COMPUTING THE CASSELS–TATE PAIRING ON THE 3-SELMER GROUP OF AN ELLIPTIC CURVE

TOM FISHER AND RACHEL NEWTON

Abstract. We extend the method of Cassels for computing the Cassels–Tate pairing on the 2-Selmer group of an elliptic curve, to the case of 3-Selmer groups. This requires significant modifications to both the local and global parts of the calculation. Our method is practical in sufficiently small examples, and can be used to improve the upper bound for the rank of an elliptic curve obtained by 3-descent.

Introduction

The determination of the Mordell–Weil group $E(K)$ of an elliptic curve E over a number field K is usually tackled by means of computing the n-Selmer group $S^{(n)}(E/K)$ for some integer $n \geq 2$. Since $E(K)/nE(K)$ injects into $S^{(n)}(E/K)$, and the latter is finite and effectively computable, this approach gives an upper bound for the rank of $E(K)$. However, this upper bound will not be sharp if the Tate–Shafarevich group $Ш(E/K)$ contains elements of order n.

Let p be a prime. The Kummer exact sequences for multiplication-by-p and multiplication-by-p^2 on E fit into a commutative diagram

$$\begin{tikzcd} E(K) \arrow[r, "p^2"] \arrow[d, "p"'] & E(K) \arrow[r] \arrow[d, equal] & S^{(p^2)}(E/K) \arrow[r] \arrow[d, "\alpha"] & Ш(E/K)[p^2] \arrow[r] \arrow[d, "p"'] & 0 \\ E(K) \arrow[r, "p"] & E(K) \arrow[r] & S^{(p)}(E/K) \arrow[r] & Ш(E/K)[p] \arrow[r] & 0. \end{tikzcd}$$

We therefore have inclusions

$$E(K)/pE(K) \subset \mathrm{Im}(\alpha) \subset S^{(p)}(E/K). \tag{1}$$

Cassels [7] constructed an alternating bilinear pairing

$$S^{(p)}(E/K) \times S^{(p)}(E/K) \to \mathbb{Q}/\mathbb{Z} \tag{2}$$

whose kernel is the image of α. If we compute this pairing, and find it is non-trivial, then by (1) we get a better upper bound for the rank of $E(K)$ than was obtained by computing $S^{(p)}(E/K)$. In such cases, we also learn that the p-torsion of $Ш(E/K)$ is non-trivial.

Date: 6th June 2013.

Cassels [8] showed how to compute the pairing (2) in the case $p = 2$. We now generalise to the case $p = 3$. Therefore, as a starting point for our work, we rely on the algorithms for computing $S^{(3)}(E/K)$, as described in [34], and for representing its elements as plane cubics, as described in [11]. Cassels' method (in the case $p = 2$) involves both a local part (computing a certain local pairing), and a global part (solving conics over the field of definition of a 2-torsion point of E). Both parts require significant modification when $p > 2$.

In the case $p = 2$, the local pairing turns out to be the Hilbert norm residue symbol. However, since the local pairing is symmetric and the Hilbert norm residue symbol is skew-symmetric, this cannot be true for $p > 2$. A further difficulty is that on passing to a finite extension of local fields, the values of the local pairing are multiplied by the degree of the field extension. So if $[K_v(E[p]) : K_v]$ is divisible by p, then we cannot reduce to the case, treated in [30], where E has all p-torsion points defined over K_v. In Section 2, we nonetheless show how to write the local pairing (for p odd) in terms of Hilbert norm residue symbols, and make this completely explicit in the case $p = 3$.

In Section 3, we generalise the global part of Cassels' method to the case $p = 3$. In fact, we solve a more general problem about $3 \times 3 \times 3$ cubes (as studied in [3], [14], [22], [29]), using the work of Haile [20] and Kuo [26] on the generalisation of Clifford algebras to cubic forms. Our solution to this more general problem works by reducing it to that of trivialising a 3×3 matrix algebra over a field L. In our application to computing the Cassels–Tate pairing, L is the field of definition of a 3-torsion point of E.

The problem of trivialising an $n \times n$ matrix algebra (that is, given structure constants for an L-algebra known to be isomorphic to $\mathrm{Mat}_n(L)$, find such an isomorphism explicitly) is equivalent in the case $n = 2$ to solving a conic. For $n > 2$, this problem has been studied in [19, Section 5], [11, Paper III, Section 6], [24], with the result that practical algorithms are available if both n and the discriminant of the number field L are sufficiently small. However, since for us L is the field of definition of a 3-torsion point (which typically has degree 8), we have so far only been able to compute a few small examples.

In Section 4, we illustrate our work by computing the Cassels–Tate pairing on the 3-Selmer group of a specific elliptic curve $E/\mathbb{Q}$. To make the example interesting E was chosen from Cremona's tables [10] so that it does not admit any rational 3-isogenies and $Ш(E/\mathbb{Q})[3] \neq 0$. To make the computations practical we also chose E so that the degree 8 number field L has reasonably small discriminant. Strictly speaking, we only compute the pairing up to a global choice of sign, but this does not matter for applications.

Computing the pairing (2) gives the same information (in terms of improving our upper bound for the rank) as a p^2-descent. In [8], Cassels claims that his method (for $p = 2$) is more efficient than performing a 4-descent, as described in [27]. Subject to finding a better algorithm for trivialising matrix algebras over number fields, our method (for $p = 3$) should also be more efficient than performing a 9-descent, as described in [13]. One advantage of computing the pairing, compared to performing a p^2-descent directly, is that fewer class group calculations are required. Another advantage is that we only need to compute the pairing on a basis for $S^{(p)}(E/K)$, whereas p^2-descent must be run on every element of $S^{(p)}(E/K)$.

The pairing (2) is, in fact, induced by a pairing

$$\langle\ ,\ \rangle : Ш(E/K) \times Ш(E/K) \to \mathbb{Q}/\mathbb{Z}$$

and this is the form in which the Cassels–Tate pairing is usually written. Following the terminology in [31], the original definition in [7, Section 3] is called the "homogeneous space definition" (see also [28, I, Remark 6.11], [16, Section 2.2]), whereas the variant used in [7, Section 6] is called the "Weil pairing definition" (see also [28, I, Proposition 6.9], [16, Section 2.2]). Both the method in [8] and our generalisation use the Weil pairing definition.

In Section 1, we use the description of $H^1(K, E[p])$ in [34] to make the pairing explicit for $p > 2$. The formula we give is for $\langle x, y\rangle$ where $x, y \in Ш(E/K)$ and $py = 0$. Since we do not require $px = 0$, our work might be described (following [36]) as doing a p^n-descent for all n. We take p an odd prime, as the case $p = 2$ is already described in [8], [18], [36].

The Weil pairing definition was used in [6], where Cassels computed the pairing on the 3-isogeny Selmer groups of certain elliptic curves with j-invariant 0. This is currently being generalised to other isogenies of prime degree by the first author's student M. van Beek. The homogeneous space definition has also been used for explicit computation, most notably in the Magma [5] implementation of the pairing on $S^{(2)}(E/\mathbb{Q})$ due to S. Donnelly. It might be interesting to investigate how this approach generalises to the case $p = 3$, but we have not done so.

We write $H^i(K, -)$ for the Galois cohomology group $H^i(\mathrm{Gal}(\overline{K}/K), -)$, and $E[p]$ for the kernel of multiplication-by-p on $E(\overline{K})$. The completion of a number field K at a place v is denoted K_v. We write M_K for the set of all places of K. Since we take p an odd prime, we can ignore the infinite places.

A Magma file containing some of the formulae in Sections 3 and 4 may be found accompanying the arXiv version of this article.

Acknowledgements. We thank Manjul Bhargava, Wei Ho and Hendrik Lenstra for useful mathematical conversations and for pointing out some of the references. All computer calculations in Sections 3 and 4 were performed using Magma [5]. The second author is grateful for funding from DIAMANT.

1. The Cassels–Tate pairing

Let K be a field of characteristic 0, and $\overline{K}$ its algebraic closure. Let E/K be an elliptic curve and p an odd prime. The p-torsion subgroup $E[p]$ may be regarded as a 2-dimensional affine space over $\mathbb{F}_p$. We write $\mathbb{P}(E[p])$ for the set of lines passing through 0, and Λ for the set of lines not passing through 0. The étale algebra of X, a finite set with Galois action, is the K-algebra $R = \mathrm{Map}_K(X, \overline{K})$ of all Galois equivariant maps from X to $\overline{K}$. It is a product of field extensions of K, one for each Galois orbit of elements in X. We also write $\overline{R} = R \otimes_K \overline{K} = \mathrm{Map}(X, \overline{K})$ for the $\overline{K}$-algebra of all maps from X to $\overline{K}$, and let $\mathrm{Gal}(\overline{K}/K)$ act on these maps in the natural way, that is, by conjugation.

Let L^+, L, L' and M be the étale algebras of $\mathbb{P}(E[p])$, $E[p] \setminus \{0\}$, Λ and

$$\{(T, \lambda) \in (E[p] \setminus \{0\}) \times \Lambda : T \in \lambda\}.$$

These are K-algebras of dimensions $p+1$, p^2-1, p^2-1 and $p(p^2-1)$. There are natural inclusions $L^+ \subset L \subset M$ and $L' \subset M$. We fix $\nu \in \mathbb{Z}$ a primitive root mod p and let σ_ν be the generator of $\mathrm{Aut}(L/L^+)$ induced by multiplication-by-ν on $E[p]$. The inclusion $L \subset M$ followed by the norm map $N_{M/L'}$ is given by

$$(T \mapsto \alpha_T) \mapsto (\lambda \mapsto \textstyle\prod_{T \in \lambda} \alpha_T).$$

Let $w : E[p] \to \mu_p(\overline{L})$ be the map induced by the Weil pairing. This induces a group homomorphism

$$w_1 : H^1(K, E[p]) \to L^\times/(L^\times)^p. \tag{3}$$

Explicitly, if $\xi \in H^1(K, E[p])$ is represented by a cocycle $(\sigma \mapsto \xi_\sigma)$ then by Hilbert's theorem 90, there exists $\gamma \in \overline{L}^\times$ such that $w(\xi_\sigma) = \sigma(\gamma)/\gamma$ for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$. Then $\alpha = \gamma^p$ belongs to $L^\times$ and we define $w_1(\xi) = \alpha \mod (L^\times)^p$.

Lemma 1.1. *The map w_1 is injective and has image*

$$\left\{ \alpha \in L^\times/(L^\times)^p \;\middle|\; \begin{array}{rl} \sigma_\nu(\alpha) \equiv \alpha^\nu & \mod (L^\times)^p \\ N_{M/L'}(\alpha) \equiv 1 & \mod (L'^\times)^p \end{array} \right\}.$$

Proof. Injectivity is proved in [15, Section 3] and [34, Corollary 5.1]. The image is described in [34, Corollary 5.9 and Proposition 5.10]. □

We now suppose K is a number field. Let C/K be a principal homogeneous space under E. Then C is a smooth curve of genus one with Jacobian E. We further suppose that C is everywhere locally soluble, that is, $C(K_v) \neq \emptyset$ for all places v of K. We write "sum" for the natural isomorphism $\mathrm{Pic}^0(C) \cong E$. We make frequent use of the fact that a divisor on C is principal if and only if it has degree 0 and sum 0.

