  $\text{ord}_q(\text{BSD}(E)) = 0, -1$ . Once this is determined, computing  $\delta_{E,q}$  then reduces to identifying  $\text{im}(\overline{\rho_{E,q}})$  or  $\text{im}(\overline{\rho_{E,q^2}})$ , 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 [RSZB22, Corollary 1.3.1 and Corollary 12.3.3].

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

1. If  $\text{ord}_3(\text{BSD}(E)) > 0$ , then  $\delta_{E,3}(0) = 1$  and  $\delta_{E,3}(1) = \delta_{E,3}(2) = 0$ .
2. If  $\text{ord}_3(\text{BSD}(E)) = 0$  and  $3 \mid \#\text{tor}(E)$ , then  $\delta_{E,3}(0) = 1$  and  $\delta_{E,3}(1) = \delta_{E,3}(2) = 0$ .
3. If  $\text{ord}_3(\text{BSD}(E)) = 0$  and  $3 \nmid \#\text{tor}(E)$ , then  $(\delta_{E,3}(0), \delta_{E,3}(1), \delta_{E,3}(2))$  is given in Table 1.
4. If  $\text{ord}_3(\text{BSD}(E)) = -1$ , then  $(\delta_{E,3}(0), \delta_{E,3}(1), \delta_{E,3}(2))$  is given in Table 2.

In particular,  $(\delta_{E,3}(0), \delta_{E,3}(1), \delta_{E,3}(2))$  only depends on  $\text{BSD}(E)$  and on  $\text{im}(\overline{\rho_{E,9}})$ , and can only be one of

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

*Proof.* The fact that there are only four possibilities is an immediate consequence of Theorem 4.4. By Proposition 6.1, the first statement follows immediately under the assumption that  $\text{ord}_3(\mathcal{L}(E)) = \text{ord}_3(\text{BSD}(E))$ , while the second statement follows from  $3 \mid 1 + \det(M) - \text{tr}(M)$  for all  $M \in \text{im}(\overline{\rho_{E,3}})$  whenever  $3 \mid \#\text{tor}(E)$ . The final statement follows from the first four, so it remains to prove the third and fourth statements.

For the third statement, it suffices to consider  $G_{E,3} = \text{im}(\overline{\rho_{E,3}}) \cap \text{SL}(3)$ , and there are only 5 possibilities for  $\text{im}(\overline{\rho_{E,3}})$  when  $\overline{\rho_{E,3}}$  is not surjective, as tabulated in Table 1. If  $\overline{\rho_{E,3}}$  is surjective, then  $\delta_{E,3}(\lambda)$  is already computed in the final statement in Proposition 6.1, while the other 5 cases are similar but easier computations. For instance, if  $\text{im}(\overline{\rho_{E,3}})$  is 3B.1.2, then  $G_{E,3}$  is conjugate to the subgroup of unipotent upper triangular matrices in  $\text{SL}(3)$ , so counting the six matrices with each trace yields  $\delta_{E,3}(0) = 1$  and  $\delta_{E,3}(1) = \delta_{E,3}(2) = 0$ . Note that when  $\delta_{E,3}(1) \neq \delta_{E,3}(2)$ , the residue of  $\text{BSD}(E)$  modulo 3 would swap  $\delta_{E,3}(1)$  and  $\delta_{E,3}(2)$ , such as in the case of  $\text{SL}(3) \subseteq \text{im}(\overline{\rho_{E,3}})$  where  $\delta_{E,3}(1) = \frac{1}{4}$  precisely if  $\text{BSD}(E) \equiv 1 \pmod{3}$  and  $\delta_{E,3}(1) = \frac{3}{8}$  otherwise.

