J. reine angew. Math., Ahead of Print
DOI 10.1515/crelle-2020-0036

Journal für die reine und angewandte Mathematik

On a BSD-type formula for L-values of Artin twists of elliptic curves

By *Vladimir Dokchitser* at University College London,
Robert Evans at King's College London and *Hanneke Wiersema* at King's College London

Abstract. This is an investigation into the possible existence and consequences of a Birch–Swinnerton-Dyer-type formula for L-functions of elliptic curves twisted by Artin representations. We translate expected properties of L-functions into purely arithmetic predictions for elliptic curves, and show that these force some peculiar properties of the Tate–Shafarevich group, which do not appear to be tractable by traditional Selmer group techniques. In particular, we exhibit settings where the different p-primary components of the Tate–Shafarevich group do not behave independently of one another. We also give examples of "arithmetically identical" settings for elliptic curves twisted by Artin representations, where the associated L-values can nonetheless differ, in contrast to the classical Birch–Swinnerton-Dyer conjecture.

1. Introduction

The Birch–Swinnerton-Dyer conjecture classically provides a connection between the arithmetic of elliptic curves and their L-functions. This link is in many ways still mysterious. Indeed, some properties of L-functions do not obviously correspond to arithmetic properties of elliptic curves and vice versa, a classical example being the compatibility of the conjecture with isogenies, which is a highly non-trivial theorem of Cassels. In this article we focus on factorisation of L-functions: when $E/\mathbb{Q}$ is an elliptic curve and $F/\mathbb{Q}$ a finite extension, $L(E/F, s)$ factorises as a product of L-functions of twists of E by Artin representations $L(E, \rho, s)$. We investigate what standard conjectures say specifically for these twisted L-functions. Ideally, we would like to give a BSD-type formula for the leading term at $s = 1$ for $L(E, \rho, s)$, but, as we shall explain, there is a significant barrier to this. However, we shall provide a tool for extracting explicit arithmetic predictions, and illustrate its use by exhibiting new phenomena about the behaviour of Tate–Shafarevich groups, Selmer groups and rational points.

The first named author was supported by a Royal Society University Research Fellowship. The third named author was supported by the Engineering and Physical Sciences Research Council (EP/L015234/1), through the EPSRC Centre for Doctoral Training in Geometry and Number Theory (the London School of Geometry and Number Theory) at University College London.

1.1. BSD formula for Artin twists. The Birch–Swinnerton-Dyer conjecture states that

$$\operatorname{ord}_{s=1} L(E/F, s) = \operatorname{rk} E/F,$$

and that the leading term of the Taylor series at $s = 1$ of the L-function is given by

$$(\dagger) \qquad \lim_{s\to 1} \frac{L(E/F,s)}{(s-1)^r} \cdot \frac{\sqrt{|\Delta_F|}}{\Omega_+(E)^{r_1+r_2}|\Omega_-(E)|^{r_2}} = \frac{\operatorname{Reg}_{E/F}\,|Ш_{E/F}|C_{E/F}}{|E(F)_{\mathrm{tors}}|^2},$$

where r is the order of the zero, (r_1, r_2) is the signature of F, $\Omega_\pm$ are the periods of E and $C_{E/F}$ is the product of Tamagawa numbers and other local fudge factors from finite places (see Section 1.5). Of course, the formula implicitly assumes that the Tate–Shafarevich group $Ш_{E/F}$ is finite.

Just as the Dedekind ζ-function can be expressed as a product of Artin L-functions, so the L-function $L(E/F, s)$ can be written as a product of twisted L-functions $L(E, \rho, s)$ for Artin representations that factor through the Galois closure of $F/\mathbb{Q}$. The (conjectural) analogue of the Birch–Swinnerton-Dyer rank formula is well known in this context (see e.g. [10, Section 2]):

Conjecture 1. For an elliptic curve $E/\mathbb{Q}$ and an Artin representation ρ over $\mathbb{Q}$,

$$\operatorname{ord}_{s=1} L(E, \rho, s) = \langle \rho, E(K)_{\mathbb{C}} \rangle.$$

Here, and throughout, $E(K)_{\mathbb{C}} = E(K) \otimes_{\mathbb{Z}} \mathbb{C}$, where K is any finite Galois extension of $\mathbb{Q}$ such that ρ factors through $\mathrm{Gal}(K/\mathbb{Q})$, and $\langle \cdot, \cdot \rangle$ denotes the usual representation theoretic inner product of characters. In other words, the conjecture predicts that, for an (irreducible) ρ, the order of vanishing of $L(E, \rho, s)$ is the "multiplicity" of ρ in the group of K-rational points of E.

However, the situation with the second part of the Birch–Swinnerton-Dyer conjecture appears to be much more difficult.

Problem 2. Formulate a BSD-like formula for the leading term at $s = 1$ of $L(E, \rho, s)$.

There appears to be a barrier to finding such an expression, as there are "arithmetically identical" settings giving rise to different L-values. We write $\mathscr{L}(E, \rho)$ for the modification of the leading term of $L(E, \rho, s)$ analogous to the left-hand side of (†) (see Definition 12).

Example 3 (see also Section 4). The elliptic curves with Cremona labels $E = 307\mathrm{a}1$ and $E' = 307\mathrm{c}1$ have the same conductor, same discriminant, trivial Tate–Shafarevich group, no rational points and trivial local Tamagawa numbers both over $\mathbb{Q}$ and over $\mathbb{Q}(\zeta_{11})^+$. However, for a Dirichlet character χ of order 5 and conductor 11, one has $\mathscr{L}(E, \chi) \neq \mathscr{L}(E', \chi)$. Specifically, $\mathscr{L}(E, \chi) = 1$, while $\mathscr{L}(E', \chi) = (\frac{1\pm\sqrt{5}}{2})^2$, the sign of $\pm\sqrt{5}$ depending on the choice of χ.

1.2. An arithmetic conjecture and its consequences. We will not propose an exact expression for the hypothetical $\mathrm{BSD}(E, \rho)$ term for the conjectural formula

$$\text{“}\mathscr{L}(E, \rho) = \mathrm{BSD}(E, \rho)\text{”}.$$

However, based on the behaviour of L-functions, we will show that $\mathrm{BSD}(E, \rho)$ must satisfy

the list of properties given in Conjecture 4 below. One of the roles of $\mathrm{BSD}(E,\rho)$ is that it lets one decompose the Birch–Swinnerton-Dyer quotient

$$\mathrm{BSD}(E/F) = \frac{\mathrm{Reg}_{E/F}\,|Ш_{E/F}|C_{E/F}}{|E(F)_{\mathrm{tors}}|^2}$$

according to Artin representations, analogously to the factorisation of L-functions. This may at first glance look almost vacuous, but, as we will explain, the existence of such a decomposition has a range of consequences for Selmer groups, Tate–Shafarevich groups and ranks of elliptic curves.

We write $\mathbb{Q}(\rho)$ for the field generated by the values of the character of ρ, write ρ^* for the dual representation, and w_ρ and $w_{E,\rho}$ for the root number of ρ and of the twist of E by ρ, respectively.

Conjecture 4. Let $E/\mathbb{Q}$ be an elliptic curve. For every Artin representation ρ over $\mathbb{Q}$ there is an invariant $\mathrm{BSD}(E,\rho)\in\mathbb{C}^\times$ with the following properties. Let ρ and τ be Artin representations that factor through $\mathrm{Gal}(K/\mathbb{Q})$.

(C1) $\mathrm{BSD}(E/F) = \mathrm{BSD}(E, \mathrm{Ind}_{F/\mathbb{Q}}\,\mathbf{1})$ for a number field F (and $Ш_{E/F}$ is finite).

(C2) $\mathrm{BSD}(E,\rho\oplus\tau) = \mathrm{BSD}(E,\rho)\,\mathrm{BSD}(E,\tau)$.

(C3) $\mathrm{BSD}(E,\rho) = \mathrm{BSD}(E,\rho^*)\cdot(-1)^r w_{E,\rho} w_\rho^{-2}$, where $r = \langle\rho, E(K)_{\mathbb{C}}\rangle$.

(C4) If ρ is self-dual, then $\mathrm{BSD}(E,\rho)\in\mathbb{R}$ and $\operatorname{sign}\mathrm{BSD}(E,\rho) = \operatorname{sign} w_\rho$.

If $\langle\rho, E(K)_{\mathbb{C}}\rangle = 0$, then moreover:

(C5) $\mathrm{BSD}(E,\rho)\in\mathbb{Q}(\rho)^\times$ and $\mathrm{BSD}(E,\rho^{\mathfrak{g}}) = \mathrm{BSD}(E,\rho)^{\mathfrak{g}}$ for all $\mathfrak{g}\in\mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})$.

(C6) If ρ is a non-trivial primitive Dirichlet character of order d, and either the conductors of E and ρ are coprime or E is semistable and has no non-trivial isogenies over $\mathbb{Q}$, then $\mathrm{BSD}(E,\rho)\in\mathbb{Z}[\zeta_d]$.

Theorem 5 (see Corollary 25). *Conjecture* 4 *holds assuming the analytic continuation of L-functions $L(E,\rho,s)$, their functional equation, the Birch–Swinnerton-Dyer conjecture, Deligne's period conjecture, Stevens's Manin constant conjecture for $E/\mathbb{Q}$ and the Riemann hypothesis for $L(E,\rho,s)$.*

Note that the statement of the conjecture is free of L-functions. Morally, it should be purely a property of Selmer groups. However, it has some consequences that do not appear to be tractable with classical Selmer group techniques, as we now illustrate.

Theorem 6 (see Theorem 28, Example 29). *Let ℓ and p be primes such that the primes above p in $\mathbb{Q}(\zeta_\ell)$ are non-principal and have residue degree* 2. *If Conjecture* 4 *holds, then, for every semistable elliptic curve $E/\mathbb{Q}$ with no non-trivial isogenies, $|Ш_{E/\mathbb{Q}}[p]| = 1$ and $c_v = 1$ for all rational primes v, and for every cyclic extension $F/\mathbb{Q}$ of degree ℓ with $E(F) = E(\mathbb{Q})$,*

$$\text{if } |Ш_{E/F}[p^\infty]| = p^2, \text{ then } |Ш_{E/F}[q^\infty]| \neq 1 \text{ for some } q \neq p.$$

Roughly speaking, in the setting of the theorem the presence of the p-primary part of Ш forces some other part of Ш to be non-trivial too. It would be interesting to have a purely Selmer theoretic method that can explain such behaviour.

Conjecture 4 can also be used to show that purely local constraints can force certain Selmer groups of E over extensions $F/\mathbb{Q}$ to become non-trivial. More usual methods for achieving such criteria either use Galois module structures or Iwasawa theoretic methods (both can be used to make $\mathrm{Sel}_p(E/F)$ non-trivial for $p|[F:\mathbb{Q}]$, see e.g. [1, 9]) or use some form of the parity conjecture (this requires $[F:\mathbb{Q}]$ to be even).

Theorem 7 (see Corollary 31). *Suppose Conjecture* 4 *holds. There is an (explicit) Galois number field F of odd degree and (explicit) rational prime ℓ, such that every elliptic curve $E/\mathbb{Q}$ with additive reduction at ℓ of Kodaira type III and good reduction at other primes that ramify in $F/\mathbb{Q}$ has a non-trivial p-Selmer group $\mathrm{Sel}_p(E/F)$ for some prime $p \nmid [F:\mathbb{Q}]$.*

We will also show that Conjecture 4 can be used to establish purely theoretical results, such as the following case of the Birch–Swinnerton-Dyer conjecture for twists of elliptic curves by dihedral Artin representations (below D_{2pq} denotes the dihedral group of order $2pq$). As far as we are aware, this does not follow from known cases of the parity conjecture.

Theorem 8 (see Theorem 35). *Let $F/\mathbb{Q}$ be a Galois extension with Galois group D_{2pq}, with $p, q \equiv 3 \bmod 4$ primes, and let ρ be a faithful irreducible Artin representation that factors through $F/\mathbb{Q}$. If Conjecture* 4 *holds, then for every semistable elliptic curve $E/\mathbb{Q}$, if $\mathrm{ord}_{s=1} L(E,\rho,s)$ is odd, then $\langle \rho, E(F)_{\mathbb{C}} \rangle > 0$.*

We stress once again that Conjecture 4 ought to be purely a statement about Selmer groups, although we do not understand the extra structure on Selmer groups or on Ш that causes it: our justification of the conjecture relies on L-functions. For applications like Theorem 8 it is clearly important to find a proof that does not assume the Birch–Swinnerton-Dyer conjecture.

Problem 9. Justify Conjecture 4 assuming the Tate–Shafarevich conjecture but not the Birch–Swinnerton-Dyer conjecture.

Remark 10. The conjecture completely determines the value of $\mathrm{BSD}(E,\rho)$ for Artin representations ρ whose character is $\mathbb{Q}$-valued. Indeed, for a finite group G, the image of the Burnside ring in the rational representation ring has finite index. Thus, if ρ factors through $\mathrm{Gal}(K/\mathbb{Q})$ where $K/\mathbb{Q}$ is a finite Galois extension, there are intermediate fields F_i, F_j' of $K/\mathbb{Q}$ and a positive integer m such that $\rho^{\oplus m} \oplus \bigoplus_i \mathrm{Ind}_{F_i/\mathbb{Q}} \mathbf{1} \simeq \bigoplus_j \mathrm{Ind}_{F_j'/\mathbb{Q}} \mathbf{1}$, and so (C1), (C2) and (C4) imply that $\mathrm{BSD}(E,\rho)$ is the unique real number such that

$$\mathrm{BSD}(E,\rho)^m = \frac{\prod_j \mathrm{BSD}(E/F_j')}{\prod_i \mathrm{BSD}(E/F_i)}$$

and

$$\operatorname{sign} \mathrm{BSD}(E,\rho) = \operatorname{sign} w_\rho.$$

Remark 11. As illustrated in Theorem 8 above, our method sometimes allows us to predict the existence of points of infinite order on elliptic curves (see also Section 3.3, and Theorem 33 for an example with a quaternion Galois group). We have not found a setting where we can predict the existence of rational points which is not already predicted by the

parity conjecture, or which outright contradicts it. The computations arising in our approach look very different from the theory of local root numbers, but (rather magically) always match.

1.3. L-values of Artin twists of elliptic curves. The heart of our approach to deriving Conjecture 4 lies in extracting precise consequences of L-function conjectures in the setting of Artin twists of elliptic curves. For the "L-function side" of the sought Birch–Swinnerton-Dyer formula for twists we use the following modification of the leading term of $L(E,\rho,s)$ at $s=1$. This is very carefully chosen so as to mesh well with the Birch–Swinnerton-Dyer conjecture over number fields, the functional equation and Deligne's period conjecture for Artin twists of elliptic curves (see Section 2.4) at the same time. We will show that it satisfies the analogues of (C1)–(C6) of Conjecture 4, which is our justification for the conjecture.

Definition 12. For an elliptic curve $E/\mathbb{Q}$ and an Artin representation ρ over $\mathbb{Q}$, we write

$$\mathscr{L}(E,\rho) = \lim_{s\to 1} \frac{L(E,\rho,s)}{(s-1)^r} \cdot \frac{\sqrt{\mathfrak{f}_\rho}}{\Omega_+(E)^{d^+(\rho)}|\Omega_-(E)|^{d^-(\rho)} w_\rho},$$

where $r = \operatorname{ord}_{s=1} L(E,\rho,s)$ is the order of the zero at $s=1$, $\sqrt{\mathfrak{f}_\rho}$ denotes the (positive) square root of the positive generator for the conductor $\mathfrak{f}_\rho$ of ρ, and $d^\pm(\rho)$ are the dimensions of the ± 1-eigenspaces of complex conjugation in its action on ρ.

Theorem 13 (Theorem 24, Corollary 26). *Let $E/\mathbb{Q}$ be an elliptic curve and let ρ be an Artin representation over $\mathbb{Q}$. Fix ζ satisfying $\zeta^2 = w_\rho^2 w_{E,\rho}^{-1}$. Suppose that for all Artin representations ψ over $\mathbb{Q}$, the L-functions $L(E,\psi,s)$ have analytic continuation to $\mathbb{C}$ and satisfy the functional equation, Deligne's period conjecture and have no zeros in the interval $(1,\infty)$. Suppose also that Stevens's Manin constant conjecture holds for $E/\mathbb{Q}$ and the Birch–Swinnerton-Dyer conjecture holds for E over number fields. Then:*

(1) $\mathscr{L}(E, \operatorname{Ind}_{F/\mathbb{Q}} \mathbf{1}) = \operatorname{BSD}(E/F)$ *for a number field F.*

(2) $\mathscr{L}(E,\rho\oplus\rho') = \mathscr{L}(E,\rho)\mathscr{L}(E,\rho')$.