For each $0 \neq T \in E[p]$, there is a degree 0 divisor $\mathfrak{a}_T$ on C with $\mathrm{sum}(\mathfrak{a}_T) = T$. Since C is everywhere locally soluble we can choose the divisors $\mathfrak{a}_T$ so that the map $T \mapsto \mathfrak{a}_T$ is Galois equivariant. The proof of this, as given in [7, Lemma 7.1] or [36, Lemma 1], uses the local-to-global principle for the Brauer group of $K(T)$. Since $\mathrm{sum}(p\mathfrak{a}_T) = pT = 0$, there are rational functions $f_T \in \overline{K}(C)$ with $\mathrm{div}(f_T) =$

$p\mathfrak{a}_T$. By Hilbert's theorem 90, we may scale the f_T so that $f = (T \mapsto f_T)$ is Galois equivariant. Then f is an element of $L(C) = L \otimes_K K(C) = \mathrm{Map}_K(E[p] \setminus \{0\}, \overline{K}(C))$.

The following lemma specifies a scaling of f that is unique up to multiplication by elements in the image of w_1. We abbreviate $N_{M(C)/L'(C)}$ as $N_{M/L'}$.

Lemma 1.2. *Let $f \in L(C)$ as above. After multiplying f by a suitable element of $L^\times$, there exist $r \in L(C)$ and $s \in L'(C)$ such that*

$$\sigma_\nu(f)/f^\nu = r^p \qquad \textit{and} \qquad N_{M/L'}(f) = s^p. \tag{4}$$

Proof. We choose $r \in L(C)$ and $s \in L'(C)$ satisfying

$$\mathrm{div}(r_T) = \mathfrak{a}_{\nu T} - \nu\mathfrak{a}_T \qquad \text{and} \qquad \mathrm{div}(s_\lambda) = \textstyle\sum_{T\in\lambda} \mathfrak{a}_T.$$

Then (4) holds up to scalars. The construction of s uses the fact that the points on a line λ sum to zero, which in turn depends on the fact p is odd.

To remove the scalars, we use the result of Tate [7, Lemmas 5.1 and 6.1] that, since C is everywhere locally soluble, its class in $H^1(K,E)$ is divisible by p. If C and C_1 correspond to classes x and x_1 in $H^1(K,E)$ with $px_1 = x$ then there is a commutative diagram

$$\begin{tikzcd} C_1 \arrow[r, "\pi"] \arrow[d] & C \arrow[d] \\ E \arrow[r, "{[p]}"] & E \end{tikzcd}$$

where π is a morphism defined over K, and the vertical maps are isomorphisms defined over $\overline{K}$. We say that $\pi : C_1 \to C$ is a p-covering. For $\mathfrak{b}$ a divisor on E we have $\mathrm{sum}([p]^*\mathfrak{b}) = p\,\mathrm{sum}(\mathfrak{b})$. So there exists $g \in L(C_1)$ with $\mathrm{div}(g_T) = \pi^*\mathfrak{a}_T$. We now scale f so that $\pi^* f = g^p$, and scale r and s so that

$$\pi^* r = \sigma_\nu(g)/g^\nu \qquad \text{and} \qquad \pi^* s = N_{M/L'}(g).$$

It is then easy to check that (4) holds exactly. □

Let v be a place of K. By the Weil pairing, cup product and the local invariant map there is a pairing

$$(\ ,\ )_v : H^1(K_v, E[p]) \times H^1(K_v, E[p]) \to \mathbb{Q}/\mathbb{Z}. \tag{5}$$

It is known (see [28, I, Theorem 3.2],[37]) that $(\ ,\ )_v$ is symmetric and non-degenerate, and that the image of $E(K_v)/pE(K_v)$ is a maximal isotropic subspace. The last of these facts is referred to as *Tate local duality.* The local analogue of (3) is a map $w_{1,v}$ that fits in a commutative diagram

$$\begin{tikzcd} H^1(K, E[p]) \arrow[r, "w_1"] \arrow[d, "\mathrm{res}_v"'] & L^\times/(L^\times)^p \arrow[d] \\ H^1(K_v, E[p]) \arrow[r, "w_{1,v}"] & L_v^\times/(L_v^\times)^p \end{tikzcd}$$

where $L_v = L \otimes_K K_v$. We write $[\ ,\ ]_v$ for the pairing induced by $(\ ,\ )_v$ on the image of $w_{1,v}$. Since the local invariants of an element in $\mathrm{Br}(K)$ sum to zero, we have the "product formula" [1]

$$\sum_{v \in M_K} [\alpha, \beta]_v = 0 \tag{6}$$

for all $\alpha, \beta \in \mathrm{Im}(w_1)$.

Theorem 1.3. *Let $x, y \in Ш(E/K)$ with $py = 0$. Let C/K be a principal homogeneous space under E representing x, and let $\eta \in S^{(p)}(E/K)$ be an element that maps to y. Let $f \in L(C)$ be scaled as in Lemma 1.2, and for each place v of K choose a point $P_v \in C(K_v)$, avoiding the zeros and poles of the rational functions f_T. Then the Cassels–Tate pairing is given by*

$$\langle x, y \rangle = \sum_{v \in M_K} [f(P_v), w_1(\eta)]_v. \tag{7}$$

Proof. We start by checking that (7) is well-defined as a function of x and η. Lemmas 1.1 and 1.2 show that $f(P_v)$ is in the image of $w_{1,v}$, and so is a valid argument for $[\ ,\ ]_v$. It is shown in [33, Theorem 2.3] that evaluating f on degree 0 divisors gives an explicit realisation of the connecting map $\delta_v : E(K_v)/pE(K_v) \to H^1(K_v, E[p])$. So by Tate local duality each of the summands in (7) is independent of the choice of $P_v \in C(K_v)$. The pairing (7) is also independent of the choice of scaling of f as in Lemma 1.2, by the product formula (6).

Next, we check that (7) agrees with one of the standard definitions of the Cassels–Tate pairing. By the proof of Lemma 1.2, there is a p-covering $\pi : C_1 \to C$ defined over K, and we may scale f so that $\pi^* f = g^p$ for some $g \in L(C_1)$. Since C is everywhere locally soluble, for each place v of K there is a p-covering $\pi_v : C_{1,v} \to C$ defined over K_v with $C_{1,v}(K_v) \neq \emptyset$. Now $\pi_v : C_{1,v} \to C$ is the twist of $\pi : C_1 \to C$ by some $\xi_v \in H^1(K_v, E[p])$. The "Weil pairing definition" of the Cassels–Tate pairing (see [7, Section 6], [16, Section 2.2] or [28, I, Proposition 6.9]) says that

$$\langle x, y \rangle = \sum_{v \in M_K} (\xi_v, \mathrm{res}_v \eta)_v. \tag{8}$$

[1] This is analogous to the product formula for the Hilbert norm residue symbol.

Let $P_v \in \pi_v(C_{1,v}(K_v))$. Since $C_{1,v}(K_v)$ is infinite we may assume that P_v is not a zero or pole of f. By Lemma 1.4 applied over K_v we have

$$w_{1,v}(\xi_v) \equiv f(P_v) \mod (L_v^\times)^p.$$

It follows that the pairings (7) and (8) are the same. □

Lemma 1.4. *Let C/K and $f \in L(C)^\times$ be as before. Let $\pi_1 : C_1 \to C$ be a p-covering, and $\pi_2 : C_2 \to C$ its twist by $\xi \in H^1(K, E[p])$. Suppose that for $i = 1, 2$ we have $\pi_i^* f = \alpha_i g_i^p$ for some $\alpha_i \in L^\times$ and $g_i \in L(C_i)$. Then $w_1(\xi) \equiv \alpha_2/\alpha_1$* mod $(L^\times)^p$.

Proof. The proof is closely related to that of [33, Theorem 2.3]. There is an isomorphism ψ defined over $\overline{K}$ making the following diagram commute.

$$\begin{tikzcd} C_2 \arrow[r, "\pi_2"] \arrow[d, "\psi"'] & C \arrow[d, equal] \\ C_1 \arrow[r, "\pi_1"] & C \end{tikzcd}$$

Then $\xi \in H^1(K, E[p])$ is represented by a cocycle $(\sigma \mapsto \xi_\sigma)$ where $\sigma(\psi)\psi^{-1}$ is translation by $\xi_\sigma \in E[p]$. We have $\psi^* g_1 = \gamma g_2$ for some $\gamma \in \overline{L}^\times$. By definition of the Weil pairing

$$w(\xi_\sigma) g_1 = (\sigma(\psi)\psi^{-1})^* g_1 = (\sigma(\gamma)/\gamma) g_1.$$

It follows that $w(\xi_\sigma) = \sigma(\gamma)/\gamma$ and so $w_1(\xi) \equiv \gamma^p \equiv \alpha_2/\alpha_1 \mod (L^\times)^p$. □

The formula (7) is in fact a finite sum. This may be seen by Tate local duality, and the following lemma. We write $\mathcal{O}_v \subset L_v$ for the product of valuation rings of the constituent fields, and l_v for the product of residue fields.

Lemma 1.5. *Let C/K and $f \in L(C)^\times$ be as in Theorem 1.3.*

(i) *If $v \nmid p\infty$ is a prime of good reduction for E then*

$$\operatorname{Im}(w_{1,v} \circ \delta_v) = \operatorname{Im}(w_{1,v}) \cap \mathcal{O}_v^\times/(\mathcal{O}_v^\times)^p.$$

(ii) *If $v \nmid p\infty$ is a prime of good reduction for C, and f reduces mod v to $\widetilde{f} \in l_v(\widetilde{C})^\times$ then*

$$f(P_v) \in \operatorname{Im}(w_{1,v}) \cap \mathcal{O}_v^\times/(\mathcal{O}_v^\times)^p$$

for all $P_v \in C(K_v)$ avoiding the zeros and poles of the f_T.

Proof. (i) It is well known that $\operatorname{Im}(\delta_v)$ is the unramified subgroup of $H^1(K_v, E[p])$. See for example [34, Proposition 3.2], where this is proved under slightly weaker assumptions on v. We then use that $\mathcal{O}_v^\times/(\mathcal{O}_v^\times)^p$ is the kernel of the natural map

$$(L \otimes_K K_v)^\times/\{p\text{th powers}\} \to (L \otimes_K K_v^{\mathrm{nr}})^\times/\{p\text{th powers}\}.$$

(ii) By (i) and the proof of Theorem 1.3 it suffices to prove this for just one choice of P_v. If the residue field k_v of K_v is sufficiently large then there exists $\widetilde{P}_v \in \widetilde{C}(k_v)$ avoiding the zeros and poles of the $\widetilde{f}_T$. We then use Hensel's lemma to lift $\widetilde{P}_v$ to $P_v \in C(K_v)$, and see that $f(P_v)$ is a unit. If k_v is too small then we rectify this by making an unramified extension. □

We would like to use Theorem 1.3 to compute the Cassels–Tate pairing. There are essentially two problems.