For the fourth statement, it suffices to consider  $G_{E,9}$ , and by the classification this is the projection onto  $\text{GL}(9)$  of 21 different possible  $\text{im}(\rho_{E,3})$ , as tabulated in Table 2. For instance, if  $\text{im}(\rho_{E,3})$  is 3.8.0.1, then  $G_{E,9}$  is the preimage of the subgroup of  $\text{SL}(3)$  generated by  $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$  and  $\begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}$  under the canonical projection  $\text{GL}(9) \rightarrow \text{GL}(3)$ . This preimage in  $\text{GL}(9)$  consists of 243 matrices, of which 135 have trace 0 and 54 have trace 1 and 2 each, so  $\delta_{E,3}(0) = \frac{135}{243} = \frac{5}{9}$  and  $\delta_{E,3}(1) = \delta_{E,3}(2) = \frac{54}{243} = \frac{2}{9}$ . The other 20 cases are similar but easier computations, noting again the residue of  $3\text{BSD}(E)$  modulo 3 when  $\delta_{E,3}(1) \neq \delta_{E,3}(2)$ , such as in the case of 27.648.18.1 where  $\delta_{E,3}(1) = 0$  precisely if  $3\text{BSD}(E) \equiv 2 \pmod{3}$  and  $\delta_{E,3}(1) = \frac{2}{3}$  otherwise.  $\square$

**Remark 6.5.** The first case happens when  $3 \nmid \#\text{tor}(E)$  but  $3 \mid \text{Tam}(E) \# \text{III}(E)$ , such as for the elliptic curve 50b4 where  $\text{BSD}(E) = 3$ , and the second case happens when  $9 \mid \text{Tam}(E) \# \text{III}(E)$ , such as for the elliptic curve 84a1 where  $\text{BSD}(E) = \frac{1}{2}$ . Note also that if  $\text{im}(\overline{\rho_{E,3}})$  is 3Cs.1.1, a much easier argument to prove that  $\delta_{E,3}(0) = 1$  and  $\delta_{E,3}(1) = \delta_{E,3}(2) = 0$  is to observe that  $G_{E,3}$  is trivial, so  $E(\mathbb{F}_p)$  acquires full 3-torsion for any  $p \equiv 1 \pmod{3}$ , and thus  $\mathcal{L}(E, \chi) \equiv -\text{BSD}(E) \# E(\mathbb{F}_p) \equiv 0 \pmod{3}$  always.

**Remark 6.6.** Assuming the 3-part of the Birch–Swinnerton-Dyer conjecture holds, Theorem 6.4 then describes the densities of the sign  $u$  determined in Corollary 5.2, and hence the actual densities of  $\mathcal{L}(E, \chi)$ .

## 7 Twisted L-values of Kisilevsky–Nam

The computation of residual densities was originally motivated by the statistical data in Kisilevsky–Nam [KN22, Section 7]. They numerically computed millions of modified twisted L-values by fixing the elliptic curve and varying the character, but considered an alternative normalisation given by

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

in contrast to the normalisation factor  $\zeta$  in Proposition 5.1. Under the implicit assumption that  $\mathcal{L}(E, \chi) \in \mathbb{Z}[\zeta_q]$ , they showed that  $\mathcal{L}^+(E, \chi) \in \mathbb{Z}[\zeta_q]^+$  [KN22, Proposition 2.1], so that  $\text{Nm}_q^+(\mathcal{L}^+(E, \chi)) \in \mathbb{Z}$ . Fixing six elliptic curves  $E$  and five small orders  $q$ , they varied the character  $\chi$  over millions of conductors  $p$ , empirically determined the greatest common divisor  $\text{gcd}_{E,q}$  of all the integers  $\text{Nm}_q^+(\mathcal{L}^+(E, \chi))$ , and considered

$$\tilde{\mathcal{L}}^+(E, \chi) := \frac{\text{Nm}_q^+(\mathcal{L}^+(E, \chi))}{\text{gcd}_{E,q}}.$$

**Remark 7.1.** The definition of  $\tilde{\mathcal{L}}^+(E, \chi)$  is equivalent to that of  $A_\chi$  defined by Kisilevsky–Nam when  $q$  is odd and  $L(E, 1) \neq 0$ , since  $\chi(N) = -1$  never occurs and the global root number is always 1 [KN22, Section 2.2]. Their definition of  $\mathcal{L}(E, \chi)$  has an extra factor of 2, but this is cancelled out after division by  $\text{gcd}_{E,q}$ .