(3) $\mathscr{L}(E,\rho^*) = (-1)^r\zeta^2\mathscr{L}(E,\rho)$, *where* $r = \operatorname{ord}_{s=1} L(E,\rho,s)$.

(4) *If $\rho \simeq \rho^*$ then $\mathscr{L}(E,\rho)\in\mathbb{R}$ and $w_\rho\cdot\mathscr{L}(E,\rho) > 0$.*

Henceforth suppose that moreover $L(E,\rho,1)\neq 0$. Then:

(5) $\mathscr{L}(E,\rho)\in\mathbb{Q}(\rho)$.

(6) $\mathscr{L}(E,\rho)\cdot\mathcal{O}_{\mathbb{Q}(\rho)}$ *is invariant under complex conjugation as a fractional ideal of $\mathbb{Q}(\rho)$.*

(7) $\mathscr{L}(E,\rho^{\mathfrak{g}}) = \mathscr{L}(E,\rho)^{\mathfrak{g}}$ *for all* $\mathfrak{g}\in\operatorname{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})$.

(8) ζ *is a root of unity. If $\mathfrak{f}_E$ is coprime to $\mathfrak{f}_\rho$, then* $\zeta^2 = (-1)^{d^-(\rho)} w_E^{\dim\rho}\det\rho(\mathfrak{f}_E)$, *where* $\det\rho$ *is regarded as a primitive Dirichlet character (see Notation* 15*).*

(9) $\zeta\cdot\mathscr{L}(E,\rho)\in\mathbb{Q}(\rho,\zeta)^+$*; in particular,* $\arg\mathscr{L}(E,\rho) = \arg\pm\zeta^{-1}$.

(10) *If ρ is a non-trivial primitive Dirichlet character of order d, and either $\mathfrak{f}_\rho$ is coprime to $\mathfrak{f}_E$ or E is semistable and has no non-trivial isogenies over $\mathbb{Q}$, then $\mathscr{L}(E,\rho)\in\mathbb{Z}[\zeta_d]$.*

Let

$$B = \sqrt[m]{\frac{\prod_j \operatorname{BSD}(E/F_j')}{\prod_i \operatorname{BSD}(E/F_i)}}$$

for any number fields F_i, F'_j and positive integer m that satisfy[1)]

$$\Big(\bigoplus_{\mathfrak{g}\in\mathscr{G}} \rho^{\mathfrak{g}}\Big)^m \oplus \bigoplus_i \mathrm{Ind}_{F_i/\mathbb{Q}}\,\mathbf{1} = \bigoplus_j \mathrm{Ind}_{F'_j/\mathbb{Q}}\,\mathbf{1},$$

where $\mathscr{G} = \mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})$. *Then:*

(11) $N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathscr{L}(E,\rho)) = \pm B$, *with sign* $+$ *if* m *is odd.*

(12) $N_{\mathbb{Q}(\rho)^+/\mathbb{Q}}(\zeta\cdot\mathscr{L}(E,\rho)) = \pm\sqrt{B}$ *if* $\rho \not\simeq \rho^*$ *and* $\zeta \in \mathbb{Q}(\rho)$.

(13) $N_{\mathbb{Q}(\rho,\xi)^+/\mathbb{Q}}(\zeta\cdot\mathscr{L}(E,\rho)) = \pm B$ *if* $\rho \not\simeq \rho^*$ *and* $\zeta \notin \mathbb{Q}(\rho)$.

Remark 14. The hypothesis that $L(E,\rho,s)$ has no zeros in the interval $(1,\infty)$ is an immediate consequence of the Riemann Hypothesis. The main reason why most of the results above require the assumption that the L-value is non-zero is that it features in Deligne's period conjecture. It might be possible to extend the predictions to the higher rank case using the motivic L-value conjectures (Beilinson, Bloch–Kato, Equivariant Tamagawa Number Conjecture). These may also let one generalise the integrality statement (10) to other Artin representations and to pin down the ideal generated by $\mathscr{L}(E,\rho)$ more precisely. We will not attempt to address this here.

1.4. Layout. This paper is split into three parts.

In Section 2 we extract the explicit L-value predictions of Theorem 13 from the classical conjectures and deduce Theorem 5 from them. The key technical step here is to express the periods associated to an Artin twist of an elliptic curve to the classical periods $\Omega_\pm$ (Corollary 23).

In Section 3 we develop the arithmetic consequences for elliptic curves, including Theorems 6, 7 and 8. The main ingredient is Proposition 27, which, based on Conjecture 4, lets us link easily controllable local invariants to ranks and the Tate–Shafarevich group. In view of Theorem 5 these results are all consequences of the classical conjectures on L-functions.

In Section 4 we discuss explicit examples of L-values of twists of elliptic curves by Dirichlet characters and illustrate the difficulty of refining Theorem 13 to a clean BSD-type prediction for the value of $\mathscr{L}(E,\rho)$. We end by giving several tables of examples of a similar kind to Example 3.

We have kept the three sections largely independent of one another. In particular, the reader who does not wish to grapple with the motivic background can skip directly to the arithmetic applications in Section 3 or the L-value examples in Section 4.

1.5. Notation. We fix (once and for all) an algebraic closure $\overline{\mathbb{Q}}$ inside $\mathbb{C}$. All our number fields will be subfields of this choice of $\overline{\mathbb{Q}}$.

Formally, all our Artin representations will be $\mathbb{C}$-valued; that is, defined by a group homomorphism $\rho : G_K \to \mathrm{Aut}_{\mathbb{C}}(V)$ that factors through $\mathrm{Gal}(F/K)$ for some finite Galois extension F/K and some finite-dimensional complex vector space V. We will typically work with isomorphism classes of Artin representations, without explicitly mentioning it.

[1)] These exist by Remark 10.

The following notation is used throughout the paper:

- E: an elliptic curve defined over $\mathbb{Q}$.
- $c_v(E/F)$: the local Tamagawa number of E/F_v.
- G_F: the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ of a number field $F \subseteq \overline{\mathbb{Q}}$.
- $\mathrm{Frob}_{\mathfrak{p}}$: (arithmetic) Frobenius element at a prime $\mathfrak{p}$.
- ρ^*: the dual representation of an Artin representation ρ.
- $\mathbb{Q}(\rho)$: the (abelian) extension of $\mathbb{Q}$ generated by the character values of ρ.
- $\rho^{\mathfrak{g}}$: for $\mathfrak{g} \in \mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})$, the Artin representation with character $\mathrm{Tr}\,\rho^{\mathfrak{g}} = \mathfrak{g} \circ \mathrm{Tr}\,\rho$.
- $d^{\pm}(\rho)$: the dimension of the ±1-eigenspace of complex conjugation on ρ.
- $\mathfrak{f}_\rho$: the Artin conductor of ρ.
- $\mathfrak{f}_E$: the conductor of $E/\mathbb{Q}$.
- w_ρ: the Artin root number of ρ.
- w_E: the root number of $E/\mathbb{Q}$ (the sign in the functional equation).
- $w_{E,\rho}$: the root number of the twist $E/\mathbb{Q}$ by ρ (see Section 2.5).
- $\mathrm{Ind}_{F/K}\,\rho$: $\mathrm{Ind}_{G_F}^{G_K}\,\rho$ for a field extension F/K and an Artin representation ρ over F.
- $\ominus$: the formal difference of Artin representations, i.e. $\rho_1 \ominus \rho_2 = \rho_3 \Leftrightarrow \rho_1 = \rho_2 \oplus \rho_3$.
- ζ_n: a primitive n-th root of unity.
- $N_{F/K}$: the norm map from F to K.

Notation 15. We use the convention (as in [7] Section 3.2) that the Euler factor at a prime p of $L(E,\rho,s)$ is

$$\det\bigl(\mathrm{Id} - \mathrm{Frob}_p^{-1}\, p^{-s} \;\big|\; (H^1_\ell(E)\otimes\rho)^{I_p}\bigr),$$

where I_p is the inertia group at p, $H^1_\ell(E) = H^1_{et}(E,\mathbb{Q}_\ell)\otimes_{\mathbb{Q}_\ell}\mathbb{C}$ for any embedding $\mathbb{Q}_\ell \hookrightarrow \mathbb{C}$ and any prime $\ell \neq p$.

To identify 1-dimensional Artin representations with Dirichlet characters, we use the isomorphism $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times$ given by $\sigma_a \leftrightarrow a$ for $\sigma_a : \zeta_n \to \zeta_n^a$.

We caution the reader that with these normalisations, if $L(E,s) = \sum a_n n^{-s}$ and χ is a primitive Dirichlet character of conductor coprime to that of E, then

$$L(E,\chi,s) = \sum_{n=1}^{\infty} \overline{\chi(n)} a_n n^{-s}.$$

Notation 16. Given an elliptic curve $E/\mathbb{Q}$, let ω be a global minimal differential on E, let c_∞ be the number of connected components of $E(\mathbb{R})$ and let $\gamma^{\pm}$ be a generator for the subgroup of $H_1(E(\mathbb{C}),\mathbb{Z})$ where complex conjugation acts as multiplication by ±1.

We define the $\pm$-periods of E to be

$$\Omega_+(E) = c_\infty \cdot \int_{\gamma^+} \omega \quad \text{and} \quad \Omega_-(E) = \int_{\gamma^-} \omega,$$

with $\gamma^{\pm}$ oriented so that $\Omega_+(E) \in \mathbb{R}_{>0}$ and $\Omega_-(E) \in i\mathbb{R}_{>0}$.

Notation 17. For an elliptic curve $E/\mathbb{Q}$ and a number field F, we define

$$C_{E/F} = \prod_v c_v(E/F) \left| \frac{\omega}{\omega_v^{\min}} \right|_v,$$

where v runs over the finite places of F, ω is a global minimal differential for $E/\mathbb{Q}$ and $\omega_v^{\min}$ is a minimal differential at v. By $\omega/\omega_v^{\min}$ we mean any scalar $\lambda \in F^\times$ that satisfies $\omega = \lambda\omega_v^{\min}$. In terms of minimal discriminants, if E is given by a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with discriminant Δ_E and $\omega = \frac{dx}{2y+a_1x+a_3}$, then

$$\left| \frac{\omega}{\omega_v^{\min}} \right|_v^{-12} = \left| \frac{\Delta_E}{\Delta_{E,v}^{\min}} \right|_v.$$

Notation 18. For an elliptic curve $E/\mathbb{Q}$ and a number field F, we define

$$\mathrm{BSD}(E/F) = \frac{\mathrm{Reg}_{E/F}\, |Ш_{E/F}| C_{E/F}}{|E(F)_{\mathrm{tors}}|^2}.$$

We also briefly recall Stevens's version of the Manin constant conjecture ([12, Conjecture I]):

Conjecture 19 (Stevens's Manin constant conjecture). Every elliptic curve over $\mathbb{Q}$ of conductor N admits a modular parametrisation $X_1(N) \to E$ with Manin constant 1.

Acknowledgement. The authors would like to thank the referee for their careful reading of the manuscript and their suggestions and corrections, Chris Wuthrich for pointing out an issue in our original claim about integrality of L-values and for fixing it in [16], and David Burns for his valuable comments on a draft of the present article.

2. Artin twists of elliptic curves

In order to explain the implications of Deligne's period conjecture for Artin twists of elliptic curves, we first recall the relevant definitions from the theory of motives. We shall follow closely the presentations given in [4, Section 4] and [15, Section 2] and refer the reader to Deligne's article [5] for a more detailed account.

Notation 20. The following additional notation applies only in this section:

- ι: the element of $G_{\mathbb{Q}}$ corresponding to complex conjugation.
- $\mathfrak{F}$: a number field (inside our fixed algebraic closure $\overline{\mathbb{Q}}$, as always).
- $\mathfrak{F}_{\mathbb{C}}$: the ring $\mathfrak{F} \otimes \mathbb{C}$ (unadorned tensor products are over $\mathbb{Q}$).
- $\mathfrak{F}_\ell$: the ring $\mathfrak{F} \otimes \mathbb{Q}_\ell \simeq \prod_{\lambda|\ell} \mathfrak{F}_\lambda$, where $\mathfrak{F}_\lambda$ is the completion of $\mathfrak{F}$ at the prime λ.
- $\Sigma_{\mathfrak{F}}$: the set of real and complex embeddings $\mathfrak{F} \to \mathbb{C}$.
- $\varepsilon(\rho)$: the epsilon factor of an Artin representation ρ at $s = 0$, i.e. $\varepsilon(\rho) = w_\rho\sqrt{\mathfrak{f}_\rho}$.

2.1. Motives. It will be sufficient for our purposes to view motives in the naive sense; that is, as a collection of vector spaces with certain additional structures and comparison isomorphisms between them. In particular, a *(homogeneous) motive* M over $\mathbb{Q}$ with coefficients in a number field $\mathfrak{F}$, dimension d and weight w carries the following data:

(i) (a) A d-dimensional $\mathfrak{F}$-vector space $H_B(M)$ (the *Betti realisation*).

(b) An $\mathfrak{F}$-linear involution F_∞ on $H_B(M)$.

(c) A Hodge decomposition into free $\mathfrak{F}_{\mathbb{C}}$-modules

$$H_B(M) \otimes \mathbb{C} = \bigoplus_{r+s=w} H^{r,s}(M)$$

such that $F_\infty H^{r,s}(M) = H^{s,r}(M)$.

(ii) (a) A d-dimensional $\mathfrak{F}$-vector space $H_{\mathrm{dR}}(M)$ (the *de Rham realisation*).

(b) A decreasing filtration $\{F^k H_{\mathrm{dR}}(M) : k \in \mathbb{Z}\}$ of $\mathfrak{F}$-subspaces of $H_{\mathrm{dR}}(M)$.

(iii) (a) For each prime ℓ, a free $\mathfrak{F}_\ell$-module $H_\ell(M)$ of rank d (the *ℓ-adic realisation*).

(b) For each prime ℓ, a continuous action of $G_{\mathbb{Q}}$ on $H_\ell(M)$.

(iv) A comparison isomorphism between $\mathfrak{F}_{\mathbb{C}}$-modules

$$I_{M,\infty} : H_B(M) \otimes \mathbb{C} \xrightarrow{\sim} H_{\mathrm{dR}}(M) \otimes \mathbb{C}$$

such that $I_{M,\infty} \circ (F_\infty \otimes \iota) = (\mathrm{id} \otimes \iota) \circ I_{M,\infty}$ and

$$I_{M,\infty}\Big(\bigoplus_{r \geq k} H^{r,s}(M)\Big) = F^k H_{\mathrm{dR}}(M) \otimes \mathbb{C}.$$

Remark 21. Comparison isomorphisms between other realisations are also part of the data carried by M; however, as we shall not need these for the work that follows, we choose to omit them here and refer the interested reader to [15, Sections 2.5 and 2.6].

2.2. Motivic L-functions. Let M be a motive over $\mathbb{Q}$ with coefficients in $\mathfrak{F}$. For any prime number ℓ, identifying $\mathfrak{F}_\ell$ with $\prod_{\lambda|\ell} \mathfrak{F}_\lambda$ gives rise to a decomposition

$$H_\ell(M) = \bigoplus_{\lambda|\ell} H_\lambda(M),$$

where $H_\lambda(M)$ is the image of $H_\ell(M)$ under scalar multiplication by unity in $\mathfrak{F}_\lambda$.

For each prime number p, let $D_p \subseteq G_{\mathbb{Q}}$ be a choice of decomposition group at p and let $I_p \subseteq D_p$ be the corresponding inertia subgroup. The *local polynomial of M at p* is

$$P_p(M,t) = \det\big(\mathrm{id} - t\,\mathrm{Frob}_p^{-1} \;\big|\; H_\lambda(M)^{I_p}\big),$$

where λ is a prime of $\mathfrak{F}$ not lying over p. We assume the standard hypothesis that $P_p(M,t)$ is independent of the choice of λ and has coefficients in $\mathfrak{F}$. For each $\sigma \in \Sigma_{\mathfrak{F}}$, we define

$$L(\sigma, M, s) = \prod_p \sigma P_p(M, p^{-s})^{-1} \in \mathbb{C},$$

where $\sigma P_p(M, X) \in \sigma\mathfrak{F}[X] \subset \mathbb{C}[X]$; the expression converges for s with sufficiently large real part. It is conjectured that each $L(\sigma, M, s)$ admits a meromorphic continuation to the entire complex plane which satisfies a functional equation of the form

$$L_\infty(M, s)L(\sigma, M, s) = \varepsilon(\sigma, M, s)L_\infty(M^*, 1 - s)L(\sigma, M^*, 1 - s),$$

where the Euler factor at infinity $L_\infty(M, s)$ is a product of gamma functions which does not depend on σ (see [5, Proposition 2.5]) and the epsilon factor $\varepsilon(\sigma, M, s)$ is a product of a constant and an exponential (see [14] for the details and extra hypotheses required for this construction).