- Computing the local pairing $[\ ,\ ]_v$. This is the subject of Section 2.
- Computing the rational functions f_T. In Section 3 we describe a method for doing this in the case where $p = 3$ and C is a plane cubic.

In the case $p = 2$, the pairing $[\ ,\ ]_v$ can be written as a product of Hilbert norm residue symbols. This is used implicitly in Cassels' paper [8], and a detailed proof is given in [18]. Our generalisation to the case $p = 3$ is necessarily more complicated since $[\ ,\ ]_v$ is symmetric, whereas the Hilbert norm residue symbol is skew-symmetric.

Cassels' method for computing the f_T requires us to solve conics over the field of definition of a 2-torsion point on E. The conics arise by a geometric construction that seems very special to the case $p = 2$. Nonetheless, we have found a practical method for reducing the problem in the case $p = 3$ to that of "trivialising a matrix algebra" over the field of definition of a 3-torsion point on E.

2. Computing the local pairing

We keep the notation of Section 1, up to and including Lemma 1.1, but now take K a p-adic field. In this section, we compute the local pairing $[\ ,\ ]_K$ on the image of w_1. Since $[\ ,\ ]_K$ is symmetric, and p is odd, it is equivalent to compute the quadratic form $\varphi_K : \mathrm{Im}(w_1) \to \frac{1}{p}\mathbb{Z}/\mathbb{Z}$ satisfying

$$[\alpha, \beta]_K = \varphi_K(\alpha\beta) - \varphi_K(\alpha) - \varphi_K(\beta) \tag{9}$$

for all $\alpha, \beta \in \mathrm{Im}(w_1)$.

We fix $\zeta_p \in \overline{K}$ a primitive pth root of unity.

Let $T_1, \ldots, T_m \in E[p] \setminus \{0\}$ be representatives for the $\mathrm{Gal}(\overline{K}/K)$-orbits. Then $L = L_1 \times \ldots \times L_m$ where $L_j = K(T_j) \subset \overline{K}$. We write $\{\ ,\ \}_j$ for the Hilbert norm residue symbol on $L_j(\zeta_p)^\times/(L_j(\zeta_p)^\times)^p$. This takes values in μ_p.

Let $\iota : L' \otimes_K K(\zeta_p) \cong L \otimes_K K(\zeta_p)$ be the isomorphism induced by the bijection

$$\begin{aligned} E[p] \setminus \{0\} &\leftrightarrow \Lambda \\ T &\mapsto \{S \in E[p] : e_p(S, T) = \zeta_p\} \end{aligned} \tag{10}$$

This depends on the choice of ζ_p.

Let $\mathrm{Ind}_{\zeta_p} : \mu_p \cong \frac{1}{p}\mathbb{Z}/\mathbb{Z}$ be the isomorphism that maps $\zeta_p \mapsto \frac{1}{p}$.

Theorem 2.1. *Assume p is an odd prime. Let $\alpha \in L$ represent an element in the image of $w_1 : H^1(K, E[p]) \to L^\times/(L^\times)^p$. Then we may associate to α an element $\alpha' \in L'$ such that for each $1 \le j \le m$,*

$$[L_j(\zeta_p) : K]\varphi_K(\alpha) = \begin{cases} \mathrm{Ind}_{\zeta_p}\{\alpha(T_j), \iota(\alpha')(T_j)\}_j & \text{if } \iota(\alpha')(T_j) \neq 0, \\ 0 & \text{otherwise.} \end{cases}$$

If $p = 3$ then we may take

$$\alpha' = \mathrm{Tr}_{M/L'}(\alpha) - 3N_{M/L'}(\alpha)^{1/3}$$

where the cube root is chosen as specified in Proposition 2.16(i).

Remark 2.2. Theorem 2.1 can be used to compute $\varphi_K(\alpha)$ in all cases, since the degree $[L_j(\zeta_p) : K]$ is coprime to p for at least one j.

The proof of Theorem 2.1 uses several constructions from [11], the most important of which is described in Proposition 2.7 below.

Following [11], let $R = \mathrm{Map}_K(E[p], \overline{K})$ be the étale algebra of $E[p]$, and let $\overline{R} = \mathrm{Map}(E[p], \overline{K}) = R \otimes_K \overline{K}$. Writing $E[p] = \{0\} \cup (E[p] \setminus \{0\})$ there are decompositions $R = K \times L$ and $\overline{R} = \overline{K} \times \overline{L}$. The Weil pairing induces a map $w : E[p] \to \mu_p(\overline{R})$ given by $S \mapsto (T \mapsto e_p(S, T))$. There is then an exact sequence

$$0 \longrightarrow E[p] \xrightarrow{w} \overline{R}^\times \xrightarrow{\partial} \partial\overline{R}^\times \longrightarrow 0$$

where the map

$$\partial : \overline{R}^\times \to (\overline{R} \otimes_{\overline{K}} \overline{R})^\times = \mathrm{Map}(E[p] \times E[p], \overline{K}^\times)$$

is defined by $\partial\beta(S, T) = \beta(S)\beta(T)/\beta(S + T)$ for all $S, T \in E[p]$. Taking Galois cohomology gives an injective group homomorphism

$$w_2 : H^1(K, E[p]) \to (R \otimes_K R)^\times/\partial R^\times.$$

Let $\gamma \in \overline{L}^\times$ be as described in the definition of w_1 (see Section 1). We extend γ to an element of $\overline{R}^\times$ by setting $\gamma(0) = 1$. Then $\rho = \partial\gamma \in (R \otimes_K R)^\times$ and $w_2(\xi) = \rho \mod \partial R^\times$. It is convenient to summarise this situation as follows.

Definition 2.3. Let $\xi \in H^1(K, E[p])$. We call $\alpha \in L^\times$, $\rho \in (R \otimes_K R)^\times$ *compatible* representatives for $w_1(\xi)$ and $w_2(\xi)$ if there exist a cocycle $(\sigma \mapsto \xi_\sigma) \in Z^1(K, E[p])$ representing ξ and $\gamma \in \overline{R}^\times$ such that all of the following conditions are satisfied.

(i) For all $\sigma \in G_K$ and all $T \in E[p]$, we have $e_p(\xi_\sigma, T) = (\sigma\gamma/\gamma)(T)$;
(ii) $\gamma(0) = 1$ and for all $T \in E[p] \setminus \{0\}$, $\gamma(T)^p = \alpha(T)$;
(iii) $\rho = \partial\gamma$.

Definition 2.4. Let ρ represent an element in the image of w_2. Following [11], we define a new multiplication $*_\rho$ on the $\overline{K}$-vector space $\overline{R}$ as follows. For all $f, g \in \overline{R}$ and for all $T \in E[p]$,

$$(f *_\rho g)(T) = \sum_{T_1+T_2=T} e_p^{1/2}(T_1, T_2)\rho(T_1, T_2) f(T_1) g(T_2)$$

where $e_p^{1/2}(T_1, T_2) \in \mu_p$ is the square root of the Weil pairing. For each $T \in E[p]$, let $\delta_T \in \overline{R}$ be the indicator function

$$\delta_T(S) = \begin{cases} 1 & \text{if } S = T, \\ 0 & \text{if } S \neq T. \end{cases}$$

The indicator function δ_0 is the identity for the multiplication $*_\rho$. For all $S, T \in E[p]$, we have

$$\delta_S *_\rho \delta_T = e_p^{1/2}(S, T)\rho(S, T)\delta_{S+T}$$

and therefore

$$\delta_S *_\rho \delta_T = e_p(S, T)\delta_T *_\rho \delta_S \tag{11}$$

since ρ is symmetric and e_p is skew-symmetric.

Lemma 2.5. *Let $\xi \in H^1(K, E[p])$ and let $\alpha \in L^\times$, $\rho \in (R \otimes_K R)^\times$ be compatible representatives for $w_1(\xi)$ and $w_2(\xi)$ respectively. Then for all $T \in E[p] \setminus \{0\}$, we have*

$$\delta_T^p = \underbrace{\delta_T *_\rho \delta_T *_\rho \cdots *_\rho \delta_T}_{p \text{ times}} = \alpha(T)\delta_0.$$

Therefore, δ_T is invertible with respect to the multiplication $*_\rho$.

Proof. Let $\gamma \in \overline{R}^\times$ be as in Definition 2.3. Then

$$\begin{aligned} \underbrace{\delta_T *_\rho \delta_T *_\rho \cdots *_\rho \delta_T}_{p \text{ times}} &= \prod_{i=1}^{p-1} \rho(T, iT)\delta_0 = \prod_{i=1}^{p-1} \frac{\gamma(T)\gamma(iT)}{\gamma((i+1)T)}\delta_0 \\ &= \frac{\gamma(T)^p}{\gamma(pT)}\delta_0 = \frac{\alpha(T)}{\gamma(0)}\delta_0 = \alpha(T)\delta_0. \end{aligned}$$

Since $\alpha \in L^\times$, we have $\alpha(T) \in \overline{K}^\times$ and therefore δ_T is invertible. □

Definition 2.6. Denote by A_ρ the algebra which is the K-vector space $R = \mathrm{Map}_K(E[p], \overline{K})$ equipped with the new multiplication $*_\rho$.

Proposition 2.7. *Let $\xi \in H^1(K, E[p])$ and choose $\rho \in (R \otimes_K R)^\times$ such that $w_2(\xi) = \rho \mod \partial R^\times$. Then A_ρ is a central simple algebra of dimension p^2 over K and $\varphi_K(w_1(\xi)) = \mathrm{inv}_K(A_\rho)$.*

Proof. Let $\mathrm{Ob}_K : H^1(K, E[p]) \to \mathrm{Br}(K)$ be the period-index obstruction map, as defined in [11], [30]. In [38], it is shown that the pairing

$$H^1(K, E[p]) \times H^1(K, E[p]) \to \mathrm{Br}(K)$$

defined by cup-product and the Weil pairing, is also given by

$$(\xi, \eta) \mapsto \mathrm{Ob}_K(\xi + \eta) - \mathrm{Ob}_K(\xi) - \mathrm{Ob}_K(\eta).$$

Comparing with (9), we have $\varphi_K(w_1(\xi)) = \mathrm{inv}_K(\mathrm{Ob}_K(\xi))$.

In [11, Section 4.3], it is shown that $\mathrm{Ob}_K(\xi)$ is represented by a certain central simple algebra of dimension p^2 over K. Then Lemmas 4.5, 3.10 and 3.11 of [11] show that this algebra is A_ρ. □

We will make use of the following lemma in our study of the central simple algebra A_ρ.