**Remark 7.2.** In the interpretation of Proposition 5.1, the integer  $\text{gcd}_{E,q}$  is predicted to arise from contributions by the greatest common divisors of  $\text{BSD}(E/K) / \text{BSD}(E)$  ranging over various number fields  $K$  of degree  $q$  over  $\mathbb{Q}$  coming from characters of order  $q$ , but this will not be discussed here.

As their normalisation differs from that in Proposition 5.1 [KN22, Remark 1], the resulting residual densities are skewed. More precisely, define  $X_{E,q}^{<n}$  as before, and define the analogous residual densities  $\delta'_{E,q}$  of  $\tilde{\mathcal{L}}^+(E, \chi)$  to be the natural densities of  $\tilde{\mathcal{L}}^+(E, \chi)$  modulo  $q$ , or in other words

$$\delta_{E,q}(\lambda) := \lim_{n \rightarrow \infty} \frac{\#\left\{ \chi \in X_{E,q}^{<n} \mid \tilde{\mathcal{L}}^+(E, \chi) \equiv \lambda \pmod{q} \right\}}{\#X_{E,q}^{<n}}, \quad \lambda \in \mathbb{F}_q,$$

if such a limit exists. In the simplest case where  $q = 3$  and  $3 \nmid \text{gcd}_{E,3}$ , there is no norm, and so

$$\tilde{\mathcal{L}}^+(E, \chi) \equiv \begin{cases} \mathcal{L}(E, \chi) \text{gcd}_{E,3} & \text{if } \chi(N) = 1 \\ 2\mathcal{L}(E, \chi) \text{gcd}_{E,3} & \text{otherwise} \end{cases},$$

which becomes amenable to a similar computation to that of Proposition 6.1 provided  $\chi(N)$  is known. For certain elliptic curves,  $\chi(N)$  depends completely on  $\#E(\mathbb{F}_p)$  due to a shared action of Frobenius in  $\text{GL}(3)$ .

**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  $\psi_{E,3}$ , and let  $\chi$  be a cubic character of odd prime conductor  $p \nmid N$ . Then  $\text{im}(\overline{\rho_{E,3}}) = \text{GL}(3)$  and  $\text{Gal}(K/\mathbb{Q}) \cong \text{PGL}(3)$ . Furthermore, if  $p$  does not split completely in  $K$ , then  $\#E(\mathbb{F}_p) \equiv 2 \pmod{3}$  if and only if  $\chi(N) = 1$ . Otherwise, if  $p$  splits completely in  $K$ , then  $\#E(\mathbb{F}_p) \not\equiv 2 \pmod{3}$  and  $\chi(N) = 1$ .*

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

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

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

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

$$\text{Fr}_p(\zeta_3) \equiv \zeta_3^p \pmod{\pi}, \quad \text{Fr}_p(\sqrt[3]{N}) \equiv \sqrt[3]{N^p} \pmod{\pi}.$$

Clearly  $\text{Fr}_p$  fixes  $\zeta_3$ , so that  $\text{Fr}_p \in \text{Gal}(K/\mathbb{Q}(\zeta_3))$ . Claim that, when  $p$  does not split completely in  $K$ , the condition  $\text{Fr}_p \in \text{Gal}(K/F)$  is equivalent to  $\#E(\mathbb{F}_p) \equiv 2 \pmod{3}$  and to  $\chi(N) = 1$ . On one hand, this means that  $\text{Fr}_p$  fixes  $\sqrt[3]{N}$ , or equivalently that  $\sqrt[3]{N^{p-1}} \equiv 1 \pmod{p}$ , which is precisely the condition that  $\chi(N) = 1$ . On the other hand, this also means that  $\text{Fr}_p^2 = 1$  in  $\text{Gal}(K/\mathbb{Q}(\zeta_3))$ , which is equivalent to  $\text{Fr}_p$  having order exactly 2 in  $\text{Gal}(K/\mathbb{Q}(\zeta_3))$ . By the Cayley–Hamilton theorem, these are precisely the trace 0 matrices in  $\text{PGL}(3)$ , or equivalently the trace 0 matrices in  $\text{GL}(3)$ , which proves the equivalence with  $a_p(E) = 0$ . If  $p$  splits completely in  $K$ , then  $\text{Fr}_p = 1$  in  $\text{Gal}(K/\mathbb{Q}(\zeta_3))$ , but these never have trace 0 in  $\text{PGL}(3)$  or  $\text{GL}(3)$ .  $\square$