It is convenient, by identifying $\mathfrak{F}_\mathbb{C}$ with $\mathbb{C}^{\Sigma_\mathfrak{F}}$ via the usual canonical isomorphism of $\mathbb{C}$-algebras,

$$x \otimes z \mapsto (z\sigma(x) : \sigma \in \Sigma_\mathfrak{F}),$$

to form a single L-function associated with M which takes values in $\mathfrak{F}_\mathbb{C}$:

$$L(M, s) = (L(\sigma, M, s) : \sigma \in \Sigma_\mathfrak{F}).$$

2.3. Periods. Let M be a motive over $\mathbb{Q}$ with coefficients in $\mathfrak{F}$. For simplicity, we shall restrict to the case where M has odd weight w. Let $H_B(M)^\pm$ denote the ±1-eigenspaces of the endomorphism F_∞ and let

$$H_{\mathrm{dR}}(M)^\pm = \frac{H_{\mathrm{dR}}(M)}{F^{1+\lfloor w/2\rfloor}H_{\mathrm{dR}}(M)}$$

for both choices of sign. The *$\pm$-period map* $\alpha_M^\pm$ of M is the composition of the following $\mathfrak{F}_\mathbb{C}$-linear maps:

$$H_B(M)^\pm \otimes \mathbb{C} \to H_B(M) \otimes \mathbb{C} \xrightarrow{\sim} H_{\mathrm{dR}}(M) \otimes \mathbb{C} \to H_{\mathrm{dR}}(M)^\pm \otimes \mathbb{C},$$

where the first map is induced by inclusion, the second map is the Betti-de Rham comparison isomorphism, and the last map is induced by the natural quotient map. It follows from [5, Section 1.7] that $\alpha_M^\pm$ is an isomorphism. The *$\pm$-period* of M, denoted by $c^\pm(M)$, is defined to be the residue class

$$\det(\alpha_M^\pm) \bmod \mathfrak{F}^\times$$

in $\mathfrak{F}_\mathbb{C}^\times/\mathfrak{F}^\times$, where the determinant of the $\pm$-period map is calculated with respect to $\mathfrak{F}$-bases. As above, by identifying $\mathfrak{F}_\mathbb{C}$ with $\mathbb{C}^{\Sigma_\mathfrak{F}}$, we can also view $c^\pm(M)$ as a "tuple"

$$c^\pm(M) = (c^\pm(\sigma, M) \in \mathbb{C}^\times/\mathfrak{F}^\times : \sigma \in \Sigma_\mathfrak{F}).$$

2.4. Deligne's period conjecture. Let M be a motive over $\mathbb{Q}$ with coefficients in $\mathfrak{F}$. We retain the assumption that M has odd weight. We say that M is *critical (at $s = 0$)* if, whenever $j < k$ and $H^{j,k}(M) \neq 0$, one has $j < 0$ and $k \geq 0$. See [4, Lemma 3] for a proof that this is equivalent to the definition of criticality given in [5].

Suppose that M is critical and fix a choice of representative for the period $c^+(M)$ in $\mathfrak{F}_\mathbb{C}^\times$. Then [5, Conjectures 2.7 and 2.8] assert that:

(1) $\mathrm{ord}_{s=0} L(\sigma, M, s)$ is independent of $\sigma \in \Sigma_\mathfrak{F}$ and is non-negative.

(2) If $L(M, 0) \neq 0$, there exists $x \in \mathfrak{F}^\times$ such that, for all $\sigma \in \Sigma_\mathfrak{F}$, one has

$$L(\sigma, M, 0) = \sigma(x)c^+(\sigma, M).$$

2.5. The motive associated to a twist. Let E be an elliptic curve over $\mathbb{Q}$ and let ρ be an Artin representation over $\mathbb{Q}$. Choose any finite abelian extension $\mathfrak{F}/\mathbb{Q}$ over which ρ can be realised and let τ be an $\mathfrak{F}$-linear representation of $G_{\mathbb{Q}}$ such that $\mathbb{C} \otimes_{\mathfrak{F}} \tau \simeq \rho$.

In order to understand Deligne's period conjecture in the setting of Artin twists of elliptic curves, we are led to consider the tensor product motive $h^1(E)(1) \otimes [\tau]$, whose associated realisations and comparison isomorphisms arise by taking the tensor product of the corresponding data for the motives $h^1(E)(1)$ and $[\tau]$ (see [15, Examples 2.1B and 2.1C] for detailed information about the latter two motives). In particular, one has that

$$L(h^1(E)(1) \otimes [\tau], s) = (L(E, \rho^\gamma, s+1) : \gamma \in \mathrm{Gal}(\mathfrak{F}/\mathbb{Q})),$$

where $L(E, \rho, s)$ is the Artin-twisted Hasse–Weil L-function whose construction is described explicitly in [7, Section 3.2]. We recall from [7, Section 3.2] that $L(E, \rho, s)$ is conjectured to admit an analytic continuation to the whole complex plane which satisfies a functional equation of the form

$$\Gamma_{\mathbb{C}}(s)^{\dim \rho} L(E, \rho, s) = \varepsilon(E, \rho, s) \Gamma_{\mathbb{C}}(2-s)^{\dim \rho} L(E, \rho^*, 2-s),$$

where $\Gamma_{\mathbb{C}}(s) = 2(2\pi)^{-s}\Gamma(s)$ and the epsilon factor $\varepsilon(E, \rho, s)$ has the form $w_{E,\rho} \cdot N_{E,\rho}^{1-s}$, where $w_{E,\rho} \in \mathbb{C}$ has absolute value 1 (the root number of the twist) and $N_{E,\rho}$ is a positive integer (the conductor of the twist). Finally, we recall that one has the following "Artin formalism":

(1) $L(E, \rho_1 \oplus \rho_2, s) = L(E, \rho_1, s) L(E, \rho_2, s)$,

(2) $L(E, \mathrm{Ind}_{F/\mathbb{Q}} \mathbf{1}, s) = L(E/F, s)$,

where $L(E/F, s)$ is the usual ("un-twisted") Hasse-Weil L-function of E/F.

The following theorem will allow us to find an explicit representative for the period $c^+(h^1(E)(1) \otimes [\tau])$ in terms of the periods associated with the motives $h^1(E)(1)$ and $[\tau]$.

Theorem 22. *Let M be a motive over $\mathbb{Q}$ with rational coefficients such that*

(1) *M has dimension 2 and weight -1,*

(2) $\dim_{\mathbb{Q}} H_B(M)^{\pm} = 1$,

(3) $H_B(M) \otimes_{\mathbb{Q}} \mathbb{C} = H^{0,-1}(M) \oplus H^{-1,0}(M)$.

Let N be a motive over $\mathbb{Q}$ with coefficients in a number field $\mathfrak{F}$ such that

(1) *N has dimension d and weight 0,*

(2) $H_B(N) \otimes_{\mathbb{Q}} \mathbb{C} = H^{0,0}(N)$.

Under these conditions, the motive $M \otimes N$ is critical and

$$c^+(M \otimes N) = c^+(M)^\mu c^-(M)^\nu \det(I_{N,\infty}) \bmod \mathfrak{F}^\times,$$

where $\mu = \dim_{\mathfrak{F}}(H_B(N)^+)$, $\nu = \dim_{\mathfrak{F}}(H_B(N)^-)$ and $\det(I_{N,\infty})$ is computed using $\mathfrak{F}$-bases.

Proof. The tensor product motive $M \otimes N$ is specified by the data obtained by taking the tensor product of the realisations of M and N and their additional structures; in particular, $M \otimes N$ is a motive of dimension $2d$ and weight -1 such that

(a) $H_B(M \otimes N) = H_B(M) \otimes_{\mathbb{Q}} H_B(N)$ as an $\mathfrak{F}$-vector space.

(b) $F_\infty(M \otimes N) = F_\infty(M) \otimes_{\mathbb{Q}} F_\infty(N)$ as an $\mathfrak{F}$-linear involution.

(c) $H_{\mathrm{dR}}(M \otimes N) = H_{\mathrm{dR}}(M) \otimes_{\mathbb{Q}} H_{\mathrm{dR}}(N)$ as an $\mathfrak{F}$-vector space.

(d) The de Rham filtration on $H_{\mathrm{dR}}(M \otimes N)$ is

$$F^k H_{\mathrm{dR}}(M \otimes N) = \begin{cases} H_{\mathrm{dR}}(M \otimes N) & \text{if } k \leq -1, \\ F^0 H_{\mathrm{dR}}(M) \otimes_{\mathbb{Q}} H_{\mathrm{dR}}(N) & \text{if } k = 0, \\ 0 & \text{if } k \geq 1. \end{cases}$$

(e) The Betti–de Rham comparison isomorphism $I_{M\otimes N,\infty}$ is

$$(H_B(M) \otimes_{\mathbb{Q}} H_B(N)) \otimes_{\mathbb{Q}} \mathbb{C} \xrightarrow{I_{M,\infty}\otimes_{\mathbb{C}} I_{N,\infty}} (H_{\mathrm{dR}}(M) \otimes_{\mathbb{Q}} H_{\mathrm{dR}}(N)) \otimes_{\mathbb{Q}} \mathbb{C}$$

viewed as an isomorphism of $\mathfrak{F}_{\mathbb{C}}$-modules, where we have identified

$$(H_B(M) \otimes_{\mathbb{Q}} H_B(N)) \otimes_{\mathbb{Q}} \mathbb{C} = (H_B(M) \otimes_{\mathbb{Q}} \mathbb{C}) \otimes_{\mathbb{C}} (H_B(N) \otimes_{\mathbb{Q}} \mathbb{C})$$

and similarly for the de Rham realisations.

It follows easily from properties (a)–(d) that

$$\begin{aligned} H_{\mathrm{dR}}(M \otimes N)^+ &= \frac{H_{\mathrm{dR}}(M) \otimes_{\mathbb{Q}} H_{\mathrm{dR}}(N)}{F^0 H_{\mathrm{dR}}(M) \otimes_{\mathbb{Q}} H_{\mathrm{dR}}(N)} \\ &= \frac{H_{\mathrm{dR}}(M)}{F^0 H_{\mathrm{dR}}(M)} \otimes_{\mathbb{Q}} H_{\mathrm{dR}}(N) \\ &= H_{\mathrm{dR}}(M)^+ \otimes_{\mathbb{Q}} H_{\mathrm{dR}}(N), \\ H_B(M \otimes N)^+ &= (H_B(M) \otimes_{\mathbb{Q}} H_B(N))^+ \\ &= (H_B(M)^+ \otimes_{\mathbb{Q}} H_B(N)^+) \oplus (H_B(M)^- \otimes_{\mathbb{Q}} H_B(N)^-). \end{aligned}$$

We choose bases for our various spaces as follows:

(1) a $\mathbb{Q}$-basis $\{\gamma^+\}$ (resp. $\{\gamma^-\}$) for $H_B(M)^+$ (resp. $H_B(M)^-$),

(2) a $\mathbb{Q}$-basis $\{\omega_0\}$ for $F^0 H_{\mathrm{dR}}(M)$ and extend to a basis $\{\omega_0, \omega_1\}$ for $H_{\mathrm{dR}}(M)$,

(3) an $\mathfrak{F}$-basis $\{v_1^+, \ldots, v_\mu^+\}$ (resp. $\{v_1^-, \ldots, v_\nu^-\}$) for $H_B(N)^+$ (resp. $H_B(N)^-$),

(4) an $\mathfrak{F}$-basis $\{w_1, \ldots, w_d\}$ for $H_{\mathrm{dR}}(N)$.

In terms of these bases, we have

$$I_{M,\infty}(\gamma^\pm \otimes 1) = \omega_0 \otimes \eta_0^\pm + \omega_1 \otimes \eta_1^\pm \qquad \text{for some } \eta_0^\pm, \eta_1^\pm \in \mathbb{C},$$

$$I_{N,\infty}(v_j^\pm \otimes 1) = \sum_{i=1}^{d} (b_{ij}^\pm \otimes \xi_{ij}^\pm)(w_i \otimes 1) \quad \text{for some } b_{ij}^\pm \otimes \xi_{ij}^\pm \in \mathfrak{F}_{\mathbb{C}},$$

and so it follows from (e) that

$$\begin{aligned} I_{M\otimes N,\infty}(\gamma^\pm \otimes v_j^\pm \otimes 1) = &\sum_{i=1}^{d} (b_{ij}^\pm \otimes \eta_0^\pm \xi_{ij}^\pm)(\omega_0 \otimes w_i \otimes 1) \\ &+ \sum_{i=1}^{d} (b_{ij}^\pm \otimes \eta_1^\pm \xi_{ij}^\pm)(\omega_1 \otimes w_i \otimes 1). \end{aligned}$$

Hence, with respect to these bases, the matrix of $\alpha^+_{M\otimes N}$ has ij-th component

$$A_{ij} = \begin{cases} (1 \otimes \eta_1^+)(b_{ij} \otimes \xi_{ij}^+) & \text{if } j \leq \mu, \\ (1 \otimes \eta_1^-)(b_{ij} \otimes \xi_{ij}^+) & \text{if } \mu < j \leq n, \end{cases}$$

and so taking the determinant yields the desired expression

$$\begin{aligned} c^+(M\otimes N) &= (1\otimes\eta_1^+)^\mu(1\otimes\eta_1^-)^\nu \det(I_{N,\infty}) \bmod \mathfrak{F}^\times \\ &= c^+(M)^\mu c^-(M)^\nu \det(I_{N,\infty}) \bmod \mathfrak{F}^\times. \end{aligned}$$

Finally, to see that $M\otimes N$ is critical, we simply observe that

$$H_B(M\otimes N)\otimes\mathbb{C} = H^{0,-1}(M\otimes N)\oplus H^{-1,0}(M\otimes N),$$

where, viewed as $\mathfrak{F}_\mathbb{C}$-modules, we have

$$\begin{aligned} H^{0,-1}(M\otimes N) &= H^{0,-1}(M)\otimes_\mathbb{C} H^{0,0}(N), \\ H^{-1,0}(M\otimes N) &= H^{-1,0}(M)\otimes_\mathbb{C} H^{0,0}(N). \end{aligned}$$ □

Corollary 23. *Let E be an elliptic curve over $\mathbb{Q}$ and ρ be an Artin representation over $\mathbb{Q}$. Let $\mathfrak{F}/\mathbb{Q}$ be a finite abelian extension over which ρ can be realised and let τ be an $\mathfrak{F}$-linear representation of $G_\mathbb{Q}$ such that $\mathbb{C}\otimes_\mathfrak{F}\tau\simeq\rho$. Then $h^1(E)(1)\otimes[\tau]$ is a critical motive and the component of $c^+(h^1(E)(1)\otimes[\tau])$ corresponding to our fixed embedding $\mathfrak{F}\subseteq\overline{\mathbb{Q}}\subseteq\mathbb{C}$ is*

$$\frac{\Omega_+(E)^{d^+(\rho)}|\Omega_-(E)|^{d^-(\rho)}w_\rho}{\sqrt{\mathfrak{f}_\rho}} \bmod \mathfrak{F}^\times.$$

Proof. Applying Theorem 22 with $M = h^1(E)(1)$ and $N=[\tau]$ yields

$$c^+(h^1(E)(1)\otimes[\tau]) = \Omega_+(E)^{d^+(\tau)}\Omega_-(E)^{d^-(\tau)}\det(I_{\tau,\infty}) \bmod \mathfrak{F}^\times.$$

Moreover, it follows from [5, formula 5.6.1] that

$$i^{d^-(\tau)}\det(I_{\tau,\infty}) = (\varepsilon(\tau^\gamma) : \gamma\in\mathrm{Gal}(\mathfrak{F}/\mathbb{Q})) \bmod \mathfrak{F}^\times,$$

and so, since $d^\pm(\tau)=d^\pm(\rho)$, $\varepsilon(\tau)=\varepsilon(\rho)$ and $\Omega_-(E)^{d^-(\tau)} = i^{d^-(\tau)}|\Omega_-(E)|^{d^-(\tau)}$, we see that

$$\Omega_+(E)^{d^+(\rho)}|\Omega_-(E)|^{d^-(\rho)}\varepsilon(\rho) \bmod \mathfrak{F}^\times$$

is equal to the component of $c^+(h^1(E)(1)\otimes[\tau])$ corresponding to the identity in $\mathrm{Gal}(\mathfrak{F}/\mathbb{Q})$. Therefore, since $\varepsilon(\rho) = w_\rho\sqrt{\mathfrak{f}_\rho}$, the result follows on dividing through by $\mathfrak{f}_\rho$. □

2.6. Properties of $\mathscr{L}(E,\rho)$. We now turn to L-values and the proof of Theorem 13.

Theorem 24. *Let $E/\mathbb{Q}$ be an elliptic curve and let ρ and ρ' be Artin representations over $\mathbb{Q}$. Suppose that $L(E,\rho,s)$ and $L(E,\rho',s)$ admit an analytic continuation to $\mathbb{C}$.*

(L1) *If $\rho=\mathrm{Ind}_{F/\mathbb{Q}}\mathbf{1}$ for a number field F, then*

$$\mathscr{L}(E,\rho) = \lim_{s\to1}\frac{L(E/F,s)}{(s-1)^r}\cdot\frac{\sqrt{|\Delta_F|}}{\Omega_+(E)^{r_1+r_2}|\Omega_-(E)|^{r_2}},$$

where (r_1,r_2) is the signature of F and $r=\mathrm{ord}_{s=1}L(E/F,s)$.