Lemma 2.8. *Suppose that $A, B \in \mathrm{GL}_n(K)$ satisfy $A^n = B^n = I_n$ and $AB = \zeta_n BA$ for some primitive nth root of unity $\zeta_n \in K$.*

(i) *If $C \in \mathrm{Mat}_n(K)$ satisfies $CB = \zeta_n BC$, then C^n is a scalar matrix.*
(ii) *The matrices $A^r B^s$ for $0 \leq r, s \leq n-1$ form a basis for $\mathrm{Mat}_n(K)$ as a K-vector space.*

Proof. (i) Since $B^n = I_n$, all eigenvalues of B are nth roots of unity. If v is an eigenvector with eigenvalue λ, then $A^{-m}v$ is an eigenvector with eigenvalue $\zeta_n^m \lambda$. So B has n distinct eigenvalues, namely the nth roots of unity. Changing basis, we may assume that $B = (b_{ij})$ is a diagonal matrix with $b_{ii} = \zeta_n^i$. If $C \in \mathrm{Mat}_n(K)$ satisfies $CB = \zeta_n BC$, then C is of the form (c_{ij}) where $c_{ij} = 0$ unless $j \equiv i + 1 \pmod{n}$. Therefore, $C^n = c_{12}c_{23} \dots c_{(n-1)n}c_{n1}I_n$.

(ii) Both A and B act by conjugation on $\mathrm{Mat}_n(K)$. The matrix $A^r B^s$ is an eigenvector with eigenvalue ζ^s for conjugation by A, and also an eigenvector with eigenvalue ζ^{-r} for conjugation by B. Eigenvectors with distinct eigenvalues are linearly independent. Thus, the matrices $A^r B^s$ for $0 \leq r, s \leq n-1$ are a K-basis for $\mathrm{Mat}_n(K)$. □

Proposition 2.9. *Let $\rho \in (R \otimes_K R)^\times$ represent an element in the image of w_2. For each $\lambda \in \Lambda$, let $\delta_\lambda = \sum_{S \in \lambda} \delta_S$ be the indicator function of λ. Then*

$$\delta_\lambda^p = \underbrace{\delta_\lambda *_\rho \dots *_\rho \delta_\lambda}_{p \text{ times}} \in \overline{K}\delta_0.$$

Proof. We have $\delta_\lambda \in A_\rho \otimes \overline{K}$, which is the $\overline{K}$-vector space $\mathrm{Map}(E[p], \overline{K})$ equipped with the multiplication $*_\rho$. Proposition 2.7 tells us that A_ρ is a central simple algebra of dimension p^2 over K, so $A_\rho \otimes \overline{K} \cong \mathrm{Mat}_p(\overline{K})$. Under this isomorphism, the element δ_0 is identified with the identity matrix I_p. By (10), there exists $T \in E[p] \setminus \{0\}$ such that $\lambda = \{S \in E[p] : e_p(S,T) = \zeta_p\}$. Let $S \in \lambda$. Then equation (11) gives

$$\delta_S *_\rho \delta_T = e_p(S,T)\delta_T *_\rho \delta_S = \zeta_p \delta_T *_\rho \delta_S,$$

and therefore $\delta_\lambda *_\rho \delta_T = \zeta_p \delta_T *_\rho \delta_\lambda$. By Lemma 2.5, δ_S and δ_T are invertible. Now apply the first part of Lemma 2.8, with A and B scalar multiples of δ_S and δ_T, and $C = \delta_\lambda$ to see that $\delta_\lambda^p \in \overline{K}\delta_0$. $\square$

By Proposition 2.9, there exists $\alpha' \in L'$ defined by

$$\delta_\lambda^p = \delta_\lambda *_\rho \cdots *_\rho \delta_\lambda = \alpha'(\lambda)\delta_0.$$

We prove Theorem 2.1 for this choice of α'. The key step is the calculation of the local invariant of the central simple algebra A_ρ. This is achieved by writing A_ρ as a cyclic algebra (after a field extension). To this end, we recall the definition of a cyclic algebra and its relation to the Hilbert norm residue symbol, as defined in [35].

Definition 2.10. Let ℓ/k be a cyclic field extension of degree n. Let σ be a generator of $\mathrm{Gal}(\ell/k)$ and let $b \in k^\times$. Let $\chi : G_k \twoheadrightarrow \mathrm{Gal}(\ell/k) \to \frac{1}{n}\mathbb{Z}/\mathbb{Z}$ be the continuous character of the absolute Galois group of k which factors through $\mathrm{Gal}(\ell/k)$ and sends σ to $\frac{1}{n}$ (mod $\mathbb{Z}$). Then the *cyclic algebra* (χ, b) is defined as

$$(\chi, b) = \left\{ \sum_{i=0}^{n-1} a_i v^i \mid a_i \in \ell \right\}$$

with multiplication $v^n = b$ and $vav^{-1} = \sigma(a)$ for all $a \in \ell$. The algebra (χ, b) is a central simple algebra over k of dimension n^2.

The following definition of the Hilbert norm residue symbol is given in [35, Ch. XIV, §2].

Definition 2.11. Suppose that K contains a primitive nth root of unity ζ_n. Let $a, b \in K^\times$ and let $\alpha \in \overline{K}$ satisfy $\alpha^n = a$. Define a continuous character $\chi_a : G_K \to \frac{1}{n}\mathbb{Z}/\mathbb{Z}$ by $\chi_a : (\alpha \mapsto \zeta_n^i \alpha) \mapsto i/n \pmod{\mathbb{Z}}$. Then the *Hilbert norm residue symbol* $\{a, b\}_K$ is defined as $\{a, b\}_K = \zeta_n^{n \,\mathrm{inv}_K(\chi_a, b)}$.

Thus, if we can express the central simple algebra A_ρ as a cyclic algebra then, by Proposition 2.7, we will have reduced the problem of computing φ_K to a Hilbert symbol computation. There are well-known explicit formulae for the Hilbert norm residue symbol for extensions of prime degree. See, for example, [35].

Lemma 2.12. *Let F/K be a finite extension of fields. Let $\alpha \in L^\times$ represent an element in the image of w_1. Then $\varphi_F(\alpha) = [F : K]\varphi_K(\alpha)$.*

Proof. Write $L_F = L \otimes_K F = \mathrm{Map}_F(E[p]\backslash\{0\}, \overline{K})$. The natural inclusion $L \hookrightarrow L_F$ gives rise to a natural map $L^\times/(L^\times)^p \to L_F^\times/(L_F^\times)^p$ which makes the following diagram commute.

$$\begin{tikzcd}
L^\times/(L^\times)^p \arrow[d] & H^1(K, E[p]) \arrow[l, "w_1"'] \arrow[r, "\mathrm{Ob}_K"] \arrow[d, "\mathrm{res}"'] & \mathrm{Br}(K) \arrow[r, "\mathrm{inv}_K"] \arrow[d, "\mathrm{res}"'] & \mathbb{Q}/\mathbb{Z} \arrow[d, "\times[F:K]"] \\
L_F^\times/(L_F^\times)^p & H^1(F, E[p]) \arrow[l, "w_1"'] \arrow[r, "\mathrm{Ob}_F"] & \mathrm{Br}(F) \arrow[r, "\mathrm{inv}_F"] & \mathbb{Q}/\mathbb{Z}
\end{tikzcd} \tag{12}$$

So if $\xi \in H^1(K, E[p])$, and $\alpha \in L^\times$ represents $w_1(\xi)$, then the same α also represents $w_1(\mathrm{res}\,\xi)$. Thus,

$$\varphi_F(\alpha) = \mathrm{inv}_F(\mathrm{Ob}_F(\mathrm{res}\,\xi)) = [F:K]\,\mathrm{inv}_K(\mathrm{Ob}_K(\xi)) = [F:K]\varphi_K(\alpha).$$

□

Lemma 2.12 shows that, in proving the first part of Theorem 2.1, we are free to replace K by $L_j(\zeta_p)$. So it suffices to prove the following special case.

Theorem 2.13. *Suppose that $T \in E[p] \setminus \{0\}$ is defined over K and that $\zeta_p \in K$. Let $\xi \in H^1(K, E[p])$ and let $\alpha \in L^\times$, $\rho \in (R \otimes_K R)^\times$ be compatible representatives for $w_1(\xi)$ and $w_2(\xi)$ respectively. Write $\{\ ,\ \}_K$ for the Hilbert norm residue symbol on $K^\times/(K^\times)^p$ taking values in μ_p. Define $\alpha' \in L'$ by $\delta_\lambda^p = \underbrace{\delta_\lambda *_\rho \cdots *_\rho \delta_\lambda}_{p\ times} = \alpha'(\lambda)\delta_0$ for all $\lambda \in \Lambda$. Then*

$$\varphi_K(\alpha) = \begin{cases} \mathrm{Ind}_{\zeta_p}\{\alpha(T), \iota(\alpha')(T)\}_K & \text{if } \iota(\alpha')(T) \neq 0, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Proposition 2.7 states that A_ρ is a central simple algebra of dimension p^2 over K, and that $\varphi_K(\alpha) = \mathrm{inv}_K(A_\rho)$. The Artin-Wedderburn Theorem tells us that either A_ρ is a division ring or $A_\rho \cong \mathrm{Mat}_p(K)$ has local invariant zero. The multiplication on A_ρ is understood to be that given by $*_\rho$ and henceforth we omit $*_\rho$ from the notation. Let $\ell = \{S \in E[p] : e_p(S,T) = \zeta_p\} \in \Lambda$ and recall that $\delta_\ell = \sum_{S\in\ell} \delta_S$ is the indicator function of ℓ. By definition of ι, we have $\iota(\alpha')(T) = \alpha'(\ell)$. The element $\alpha' \in L'$ is defined by $\delta_\lambda^p = \alpha'(\lambda)\delta_0$ for all $\lambda \in \Lambda$. So δ_ℓ is invertible if and only if $\iota(\alpha')(T) = \alpha'(\ell) \neq 0$. If δ_ℓ is not invertible, then A_ρ is not a division ring and therefore $\varphi_K(\alpha) = \mathrm{inv}_K(A_\rho) = 0$. From now on, we will assume that δ_ℓ is invertible. Applying (11) to each $S \in \ell$, we see that $\delta_\ell\delta_T = \zeta_p\delta_T\delta_\ell$. Lemma 2.5 shows that $\delta_T^p = \alpha(T)\delta_0$ and consequently δ_T is invertible. The second part of Lemma 2.8 implies that the elements $\delta_\ell^r\delta_T^s$ for $0 \le r, s \le p-1$ are linearly independent over $\overline{K}$ and therefore form a K-basis for A_ρ.

First, suppose that $\alpha(T) \notin (K^\times)^p$. In this case, δ_T generates a degree p cyclic extension isomorphic to $K(\sqrt[p]{\alpha(T)})/K$ inside A_ρ. Define $\chi = \chi_{\alpha(T)} : G_K \to \frac{1}{p}\mathbb{Z}/\mathbb{Z}$ as in Definition 2.11 and observe that $A_\rho \cong (\chi, \alpha'(\ell)) = (\chi, \iota(\alpha')(T))$ is a cyclic algebra with local invariant equal to $\mathrm{Ind}_{\zeta_p}\{\alpha(T), \iota(\alpha')(T)\}_K$.

Now suppose, on the contrary, that $\alpha(T) \in (K^\times)^p$. In this case, the Hilbert symbol $\{\alpha(T), \iota(\alpha')(T)\}_K$ is trivial and also $\delta_T - \sqrt[p]{\alpha(T)}\delta_0$ is a zero divisor in A_ρ, whereby $\varphi_K(\alpha) = \mathrm{inv}_K(A_\rho) = 0$. □

In order to complete the proof of Theorem 2.1, it remains to characterise α' in the special case $p = 3$.