**Remark 7.4.** The first assumption is necessary, evident in the elliptic curve 50b1 with  $F \subseteq K$  but  $\text{im}(\overline{\rho_{E,3}})$  is 3B, where 7 does not split completely in  $K$  but  $\#E(\mathbb{F}_7) = 10 \equiv 1 \pmod{3}$  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  $F \not\subseteq K$ , where 13 does not split completely in  $K$  but  $\#E(\mathbb{F}_{13}) = 16 \equiv 1 \pmod{3}$  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  $\#E(\mathbb{F}_{19}) = 20 \equiv 2 \pmod{3}$  and  $\chi(11) = \overline{\chi(11)} = 1$ . If  $p$  does split completely in  $K$ , then both  $\#E(\mathbb{F}_p) \equiv 0 \pmod{3}$  and  $\#E(\mathbb{F}_p) \equiv 1 \pmod{3}$  are possible, such as for the elliptic curve 11a1, where  $\#E(\mathbb{F}_{337}) = 360 \equiv 0 \pmod{3}$  and  $\#E(\mathbb{F}_{193}) = 190 \equiv 1 \pmod{3}$ . Finally, note that this argument only works for cubic characters, as  $\text{PGL}(q)$  is almost simple for  $q > 3$  and admits few non-trivial surjections.

For elliptic curves satisfying this property, the residual density of  $\tilde{\mathcal{L}}^+(E, \chi)$  is easy to compute.

**Proposition 7.5.** *Let  $E$  be an elliptic curve of conductor  $N$  with no rational 3-isogeny such that  $3 \nmid c_0(E)$  and  $3 \nmid \text{gcd}_{E,3}$ , and the splitting field  $F$  of  $X^3 - N$  lies in the splitting field  $K$  of the 3-division polynomial  $\psi_{E,3}$ , and let  $\chi$  be a cubic character of odd prime conductor  $p \nmid N$ . Then*

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

In particular,

$$\delta'_{E,3}(0) = \frac{9}{24}, \quad \delta'_{E,3}(1) = \frac{15}{24}, \quad \delta'_{E,3}(2) = \frac{1}{24}.$$

*Proof.* By Corollary 3.7 and the assumptions that  $3 \nmid c_0(E)$  and  $3 \nmid \text{gcd}_{E,3}$ ,

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

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

**Remark 7.6.** Elliptic curves with discriminant  $\Delta = \pm N^n$  for some  $3 \nmid n$  satisfy this property, since  $\sqrt[3]{N}$  can then be expressed in terms of  $\sqrt[3]{\Delta}$  [Ser72, Section 5.3b]. This completely explains the numerical data by Kisilevsky–Nam for the elliptic curve 11a1 where  $\text{gcd}_{E,3} = 5$  and the elliptic curves 15a1 and 17a1 where  $\text{gcd}_{E,3} = 4$ , all of which satisfy the assumptions of Proposition 7.5. The same method cannot explain the density patterns when  $3 \mid \text{gcd}_{E,3}$ , 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  $3 \nmid c_0(E)$  and  $L(E, 1) \neq 0$ , but in general there are many elliptic curves with each prescribed mod-3 or 3-adic Galois image.