(L2) $\mathscr{L}(E,\rho\oplus\rho') = \mathscr{L}(E,\rho)\mathscr{L}(E,\rho')$.

(L3) *If the functional equation for $L(E,\rho,s)$ holds near $s=1$, then*

$$\mathscr{L}(E,\rho) = \frac{(-1)^r w_{E,\rho}}{w_\rho^2}\,\mathscr{L}(E,\rho^*),$$

where $r = \operatorname{ord}_{s=1} L(E,\rho,s)$.

(L4) *If ρ is self-dual i.e. $\rho \simeq \rho^*$, then*

(i) $\mathscr{L}(E,\rho) \in \mathbb{R}$,

(ii) $\operatorname{sign} \mathscr{L}(E,\rho) = \operatorname{sign} w_\rho$, *providing that $L(E,\rho,s) \neq 0$ for all real $s > 1$.*

(L5) *If $L(E,\rho,1) \neq 0$ and Deligne's period conjecture holds for the twist of E by ρ, then*

(i) $\mathscr{L}(E,\rho) \in \mathbb{Q}(\rho)^\times$,

(ii) $\mathscr{L}(E,\rho^{\mathfrak{g}}) = \mathscr{L}(E,\rho)^{\mathfrak{g}}$ *for all* $\mathfrak{g} \in \operatorname{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})$.

(L6) *If ρ is a non-trivial primitive Dirichlet character of order d, and either*

(i) *E is semistable and has no non-trivial isogenies over $\mathbb{Q}$, or*

(ii) *Stevens's Manin constant conjecture holds for $E/\mathbb{Q}$ and $\mathfrak{f}_\rho$ is coprime to $\mathfrak{f}_E$,*

then $\mathscr{L}(E,\rho) \in \mathbb{Z}[\zeta_d]$.

Proof. For any Artin representation ρ over $\mathbb{Q}$, we shall denote the leading coefficient in the Taylor series expansion of $L(E,\rho,s)$ at $s=1$ by $\widehat{L}(E,\rho,1)$. In this notation, Definition 12 states that

$$\mathscr{L}(E,\rho) = \frac{\sqrt{\mathfrak{f}_\rho}\,\widehat{L}(E,\rho,1)}{\Omega_+(E)^{d^+(\rho)}|\Omega_-(E)|^{d^-(\rho)} w_\rho}.$$

Recall (from [8], for example) that for an Artin representation ρ over a number field F, the conductor $\mathfrak{f}_\rho$ and root number w_ρ are, respectively, an integral ideal of F and a complex number of absolute value 1, and that they have the following formal properties:

(1) $\mathfrak{f}_{\rho_1\oplus\rho_2} = \mathfrak{f}_{\rho_1}\mathfrak{f}_{\rho_2}$ and $w_{\rho_1\oplus\rho_2} = w_{\rho_1} w_{\rho_2}$,

(2) $\mathfrak{f}_{\operatorname{Ind}_{L/F}(\rho)} = \operatorname{disc}(L/F)^{\dim\rho} N_{L/F}(\mathfrak{f}_\rho)$ and $w_{\operatorname{Ind}_{L/F}(\rho)} = w_\rho$.

We refer to these as "Artin formalism", analogously to the case of L-functions given in Section 2.5.

(L1) By Artin formalism for the other factors, it suffices to prove that

$$d^+(\operatorname{Ind}_{F/\mathbb{Q}} \mathbf{1}) = r_1 + r_2 \quad \text{and} \quad d^-(\operatorname{Ind}_{F/\mathbb{Q}} \mathbf{1}) = r_2.$$

Since $\operatorname{Ind}_{F/\mathbb{Q}} \mathbf{1}$ is the permutation module $G_\mathbb{Q}/G_F$, we have

$$d^+ + d^- = [F:\mathbb{Q}] \quad \text{and} \quad d^+ - d^- = \operatorname{tr}(\operatorname{Ind}_{F/\mathbb{Q}}(\mathbf{1})(\iota)),$$

where $\iota \in G_\mathbb{Q}$ is complex conjugation. However, we also have that

$$\operatorname{tr}(\operatorname{Ind}_{F/\mathbb{Q}}(\mathbf{1})(\iota)) = \#\text{singleton orbits of } \iota \text{ in } G_\mathbb{Q}/G_F = r_1,$$

and so $d^+ + d^- = r_1 + 2r_2$ and $d^+ - d^- = r_1$ and the claim now follows.

(L2) By Artin formalism for the other factors, it suffices to note the identity

$$d^{\pm}(\rho \oplus \rho') = d^{\pm}(\rho) + d^{\pm}(\rho').$$

(L3) Applying $\frac{d^r}{ds^r}|_{s=1}$ to the functional equation for $L(E, \rho, s)$ yields

$$\widehat{L}(E, \rho, 1) = w_{E,\rho} \cdot (-1)^r \widehat{L}(E, \rho^*, 1),$$

and so, since $\mathfrak{f}_{\rho^*} = \mathfrak{f}_\rho$ and $d^{\pm}(\rho^*) = d^{\pm}(\rho)$, we have

$$\frac{\sqrt{\mathfrak{f}_\rho}\,\widehat{L}(E, \rho, 1)}{\Omega_+(E)^{d^+(\rho)}|\Omega_-(E)|^{d^-(\rho)} w_\rho} = (-1)^r \frac{w_{E,\rho} w_{\rho^*}}{w_\rho} \frac{\sqrt{\mathfrak{f}_{\rho^*}}\,\widehat{L}(E, \rho^*, 1)}{\Omega_+(E)^{d^+(\rho^*)}|\Omega_-(E)|^{d^-(\rho^*)} w_{\rho^*}}$$

which, on recalling that $w_\rho w_{\rho^*} = w_{\rho\oplus\rho^*} = 1$, simplifies to the given formula.

(L4) For sufficiently large $s \in \mathbb{R}$, we can express $L(E, \rho, s)$ as a Dirichlet series and, as the character of ρ is real-valued, it follows that the coefficients of this series are real. Hence, one has $L(E, \rho, s) = \overline{L(E, \rho, \overline{s})}$ on a right-half of the real line. Since $L(E, \rho, s)$ is analytic everywhere in $\mathbb{C}$ (conjecturally), it follows that $L(E, \rho, s) = \overline{L(E, \rho, \overline{s})}$ for all $s \in \mathbb{C}$ and so, in particular, that $\widehat{L}(E, \rho, 1) \in \mathbb{R}$. Moreover, since ρ is self-dual, we have $w_\rho = \pm 1$ and so it follows that $\mathscr{L}(E, \rho) \in \mathbb{R}$.

We see from the Euler product that $L(E, \rho, s) \geq 0$ for all sufficiently large $s \in \mathbb{R}$ and so, since $L(E, \rho, s)$ is continuous and, by hypothesis, nowhere zero on $(1, \infty)$, the intermediate value theorem implies that $\widehat{L}(E, \rho, 1) > 0$. It thus follows that $\mathscr{L}(E, \rho) w_\rho \in \mathbb{R}_{>0}$.

(L5) As in Section 2.5, let $\mathfrak{F}/\mathbb{Q}$ be a finite abelian extension over which ρ can be realised and let τ be an $\mathfrak{F}$-linear representation of $G_\mathbb{Q}$ such that $\mathbb{C} \otimes_{\mathfrak{F}} \tau \simeq \rho$. By Corollary 23, the motive $h^1(E)(1) \otimes [\tau]$ is critical and moreover, if $L(E, \rho, 1) \neq 0$ and Deligne's period conjecture holds, then

(i) $\mathscr{L}(E, \rho) \in \mathfrak{F}^\times$,

(ii) $\mathscr{L}(E, \rho^\gamma) = \mathscr{L}(E, \rho)^\gamma$ for all $\gamma \in \mathrm{Gal}(\mathfrak{F}/\mathbb{Q})$.

The result follows from this on noting that $\rho^\gamma \simeq \rho$ for all $\gamma \in \mathrm{Gal}(\mathfrak{F}/\mathbb{Q}(\rho))$.

(L6) (i) This follows directly from [16, Theorem 1]. (ii) In this case $\mathfrak{f}_\rho$ is not divisible by any prime where E has bad reduction, so the claim follows from [16, Theorem 2a]. □

Corollary 25. *Let E be an elliptic curve over $\mathbb{Q}$, and suppose that $L(E, \rho, s)$ has an analytic continuation to $\mathbb{C}$ for all Artin representations ρ over $\mathbb{Q}$, and take* $\mathrm{BSD}(E, \rho)$ *to be $\mathscr{L}(E, \rho)$. Then* (C1)–(C6) *of Conjecture* 4 *hold subject to the following conditions:*

(C1) *The Birch–Swinnerton-Dyer conjecture holds for E over number fields.*

(C2) *Unconditional.*

(C3) *$L(E, \rho, s)$ satisfies the functional equation and Conjecture* 1.

(C4) *$L(E, \rho, s)$ has no zeros in the interval $(1, \infty)$.*

(C5) *$L(E, \rho, s)$ satisfies Deligne's period conjecture.*

(C6) *Stevens's Manin constant conjecture holds for $E/\mathbb{Q}$.*

In the following corollary we prove the remaining parts of Theorem 13. In particular, parts (1)–(4) record some of the formal consequences of the (conjectural) properties (L1)–(L5) stated in Theorem 24 and parts (5)–(7) use the classical Birch–Swinnerton-Dyer conjecture to make predictions about the norm of $\mathscr{L}(E, \rho)$.

Corollary 26. *Let $E/\mathbb{Q}$ be an elliptic curve and let ρ be an Artin representation over $\mathbb{Q}$. Suppose that $L(E,\rho,s)$ admits an analytic continuation to all of $\mathbb{C}$ and that $L(E,\rho,1)\neq 0$. Suppose moreover that $L(E,\rho,s)$ satisfies the functional equation, Deligne's period conjecture and has no zeros in the interval $(1,\infty)$. Then:*

(1) $U(E,\rho) := \frac{\mathscr{L}(E,\rho^*)}{\mathscr{L}(E,\rho)}$ *is a root of unity in $\mathbb{Q}(\rho)$.*

(2) $\mathscr{L}(E,\rho)\cdot\mathcal{O}_{\mathbb{Q}(\rho)}$ *is invariant as a fractional ideal under complex conjugation.*

(3) $\zeta\cdot\mathscr{L}(E,\rho)\in\mathbb{Q}(\rho,\zeta)^+$ *where $\zeta\in\mathbb{C}$ is such that $\zeta^2 = U(E,\rho)$.*

(4) $U(E,\rho) = w_\rho^2 w_{E,\rho}^{-1}$ *and, if $\mathfrak{f}_E$ is coprime to $\mathfrak{f}_\rho$, this equals $(-1)^{d^-(\rho)} w_E^{\dim\rho}\det\rho(\mathfrak{f}_E)$, where* det ρ *is regarded as a primitive Dirichlet character.*

Let $\mathfrak{G} = \mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})$ and choose number fields F_i, F_j' and a positive integer m such that

$$\Big(\bigoplus_{\mathfrak{g}\in\mathfrak{G}}\rho^{\mathfrak{g}}\Big)^{\oplus m}\oplus\bigoplus_i \mathrm{Ind}_{F_i/\mathbb{Q}}\mathbf{1}\simeq\bigoplus_j\mathrm{Ind}_{F_j'/\mathbb{Q}}\mathbf{1}$$

(these exist by Remark 10*), and write B for the unique positive real number such that*

$$B^m = \frac{\prod_j \mathrm{BSD}(E/F_j')}{\prod_i \mathrm{BSD}(E/F_i)}.$$

Suppose that the Birch–Swinnerton-Dyer conjecture holds for E over number fields. Then:

(5) $N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathscr{L}(E,\rho)) = \pm B$, *with sign $+$ if m is odd.*

(6) *If $\rho\not\simeq\rho^*$ and $\zeta\in\mathbb{Q}(\rho)$, then $N_{\mathbb{Q}(\rho)^+/\mathbb{Q}}(\zeta\cdot\mathscr{L}(E,\rho)) = \pm\sqrt{B}$.*

(7) *If $\rho\not\simeq\rho^*$ and $\zeta\notin\mathbb{Q}(\rho)$, then $N_{\mathbb{Q}(\rho,\zeta)^+/\mathbb{Q}}(\zeta\cdot\mathscr{L}(E,\rho)) = \pm B$.*

Proof. (1) It follows from (L5) that $U(E,\rho)\in\mathbb{Q}(\rho)$ and that

$$U(E,\rho)^{\mathfrak{g}} = \overline{\mathscr{L}(E,\rho^{\mathfrak{g}})}/\mathscr{L}(E,\rho^{\mathfrak{g}})\quad\text{for all }\mathfrak{g}\in\mathfrak{G}.$$

In particular, one has $|U(E,\rho)^{\mathfrak{g}}| = 1$ for all $\mathfrak{g}\in\mathfrak{G}$, and so $U(E,\rho)$ is indeed a root of unity.

(2) This follows directly from (1) on noting that, by (L5), one has

$$\mathscr{L}(E,\rho^*) = \overline{\mathscr{L}(E,\rho)}.$$

(3) It follows from (L2) and (L5) that

$$\begin{aligned}\mathscr{L}(E,\rho^{\mathfrak{g}}\oplus(\rho^{\mathfrak{g}})^*) &= U(E,\rho^{\mathfrak{g}})\mathscr{L}(E,\rho^{\mathfrak{g}})^2\\ &= (U(E,\rho)\mathscr{L}(E,\rho)^2)^{\mathfrak{g}}\quad\text{for all }\mathfrak{g}\in\mathfrak{G},\end{aligned}$$

and so, recalling that $w_{\rho^{\mathfrak{g}}\oplus(\rho^{\mathfrak{g}})^*} = 1$ for any $\mathfrak{g}\in\mathfrak{G}$, it follows from (L4) that

$$(U(E,\rho)\mathscr{L}(E,\rho)^2)^{\mathfrak{g}}\in\mathbb{R}_{>0}\quad\text{for all }\mathfrak{g}\in\mathfrak{G}.$$

Hence, taking $\zeta\in\mathbb{C}$ such that $\zeta^2 = U(E,\rho)$, we see that $\zeta\cdot\mathscr{L}(E,\rho)\in\mathbb{Q}(\rho,\zeta)^+$.

(4) The first statement follows immediately from (L3) and the second from [7, Theorem 16].

(5) Writing $R(\rho) = \bigoplus_{\mathfrak{g}\in\mathfrak{G}} \rho^{\mathfrak{g}}$, it follows from (L2) and (L5) that

$$\mathscr{L}(E, R(\rho)) = N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathscr{L}(E, \rho)).$$

However, since $R(\rho)^{\oplus m} \oplus \bigoplus_i \mathrm{Ind}_{F_i/\mathbb{Q}} \mathbf{1} \simeq \bigoplus_j \mathrm{Ind}_{F_j'/\mathbb{Q}} \mathbf{1}$, another application of (L2) gives

$$\mathscr{L}(E, R(\rho))^m = \frac{\prod_j \mathscr{L}(E, \mathrm{Ind}_{F_j'/\mathbb{Q}} \mathbf{1})}{\prod_i \mathscr{L}(E, \mathrm{Ind}_{F_i/\mathbb{Q}} \mathbf{1})}.$$

Hence, by (L1) together with the Birch–Swinnerton-Dyer conjecture, we get

$$\mathscr{L}(E, R(\rho))^m = B^m,$$

and so the result follows on taking m-th roots.