Proposition 2.14. *Let $\xi \in H^1(K, E[3])$ and let $\alpha \in L^\times$, $\rho \in (R \otimes_K R)^\times$ be compatible representatives for $w_1(\xi)$ and $w_2(\xi)$ respectively. If $\lambda = \{S_1, S_2, S_3\} \in \Lambda$ then $\delta_\lambda^3 = \alpha'(\lambda)\delta_0$ where*

$$\alpha'(\lambda) = \alpha(S_1) + \alpha(S_2) + \alpha(S_3) - 3\rho(S_1, S_2)\rho(S_3, -S_3).$$

Proof. Since $\delta_\lambda^3 \in \overline{K}\delta_0$, only the terms $\delta_{S_i}\delta_{S_j}\delta_{S_k}$ where $S_i + S_j + S_k = 0$ make a contribution. Since the points on a line sum to zero, we have $S_1 + S_2 + S_3 = 0$ and therefore,

$$\begin{aligned}
\delta_\lambda^3 &= \Big(\sum_{S\in\lambda} \delta_S\Big)^3 = \sum_{S\in\lambda} \delta_S^3 + \sum_{\{i,j,k\}=\{1,2,3\}} \delta_{S_i}\delta_{S_j}\delta_{S_k} \\
&= \sum_{S\in\lambda} \delta_S^3 + \sum_{i<j} (\delta_{S_i}\delta_{S_j} + \delta_{S_j}\delta_{S_i})\delta_{-S_i-S_j} \\
&= \sum_{S\in\lambda} \delta_S^3 + \sum_{i<j} \left(e_3^{1/2}(S_i, S_j) + e_3^{1/2}(S_j, S_i)\right) \rho(S_i, S_j)\delta_{S_i+S_j}\delta_{-S_i-S_j}
\end{aligned}$$

Since λ does not pass through zero, $e_3^{1/2}(S_i, S_j)$ is a primitive cube root of unity and, consequently, $e_3^{1/2}(S_i, S_j) + e_3^{1/2}(S_j, S_i) = -1$. Lemma 2.5 shows that $\delta_S^3 = \alpha(S)\delta_0$ for all $S \in \lambda$. Therefore, $\delta_\lambda^3 = \alpha'(\lambda)\delta_0$ where

$$\alpha'(\lambda) = \sum_{S\in\lambda} \alpha(S) - \sum_{i<j} \rho(S_i, S_j)\rho(S_i + S_j, -S_i - S_j).$$

Let $\gamma \in \overline{R}^\times$ be as in Definition 2.3. For $i < j$, we expand

$$\begin{aligned}
\rho(S_i, S_j)\rho(S_i + S_j, -S_i - S_j) &= \gamma(S_i)\gamma(S_j)\gamma(S_i + S_j)^{-1}\gamma(S_i + S_j)\gamma(-S_i - S_j)\gamma(0)^{-1} \\
&= \gamma(S_i)\gamma(S_j)\gamma(S_k)
\end{aligned}$$

where $\{i, j, k\} = \{1, 2, 3\}$. Therefore,

$$\begin{aligned}
\alpha'(\lambda) &= \sum_{S\in\lambda} \alpha(S) - 3\prod_{S\in\lambda} \gamma(S) \\
&= \alpha(S_1) + \alpha(S_2) + \alpha(S_3) - 3\rho(S_1, S_2)\rho(S_3, -S_3).
\end{aligned}$$

□

Corollary 2.15. *In the case $p = 3$, Theorem 2.1 holds with $\alpha' = \mathrm{Tr}_{M/L'}(\alpha) - 3N_{M/L'}(\alpha)^{1/3}$ for some choice of cube root.*

Proof. With notation as in the previous proof we have

$$\sum_{S\in\lambda} \alpha(S) = \mathrm{Tr}_{M/L'}(\alpha)(\lambda) \quad \text{and} \quad \prod_{S\in\lambda} \gamma(S)^3 = \prod_{S\in\lambda} \alpha(S) = N_{M/L'}(\alpha)(\lambda).$$

□

If the only element $x \in L'$ satisfying $x^3 = 1$ is the element 1 itself, then Corollary 2.15 defines α' uniquely in the case $p = 3$. However, if L' contains a non-trivial cube root of unity, then we must do more to pin down the correct choice of cube root of $N_{M/L'}(\alpha)$.

Proposition 2.16. *Let $\xi \in H^1(K, E[3])$, and $\alpha \in L^\times$ a representative for $w_1(\xi)$.*

(i) *There exist $r \in L^+$ and $s \in L'$ such that $N_{L/L^+}(\alpha) = r^3$, $N_{M/L'}(\alpha) = s^3$, $\alpha N_{L^+/K}(r) = rN_{M/L}(s)$ and $N_{L/K}(\alpha) = N_{L'/K}(s)$.*

(ii) *If r and s are as in (i) then there exists $\rho \in (R \otimes_K R)^\times$, a representative for $w_2(\xi)$ compatible with α, such that for all $\lambda = \{S_1, S_2, S_3\} \in \Lambda$ we have $s(\lambda) = \rho(S_1, S_2)\rho(S_3, -S_3)$.*

Proof. (i) Let $\rho \in (R \otimes_K R)^\times$ be a representative for $w_2(\xi)$ compatible with α, and let $\gamma \in \overline{R}^\times$ be as in Definition 2.3.

We put $r(\pm T) = \gamma(T)\gamma(-T)$ and $s(\lambda) = \prod_{T\in\lambda} \gamma(T)$. It is easy to check that r and s are Galois equivariant, and so belong to L^+ and L'. We compute

$$\begin{aligned}
N_{L/L^+}(\alpha)(\pm T) &= \alpha(T)\alpha(-T) = \gamma(T)^3\gamma(-T)^3 = r(\pm T)^3,\\
N_{M/L'}(\alpha)(\lambda) &= \textstyle\prod_{T\in\lambda} \alpha(T) = \prod_{T\in\lambda} \gamma(T)^3 = s(\lambda)^3,\\
\alpha(T)N_{L^+/K}(r) &= \gamma(T)^3 \textstyle\prod_{0\neq P\in E[3]} \gamma(P) = r(\pm T) \prod_{T\in\lambda} s(\lambda) = r(\pm T)N_{M/L}(s)(T),\\
N_{L/K}(\alpha) &= \textstyle\prod_{0\neq P\in E[3]} \gamma(P)^3 = \prod_{\lambda\in\Lambda} s(\lambda) = N_{L'/K}(s).
\end{aligned}$$

(ii) If r and s are chosen as in the proof of (i), then

$$s(\lambda) = \rho(S_1, S_2)\rho(S_3, -S_3). \tag{13}$$

for all $\lambda = \{S_1, S_2, S_3\} \in \Lambda$. We must show that this still holds, for some ρ compatible with α, whenever r and s satisfy the conditions in (i).

Let $\widetilde{\Lambda} = \mathbb{P}(E[3]) \cup \Lambda$ be the set of all lines in $E[3]$. We write $\mathrm{Map}(E[3], \mu_3)/\mu_3$ for the quotient of $\mathrm{Map}(E[3], \mu_3)$ by the constant maps. We claim there is an exact sequence

$$\frac{\mathrm{Map}(E[3], \mu_3)}{\mu_3} \to \mathrm{Map}(\widetilde{\Lambda}, \mu_3) \to \frac{\mathrm{Map}(E[3], \mu_3)}{\mu_3} \times \mu_3 \tag{14}$$

where the first map is $\theta \mapsto (\lambda \mapsto \prod_{T\in\lambda} \theta(T))$ and second map is

$$\phi \mapsto (T \mapsto \textstyle\prod_{T\in\lambda\in\widetilde{\Lambda}} \phi(\lambda), \prod_{\lambda\in\Lambda} \phi(\lambda)).$$

The exactness is checked by linear algebra over $\mathbb{F}_3$.

If we change our choices of r and s in (i), then they change by an element $\phi \in \mathrm{Map}(\widetilde{\Lambda}, \mu_3)$. If both choices of r and s satisfy $\alpha N_{L^+/K}(r) = rN_{M/L}(s)$, then ϕ has the property that $\prod_{T\in\lambda\in\widetilde{\Lambda}} \phi(\lambda)$ is independent of $T \in E[3]$. If both choices of s satisfy $N_{L/K}(\alpha) = N_{L'/K}(s)$, then ϕ has the property that $\prod_{\lambda\in\Lambda} \phi(\lambda) = 1$. So, by the exact sequence (14), there exists $\theta \in \mathrm{Map}(E[3], \mu_3)$ with $\theta(0) = 1$ and $\phi(\lambda) = \prod_{T\in\lambda} \theta(T)$ for all $\lambda \in \widetilde{\Lambda}$. It is easy to write the map

$$\partial\theta : E[3] \times E[3] \to \mu_3\,; \quad (S, T) \mapsto \theta(S)\theta(T)/\theta(S + T)$$

in terms of ϕ. Hence, if ϕ is Galois equivariant then so is $\partial\theta$.

Since R and L are the étale algebras of $E[3]$ and $E[3] \setminus \{0\}$, we have $R = K \times L$, and there is a natural inclusion $L^\times \subset R^\times$. We may then view w_1, as defined in (3), as a map $w_1 : H^1(K, E[3]) \to R^\times/(R^\times)^3$. It fits in the exact sequence

$$0 \longrightarrow E(K)[3] \xrightarrow{w} \mu_3(R) \xrightarrow{\partial} (\partial\mu_3(\overline{R}))^{G_K} \longrightarrow H^1(K, E[3]) \xrightarrow{w_1} R^\times/(R^\times)^3$$

Lemma 1.1 states that w_1 is injective. This means that $(\partial\mu_3(\overline{R}))^{G_K} = \partial(\mu_3(R))$. Therefore, multiplying $\theta \in \mu_3(\overline{R})$ by $w(T)$ for some $T \in E[3]$, we may assume that $\theta \in \mu_3(R)$. In other words, θ itself and not just $\partial\theta$ is Galois equivariant. Then, replacing γ and ρ by $\gamma\theta$ and $\rho\partial\theta$, we see that the conditions of Definition 2.3 are still satisfied, but now (13) holds for the new s. □

Corollary 2.17. *In the case $p = 3$, let r and s be as described in Proposition 2.16. Then Theorem 2.1 holds with $\alpha' = \mathrm{Tr}_{M/L'}(\alpha) - 3s$.*

Proof. Let $\rho \in (R \otimes_K R)^\times$ be as described in part (ii) of Proposition 2.16. Then for all $\lambda = \{S_1, S_2, S_3\} \in \Lambda$, we have $s(\lambda) = \rho(S_1, S_2)\rho(S_3, -S_3)$. Using this ρ in Proposition 2.14 we get $\alpha'(\lambda) = \sum_{i=1}^{3} \alpha(S_i) - 3\rho(S_1, S_2)\rho(S_3, -S_3) = \mathrm{Tr}_{M/L'}(\alpha)(\lambda) - 3s(\lambda)$. □

Remark 2.18. In the case where $[K(E[3]) : K]$ is coprime to 3, Lemma 2.12 allows us to reduce to the case where all the 3-torsion is defined over K. If $S, T \in E[3]$ are a basis such that $e_3(S, T) = \zeta_3$, then we can choose γ in Definition 2.3 such that for $0 \le a, b \le 2$, $\gamma(aS+bT) = \gamma(S)^a\gamma(T)^b$. Consequently, we obtain $\iota(\alpha')(T) = \alpha(S)+ \alpha(S+T)+\alpha(S-T)-3\gamma(S)\gamma(S+T)\gamma(S-T) = \alpha(S)N_{K(\gamma(T))/K}(1+\gamma(T)+\gamma(T)^2)$. Thus, the relevant Hilbert norm residue symbol is $\{\alpha(T), \alpha(S)\}$ and, for $n = 3$, we recover the formula given in [30] for the period-index obstruction with full level n-structure.