### Mod-3 Galois images of elliptic curves without 3-torsion

The possible mod-3 Galois images are well-known [Zyw15, Theorem 1.2, Proposition 1.14, and Proposition 1.16], and those of elliptic curves without 3-torsion are tabulated as follows. The subgroup generators are taken from Sutherland [Sut16, Section 6.4], and are viewed as elements of  $\mathrm{GL}(3)$ . The final two columns give examples of elliptic curves with the given mod-3 Galois image with  $b = 1$  and  $b = 2$  respectively, where  $b \in \mathbb{F}_3$  is the residue of  $\mathrm{BSD}(E)$  modulo 3. The column labelled  $G_{E,3}$  lists the elements of  $G_{E,3} = \mathrm{im}(\overline{\rho_{E,3}}) \cap \mathrm{SL}(3)$  as defined in Proposition 6.1, so the residual densities can be read off directly in the column labelled  $\delta_{E,3}$  as ordered triples  $(\delta_{E,3}(0), \delta_{E,3}(-b), \delta_{E,3}(b))$ , which is used in Theorem 6.4.

Table 1: mod-3 Galois images of elliptic curves without 3-torsion

$\mathrm{im}(\overline{\rho_{E,3}})$	Generators of $\mathrm{im}(\overline{\rho_{E,3}})$	$G_{E,3}$	$\delta_{E,3}$	$b = 1$	$b = 2$
$\mathrm{GL}(3)$	$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 2 & 0 \end{pmatrix}$	$\mathrm{SL}(3)$	$\frac{3}{8}, \frac{3}{8}, \frac{1}{4}$	11a2	11a1
3B.1.2	$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$	1, 0, 0	19a2	14a3
3B	$\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 2 & 2 \\ 0 & 2 \end{pmatrix}$	$\frac{1}{2}, \frac{1}{2}, 0$	50b3	50b1
3Cs	$\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$	$\frac{1}{2}, \frac{1}{2}, 0$	304e2	304b2
3Nn	$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$ $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 2 & 2 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}$	$\frac{1}{8}, \frac{1}{8}, \frac{3}{4}$	704e1	245b1
3Ns	$\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}$	$\frac{1}{4}, \frac{1}{4}, \frac{1}{2}$	1690d1	338d1

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

### 3-adic Galois images of elliptic curves with 3-torsion

The possible 3-adic Galois images are classified [RSZB22, Corollary 1.3.1 and Corollary 12.3.3], and those of elliptic curves with 3-torsion are tabulated as follows. The subgroup generators are taken from Rouse–Sutherland–Zureick–Brown [RSZB22, Software Repository], and are viewed as elements of  $\mathrm{GL}(3^m)$  if their corresponding 3-adic Galois images are of the form  $3^m.i.g.n.$  The column labelled  $M_{E,3}$  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 final two columns give examples of elliptic curves with the given 3-adic Galois image with  $b = 1$  and  $b = 2$  respectively, where  $b \in \mathbb{F}_3$  is the residue of  $3 \mathrm{BSD}(E)$  modulo 3. The column labelled  $\#G_{E,9}$  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 labelled  $\delta_{E,3}$  as ordered triples  $(\delta_{E,3}(0), \delta_{E,3}(-b), \delta_{E,3}(b))$ , which is used in Theorem 6.4.