(6) and (7) Let $\Gamma = \mathrm{Gal}(\mathbb{Q}(\rho, \zeta)/\mathbb{Q})$ and $\mathrm{H} = \mathrm{Gal}(\mathbb{Q}(\rho, \zeta)^+/\mathbb{Q})$. If $\rho \not\simeq \rho^*$, then

$$\bigoplus_{\gamma\in\Gamma} \rho^\gamma \simeq \bigoplus_{\eta\in\mathrm{H}} (\rho \oplus \rho^*)^\eta,$$

and so it follows from (L2), (L3), (L4) and (L5) that

$$\mathscr{L}\left(E, \bigoplus_{\gamma\in\Gamma} \rho^\gamma\right) = N_{\mathbb{Q}(\rho,\zeta)^+/\mathbb{Q}}(\mathscr{L}(E, \rho \oplus \rho^*)) = N_{\mathbb{Q}(\rho,\zeta)^+/\mathbb{Q}}(\zeta \cdot \mathscr{L}(E, \rho))^2.$$

On the other hand, (L2) gives us

$$\mathscr{L}\left(E, \bigoplus_{\gamma\in\Gamma} \rho^\gamma\right) = \begin{cases} \mathscr{L}(E, R(\rho)) & \text{if } \zeta \in \mathbb{Q}(\rho), \\ \mathscr{L}(E, R(\rho))^2 & \text{if } \zeta \notin \mathbb{Q}(\rho), \end{cases}$$

and so the results follow from L1 together with the Birch–Swinnerton-Dyer conjecture. □

3. Arithmetic applications

In order to obtain arithmetic applications of Conjecture 4 we shall make use of (C5), which is the analogue of the Galois equivariance property of L-values. As we do not have an exact expression for $\mathrm{BSD}(E, \rho)$ in general, we shall take the following approach. The representation $\tau = \bigoplus_{\mathfrak{g}\in\mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})} \rho^{\mathfrak{g}}$ has rational trace and hence $\mathrm{BSD}(E, \tau)$ can, on the one hand, be expressed in terms of BSD-quotients $\mathrm{BSD}(E/K_i)$ for suitable fields K_i (see Remark 10), and, on the other hand, is the norm of $\mathrm{BSD}(E, \rho)$ from $\mathbb{Q}(\rho)$ to $\mathbb{Q}$ by (C5). As we shall illustrate, this places non-trivial constraints on the $\mathrm{BSD}(E/K_i)$, and hence on ranks and the Tate–Shafarevich groups. We stress that the expression is the norm of an *element* of $\mathbb{Q}(\rho)$, rather than just of a fractional ideal.

Proposition 27. *Let G be a finite group and ρ an irreducible representation. Write*

$$\left(\bigoplus_{\mathfrak{g}\in\mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})} \rho^{\mathfrak{g}}\right)^{\oplus m} = \left(\bigoplus_i \mathrm{Ind}_{H_i}^G \mathbf{1}\right) \ominus \left(\bigoplus_j \mathrm{Ind}_{H_j'}^G \mathbf{1}\right)$$

for some $m \in \mathbb{Z}$ and some subgroups $H_i, H_j' < G$. If Conjecture 4 (C1), (C2), (C5) *hold, then for every elliptic curve $E/\mathbb{Q}$ and Galois extension $F/\mathbb{Q}$ with Galois group G, either*

$$\langle \rho, E(F)_{\mathbb{C}} \rangle > 0$$

or

$$\frac{\prod_i \mathrm{BSD}(E/F^{H_i})}{\prod_j \mathrm{BSD}(E/F^{H_j'})} = N_{\mathbb{Q}(\rho)/\mathbb{Q}}(x)^m$$

for some $x \in \mathbb{Q}(\rho)$. Moreover, if ρ is non-trivial, G is abelian of exponent d and (C6) *of Conjecture* 4 *holds, then one can take $x \in \mathbb{Z}[\zeta_d]$ provided that either $\mathfrak{f}_E$ and $\mathfrak{f}_\rho$ are coprime, or E is semistable and has no non-trivial isogenies.*

Proof. If $\langle \rho, E(F)_{\mathbb{C}} \rangle = 0$, then the formula is satisfied by $x = \mathrm{BSD}(E, \rho)$. □

In order to make use of the above theorem in specific settings, we will need to control the various terms in the BSD factors of the formula. For convenience of the reader we have recorded in Section 3.4 some standard facts about Selmer groups, Tamagawa numbers and the term $|\omega/\omega^{\min}|$ that will be used in our computations.

3.1. Interplay between p-primary parts of the Tate–Shafarevich group. For our first application we will take the simplest setting, when the Galois group is cyclic of prime order, and make use of the fact that the ratio of BSD-terms is the norm of a *principal* ideal. The basic idea is that if the p-part of this number cannot be expressed as the norm of a principal ideal, then, necessarily, the q-primary part must be non-trivial for some other prime q.

Theorem 28. *Let ℓ, p be primes such that the primes above p in $\mathbb{Q}(\zeta_\ell)$ are non-principal and have residue degree* 2*. If Conjecture* 4 *holds, then for every semistable elliptic curve $E/\mathbb{Q}$ with no non-trivial isogenies, with $|Ш_{E/\mathbb{Q}}[p]| = 1$ and $c_v = 1$ for all rational primes v, and for every cyclic extension $F/\mathbb{Q}$ of degree ℓ with $E(F) = E(\mathbb{Q})$,*

$$\text{if } |Ш_{E/F}[p^\infty]| = p^2, \text{ then } |Ш_{E/F}[q^\infty]| \neq 1 \text{ for some } q \neq p, \ell.$$

Proof. We will in fact prove the stronger statement that $Ш_{E/\mathbb{Q}}[q^\infty]$ is strictly smaller than $Ш_{E/F}[q^\infty]$ for some $q \neq p, \ell$. The fact that it is a subgroup for all $q \neq \ell$ is standard: it is true for q^k-Selmer groups by Lemma 36, and as $E(\mathbb{Q}) = E(F)$ it is also true for $Ш[q^\infty]$.

A 1-dimensional faithful representation χ of $\mathrm{Gal}(F/\mathbb{Q}) \simeq C_\ell$ has $\mathbb{Q}(\chi) = \mathbb{Q}(\zeta_\ell)$. Now

$$\sum_{\mathfrak{g} \in \mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q})} \chi^{\mathfrak{g}} = \mathbb{C}[G] \ominus \mathbf{1},$$

so by Proposition 27,

$$\frac{\mathrm{BSD}(E/F)}{\mathrm{BSD}(E/\mathbb{Q})} = N_{\mathbb{Q}(\zeta_\ell)/\mathbb{Q}}(x) \quad \text{for some } x \in \mathbb{Z}[\zeta_\ell].$$

Since $E(F) = E(\mathbb{Q})$, it follows that $E(F)_{\mathrm{tors}} = E(\mathbb{Q})_{\mathrm{tors}}$ and $\mathrm{Reg}_{E/F} = \ell^{\mathrm{rk}\, E/\mathbb{Q}} \mathrm{Reg}_{E/\mathbb{Q}}$ (Lemma 36 (2)). As $E/\mathbb{Q}$ is semistable, the contributions to $C_{E/F}$ and $C_{E/\mathbb{Q}}$ only come from Tamagawa numbers (Lemma 36 (5)). These are trivial over $\mathbb{Q}$ by hypothesis, so are also trivial at all primes that split in $F/\mathbb{Q}$; if v is a prime of multiplicative reduction that does not split, then the corresponding Tamagawa number over F is 1 unless the reduction is split multiplicative and the prime ramifies, in which case it is ℓ (Lemma 36 (4)). Putting this together, we

deduce that

$$\frac{|Ш_{E/F}|}{|Ш_{E/\mathbb{Q}}|}\cdot \ell^n = N_{\mathbb{Q}(\zeta_\ell)/\mathbb{Q}}(x) \quad \text{for some } n\in\mathbb{Z}.$$

Note that ℓ is totally ramified in $\mathbb{Q}(\zeta_\ell)$ and the ideal above it $(\zeta_\ell - 1)$ is principal. Thus if $Ш_{E/F}[q^\infty] = Ш_{E/\mathbb{Q}}[q^\infty]$ for all $q \neq p, \ell$, it would follow that p^2 is the norm of a principal ideal of $\mathbb{Z}[\zeta_\ell]$. By assumption, the primes above p have norm p^2 and are non-principal, so this is not the case. □

Example 29. Let $E/\mathbb{Q}$ be a semistable elliptic curve with no non-trivial isogenies, with $\prod_v c_v = 1$ and $Ш_{E/\mathbb{Q}} = 1$, and let $F/\mathbb{Q}$ be the degree 229 subfield of $\mathbb{Q}(\zeta_{2749})$. In this setting, if $E(\mathbb{Q}) = E(F)$, then $|Ш(E/F)| \neq p^2$, for the prime $p = 1148663$. Indeed, p is a prime which has residue degree 2 in $\mathbb{Q}(\zeta_{229})$, and the prime above it is non-principal (this is hard to achieve, which is why $\ell = 229$ is taken to be so large), so this is a consequence of the above theorem. However, it is perfectly possible for such a curve to have

$$E(\mathbb{Q}) = E(F) \quad \text{and} \quad |Ш(E/F)| = p^2 \times (\text{integer coprime to } p),$$

as, for instance, is the case for the elliptic curve 2749a1. (This is based on a Magma computation of the analytic order of Ш and the analytic rank, and assumes the BSD conjecture.)

3.2. Forcing non-trivial Selmer groups. The BSD-terms $\mathrm{BSD}(E/F^{H_i})$ in Proposition 27 are composed of "hard" global invariants (Tate–Shafarevich group and points of infinite order) and "easy" local invariants (Tamagawa numbers and differentials). We will now illustrate how the result can be used to make the easy local data force non-trivial behaviour of global invariants. Once again, we will exploit the fact that the ratio of BSD-terms is the norm of a principal ideal. We focus on non-abelian groups of the form $G = C_{q_1q_2} \rtimes C_r$, and begin by simplifying the norm condition.

Theorem 30. *Let q_1, q_2, r be three distinct odd primes such that $q_1, q_2 \equiv 1 \bmod r$, but $q_1, q_2 \not\equiv 1 \bmod r^2$, and with q_1 an r-th power in $\mathbb{Z}/q_2\mathbb{Z}$ and vice versa. Let $G = C_{q_1q_2} \rtimes C_r$ with C_r acting non-trivially on both the C_{q_1} and C_{q_2} subgroups. If Conjecture* 4 *holds, then for every elliptic curve $E/\mathbb{Q}$ and every Galois extension $F/\mathbb{Q}$ with Galois group G, either* $\mathrm{rk}\, E/F > 0$ *or*

$$\frac{\mathrm{BSD}(E/F^{C_r})\,\mathrm{BSD}(E/\mathbb{Q})}{\mathrm{BSD}(E/F^{C_{q_1}\rtimes C_r})\,\mathrm{BSD}(E/F^{C_{q_2}\rtimes C_r})} = q_1^a q_2^b k$$

for some $a, b \in \mathbb{Z}$ and $k \in \mathbb{Q}$ with $k \equiv 1 \bmod q_1q_2$.

Proof. Let ψ be a faithful 1-dimensional representation of $C_{q_1q_2}$ and $\rho = \mathrm{Ind}_{C_{q_1q_2}}^G \psi$. This is a faithful r-dimensional irreducible representation of G, and

$$\mathbb{Q}(\rho) = \mathbb{Q}(\zeta_{q_1q_2})^{C_r}$$

with the C_r action coming from $C_r \subset \mathrm{Aut}(C_{q_1q_2}) = (\mathbb{Z}/q_1q_2\mathbb{Z})^\times = \mathrm{Gal}(\mathbb{Q}(\zeta_{q_1q_2})/\mathbb{Q})$. Applying Proposition 27 to the identity

$$\bigoplus_{\mathfrak{g}\in\mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})} \rho^{\mathfrak{g}} = \mathrm{Ind}_{C_r}^G \mathbf{1} \oplus \mathbf{1} \ominus \mathrm{Ind}_{C_{q_1}\rtimes C_r}^G \mathbf{1} \ominus \mathrm{Ind}_{C_{q_2}\rtimes C_r}^G \mathbf{1}$$

shows that either $\mathrm{rk}\, E/F > 0$ or the ratio of the BSD terms in the statement is a norm of an element $x \in \mathbb{Q}(\rho)$.

It thus suffices to show that the norm of every non-zero principal ideal (x) in $\mathbb{Q}(\rho)$ is of the form $q_1^a q_2^b k$, for some $a, b \in \mathbb{Z}$ and $k \in \mathbb{Q}$ with $k \equiv 1 \bmod q_1 q_2$. Observe that

$$\mathbb{Q}(\zeta_{q_1 q_2}) = \mathbb{Q}(\rho)(\zeta_{q_1}) = \mathbb{Q}(\rho)(\zeta_{q_2}).$$

In particular, $\mathbb{Q}(\zeta_{q_1 q_2})/\mathbb{Q}(\rho)$ is unramified at all primes, so by class field theory

$$\prod_{\mathfrak{p}} \mathrm{Frob}_{\mathfrak{p}}^{\mathrm{ord}_{\mathfrak{p}} x} = \mathrm{id} \in \mathrm{Gal}(\mathbb{Q}(\zeta_{q_1 q_2})/\mathbb{Q}(\rho)),$$

the product taken over the primes of $\mathbb{Q}(\rho)$ (all the infinite places being complex as r is odd). By hypothesis, q_1 is an r-th power in $\mathbb{F}_{q_2}$ and $r^2 \nmid |\mathbb{F}_{q_2}^\times|$, so $\mathbb{F}_{q_2}(\zeta_{q_1})/\mathbb{F}_{q_2}$ has degree coprime to r; hence every prime above q_2 must split in $\mathbb{Q}(\rho)(\zeta_{q_1})/\mathbb{Q}(\rho)$, that is $\mathrm{Frob}_{\mathfrak{p}} = \mathrm{id}$ for every $\mathfrak{p} \mid q_2$. Similarly $\mathrm{Frob}_{\mathfrak{p}} = \mathrm{id}$ for every $\mathfrak{p} \mid q_1$, and hence

$$\prod_{\mathfrak{p} \mid q_1, q_2} \mathrm{Frob}_{\mathfrak{p}}^{\mathrm{ord}_{\mathfrak{p}} x} = \mathrm{id}.$$

For a prime $\mathfrak{p} \nmid q_1, q_2$ the Frobenius element is determined by $\zeta_{q_1 q_2} \mapsto \zeta_{q_1 q_2}^{N(\mathfrak{p})}$, which shows that

$$\prod_{\mathfrak{p} \nmid q_1, q_2} N(\mathfrak{p})^{\mathrm{ord}_{\mathfrak{p}} x} = 1 \in (\mathbb{Z}/q_1 q_2 \mathbb{Z})^\times,$$

and hence the norm of x is of the required form. □

Corollary 31. *Let $F/\mathbb{Q}$ be a Galois extension of degree $3q_1q_2$ that contains a Galois cubic field $K/\mathbb{Q}$ and ℓ a prime that satisfy*

- $q_1, q_2 \equiv 4$ *or* $7 \bmod 9$*, and q_1 is a cube modulo q_2 and vice versa,*
- $\lfloor \frac{q_1 q_2}{4} \rfloor - \lfloor \frac{q_1}{4} \rfloor - \lfloor \frac{q_2}{4} \rfloor \not\equiv 0 \bmod 3$*,*
- $\ell^3 \equiv 1 \bmod q_1$*, but $\ell \not\equiv 1 \bmod q_1$ and $\ell \not\equiv 1 \bmod q_2$,*
- *ℓ has residue degree* 3 *and ramification degree $q_1 q_2$ in $F/\mathbb{Q}$.*

If Conjecture 4 *holds, then every elliptic curve $E/\mathbb{Q}$ that has additive reduction at ℓ of Kodaira type III and good reduction at other primes that ramify in $F/\mathbb{Q}$, must have a non-trivial p-Selmer group for some prime $p \nmid [F : \mathbb{Q}]$.*

Proof. First note that $\mathrm{Gal}(F/\mathbb{Q}) \simeq C_{q_1 q_2} \rtimes C_3$ (the inertia group at ℓ is tame, so $C_{q_1 q_2}$ is a subgroup, and the extension is split by the Schur–Zassenhaus theorem). As $\ell \not\equiv 1 \bmod q_1$, there is no Galois extension of $\mathbb{Q}$ of degree q_1 that is ramified at ℓ, and similarly for q_2. It follows that C_3 must act non-trivially both on C_{q_1} and C_{q_2}. Moreover, q_1 and q_2 are both cubes modulo each other and are $\equiv 4$ or $7 \bmod 9$, so Theorem 30 applies with $r = 3$.