3. Global computations

In this section, $C \subset \mathbb{P}^2$ will be a smooth plane cubic defined over a number field K. We suppose that C is everywhere locally soluble. We write "sum" for the isomorphism $\mathrm{Pic}^0(C) \cong E$, where E is the Jacobian of C. The *hyperplane section* of C (i.e. intersection of C with a line) is a degree 3 effective K-rational divisor H on C, defined up to linear equivalence. If H' is another degree 3 effective K-rational divisor on C, then the linear system $|H'|$ can be used to define a new embedding $C \subset \mathbb{P}^2$ with hyperplane section H'.

We are interested in the following problem.

Problem 3.1. Given a smooth plane cubic $C \subset \mathbb{P}^2$ with hyperplane section H, and a point $P \in E(K)$, find equations for an embedding $C \to \mathbb{P}^2$ whose image is a smooth plane cubic with hyperplane section H' satisfying $\mathrm{sum}(H' - H) = P$.

As described in the proof of [36, Lemma 1], the K-rational effective divisors H' in the required linear equivalence class correspond to the K-rational points on a certain Brauer-Severi surface V. Since C is everywhere locally soluble, so is V. By the Hasse principle for Brauer-Severi varieties we know that $V(K) \neq \emptyset$, and so H' exists. Writing down equations for V and then searching for a K-rational point is unlikely to be practical. We therefore take a different approach.

First, we explain how a solution to Problem 3.1 helps us compute the Cassels–Tate pairing. In Section 1, we take $0 \neq T \in E[3]$ and, after extending our field K so that $T \in E(K)$, aim to compute $f_T \in K(E)$ with $\mathrm{div}(f_T) = 3\mathfrak{a}_T$ and $\mathrm{sum}(\mathfrak{a}_T) = T$. Solving Problem 3.1 with $P = T$ gives us $\mathfrak{a}_T$ in the form $H' - H$, and from this we can compute f_T. To say a little about what f_T looks like, we write $K[x,y,z]_d$ for the space of homogeneous polynomials of degree d, and $\mathcal{L}(D)$ for the Riemann-Roch space of a divisor D. We also suppose, for definiteness, that $H = C \cap \{x = 0\}$. It is known (see for example [4, Theorem 7.3.1]) that for any $d \geq 1$ the map

$$K[x,y,z]_d \to \mathcal{L}(dH)\,; \quad f \mapsto f/x^d$$

is surjective. Taking $d = 3$ shows we can write f_T in the form f_1/x^3 where f_1 is a ternary cubic meeting C in divisor $3H'$. By changing our choice of hyperplane section H, we could replace the denominator by the cube of any linear form.

We assume $P \neq 0$ (otherwise Problem 3.1 is trivial). The curve C may be embedded in $\mathbb{P}^2$ using either the linear system $|H|$ or the linear system $|H'|$. The first of these gives the embedding we started with. Taking both embeddings together gives a map $C \to \mathbb{P}^2 \times \mathbb{P}^2$. The image is defined by three bi-homogeneous forms of degree $(1,1)$. The coefficients may conveniently be arranged as a $3 \times 3 \times 3$ cube. These cubes have many fascinating properties. We first learnt of these from work of Bhargava and O'Neil (unpublished) and Bhargava and Ho [3]. See also [14], [22], [29].

If we arrange the coefficients of a $3 \times 3 \times 3$ cube into three 3×3 matrices, say M_1, M_2, M_3, then

$$F(x, y, z) = \det(xM_1 + yM_2 + zM_3) \tag{15}$$

is a ternary cubic. Since we can slice the cube in three different directions, this gives us three different ternary cubics. As shown in [29, Theorem 1], two of these define the image of C under the embeddings corresponding to H and H'. Moreover an isomorphism between these two plane cubics is given by the the 2×2 minors of the matrix of linear forms in (15). We can then adopt the point of view in Problem 3.1, namely that we have one curve with two different embeddings in $\mathbb{P}^2$.

We are therefore interested in the following problem.

Problem 3.2. Given a non-singular ternary cubic $F \in K[x, y, z]$, find matrices $M_1, M_2, M_3 \in \mathrm{Mat}_3(K)$ satisfying

$$F(\alpha, \beta, \gamma) = \det(\alpha M_1 + \beta M_2 + \gamma M_3).$$

This problem is also considered in [14], where an application to coding theory is suggested.

We label the coefficients of F by putting

$$\begin{aligned} F(x, y, z) = ax^3 + by^3 + cz^3 + a_2x^2y + a_3x^2z \\ + b_1xy^2 + b_3y^2z + c_1xz^2 + c_2yz^2 + mxyz. \end{aligned}$$

By a change of co-ordinates, we may assume $c = F(0, 0, 1) \neq 0$. Let A_F be the free associative K-algebra on two indeterminates x and y subject to the relations deriving from the formal identity in α and β,

$$F(\alpha, \beta, \alpha x + \beta y) = 0.$$

Explicitly, $A_F = K\{x, y\}/I$ where I is the ideal generated by the elements

$$\begin{aligned} &cx^3 + c_1x^2 + a_3x + a, \\ &c(x^2y + xyx + yx^2) + c_1(xy + yx) + c_2x^2 + mx + a_3y + a_2, \\ &c(xy^2 + yxy + y^2x) + c_2(xy + yx) + c_1y^2 + my + b_3x + b_1, \\ &cy^3 + c_2y^2 + b_3y + b. \end{aligned}$$

In solving Problem 3.2, we are free to multiply F through by a scalar. If we scale so that $F(0, 0, 1) = -1$, then without loss of generality $M_3 = -I_3$.

Lemma 3.3. *Let $F \in K[x, y, z]$ be an irreducible ternary cubic with $F(0, 0, 1) \neq 0$, and let $M_1, M_2 \in \mathrm{Mat}_3(K)$. The following are equivalent.*

(i) *$F(\alpha, \beta, \gamma) = \lambda \det(\alpha M_1 + \beta M_2 - \gamma I_3)$ for some $\lambda \in K^\times$.*

(ii) *There is a K-algebra homomorphism $A_F \to \mathrm{Mat}_3(K)$ with $x \mapsto M_1$ and $y \mapsto M_2$.*

Proof. If (i) holds then $\gamma \mapsto F(\alpha,\beta,\gamma)$ is a scalar multiple of the characteristic polynomial of $\alpha M_1 + \beta M_2$. So, by the Cayley-Hamilton theorem,

$$F(\alpha,\beta,\alpha M_1+\beta M_2) = 0. \tag{16}$$

Therefore, M_1 and M_2 satisfy the relations used to define A_F. This proves (ii). If the minimal polynomial of $\alpha M_1+\beta M_2$ has degree 3 for infinitely many $(\alpha:\beta) \in \mathbb{P}^1$ then the converse is clear. Otherwise, after replacing M_1 and M_2 by suitable linear combinations, neither has minimal polynomial of degree 3. So M_1 and M_2 each have an eigenspace of dimension at least 2. Since these eigenspaces have non-trivial intersection, it follows by (16) that $\{F=0\} \subset \mathbb{P}^2$ contains a line. This contradicts that F is irreducible. $\square$

We have now reduced Problem 3.2 to finding a K-algebra homomorphism $A_F \to \mathrm{Mat}_3(K)$. Although the connection with Problem 3.2 is new, the algebra A_F was previously studied by Kuo [26]. She showed that A_F is an Azumaya algebra of rank 9 over its centre $Z(A_F)$, and that $Z(A_F)$ is isomorphic to the co-ordinate ring of the affine curve $E \setminus \{0\}$, where E is the Jacobian of $C = \{F=0\} \subset \mathbb{P}^2$. In particular we can specialise A_F at any non-zero point of E to obtain a central simple algebra of dimension 9 over the field of definition of that point. In fact, Kuo only considered the special case $c=1$ and $a_3=b_3=c_1=c_2=0$, but the general case follows by making suitable changes of co-ordinates.

We put $r = y(cx^2+c_1x+a_3)$, $s = -(cy^2+c_2y+b_3)$ and $t = cx$. Then, using the support for finitely presented algebras in Magma [5], we were able to check that the centre $Z(A_F)$ is generated by[2]

$$\xi = c^2(xy)^2 - (cy^2+c_2y+b_3)(cx^2+c_1x+a_3) + (cm - c_1c_2)xy + a_3b_3$$

and

$$\begin{aligned}\eta = rst + str + trs + a_2(st+ts) + b_3(tr+rt) + c_1(rs+sr)\\ + (b_3c_1 - b_1c)r + (c_1a_2 - c_2a)s + (a_2b_3 - a_3b)t - 6abc + a_2b_3c_1.\end{aligned}$$

Moreover, the elements ξ and η satisfy

$$\eta^2 + A_1\xi\eta + A_3\eta = \xi^3 + A_2\xi^2 + A_4\xi + A_6, \tag{17}$$

[2]In fact, the elements δ_1 and δ_2 in the proof of [26, Lemma 2.1] are equal, and $\xi + m^2/3$ specialises to $\delta_1 = \delta_2 = \delta/2$

where

$$\begin{aligned}
A_1 &= m, \\
A_2 &= -(a_2c_2 + a_3b_3 + b_1c_1), \\
A_3 &= 9abc - (ab_3c_2 + ba_3c_1 + ca_2b_1) - (a_2b_3c_1 + a_3b_1c_2), \\
A_4 &= -3(abc_1c_2 + acb_1b_3 + bca_2a_3) \\
&\quad + a(b_1c_2^2 + b_3^2c_1) + b(a_2c_1^2 + a_3^2c_2) + c(a_2^2b_3 + a_3b_1^2) \\
&\quad + a_2c_2a_3b_3 + b_1c_1a_2c_2 + a_3b_3b_1c_1, \\
A_6 &= -27a^2b^2c^2 + 9abc(ab_3c_2 + ca_2b_1 + ba_3c_1) + \ldots + abcm^3.
\end{aligned}$$

The polynomials $A_i \in \mathbb{Z}[a, b, c, \ldots, m]$ are the coefficients of the Weierstrass equation for the Jacobian specified in [2]. These were obtained by modifying the classical formulae in [1].