Table 2: 3-adic Galois images of elliptic curves with 3-torsion

$\text{im}(\rho_{E,3})$	$\text{im}(\overline{\rho_{E,3}})$	Generators of $\text{im}(\rho_{E,3})$	$M_{E,3}$	$\#G_{E,9}$	$\delta_{E,3}$	$b = 1$	$b = 2$
3.8.0.1	3B.1.1	$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}$	$\begin{pmatrix} 4 & 0 \\ 0 & 2 \end{pmatrix}$	243	$\frac{5}{9}, \frac{2}{9}, \frac{2}{9}$	20a2	20a1
3.24.0.1	3Cs.1.1	$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix}$	81	1, 0, 0	26a1	14a1
9.24.0.1	3B.1.1	$\begin{pmatrix} 7 & 5 \\ 0 & 8 \end{pmatrix} \begin{pmatrix} 1 & 8 \\ 0 & 4 \end{pmatrix}$	$\begin{pmatrix} 4 & 0 \\ 0 & 2 \end{pmatrix}$	81	1, 0, 0	189c3	702e3
9.24.0.2	3B.1.1	$\begin{pmatrix} 7 & 3 \\ 0 & 8 \end{pmatrix} \begin{pmatrix} 7 & 2 \\ 6 & 2 \end{pmatrix}$	$\begin{pmatrix} 4 & 0 \\ 0 & 2 \end{pmatrix}$	81	$\frac{1}{3}, \frac{2}{3}, 0$		
9.72.0.1	3Cs.1.1	$\begin{pmatrix} 5 & 6 \\ 3 & 1 \end{pmatrix} \begin{pmatrix} 4 & 6 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 5 & 0 \\ 0 & 1 \end{pmatrix}$	N/A	27	1, 0, 0	54b1	
9.72.0.2	3Cs.1.1	$\begin{pmatrix} 8 & 3 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 8 & 6 \\ 0 & 4 \end{pmatrix} \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 8 & 0 \\ 0 & 4 \end{pmatrix}$	27	1, 0, 0	54a1	
9.72.0.3	3Cs.1.1	$\begin{pmatrix} 8 & 3 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 5 & 0 \\ 0 & 7 \end{pmatrix}$	$\begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix}$	27	1, 0, 0	19a1	7094c1
9.72.0.4	3Cs.1.1	$\begin{pmatrix} 2 & 3 \\ 6 & 7 \end{pmatrix} \begin{pmatrix} 1 & 6 \\ 6 & 1 \end{pmatrix} \begin{pmatrix} 4 & 3 \\ 6 & 4 \end{pmatrix}$	$\begin{pmatrix} 5 & 0 \\ 0 & 4 \end{pmatrix}$	27	1, 0, 0		
9.72.0.5	3B.1.1	$\begin{pmatrix} 1 & 2 \\ 0 & 8 \end{pmatrix} \begin{pmatrix} 1 & 7 \\ 0 & 4 \end{pmatrix}$	N/A	27	1, 0, 0	54b3	
9.72.0.6	3B.1.1	$\begin{pmatrix} 1 & 5 \\ 0 & 8 \end{pmatrix} \begin{pmatrix} 4 & 1 \\ 0 & 8 \end{pmatrix}$	$\begin{pmatrix} 4 & 0 \\ 0 & 8 \end{pmatrix}$	27	1, 0, 0		
9.72.0.7	3B.1.1	$\begin{pmatrix} 4 & 4 \\ 0 & 5 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 8 \end{pmatrix}$	$\begin{pmatrix} 4 & 0 \\ 0 & 5 \end{pmatrix}$	27	1, 0, 0		