If the Selmer group $\mathrm{Sel}_p(E/F)$ is trivial for a prime $p \nmid [F : \mathbb{Q}]$, then it is also trivial over any subfield of F (see Lemma 36 (1)), and hence neither the torsion nor Ш contribute to the p-part of the BSD quotient in the theorem. The rank over F is then also 0, so all the regulators are trivial. Thus by Theorem 30, supposing that $\mathrm{Sel}_p(E/F) = 0$ for all $p \nmid [F : \mathbb{Q}]$,

$$\frac{C_{E/F^{C_r}} \cdot C_{E/\mathbb{Q}}}{C_{E/F^{C_{q_1} \rtimes C_r}} \cdot C_{E/F^{C_{q_2} \rtimes C_r}}} = q_1^a q_2^b k$$

for some $a, b \in \mathbb{Z}$ and $k \equiv 1 \bmod q_1 q_2$. However, in our setup this is not the case, as we now explain.

First observe that all primes of good reduction, which include all ramified primes in $F/\mathbb{Q}$ apart from ℓ, have trivial Tamagawa numbers and $|\omega/\omega^{\min}|$ terms in all extensions, and hence do not contribute to the ratio of the $C_{E/*}$-terms above. If $q \neq \ell$ is a prime of bad reduction for $E/\mathbb{Q}$, then, by assumption, it is unramified in $F/\mathbb{Q}$. The minimal differential at q then remains minimal in all extensions, so that the $|\omega/\omega^{\min}|$ terms for these primes are all 1. Moreover, the decomposition group at q is either trivial or cyclic of order 3, q_1, q_2 or q_1q_2, and a straightforward case-by-case check shows that the Tamagawa numbers from the primes above q contribute a perfect cube to the above ratio of $C_{E/*}$-terms (in fact each extension of $\mathbb{Q}_q$ always appears in the expression a multiple of three times).

Finally, consider the primes above ℓ. As ℓ has ramification degree q_1q_2 in $F/\mathbb{Q}$, it is totally ramified in F^{C_r}, $F^{C_{q_1}\rtimes C_r}$ and $F^{C_{q_2}\rtimes C_r}$. Thus E has reduction type III or III* at the prime above ℓ in these fields, and the corresponding Tamagawa number is always 2 (see, for example, [11, Section IV.9]). The minimal model over $\mathbb{Q}_\ell$ does not remain minimal (valuation of the discriminant goes above 12, Lemma 36(6)) and the $|\omega/\omega^{\min}|$ terms contribute $\ell^{\lfloor\frac{3\cdot q_1q_2}{12}\rfloor}/\ell^{\lfloor\frac{3\cdot q_1}{12}\rfloor}\ell^{\lfloor\frac{3\cdot q_2}{12}\rfloor} = \ell^n$, where $n \not\equiv 0 \bmod 3$ by assumption.

Putting these computations together shows that

$$\frac{C_{E/F^{C_r}} \cdot C_{E/\mathbb{Q}}}{C_{E/F^{C_{q_1}\rtimes C_r}} \cdot C_{E/F^{C_{q_2}\rtimes C_r}}} = x^3\ell^n$$

for some $x \in \mathbb{Q}$ and integer $n \not\equiv 0 \bmod 3$. However, ℓ has order 3 in $\mathbb{F}_{q_1}^\times$ and so, as $q_1 \not\equiv 1 \bmod 9$, it is not a cube in $\mathbb{F}_{q_1}$. As q_2 is a cube mod q_1, this expression cannot be of the form $q_1^a q_2^b k$ for any $k \equiv 1 \bmod q_1q_2$, which gives the desired contradiction. □

Remark 32. Number fields satisfying the hypotheses of Corollary 31 do exist. For example, we can take $q_1 = 643$ and $q_2 = 43$. For simplicity, let us take $K = \mathbb{Q}(\zeta_9)^+$ which has class number 1 and then choose ℓ and F using class field theory as follows. First pick five candidate primes $\ell_1, \dots, \ell_5$ that satisfy the third and fourth bullet points of the corollary – these are congruence conditions, so such primes exist. As ℓ_i has residue degree 3 in K and $\ell_i^3 \equiv 1 \bmod q_1$, the group $(\mathcal{O}_K/\prod \ell_i)^\times$ has a quotient isomorphic to $(C_{q_1})^5$. The unit group of K has rank 2, so the ray class group $((\mathcal{O}_K/\prod \ell_i)^\times/\text{image of } \mathcal{O}_K^\times)$ has a $\mathrm{Gal}(K/\mathbb{Q})$-stable quotient isomorphic to $(C_{q_1})^n$ for some $n \geq 3$. In particular, as $q_1 \equiv 1 \bmod 3$ and $\mathbb{F}_{q_1}$ contains the third roots of unity, there are at least three $\mathrm{Gal}(K/\mathbb{Q})$-stable C_{q_1}-quotients whose corresponding fields F_1, F_2, F_3 under global class field theory are linearly disjoint. By construction, the F_i are Galois over $\mathbb{Q}$, have degree q_1 over K and only the ℓ_i can ramify in F_i/K. As K has class number 1 and the F_i are linearly disjoint, at least three of the ℓ_i must ramify in some of the fields. Now repeating the same construction with the same ℓ_i for q_2 similarly yields three fields F_1', F_2', F_3' of degree q_2 over K. One of the ℓ_i must ramify both in one of the F_i and in one of the F_i', say ℓ_1 ramifies in F_1 and in F_2. We can then take $F = F_1F_2$ and $\ell = \ell_1$.

3.3. Forcing points of infinite order. For our final type of application of Proposition 27, we will make the local data force the existence of points of infinite order on elliptic curves. This time, the idea is to make sure that the ratio of BSD-terms in the theorem cannot be the norm of an element at all, and hence E/F must have positive rank. In order to do this, we need a way of controlling the Tate–Shafarevich group. In general, this is very difficult, so we will simply make use of the fact that it has square order and that all squares are norms from quadratic fields.

Theorem 33. *Suppose Conjecture* 4 *holds. Let $E/\mathbb{Q}$ be an elliptic curve, $F/\mathbb{Q}$ a Galois extension with Galois group G, ρ an irreducible representation of G and*

$$\Big(\bigoplus_{\mathfrak{g}\in\mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})} \rho^{\mathfrak{g}}\Big)^{\oplus m} = \Big(\bigoplus_i \mathrm{Ind}_{F_i/\mathbb{Q}}\,\mathbf{1}\Big) \ominus \Big(\bigoplus_j \mathrm{Ind}_{F_j'/\mathbb{Q}}\,\mathbf{1}\Big)$$

for some $m\in\mathbb{Z}$ and subfields $F_i, F_j'\subseteq F$. If either $\prod_i C_{E/F_i}/\prod_j C_{E/F_j'}$ is not a norm from some quadratic subfield $\mathbb{Q}(\sqrt{D})\subset\mathbb{Q}(\rho)$, or if it is not a rational square when m is even, then E has a point of infinite order over F.

Proof. Suppose $\mathrm{rk}\,E/F=0$. By Proposition 27, $\prod \mathrm{BSD}(E/F_i)/\prod \mathrm{BSD}(E/F_j')$ is the m-th power of the norm of an element of $\mathbb{Q}(\rho)$. In particular, it is a norm from $\mathbb{Q}(\sqrt{D})$, and if m is even, it is a rational square.

As the rank is zero over F, the regulators that enter the BSD-terms are all 1. The contributions from Ш and torsion are all squares, and hence automatically norms from $\mathbb{Q}(\sqrt{D})$. It follows that the remaining expression $\prod_i C_{E/F_i}/\prod_j C_{E/F_j'}$ must be a norm from $\mathbb{Q}(\sqrt{D})$ as well, and a rational square in case m is even. □

The criterion of Theorem 33 can be applied in many Galois groups to find local conditions on elliptic curves that guarantee the existence of points of infinite order. We illustrate it on the group of quaternions, Q_8:

Corollary 34. *Suppose Conjecture* 4 *holds. Let $F/\mathbb{Q}$ be a Galois extension with Galois group Q_8. Then every elliptic curve $E/\mathbb{Q}$ with good reduction at* 2 *and* 3 *and with an odd number of potentially multiplicative primes that do not split in $F/\mathbb{Q}$ must have a point of infinite order over F.*

Proof. Let ρ be the 2-dimensional irreducible representation of Q_8 and let C_2 be the unique subgroup of Q_8 of order 2, so that

$$\rho^{\oplus 2} = \mathrm{Ind}_1^{Q_8}\,\mathbf{1} \ominus \mathrm{Ind}_{C_2}^{Q_8}\,\mathbf{1}.$$

We will show that $\frac{C_{E/F}}{C_{E/L}}$ has odd 2-adic valuation, where $L=F^{C_2}$. The result then follows from the theorem.

Observe that if a prime p splits in $F/\mathbb{Q}$, then it necessarily already splits in $L/\mathbb{Q}$. Indeed, if there is only one prime above p in L, then the decomposition group at p surjects onto Q_8/C_2. The only subgroup with this property is the whole of Q_8, so there is only one prime above p in F. It follows that split primes contribute square contributions to $\frac{C_{E/F}}{C_{E/L}}$.

As E has good reduction at 2, these primes do not contribute to the ratio: ω remains minimal in all field extensions of $\mathbb{Q}_2$ and the local Tamagawa number is always 1 (Lemma 36). At primes $v\nmid 2$, the contribution from $\mathrm{ord}_2\,|\omega/\omega^{\min}|_v$ will clearly be zero. Thus

$$\mathrm{ord}_2\,\frac{C_{E/F}}{C_{E/L}} = \sum_{p\in B} \mathrm{ord}_2(c_w/c_v),$$

where B is the set of primes of bad reduction of E that do not split in $F/\mathbb{Q}$, and where v and w are the primes above p in L and F, respectively.

If $p\in B$, then p necessarily has residue degree 2 and ramification degree 4 in $F/\mathbb{Q}$ and the prime above it ramifies in F/L, as the only possible choices for the (tame!) inertia subgroup and its cyclic quotient are $Q_8/C_4\simeq C_2$ for one of the cyclic subgroups of order 4. In

particular, if p is a prime of potentially multiplicative reduction, then E has split multiplicative reduction at v in L and $c_w = 2c_v$ (Lemma 36). If p is a prime of potentially good reduction, then the p-adic valuation δ of the minimal discriminant of $E/\mathbb{Q}_p$ determines the Kodaira type of E at v and at w. Recall that the Tamagawa number of E over a local field M is the number of Frobenius invariant points of $E(M^{nr})/E_0(M^{nr})$, so we read off from [11, Chapter 9, Table 4.1] that the pair of Tamagawa numbers c_v, c_w is either $3,3$ or $3,1$ ($\delta = 2, 10$), $1,1$ or $4,1$ ($\delta = 3, 9$, noting that L_v is a quadratic unramified extension of a field, so Frobenius has odd order on E/E_0 over L_v), $2,2$ ($\delta = 4, 8$), or $1,1$ ($\delta = 6$). Thus in all cases of potentially good reduction $\operatorname{ord}_2 c_w/c_v$ is even. The result follows. □

As a final application, we will prove a result on the Birch–Swinnerton-Dyer conjecture in dihedral extensions. This time we will classify the cases when our local BSD-term data predicts that ρ appears in $E(F)_{\mathbb{C}}$ and compare it to the corresponding root number predictions.

Theorem 35. *Suppose Conjecture* 4 *holds. Let $F/\mathbb{Q}$ be a Galois extension with Galois group D_{2pq}, with $p, q \equiv 3 \bmod 4$ primes, and let ρ be a faithful irreducible Artin representation that factors through $F/\mathbb{Q}$. Then for every semistable elliptic curve $E/\mathbb{Q}$, if* $\operatorname{ord}_{s=1} L(E, \rho, s)$ *is odd, then $\langle \rho, E(F)_{\mathbb{C}} \rangle > 0$.*

Proof. We first remark that this L-function does have an analytic continuation to $\mathbb{C}$ and satisfies the standard functional equation. (It can be expressed as a classical Rankin–Selberg product. Alternatively, ρ is induced from a 1-dimensional representation ψ of $\operatorname{Gal}(F/K)$, where K is the quadratic subfield of F, and so $L(E, \rho, s) = L(E/K, \psi, s) = L(\pi_{E/K} \otimes \psi, s)$, where $\pi_{E/K}$ is the automorphic form obtained by cyclic base change from the modular form attached to $E/\mathbb{Q}$ by modularity.)

We apply Proposition 27 to the identity

$$\bigoplus_{\mathfrak{g} \in \operatorname{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})} \rho^{\mathfrak{g}} = \operatorname{Ind}_{C_2}^{G} \mathbf{1} \ominus \operatorname{Ind}_{D_{2p}}^{G} \mathbf{1} \ominus \operatorname{Ind}_{D_{2q}}^{G} \mathbf{1} \oplus \mathbf{1},$$

where $G = D_{2pq}$. Here $\mathbb{Q}(\rho) = \mathbb{Q}(\zeta_{pq})^+$ contains the quadratic field $\mathbb{Q}(\sqrt{pq})$. Since squares are always norms from quadratic fields we deduce that either $\langle \rho, E(F)_{\mathbb{C}} \rangle > 0$ or

$$\frac{C_{E/L_{pq}} C_{E/\mathbb{Q}}}{C_{E/L_p} C_{E/L_q}} \cdot \frac{\operatorname{Reg}_{E/L_{pq}} \operatorname{Reg}_{E/\mathbb{Q}}}{\operatorname{Reg}_{E/L_p} \operatorname{Reg}_{E/L_q}} = N_{\mathbb{Q}(\sqrt{pq})/\mathbb{Q}}(x) \quad \text{for some } x \in \mathbb{Q}(\sqrt{pq}),$$

where $L_{pq} = F^{C_2}$, $L_p = F^{D_{2q}}$ and $L_q = F^{D_{2p}}$ are the intermediate fields of degree pq, p and q over $\mathbb{Q}$, respectively.

Write M for the set of primes of multiplicative reduction of $E/\mathbb{Q}$, $a_r = 1$ if the reduction at a prime $r \in M$ is split and $a_r = -1$ if it is non-split, and write e_r and f_r for the ramification and residue degree of a prime r in $F/\mathbb{Q}$, respectively. Set

$$X = \{v : \infty \text{ in } K\} \cup \{r \in M,\ e_r = 1,\ f_r = 2\} \cup \{r \in M,\ e_r = 2,\ a_r = -1\}.$$

Claim 1. *If $\langle \rho, E(F)_{\mathbb{C}} \rangle = 0$, then*

$$\frac{C_{E/L_{pq}} C_{E/\mathbb{Q}}}{C_{E/L_p} C_{E/L_q}} \cdot \frac{\operatorname{Reg}_{E/L_{pq}} \operatorname{Reg}_{E/\mathbb{Q}}}{\operatorname{Reg}_{E/L_p} \operatorname{Reg}_{E/L_q}} = (pq)^{\#X} \cdot \square,$$

where "□" is shorthand for a rational square.

Claim 2. *We have* $\operatorname{ord}_{s=1} L(E,\rho,s) \equiv \#X \bmod 2$.

Observe that pq is not the norm of any element of $\mathbb{Q}(\sqrt{pq})$: indeed, as $p \equiv 3 \bmod 4$, the norm equation $pq = a^2 - pqb^2$ is not even soluble in $\mathbb{Q}_p$. It thus follows from the two claims and the formula above that $\langle \rho, E(F)_{\mathbb{C}} \rangle > 0$, which proves the theorem.

Proof of Claim 2. The parity of the order of vanishing of the L-function is given by the root number $w_{E,\rho}$. As $E/\mathbb{Q}$ is semistable and $\dim \rho = 2$, by [7, Theorem 1],

$$w_{E,\rho} = (-1)^{\dim \rho^-} \prod_{r \in M} a_r^{\dim \rho^{I_r}} \det(\mathrm{Frob}_r \,|\rho^{I_r}),$$

where $\dim \rho^-$ is 1 or 2 according to whether K is complex or real, Frob_r is any choice of Frobenius element at r in $\mathrm{Gal}(F/\mathbb{Q})$, and ρ^{I_r} is the subspace of ρ that is pointwise fixed by the inertia subgroup I_r. If a prime $r \in M$ is unramified in $F/\mathbb{Q}$, then its contribution to the product is -1 if and only if Frob_r has order 2. If it ramifies, then the contribution is -1 if and only if I_r has order 2 (in D_{2pq}, $|I_r| = 2$ forces Frob_r to be trivial) and $a_r = -1$. In other words $w_{E,\rho} = (-1)^{\#X}$. □

Proof of Claim 1. Since $E/\mathbb{Q}$ is semistable, its global minimal differential remains minimal in all field extensions, so we can write

$$C_{E/L} = \prod_{r \in M} C_{v|r}(L)$$

with $C_{v|r}(L) = \prod_{v|r} c_v(E/L)$.