Let $0 \neq P = (x_P, y_P) \in E(K)$. Then the specialisation $A_{F,P}$ of A_F at P is the quotient of A_F by the extra relations $x_P = \xi$ and $y_P = \eta$. By the work of Kuo cited above, $A_{F,P}$ is a central simple algebra over K of dimension 9. It therefore represents an element in $\mathrm{Br}(K)[3]$. Kuo also shows that if $C = \{F = 0\} \subset \mathbb{P}^2$ has a K-rational point, then the Azumaya algebra A_F splits. By our assumption that C is everywhere locally soluble, and the local-to-global principle for the Brauer group, it follows that $A_{F,P} \cong \mathrm{Mat}_3(K)$. If we can find such an isomorphism then this immediately gives us a K-algebra homomorphism $A_F \to \mathrm{Mat}_3(K)$ and hence, by Lemma 3.3, a solution to Problem 3.2.

The following lemma shows that the point P in the statement of Problem 3.1, and the point P in the above solution to Problem 3.2 are the same.

Lemma 3.4. *Suppose we solve Problem 3.2 by finding an isomorphism* $A_{F,P} \cong \mathrm{Mat}_3(K)$ *for some* $0 \neq P \in E(K)$*. Then the* $3 \times 3 \times 3$ *cube we obtain defines a genus one curve* $C \subset \mathbb{P}^2 \times \mathbb{P}^2$ *whose projections onto each factor are plane cubics with hyperplane sections* H *and* H' *satisfying* $\mathrm{sum}(H - H') = P$.

Proof. For the proof, we may work over an algebraically closed field, and change coordinates so that $C = E$ is an elliptic curve in Weierstrass form. Moving the point P to $(x, y) = (0, 0)$, we may assume that E has Weierstrass equation

$$y^2 + a_3y = x^3 + a_2x^2 + a_4x. \tag{18}$$

The image of $(x, y) \mapsto (1 : y : x)$ is defined by the ternary cubic

$$F(x, y, z) = xy^2 + a_3x^2y - z^3 - a_2xz^2 - a_4x^2z.$$

Using (17) to compute the Jacobian, we recover the Weierstrass equation (18). Then $A_{F,P} \cong \mathrm{Mat}_3(K)$ via

$$x \mapsto \begin{pmatrix} 0 & 0 & 1 \\ -a_3 & 0 & 0 \\ -a_4 & 0 & -a_2 \end{pmatrix}, \qquad y \mapsto \begin{pmatrix} 0 & 0 & 0 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}.$$

In particular, we check that $\xi \mapsto 0$ and $\eta \mapsto 0$. The images of x, y and -1 in $\mathrm{Mat}_3(K)$ form a $3 \times 3 \times 3$ cube. Let F_i be the bi-homogeneous form whose coefficients are given by the ith rows of these matrices, as follows,

$$\begin{aligned} F_1(x_1, y_1, z_1; x_2, y_2, z_2) &= -z_1 x_2 + x_1 z_2, \\ F_2(x_1, y_1, z_1; x_2, y_2, z_2) &= -a_3 x_1 x_2 - y_1 x_2 - z_1 y_2, \\ F_3(x_1, y_1, z_1; x_2, y_2, z_2) &= -a_4 x_1 x_2 - y_1 y_2 - a_2 x_1 z_2 - z_1 z_2. \end{aligned}$$

Then F_1, F_2, F_3 define the image of $E \to \mathbb{P}^2 \times \mathbb{P}^2$ via

$$(x, y) \mapsto ((1 : y : x), (1 : -(y + a_3)/x : x)).$$

Projecting onto each factor gives two embeddings $E \subset \mathbb{P}^2$ with hyperplane sections $H = 3.0$ and $H' = 2.0 + P$. In particular, $\mathrm{sum}(H' - H) = P$. □

We have now reduced Problems 3.1 and 3.2 to the following problem.

Problem 3.5. Let K be a number field. Given structure constants for a K-algebra A known to be isomorphic to $\mathrm{Mat}_3(K)$, find such an isomorphism explicitly.

We briefly discuss two algorithms for solving this problem.

Norm equations. By a theorem of Wedderburn (see [25, Theorem 2.9.17]), every central simple algebra of dimension 9 is a cyclic algebra. By following the proof (see [19] or [21] for details), Problem 3.5 reduces to that of solving a norm equation for a cyclic cubic extension L/K. Algorithms for solving norm equations do exist (see [9, Section 7.5]), but as they involve computing the class group and units for L, they are rarely practical in the applications of interest to us.

Minimisation and reduction. This approach was first suggested by M. Stoll, but with an ad hoc approach to the reduction. The "minimisation" stage is to compute a maximal order $\mathcal{O}$ in A, using the algorithm in [23], [32]. For the "reduction" stage we compute trivialisations $A \otimes_K K_v \cong \mathrm{Mat}_3(K_v)$ for each infinite place v, and use this to embed $\mathcal{O}$ as a lattice in a Euclidean space of dimension $\dim_{\mathbb{Q}}(A) = 9[K : \mathbb{Q}]$. We then search for a zero-divisor in A by looking at short vectors in this lattice. Once a zero-divisor is found, it is easy to find an isomorphism $A \cong \mathrm{Mat}_3(K)$, as described for example in [19, Section 5]. In [11, Paper III, Section 6] it is shown that if $K = \mathbb{Q}$ then the shortest vector in the lattice is a zero-divisor. In practice, a zero-divisor can then be found by the LLL algorithm. In [24], a complexity-theoretic result is proved describing the behaviour of the algorithm over a general number field. The algorithm is only practical if the discriminant of K is sufficiently small.

4. Example

In this section, we illustrate our work by computing the Cassels–Tate pairing on the 3-Selmer group of the elliptic curve 17127b1 in [10]. This elliptic curve $E/\mathbb{Q}$ has Weierstrass equation

$$y^2 + xy + y = x^3 - x^2 - 19163564x - 34134737802. \tag{19}$$

The Galois representation $\rho_{E,3} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ is surjective. Therefore, the étale algebras L, L' and M, defined in Section 1, are fields. We find that $L = \mathbb{Q}(u)$ and $L' = \mathbb{Q}(v)$, where u and v are roots of $X^8 - 5X^6 + 6X^4 - 3 = 0$ and $X^8 - 6X^4 + 19X^2 - 3 = 0$. Moreover, $M = L(\theta)$ where $\theta^3 = 2u^6 - 6u^4 - 3u^2 + 1$. The isomorphism $\iota : L'(\zeta_3) \cong L(\zeta_3)$ and embedding $L' \subset M$ are given by

$$\begin{aligned} &v \mapsto \tfrac{1}{3}(2\zeta_3 + 1)(u^7 - 4u^5 + u^3 + 3u), \\ &v \mapsto \tfrac{1}{3}(2u^5 - 7u^3)\theta^{-1} + \tfrac{1}{3}(u^7 - 4u^5 + u^3 + 3u). \end{aligned} \tag{20}$$

The bad primes of E are 3, 11 and 173. Let $\mathcal{S}$ the set of primes of L dividing these primes, and

$$L(\mathcal{S}, 3) = \{x \in L^\times/(L^\times)^3 : \mathrm{ord}_\mathfrak{p}(x) \equiv 0 \pmod 3 \text{ for all } \mathfrak{p} \notin \mathcal{S}\}.$$

By Lemma 1.5(i), we have

$$S^{(3)}(E/\mathbb{Q}) \subset L(\mathcal{S}, 3) \cap \mathrm{Im}(w_1).$$

We find that $L(\mathcal{S}, 3) \cap \mathrm{Im}(w_1) \cong (\mathbb{Z}/3\mathbb{Z})^3$ is generated by

$$\begin{aligned} \alpha &= \tfrac{1}{2}(u^7 + u^6 - 4u^5 - 3u^4 + 2u^3 + 1), \\ \beta &= \tfrac{1}{2}(u^7 - 6u^5 + 10u^3 + 3u^2 - 3u - 5), \\ \gamma &= \tfrac{1}{2}(632u^7 - 142u^6 - 2275u^5 + 642u^4 + 629u^3 - 720u^2 + 1059u - 625), \end{aligned}$$

and that $S^{(3)}(E/\mathbb{Q}) \cong (\mathbb{Z}/3\mathbb{Z})^2$ is the subgroup generated by α and γ. Moreover, for each of the primes $p = 3, 11, 173$, we find that $H^1(\mathbb{Q}_p, E[3]) \cong (\mathbb{Z}/3\mathbb{Z})^2$ is generated by the images of β and γ.

Let $\alpha' = \mathrm{Tr}_{M/L'}(\alpha) - 3N_{M/L'}(\alpha)^{1/3}$. Since $\mu_3 \not\subset L'$, there is no ambiguity in the choice of cube root. Explicitly,

$$\alpha' = \tfrac{1}{6}(2v^7 - 2v^6 + v^5 - v^4 - 10v^3 + 19v^2 + 48v - 21).$$

Factoring into prime ideals in $\mathcal{O}_L$, we find

$$\begin{aligned} 11\mathcal{O}_L &= \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3^3, && N\mathfrak{p}_1 = N\mathfrak{p}_2 = 11, \quad N\mathfrak{p}_3 = 11^2, \\ 173\mathcal{O}_L &= \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3\mathfrak{q}_4\mathfrak{q}_5, && N\mathfrak{q}_1 = N\mathfrak{q}_2 = 173, \quad N\mathfrak{q}_3 = N\mathfrak{q}_4 = N\mathfrak{q}_5 = 173^2. \end{aligned}$$

For $p = 11$, 173 we work with the embeddings $L \subset \mathbb{Q}_p$ corresponding to $\mathfrak{p}_1$ and $\mathfrak{q}_1$. In other words, for both $p = 11$ and $p = 173$, we choose a torsion point $0 \neq T \in E[3]$ defined over $\mathbb{Q}_p$. By (20), this also gives an embedding $L' \subset \mathbb{Q}_p(\zeta_3)$. Let $\varphi_p = \varphi_{\mathbb{Q}_p}$ be as defined in Section 2. Then, up to a global choice of sign[3],

$$\varphi_p(\alpha) = \mathrm{Ind}_{\zeta_3}(\alpha, \alpha')_p,$$

where Ind_{ζ_3} is the isomorphism $\mu_3 \cong \frac{1}{3}\mathbb{Z}/\mathbb{Z}$ sending $\zeta_3 \mapsto \frac{1}{3}$, and $(\ ,\ )_p$ is the 3-Hilbert norm residue symbol on $\mathbb{Q}_p(\zeta_3)$. By Lemma 1.5(i), Tate local duality and the product formula (6), we have $\varphi_3(\alpha) + \varphi_{11}(\alpha) + \varphi_{173}(\alpha) = 0$. We use this relation to compute $\varphi_3(\alpha)$ from $\varphi_{11}(\alpha)$ and $\varphi_{173}(\alpha)$. Repeating for $\alpha, \beta, \gamma, \dots$ we find that φ_p takes values:

p	α	β	γ	$\alpha\beta$	$\beta\gamma$	$\alpha\gamma$	$\alpha\beta\gamma$
3	0	1	0	0	−1	0	1
11	0	−1	0	0	0	0	1
173	0	0	0	0	1	0	1

We have identified $\frac{1}{3}\mathbb{Z}/\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z}$ for readability. The final column is not needed in what follows, but was computed as a check on our calculations. Recalling that φ_p is a quadratic form, we can now read off using (9) that the associated symmetric bilinear form $[\ ,\ ]_p$ takes values:

$[\ ,\ ]_3$	α	β	γ
α	0	−1	0
β	−1	−1	1
γ	0	1	0

$[\ ,\ ]_{11}$	α	β	γ
α	0	1	0
β	1	1	1
γ	0	1	0

$[\ ,\ ]_{173}$	α	β	γ
α	0	0	0
β	0	0	1
γ	0	1	0

These calculations are in agreement with the fact that, since $\alpha, \gamma \in S^{(3)}(E/\mathbb{Q})$, we have $[\alpha, \alpha]_p = [\alpha, \gamma]_p = [\gamma, \gamma]_p = 0$ for all primes p. Since the local pairing (5) is non-degenerate, we could also have predicted in advance that $[\beta, \gamma]_p \neq 0$ for $p = 3, 11, 173$.