9.72.0.8	3B.1.1	$\begin{pmatrix} 7 & 7 \\ 6 & 4 \end{pmatrix} \begin{pmatrix} 7 & 7 \\ 6 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix}$	27	$\frac{1}{3}, \frac{2}{3}, 0$		
9.72.0.9	3B.1.1	$\begin{pmatrix} 4 & 2 \\ 3 & 5 \end{pmatrix} \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 7 & 2 \\ 3 & 1 \end{pmatrix}$	$\begin{pmatrix} 4 & 1 \\ 0 & 5 \end{pmatrix}$	27	$\frac{1}{3}, \frac{2}{3}, 0$		
9.72.0.10	3B.1.1	$\begin{pmatrix} 1 & 5 \\ 6 & 5 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 8 \end{pmatrix}$	$\begin{pmatrix} 4 & 0 \\ 0 & 8 \end{pmatrix}$	27	$\frac{1}{3}, \frac{2}{3}, 0$	486c1	
27.72.0.1	3B.1.1	$\begin{pmatrix} 7 & 23 \\ 0 & 5 \end{pmatrix} \begin{pmatrix} 1 & 8 \\ 9 & 16 \end{pmatrix}$	$\begin{pmatrix} 4 & 0 \\ 0 & 2 \end{pmatrix}$	81	1, 0, 0		
27.648.13.25	3B.1.1	$\begin{pmatrix} 16 & 4 \\ 0 & 16 \end{pmatrix} \begin{pmatrix} 1 & 17 \\ 0 & 26 \end{pmatrix}$	$\begin{pmatrix} 4 & 0 \\ 0 & 5 \end{pmatrix}$	27	1, 0, 0	N/A	N/A
27.648.18.1	3B.1.1	$\begin{pmatrix} 16 & 15 \\ 9 & 25 \end{pmatrix} \begin{pmatrix} 10 & 16 \\ 9 & 17 \end{pmatrix} \begin{pmatrix} 7 & 22 \\ 6 & 4 \end{pmatrix}$	$\begin{pmatrix} 4 & 1 \\ 0 & 5 \end{pmatrix}$	27	$\frac{1}{3}, \frac{2}{3}, 0$	108a1	36a1
27.1944.55.31	3Cs.1.1	$\begin{pmatrix} 2 & 18 \\ 12 & 25 \end{pmatrix} \begin{pmatrix} 16 & 18 \\ 21 & 16 \end{pmatrix}$	$\begin{pmatrix} 5 & 0 \\ 0 & 4 \end{pmatrix}$	9	1, 0, 0	N/A	N/A
27.1944.55.37	3Cs.1.1	$\begin{pmatrix} 17 & 6 \\ 21 & 10 \end{pmatrix} \begin{pmatrix} 2 & 3 \\ 3 & 25 \end{pmatrix}$	$\begin{pmatrix} 5 & 0 \\ 3 & 4 \end{pmatrix}$	9	1, 0, 0	27a1	N/A
27.1944.55.43	3B.1.1	$\begin{pmatrix} 19 & 10 \\ 18 & 8 \end{pmatrix} \begin{pmatrix} 4 & 11 \\ 3 & 16 \end{pmatrix}$	$\begin{pmatrix} 4 & 4 \\ 0 & 5 \end{pmatrix}$	9	$\frac{1}{3}, \frac{2}{3}, 0$	243b1	N/A
27.1944.55.44	3B.1.1	$\begin{pmatrix} 10 & 23 \\ 3 & 13 \end{pmatrix} \begin{pmatrix} 13 & 13 \\ 0 & 14 \end{pmatrix}$	$\begin{pmatrix} 4 & 4 \\ 0 & 5 \end{pmatrix}$	9	$\frac{1}{3}, \frac{2}{3}, 0$	N/A	N/A