The group D_{2pq} has five rational irreducible representations: trivial $\mathbf{1}$, sign ϵ, τ_p that factors through the D_{2p}-quotient and similarly τ_q and τ_{pq}. Now pick points $P_1, \dots, P_a \in E(\mathbb{Q})$ that form a basis for $E(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{Q}$, the $\mathbf{1}$-isotypical component of $E(F) \otimes \mathbb{Q}$. Complete it to a basis $P_1, \dots, P_a, Q_1, \dots, Q_b \in E(L_p)$ for $E(L_p) \otimes \mathbb{Q}$, with the Q_i belonging to the τ_p-isotypical component of $E(F) \otimes \mathbb{Q}$; and similarly to $P_1, \dots, P_a, R_1, \dots, R_b$ for $E(L_q) \otimes \mathbb{Q}$ with the R_i belonging to the τ_q-isotypical component. By assumption, τ_{pq} does not appear in $E(F) \otimes \mathbb{Q}$, so that the P_i, Q_i and R_i together form a basis for $E(L_{pq}) \otimes \mathbb{Q}$. Moreover, as the height pairing on $E(F)$ is Galois invariant, the spaces spanned by the P_i, the Q_i and the R_i are orthogonal to each other. Finally, recall that the height pairing scales under field extensions by the degree, so that the ratio of the regulators is

$$\frac{\mathrm{Reg}_{E/L_{pq}} \mathrm{Reg}_{E/\mathbb{Q}}}{\mathrm{Reg}_{E/L_p} \mathrm{Reg}_{E/L_q}} = \square \cdot q^{\mathrm{rk}\, E/L_p - \mathrm{rk}\, E/\mathbb{Q}}\, p^{\mathrm{rk}\, E/L_q - \mathrm{rk}\, E/\mathbb{Q}},$$

the square error coming from the fact that our bases span finite index sublattices of $E(\mathbb{Q})$, $E(L_p)$, $E(L_q)$ and $E(L_{pq})$ (see Lemma 36).

As the p- and q-primary parts of $Ш_{E/F}$ are finite (which is therefore also true over all the subfields), the known cases of the parity conjecture for $E/\mathbb{Q}$, E/L_p and E/L_q (see [6, Theorem 1.3]), tell us that the parity of each exponent in the above formula is determined by the corresponding root number. Thus, like for the $C_{E/*}$-terms, we can express this as a product

$$q^{\mathrm{rk}\, E/L_p - \mathrm{rk}\, E/\mathbb{Q}} = \square \cdot \prod_{r \in M \cup \{\infty\}} q^{\theta_r^{(q)}},$$

where $\theta_r^{(q)}$ is 0 or 1 depending on whether $w(E/\mathbb{Q}_r)\prod_{v|r} w(E/(L_p)_v)$ is 1 or -1; and similarly for the exponent of p. Hence

$$\frac{C_{E/L_{pq}}C_{E/\mathbb{Q}}}{C_{E/L_p}C_{E/L_q}}\cdot\frac{\mathrm{Reg}_{E/L_{pq}}\mathrm{Reg}_{E/\mathbb{Q}}}{\mathrm{Reg}_{E/L_p}\mathrm{Reg}_{E/L_q}}=\square\cdot\prod_{r\in M\cup\{\infty\}}Z_r,$$

where $Z_r = C_{v|r}(\mathbb{Q})C_{v|r}(L_p)C_{v|r}(L_q)C_{v|r}(L_{pq})q^{\theta_r^q}p^{\theta_r^p}$. Thus it now suffices to check that $Z_r = pq\square$ for $r\in X$ and $Z_r=\square$ for $r\notin X$.

To explicitly determine Z_r, we systematically work through all possibilities. Recall that the local root number $w(E/L_v)$ is $+1$ for good and non-split multiplicative reduction and -1 for split multiplicative reduction and for archimedean places. Recall also that if the Kodaira type of E/L_v is I_n, then the Tamagawa number is n if the reduction is split, and 1 or 2 if it is non-split, depending on whether n is odd or even, which we will denote by $\tilde{n}$. Finally, multiplicative reduction of type I_n becomes of type I_{en} after a ramified extension of degree e, split reduction remains split, and non-split reduction becomes split if the extension has even residue degree. We tabulate in Table 1 the contribution to the above product from a prime r depending on its ramification degree e_r and residue degree f_r in $F/\mathbb{Q}$; in D_{2pq} these uniquely determine the inertia and decomposition subgroups, and hence the splitting behaviour of r in all intermediate extension. The values are constrained by the fact that both the (tame!) inertia group is cyclic of order e_r and normal in the decomposition group with a cyclic quotient of order f_r. The entries for split and non-split multiplicative reduction of type I_n are separated by a semicolon.

Finally, note that if the quadratic field K is real, then $F/\mathbb{Q}$ is totally real, so L_p has p infinite places and $q^{\theta_\infty^q}=1$, and similarly for L_q; hence $Z_\infty=1$. If K is imaginary, then

e_r,	f_r	$C_{v\|r}(\mathbb{Q})$	$C_{v\|r}(L_p)$	$C_{v\|r}(L_q)$	$C_{v\|r}(L_{pq})$	$q^{\theta_r^{(q)}}$	$p^{\theta_r^{(p)}}$	Z_r
1,	1	$n;\tilde{n}$	$n^p;\tilde{n}^p$	$n^q;\tilde{n}^q$	$n^{pq};\tilde{n}^{pq}$	1; 1	1; 1	$\square$
1,	2	$n;\tilde{n}$	$n^{\frac{p+1}{2}};\tilde{n}n^{\frac{p-1}{2}}$	$n^{\frac{q+1}{2}};\tilde{n}n^{\frac{q-1}{2}}$	$n^{\frac{pq+1}{2}};\tilde{n}n^{\frac{pq-1}{2}}$	$q;q$	$p;p$	$pq\square$
1,	p	$n;\tilde{n}$	$n;\tilde{n}$	$n^q;\tilde{n}^q$	$n^q;\tilde{n}^q$	1; 1	1; 1	$\square$
1,	q	$n;\tilde{n}$	$n;\tilde{n}$	$n^p;\tilde{n}^p$	$n^p;\tilde{n}^p$	1; 1	1; 1	$\square$
1,	pq	$n;\tilde{n}$	$n;\tilde{n}$	$n;\tilde{n}$	$n;\tilde{n}$	1; 1	1; 1	$\square$
2,	1	$n;\tilde{n}$	$(2n)^{\frac{p-1}{2}}n;2^{\frac{p-1}{2}}\tilde{n}$	$(2n)^{\frac{q-1}{2}}n;2^{\frac{q-1}{2}}\tilde{n}$	$(2n)^{\frac{pq-1}{2}}n;2^{\frac{pq-1}{2}}\tilde{n}$	$q;1$	$p;1$	$pq\square;\square$
p,	1	$n;\tilde{n}$	$np;\tilde{n}$	$n^q;\tilde{n}^q$	$(np)^q;\tilde{n}^q$	1; 1	1; 1	$\square$
p,	2	$n;\tilde{n}$	$np;\tilde{n}$	$n^{\frac{q+1}{2}};\tilde{n}n^{\frac{q-1}{2}}$	$(np)^{\frac{q+1}{2}};\tilde{n}(np)^{\frac{q-1}{2}}$	1; 1	$p;p$	$\square$
p,	q	$n;\tilde{n}$	$np;\tilde{n}$	$n;\tilde{n}$	$np;\tilde{n}$	1; 1	1; 1	$\square$
q,	1	$n;\tilde{n}$	$nq;\tilde{n}$	$n^p;\tilde{n}^p$	$(nq)^p;\tilde{n}^p$	1; 1	1; 1	$\square$
q,	2	$n;\tilde{n}$	$nq;\tilde{n}$	$n^{\frac{p+1}{2}};\tilde{n}n^{\frac{p-1}{2}}$	$(nq)^{\frac{p+1}{2}};\tilde{n}(nq)^{\frac{p-1}{2}}$	1; 1	$q;q$	$\square$
q,	p	$n;\tilde{n}$	$nq;\tilde{n}$	$n;\tilde{n}$	$nq;\tilde{n}$	1; 1	1; 1	$\square$
$2p$,	1	$n;\tilde{n}$	$np;\tilde{n}$	$(2n)^{\frac{q-1}{2}}n;2^{\frac{q-1}{2}}\tilde{n}$	$(2np)^{\frac{q-1}{2}}np;2^{\frac{q-1}{2}}\tilde{n}$	1; 1	$p;1$	$\square$
$2q$,	1	$n;\tilde{n}$	$np;\tilde{n}$	$(2n)^{\frac{p-1}{2}}n;2^{\frac{p-1}{2}}\tilde{n}$	$(2nq)^{\frac{p-1}{2}}nq;2^{\frac{p-1}{2}}\tilde{n}$	1; 1	$q;1$	$\square$
pq,	1	$n;\tilde{n}$	$np;\tilde{n}$	$nq;\tilde{n}$	$npq;\tilde{n}$	1; 1	1; 1	$\square$
pq,	2	$n;\tilde{n}$	$np;\tilde{n}$	$nq;\tilde{n}$	$npq;\tilde{n}$	1; 1	1; 1	$\square$

Table 1. Tamagawa number and regulator ratio contributions from a prime r.

L_p has one real and $\frac{p-1}{2}$ (=odd) complex places and $q^{\theta_\infty^q} = q$, and similarly for L_q; hence $Z_\infty = pq$. Thus, indeed, $Z_r = pq\square$ for $r \in X$ and $Z_r = \square$ for $r \notin X$, as required. This finishes the proof of Claim 1.

The theorem is proved. □

3.4. Summary of some basic properties. We list some standard results regarding elliptic curves over local and global fields. We give brief proofs as, while these results are well known, they may not always be easy to find in the literature.

Lemma 36. *Let E/K be an elliptic curve over a number field, F/K a field extension of finite degree d. Let v be a finite place of K with $w|v$ a place above it in F, and ω_v and ω_w minimal differentials for E/K_v and E/F_w, respectively.*

(1) *If F/K is Galois, then $\mathrm{Sel}_n(E/K)$ identifies with a subgroup of $\mathrm{Sel}_n(E/F)$ for all n coprime to d.*

(2) *For $P, Q \in E(K)$, their Néron–Tate height pairings over K and F are related by*

$$\langle P, Q\rangle_F = d\,\langle P, Q\rangle_K.$$

(3) *If $\mathrm{rk}\, E/F = \mathrm{rk}\, E/K$, then*

$$\mathrm{Reg}_{E/F} = \frac{d^{\mathrm{rk}\, E/K}}{n^2}\,\mathrm{Reg}_{E/K},$$

where n is the index of $E(K)$ in $E(F)$.

(4) *If E/K_v has good reduction, then $c_v = 1$. If E/K_v has multiplicative reduction of Kodaira type I_n, then $n = \mathrm{ord}_v\, \Delta_{E,v}^{\min}$ and $c_v = n$ if the reduction is split, and $c_v = 1$ (respectively, 2) if the reduction is non-split and n is odd (respectively, even).*

(5) *If E/K_v has good or multiplicative reduction, then $|\omega_v/\omega_w|_w = 1$.*

(6) *If E/K_v has potentially good reduction and the residue characteristic is not 2 or 3, then*

$$\left|\frac{\omega_v}{\omega_w}\right|_w = q^{\lfloor \frac{e_{F/K}\,\mathrm{ord}_v\,\Delta_{E,v}^{\min}}{12} \rfloor},$$

where q is the size of the residue field at w.

(7) *If v has odd residue characteristic, E/K_v has potentially multiplicative reduction and F_w/K_v has even ramification degree, then E/F_w has multiplicative reduction.*

(8) *Multiplicative reduction becomes split after a quadratic unramified extension.*

Proof. (1) In the inflation-restriction sequence

$$H^1(\mathrm{Gal}(F/K), E(F)[n]) \to H^1(K, E[n]) \to H^1(F, E[n]),$$

the first term is killed both by $|\mathrm{Gal}(F/K)|$ and by n, and is therefore trivial. Thus the second map and its restriction to n-Selmer groups are injective.

(2) This follows from the definition of the height pairing, see [13, equation (1.6)]. (Note that it is *not* normalised as for the absolute height.)

(3) Follows from (2) and the fact that the height pairing is bilinear and non-degenerate.

(4) See [11, Section IV.9].

(5) As E/K_v has good or multiplicative reduction, its minimal Weierstrass model over K_v remains minimal over F_w, so ω_v is also a minimal differential over F.

(6) In this setting $\operatorname{ord}_w \Delta^{\min}_{E,w} < 12$, so the result follows from the formula in Notation 17.

(7) This follows from the theory of the Tate curve, see e.g. [11, Exercise 5.11].

(8) Clear from the definition of non-split multiplicative reduction. □

4. Arithmetically similar twists with different L-values

In this section we discuss the problem of formulating a precise Birch–Swinnerton-Dyer-type formula for twists of elliptic curves by Dirichlet characters χ. We make the information that we know about $\mathscr{L}(E,\chi)$ explicit and discuss the difficulties illustrated in Example 3. We will also give many numerical examples, for the benefit of those readers who may wish to analyse these L-values in more detail.

The numerical examples throughout this section were worked out using Magma [2]. The orders of Ш given are strictly speaking "analytic orders of Ш", that is the orders that are predicted by the Birch–Swinnerton-Dyer conjecture.

Notation 37. Recall from Notation 15 that we identify Dirichlet characters χ with their corresponding 1-dimensional Galois representations. We write K^χ for the abelian number field cut out by the kernel of χ, that is for the smallest extension $K^\chi/\mathbb{Q}$ such that χ factors through $\mathrm{Gal}(K^\chi/\mathbb{Q})$.

In the context of Dirichlet characters, we already know from Theorem 13 a substantial amount about $L(E,\chi,1)$ in terms of arithmetic data:

Theorem 38. *Suppose Stevens's Manin constant conjecture holds for $E/\mathbb{Q}$. Let χ be a non-trivial primitive Dirichlet character of order d and conductor coprime to $\mathfrak{f}_E$. Then $\mathscr{L}(E,\chi)\in\mathbb{Z}[\zeta_d]$ and, if $L(E,\chi,1)\neq 0$, then furthermore*

$$\zeta\cdot\mathscr{L}(E,\chi)\in\mathbb{R}\quad \text{for } \zeta=\chi(\mathfrak{f}_E)^{\frac{d+1}{2}}\sqrt{\chi(-1)w_E}.$$

If $\operatorname{rk} E/\mathbb{Q}=0$ *and the Birch–Swinnerton-Dyer conjecture holds for E over $\mathbb{Q}$ and K^χ, then*

$$N_{\mathbb{Q}(\zeta_d)^+/\mathbb{Q}}(\zeta\cdot\mathscr{L}(E,\chi))=\pm\frac{|E(\mathbb{Q})_{\mathrm{tors}}|}{|E(K^\chi)_{\mathrm{tors}}|}\sqrt{\frac{|Ш_{E/K^\chi}|\prod_v c_v(E/K^\chi)}{|Ш_{E/\mathbb{Q}}|\prod_p c_p(E/\mathbb{Q})}}.$$

If moreover d is odd and $\mathrm{BSD}(E/K^\chi)=\mathrm{BSD}(E/\mathbb{Q})$, *then $\mathscr{L}(E,\chi)=\zeta^{-1}u$ for some unit $u\in\mathcal{O}^\times_{\mathbb{Q}(\zeta_d)^+}$.*

Proof. The first claim follows from Theorem 13 (8)–(10) with $\rho=\chi$.

Applying Theorem 13 (12) with the identity $\bigoplus_{\mathfrak{g}\in\mathrm{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q})}\chi^{\mathfrak{g}}\oplus\mathbf{1}=\mathbb{C}[G]$ shows that

$$N_{\mathbb{Q}(\zeta_d)^+/\mathbb{Q}}(\zeta\cdot\mathscr{L}(E,\chi))=\pm\sqrt{\frac{\mathrm{BSD}(E/K^\chi)}{\mathrm{BSD}(E/\mathbb{Q})}}.$$

Since the conductor of E is coprime to that of χ, the primes of bad reduction of E are unramified in $K^\chi/\mathbb{Q}$, so a global minimal differential for $E/\mathbb{Q}$ remains minimal over K^χ and hence

all the contributions of the form $|\omega/\omega^{\min}|$ to the BSD-terms are trivial. This proves the desired second formula.

For the final claim, note that as $\mathrm{rk}\, E/\mathbb{Q} = 0$ and d is odd, we must have

$$w_E = \chi(-1) = 1,$$

so that $\zeta \in \mathbb{Q}(\zeta_d)$. The result now follows from the previous parts. □

Let us note that, under the above assumptions, we can predict the value $L(E, \chi, 1)$ from Birch–Swinnerton-Dyer-type information up to an element of norm ± 1 in $\mathbb{Q}(\zeta_d)^+$. In fact, since $\mathscr{L}(E, \chi)$ is integral, the prediction is stronger than that. For instance, if χ has order 3 and $\mathrm{BSD}(E/K^\chi) = \mathrm{BSD}(E/\mathbb{Q})$, then $L(E, \chi, 1)$ is fully determined up to a sign. However, this final ambiguity appears to be severe:

Theorem 39. *For elliptic curves $E/\mathbb{Q}$ and Dirichlet characters χ as in Theorem* 38*,*

(1) *$\mathscr{L}(E, \chi)$ cannot be expressed purely as a function of the character χ, of $E(\mathbb{Q})$, $Ш_{E/\mathbb{Q}}$, $\prod_p E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$ as abelian groups and of $E(K^\chi)$, $Ш_{E/K^\chi}$, $\prod_v E(K_v^\chi)/E_0(K_v^\chi)$ as $\mathrm{Gal}(K^\chi/\mathbb{Q})$-modules.*

(2) *The fractional ideal $(\mathscr{L}(E, \chi))$ cannot be expressed purely as a function of χ, and of $E(\mathbb{Q})$, $Ш_{E/\mathbb{Q}}$, $\prod_p E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$, $E(K^\chi)$, $Ш_{E/K^\chi}$ and $\prod_v E(K_v^\chi)/E_0(K_v^\chi)$ as abelian groups.*

Here the products are taken over all primes of $\mathbb{Q}$ and of K^χ, and E_0 denotes the usual subgroup of points of non-singular reduction.

This theorem follows from the fact that one can find curves with identical arithmetic invariants listed in (1) and (2), but with different algebraic L-values $\mathscr{L}(E, \chi)$. This is shown by the next two examples, where most of the objects listed in (1) and (2) are trivial.

Example 40. Let $E_1/\mathbb{Q}$ be the elliptic curve given by

$$y^2 + y = x^3 - 8x - 9,$$

and $E_2/\mathbb{Q}$ be another elliptic curve given by

$$y^2 + y = x^3 + x - 1,$$

which have Cremona labels 307a1 and 307c1, respectively. Let χ be the primitive Dirichlet character of order 5 and conductor 11 defined by $\chi(2) = \zeta_5$. Both curves have

$$\begin{aligned} |E_i(\mathbb{Q})| = |E_i(K^\chi)| &= |Ш_{E_i/\mathbb{Q}}| = |Ш_{E_i/K^\chi}| \\ &= \prod_p c_p(E_i/\mathbb{Q}) = \prod_v c_v(E_i/K^\chi) = 1. \end{aligned}$$

In particular, all the groups listed in Theorem 39 are trivial. In fact, the curves also have the same conductor $\mathfrak{f}_{E_i} = 307$ and the same discriminant $\Delta_{E_i} = -307$. However, their algebraic L-values differ:

$$\mathscr{L}(E_1, \chi) = 1, \quad \mathscr{L}(E_2, \chi) = \zeta_5^4(1 + \zeta_5)^2.$$

Remark 41. As the discriminants for the two curves in the above example are the same and thus in particular have the same sign, both curves have the same number of connected components over $\mathbb{R}$. In other words, one can add the group of real connected components $E(\mathbb{R})/E_0(\mathbb{R})$ to the list of groups in Theorem 39 (1), as well as the conductor and the discriminant of E.

Example 42. Let $E_1/\mathbb{Q}$ be the elliptic curve given by

$$y^2 + y = x^3 - x^2 - 1,$$

and $E_2/\mathbb{Q}$ be another elliptic curve given by

$$y^2 + xy = x^3 + x^2 - 3x - 4,$$

which have Cremona labels 291d1 and 139a1, respectively. Let χ be the primitive character of order five and conductor 31 defined by $\chi(3) = \zeta_5^3$. Both curves have

$$|E_i(\mathbb{Q})| = |E_i(K^\chi)| = |Ш_{E_i/\mathbb{Q}}| = \prod_p c_p(E_i/\mathbb{Q}) = \prod_v c_v(E_i/K^\chi) = 1$$

and

$$|Ш_{E_i/K^\chi}| = 11^2.$$

The discriminants $\Delta_{E_1} = -291$ and $\Delta_{E_2} = -139$ again have the same sign. For these curves,

$$\mathscr{L}(E_1, \chi) = 2\zeta_5^3 - \zeta_5^2 - \zeta_5 + 2 \quad \text{and} \quad \mathscr{L}(E_2, \chi) = 5\zeta_5^3 + \zeta_5^2 + \zeta_5 + 5.$$

These factorise as

$$(\mathscr{L}(E_1, \chi)) = \mathfrak{p}_1\mathfrak{p}_2 \quad \text{and} \quad (\mathscr{L}(E_2, \chi)) = \mathfrak{p}_3\mathfrak{p}_4,$$

where $\mathfrak{p}_1 = (11, 7+\zeta_5)$, $\mathfrak{p}_2 = (11, 8+\zeta_5)$, $\mathfrak{p}_3 = (11, 6+\zeta_5)$, $\mathfrak{p}_4 = (11, 2+\zeta_5)$ are the primes of $\mathbb{Q}(\zeta_5)$ above 11.

We note that it is plausible that the exact factorisation can be recovered from the Galois module structure of Ш. Unfortunately, it appears to be beyond our computational reach to check this at present. (See, however, the recent work of Burns and Castillo [3, Remark 7.4].)

Remark 43. In the above example, our results on L-values are strong enough to predict that the ideal $\mathscr{L}(E_i, \chi)$ must be either $\mathfrak{p}_1\mathfrak{p}_2$ or $\mathfrak{p}_3\mathfrak{p}_4$, though, as the example illustrates, they do not allow us decide which of the two occurs. To see why the factorisation must be one of these two, consider any Dirichlet character χ of order 5 and any elliptic curve $E/\mathbb{Q}$ satisfying the conditions of Theorem 38 and additionally

$$\frac{\mathrm{BSD}(E/K^\chi)}{\mathrm{BSD}(E/\mathbb{Q})} = 11^2.$$

Then by Theorem 13 (10), (11) and (6), $\mathscr{L}(E, \chi)$ is an element of $\mathbb{Z}[\zeta_5]$ of norm 11^2 and generates an ideal that is fixed by complex conjugation. Hence $(\mathscr{L}(E, \chi))$ must be either $\mathfrak{p}_1\mathfrak{p}_2$ or $\mathfrak{p}_3\mathfrak{p}_4$.

For those who may be interested in investigating these L-values further, we end by giving a range of further examples. All elliptic curves below are given by their Cremona labels.

Example 44. There are plenty of curves that have trivial Mordell–Weil groups, Ш and Tamagawa numbers both over $\mathbb{Q}$ and over K^χ for the same Dirichlet character χ of order 5 as in Example 40. In Table 2 we have chosen some groups of such curves that also have the

E	$\mathscr{L}(E,\chi)$	E	$\mathscr{L}(E,\chi)$	E	$\mathscr{L}(E,\chi)$	E	$\mathscr{L}(E,\chi)$	E	$\mathscr{L}(E,\chi)$
307a1	1	432g1	u^2	714b1	1	1187a1	$\zeta_5^3u^{-1}$	1216g1	$-\zeta_5^2u^2$
307c1	$\zeta_5^4u^2$	432h1	$-\zeta_5^4u^{-1}$	714h1	$-\zeta_5u^3$	1187b1	$\zeta_5^4u^{-3}$	1216k1	ζ_5u^{-1}

Table 2. Conductor $\mathfrak{f}_\chi = 11$ with $\chi(2) = \zeta_5$, $\Delta_{K^\chi} = 11^4$.

same conductors, but, as in the example, have different algebraic L-values (here $u = 1 + \zeta_5$ is a fundamental unit in $\mathbb{Q}(\zeta_5)$).

Example 45. The examples are even easier to find for cubic characters χ. As before, we will look at curves with

$$|E(\mathbb{Q})| = |E(K^\chi)| = |Ш_{E/\mathbb{Q}}| = |Ш_{E/K^\chi}| = \prod_p c_p(E/\mathbb{Q}) = \prod_v c_v(E/K^\chi) = 1.$$

All of the curves we look at in Table 3 will satisfy the conditions of Theorem 38, and thus by the same theorem we can predict the L-values up to sign. How to predict the sign is unclear, even for curves with the same conductor.

E	$\mathscr{L}(E,\chi)$	E	$\mathscr{L}(E,\chi)$	E	$\mathscr{L}(E,\chi)$	E	$\mathscr{L}(E,\chi)$	E	$\mathscr{L}(E,\chi)$
1356d1	ζ_3	3264r1	$-\zeta_3$	3540a1	$-\zeta_3$	4800i1	$-\zeta_3$		
1356f1	$-\zeta_3$	3264s1	ζ_3	3540b1	ζ_3	4800bj1	$-\zeta_3$		
						4800bm1	ζ_3		
Conductor $\mathfrak{f}_\chi = 7$ with $\chi(3) = \zeta_3^2$, $\Delta_{K^\chi} = 49$.									
222b1	-1	1392c1	-1	4386c1	-1	9024l1	$-\zeta_3^2$		
222e1	1	1392j1	1	4386m1	1	9024bf1	ζ_3^2		
Conductor $\mathfrak{f}_\chi = 13$ with $\chi(2) = \zeta_3^2$, $\Delta_{K^\chi} = 169$.									
702d1	-1	1443a1	1	5616j1	-1	12096bq1	1	19008u1	-1
702i1	1	1443b1	-1	5616o1	1	12096dc1	-1	19008bh1	1
				5616p1	1	12096dd1	1		
Conductor $\mathfrak{f}_\chi = 19$ with $\chi(2) = \zeta_3^2$, $\Delta_{K^\chi} = 381$.									
714b1	-1	2453a1	1	8138b1	1	12096x1	ζ_3		
714h1	1	2453c1	-1	8138c1	-1	12096dc1	ζ_3		
						12096dd1	$-\zeta_3$		
Conductor $\mathfrak{f}_\chi = 31$ with $\chi(3) = \zeta_3$, $\Delta_{K^\chi} = 961$.									
5885a1	$-\zeta_3$	11764a1	$-\zeta_3$	12096x1	ζ_3^2	15498h1	$-\zeta_3^2$	16590c1	1
5885d1	ζ_3	11764b1	ζ_3	12096bb1	$-\zeta_3^2$	15498i1	ζ_3^2	16590n1	-1
				12096bn1	ζ_3^2				
				12096cz1	$-\zeta_3^2$				
Conductor $\mathfrak{f}_\chi = 37$ with $\chi(2) = \zeta_3$, $\Delta_{K^\chi} = 1369$									

Table 3. Algebraic L-values for varying Dirichlet characters χ of order 3.

In these examples, the curves in each block also have discriminants of the same sign as each other and the same number of points over $\mathbb{F}_3$. The first condition ensures that they have the same number of real components. The second condition is motivated by p-adic L-functions, where the interpolation formula for L-values is adjusted by an extra term that depends on $|E(\mathbb{F}_p)|$.

Example 46. Here we give a list of curves similar to Example 42. We again take the character χ of order five and conductor 31 defined by

$$\chi(3) = \zeta_5^3,$$

and consider curves with conductor coprime to 31 with

$$|E(\mathbb{Q})| = |E(K^\chi)| = |Ш_{E/\mathbb{Q}}| = \prod_p c_p(E/\mathbb{Q}) = \prod_v c_v(E/K^\chi) = 1$$

and

$$|Ш_{E/K^\chi}| = 11^2.$$

We know from Remark 43 that the ideal $(\mathscr{L}(E,\chi))$ of $\mathcal{O}_{\mathbb{Q}(\zeta_5)}$ is either $\mathfrak{p}_1\mathfrak{p}_2$ or $\mathfrak{p}_3\mathfrak{p}_4$, where $\mathfrak{p}_1 = (11, 7+\zeta_5), \mathfrak{p}_2 = (11, 8+\zeta_5), \mathfrak{p}_3 = (11, 6+\zeta_5), \mathfrak{p}_4 = (11, 2+\zeta_5)$ are the primes of $\mathbb{Q}(\zeta_5)$ above 11. For the following list of curves $\mathscr{L}(E,\chi)$ splits as $\mathfrak{p}_1\mathfrak{p}_2$: 216b1, 216c1, 291d1, 443c1, 475a1. For the following list of curves $\mathscr{L}(E,\chi)$ splits as $\mathfrak{p}_3\mathfrak{p}_4$: 139a1, 140b1, 267b1, 333d1, 378h1, 432g1, 579a1.

References

[1] *A. Bartel*, Large Selmer groups over number fields, Math. Proc. Cambridge Philos. Soc. **148** (2010), no. 1, 73–86.

[2] *W. Bosma*, *J. Cannon* and *C. Playoust*, The Magma algebra system. I: The user language, J. Symbolic Comput. **24** (1997), 235–265.

[3] *D. Burns* and *D. M. Castillo*, On refined conjectures of Birch and Swinnerton-Dyer type for Hasse–Weil–Artin L-series, preprint 2019, `https://arxiv.org/abs/1909.03959`.

[4] *J. Coates*, Motivic p-adic L-functions, in: L-functions and arithmetic (Durham 1989), London Math. Soc. Lecture Note Ser. **153**, Cambridge University, Cambridge (1991), 141–172.

[5] *P. Deligne*, Valeurs de fonctions L et périodes d'intégrales, in: Automorphic forms, representations and L-functions, Part 2, Proc. Sympos. Pure Math. **33**, American Mathematical Society, Providence (1979), 313–346.

[6] *T. Dokchitser* and *V. Dokchitser*, Regulator constants and the parity conjecture, Invent. Math. **178** (2009), no. 1, 23–71.

[7] *V. Dokchitser*, Root numbers of non-abelian twists of elliptic curves, Proc. Lond. Math. Soc. (3) **91** (2005), no. 2, 300–324.

[8] *J. Martinet*, Character theory and Artin L-functions, in: Algebraic number fields: L-functions and Galois properties, Academic Press, London (1977), 1–87.

[9] *K. Matsuno*, Elliptic curves with large Tate–Shafarevich groups over a number field, Math. Res. Lett. **16** (2009), no. 3, 449–461.

[10] *D. E. Rohrlich*, The vanishing of certain Rankin–Selberg convolutions, in: Automorphic forms and analytic number theory, Université Montréal, Montreal (1990), 123–133.

[11] *J. H. Silverman*, Advanced topics in the arithmetic of elliptic curves, Grad. Texts in Math. **151**, Springer, New York 1994.

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

[13] *J. Tate*, On the conjectures of Birch and Swinnerton-Dyer and a geometric analog, in: Séminaire Bourbaki, Vol. 9, Société Mathématique de France, Paris (1966), 415–440, Exp. No. 306.
[14] *J. Tate*, Number theoretic background, in: Automorphic forms, representations and L-functions, Part 2, Proc. Sympos. Pure Math. **33**, American Mathematical Society, Providence (1979), 3–26.
[15] *O. Venjakob*, From the Birch and Swinnerton-Dyer conjecture to non-commutative Iwasawa theory via the equivariant Tamagawa number conjecture—a survey, in: L-functions and Galois representations, London Math. Soc. Lecture Note Ser. **320**, Cambridge University, Cambridge (2007), 333–380.
[16] *H. Wiersema* and *C. Wuthrich*, Integrality of twisted L-values of elliptic curves, preprint 2020, `https://arxiv.org/abs/2004.05492`.

Vladimir Dokchitser, University College London, 25 Gordon Street, London WC1H 0AY, United Kingdom
https://orcid.org/0000-0003-4384-4193
e-mail: v.dokchitser@ucl.ac.uk

Robert Evans, King's College London, Strand, London WC2R 2LS, United Kingdom
https://orcid.org/0000-0002-6825-8193
e-mail: robert.evans@kcl.ac.uk

Hanneke Wiersema, King's College London, Strand, London WC2R 2LS, United Kingdom
https://orcid.org/0000-0002-1211-3761
e-mail: hanneke.wiersema@kcl.ac.uk

Eingegangen 10. Mai 2020, in revidierter Fassung 5. September 2020