**Remark A.1.** Note that 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 [Col] yields no examples satisfying  $3 \nmid c_0(E)$  and  $L(E, 1) \neq 0$ , 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 parameterised by the associated modular curve, and then investigate the divisibility of Tamagawa numbers as in Lemma 4.1. Such 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.

## References

- [BC21] David Burns and Daniel Macias Castillo. On refined conjectures of Birch and Swinnerton-Dyer type for Hasse–Weil–Artin  $L$ -series, 2021.
- [BCS24] Ashay Burungale, Francesc Castella, and Christopher Skinner. Base change and Iwasawa main conjectures for  $GL_2$ , 2024.
- [BD07] Thanasis Bouganis and Vladimir Dokchitser. Algebraicity of  $L$ -values for elliptic curves in a false Tate curve tower. *Mathematical Proceedings of the Cambridge Philosophical Society*, 142(2):193–204, 2007.
- [BKY19] Dongho Byeon, Taekyung Kim, and Donggeon Yhee. A conjecture of Gross and Zagier: case  $E(\mathbb{Q})_{\text{tor}} \cong \mathbb{Z}/3\mathbb{Z}$ . *International Journal of Number Theory*, 15(9):1793–1800, 2019.
- [Ble13] Werner Bley. The equivariant Tamagawa number conjecture and modular symbols. *Mathematische Annalen*, 356(1):179–190, 2013.
- [Bon11] Cédric Bonnafé. *Representations of  $SL_2(\mathbb{F}_q)$* , volume 13 of *Algebra and Applications*. Springer-Verlag London, Ltd., London, 2011.
- [BR22] Alexander Barrios and Manami Roy. Local data of rational elliptic curves with nontrivial torsion. *Pacific Journal of Mathematics*, 318(1):1–42, 2022.
- [Col] The LMFDB Collaboration. The  $L$ -functions and modular forms database.
- [Cre92] John Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, 1992.
- [DEW21] Vladimir Dokchitser, Robert Evans, and Hanneke Wiersema. On a BSD-type formula for  $L$ -values of Artin twists of elliptic curves. *Journal für die Reine und Angewandte Mathematik. [Crelle’s Journal]*, 773:199–230, 2021.
- [Edi91] Bas Edixhoven. On the Manin constants of modular elliptic curves. In *Arithmetic algebraic geometry (Texel, 1989)*, volume 89 of *Progr. Math.*, pages 25–39. Birkhäuser Boston, Boston, MA, 1991.
- [FKK12] Jack Fearnley, Hershy Kisilevsky, and Masato Kuwata. Vanishing and non-vanishing Dirichlet twists of  $L$ -functions of elliptic curves. *Journal of the London Mathematical Society. Second Series*, 86(2):539–557, 2012.
- [GZ86] Benedict Gross and Don Zagier. Heegner points and derivatives of  $L$ -series. *Inventiones Mathematicae*, 84(2):225–320, 1986.
- [Kat04] Kazuya Kato.  $p$ -adic Hodge theory and values of zeta functions of modular forms. *Astérisque*, 295:ix, 117–290, 2004.
- [KN22] Hershy Kisilevsky and Jungbae Nam. Small algebraic central values of twists of elliptic  $L$ -functions, 2022.
- [Kol88] Victor Kolyvagin. Finiteness of  $E(\mathbb{Q})$  and  $\text{III}(E, \mathbb{Q})$  for a subclass of Weil curves. *Izvestiya Akademii Nauk SSSR. Seriya Matematicheskaya*, 52(3):522–540, 670–671, 1988.
- [KY24] Timo Keller and Mulun Yin. On the anticyclotomic Iwasawa theory of newforms at Eisenstein primes of semistable reduction, 2024.
- [Lor11] Dino Lorenzini. Torsion and Tamagawa numbers. *Université de Grenoble. Annales de l’Institut Fourier*, 61(5):1995–2037, 2011.
- [Man72] Ju. I. Manin. Parabolic points and zeta functions of modular curves. *Izvestiya Akademii Nauk SSSR. Seriya Matematicheskaya*, 36:19–66, 1972.

- [Mel23] Mentzelos Melistas. A divisibility related to the Birch and Swinnerton-Dyer conjecture. *Journal of Number Theory*, 245:150–168, 2023.
- [RSZB22] Jeremy Rouse, Andrew Sutherland, and David Zureick-Brown.  $\ell$ -adic images of Galois for elliptic curves over  $\mathbb{Q}$  (and an appendix with John Voight). *Forum of Mathematics. Sigma*, 10:Paper No. e62, 63, 2022.
- [Ser72] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Inventiones Mathematicae*, 15(4):259–331, 1972.
- [Shi71] Goro Shimura. *Introduction to the arithmetic theory of automorphic functions*, volume No. 1 of *Kanô Memorial Lectures*. Iwanami Shoten Publishers, Tokyo; Princeton University Press, Princeton, NJ, 1971. Publications of the Mathematical Society of Japan, No. 11.
- [Ste89] Glenn Stevens. Stickelberger elements and modular parametrizations of elliptic curves. *Inventiones Mathematicae*, 98(1):75–106, 1989.
- [Sut16] Andrew Sutherland. Computing images of Galois representations attached to elliptic curves. *Forum of Mathematics. Sigma*, 4:Paper No. e4, 79, 2016.
- [Č18] Kestutis Česnavičius. The Manin constant in the semistable case. *Compositio Mathematica*, 154(9):1889–1920, 2018.
- [WW22] Hanneke Wiersema and Christian Wuthrich. Integrality of twisted  $L$ -values of elliptic curves. *Documenta Mathematica*, 27:2041–2066, 2022.
- [Zyw15] David Zywina. On the possible images of the mod  $\ell$  representations associated to elliptic curves over  $\mathbb{Q}$ , 2015.