The Selmer group elements α, γ, $\alpha\gamma$, α/γ correspond to plane cubics C_m for $m = 1, \dots, 4$. We used the algorithms in [11], implemented in Magma, to compute the following equations for C_m.

$$12x^3 + 7x^2y - x^2z + 20xy^2 - 99xyz + 24xz^2 + 43y^3 + 13y^2z - 17yz^2 + 80z^3 = 0$$
$$9x^3 - 26x^2y - 7x^2z + 47xy^2 - 25xyz + 105xz^2 + 16y^3 + 47y^2z + 27yz^2 + 54z^3 = 0$$
$$x^3 + 2x^2y - 15x^2z + 40xy^2 - 11xyz + 111xz^2 + 8y^3 + 91y^2z + 131yz^2 + 344z^3 = 0$$
$$4x^3 - 2x^2y - x^2z - 9xy^2 - 41xyz + 97xz^2 + 29y^3 - 23y^2z + 257yz^2 + 282z^3 = 0$$

[3]This depends on the relationship between the embeddings (20) and the Weil pairing.

These equations have been minimised and reduced (see [12]) and so, in particular, the C_m have the same primes of bad reduction as E.

In each case $m = 1, \ldots, 4$, we used the method in Section 3 to compute a ternary cubic f_m with coefficients in L meeting C_m in 3 non-collinear points each with multiplicity 3. In our example, L is a number field, but in general a similar calculation is necessary over each constituent field of L. The rational function f_m/x^3 has divisor $3H' - 3H$, where H is the hyperplane section and H' is another effective divisor of degree 3. Then $[H' - H] \in \mathrm{Pic}^0(C_m) \cong E$ is a non-zero 3-torsion point defined over L. In our example, there are only two such points, say $\pm T$. We can switch the sign by replacing f_m by its $\mathrm{Gal}(L/L^+)$-conjugate. Determining the right choice of sign takes some care; see Remark 4.1 below.

We scaled each f_m so that (i) the rational function f_m/x^3 is as described in Lemma 1.2, (ii) the coefficients of f_m are in $\mathcal{O}_L$, and (iii) f_m and the ternary cubic defining C_m are linearly independent mod $\mathfrak{p}$ for all primes $\mathfrak{p} \notin \mathcal{S}$. In general, it might be necessary to enlarge $\mathcal{S}$ to achieve the last of these conditions. By Lemma 1.5, the only primes to contribute to the pairing will be $p = 3, 11, 173$.

The interested reader can find the f_m in the accompanying Magma file. We have also included the formula for f_1 in Appendix A.

Evaluating each f_m at a $\mathbb{Q}_p$-point[4] on C_m, we obtained the following elements of $L_p^\times/(L_p^\times)^3$, where $L_p = L \otimes_{\mathbb{Q}} \mathbb{Q}_p$.

p	f_1	f_2	f_3	f_4
3	γ	$\beta\gamma$	$\beta\gamma^2$	$\beta^2\gamma^2$
11	γ^2	1	γ	γ
173	β	$\beta^2\gamma$	1	$\beta^2\gamma^2$

Using the entries in the column headed f_1, we compute

$$\begin{aligned} \langle \alpha, \alpha \rangle &= [\gamma, \alpha]_3 + [\gamma^2, \alpha]_{11} + [\beta, \alpha]_{173} = 0, \\ \langle \alpha, \gamma \rangle &= [\gamma, \gamma]_3 + [\gamma^2, \gamma]_{11} + [\beta, \gamma]_{173} = 1. \end{aligned} \tag{21}$$

Repeating for f_2, f_3, f_4, the Cassels–Tate pairing is given by

(22)

$\langle\ ,\ \rangle$	α	γ	$\alpha\gamma$	α/γ
α	0	1	1	-1
γ	-1	0	-1	-1
$\alpha\gamma$	-1	1	0	1
α/γ	1	1	-1	0

This is in agreement with the fact that the pairing is bilinear and alternating. Had we assumed these properties from the outset, it would only have been necessary

[4]We were careful to choose points that are not p-adically close to the zeros of f_m.

to compute one non-zero value of the pairing. So the only reason for computing more than one of the f_m was to help check our calculations.

In conclusion, the Cassels–Tate pairing on $S^{(3)}(E/\mathbb{Q}) \cong (\mathbb{Z}/3\mathbb{Z})^2$ is non-zero, and hence non-degenerate. It follows that $\operatorname{rank} E(\mathbb{Q}) = 0$ and the 3-primary part of $\text{Ш}(E/\mathbb{Q})$ is $(\mathbb{Z}/3\mathbb{Z})^2$. The first of these facts could more easily be checked by 2-descent. The second could have been checked using 9-descent (as described in [13]), but our method has the advantage of not requiring any class group and unit calculations beyond those needed for the 3-descent.

Remark 4.1. Replacing f_m by its $\operatorname{Gal}(L/L^+)$-conjugate has the effect of changing the sign of every entry in the mth row of (22). We now explain how we made these sign choices in a consistent way. We limit ourselves to a few brief details, since for the applications in the last paragraph we only need that the pairing is non-zero.

We fix a 3-torsion point $T \in E(L)$, written in terms of the Weierstrass equation (19). Each plane cubic C_m corresponds to a pair of inverse elements in $S^{(3)}(E/\mathbb{Q})$. The choice of sign could be fixed by specifying an isomorphism $\operatorname{Pic}^0(C_m) \cong E$ or a covering map $C_m \to E$. Instead, we scale the ternary cubic defining C_m so that it has the same invariants c_4 and c_6 as (19). This scaling is unique up to sign, and by [17, Theorem 2.5] the choice of sign corresponds to that in $S^{(3)}(E/\mathbb{Q})$. By specialising the sign $\pm$ to $+$ in [17, Theorem 7.2], and using the torsion point T chosen above, we may scale the equations for the C_m so that they correspond to $\alpha, \gamma, \alpha\gamma, \alpha/\gamma \in L^\times/(L^\times)^3$, rather than to the inverses of these elements. Then, when computing the ternary cubic f_m in Section 3, we work with the algebra $A_{F,P}$, where F is the equation for C_m we just fixed, and P is the image of T under the isomorphism between the elliptic curves (19) and (17) which when written in the form $x = u^2x' + r$, $y = u^3y' + u^2sx' + t$ has $u = +1$.

Remark 4.2. We have only computed the Cassels–Tate pairing up to a global choice of sign. To compute it exactly, we would have to fix a sign convention for the Weil pairing and check that the embeddings (20) are compatible with it. We would also have to expand on Remark 4.1.

Appendix A. Formulae

The ternary cubic f_1 in the example of Section 4 is

$$\begin{aligned} f_1 = {} & (10u^7 - 8u^6 - 56u^5 + 42u^4 + 60u^3 - 39u^2 + 36u - 29)x^3 \\ & + \tfrac{1}{2}(76u^7 - 30u^6 - 321u^5 + 136u^4 + 173u^3 - 70u^2 + 213u - 103)x^2y \\ & + \tfrac{1}{2}(-43u^7 - 24u^6 + 118u^5 + 8u^4 - 106u^3 + 67u^2 + 15u + 43)x^2z \\ & + \tfrac{1}{2}(135u^7 - 74u^6 - 499u^5 + 260u^4 + 145u^3 - 47u^2 + 210u - 118)xy^2 \\ & + \tfrac{1}{2}(129u^7 + 48u^6 - 446u^5 - 75u^4 + 73u^3 - 15u^2 + 237u - 36)xyz \\ & + \tfrac{1}{2}(83u^7 - 19u^6 - 200u^5 + 192u^4 - 27u^3 + 78u^2 + 54u - 82)xz^2 \\ & + \tfrac{1}{2}(15u^7 - 40u^6 - 32u^5 + 79u^4 - 87u^3 + 47u^2 - 27u + 32)y^3 \\ & + \tfrac{1}{2}(-61u^7 + 46u^6 + 295u^5 - 260u^4 - 299u^3 + 149u^2 - 300u + 240)y^2z \\ & + \tfrac{1}{2}(-140u^7 + 84u^6 + 537u^5 - 314u^4 - 193u^3 + 32u^2 - 405u + 167)yz^2 \\ & + \tfrac{1}{2}(-105u^7 - 86u^6 + 276u^5 + 158u^4 + 26u^3 - 11u^2 - 189u - 115)z^3. \end{aligned}$$

References

[1] S.Y. An, S.Y. Kim, D.C. Marshall, S.H. Marshall, W.G. McCallum and A.R. Perlis, Jacobians of genus one curves, *J. Number Theory* 90 (2001), no. 2, 304–315.

[2] M. Artin, F. Rodriguez-Villegas and J. Tate, On the Jacobians of plane cubics, *Adv. Math.* 198 (2005), no. 1, 366–382.

[3] M. Bhargava and W. Ho, *On the average sizes of Selmer groups in families of elliptic curves*, in preparation.

[4] C. Birkenhake and H. Lange, *Complex abelian varieties*, Second edition, Grundlehren der Mathematischen Wissenschaften, 302, Springer-Verlag, Berlin, 2004.

[5] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system I: The user language, *J. Symb. Comp.* 24, 235-265 (1997). See also `http://magma.maths.usyd.edu.au/magma/`

[6] J.W.S. Cassels, Arithmetic on curves of genus 1, I. On a conjecture of Selmer, *J. reine angew. Math.* 202 1959 52–99.

[7] J.W.S. Cassels, Arithmetic on curves of genus 1, IV. Proof of the Hauptvermutung, *J. reine angew. Math.* 211 (1962), 95–112.

[8] J.W.S. Cassels, Second descents for elliptic curves, *J. reine angew. Math.* 494 (1998), 101–127.

[9] H. Cohen, *Advanced topics in computational number theory*, Graduate Texts in Mathematics, 193, Springer-Verlag, Berlin, 2000.

[10] J.E. Cremona, *Algorithms for modular elliptic curves*, Cambridge University Press, Cambridge, 1997. See also `http://www.warwick.ac.uk/~masgaj/ftp/data/`

[11] J.E. Cremona, T.A. Fisher, C. O'Neil, D. Simon and M. Stoll, Explicit n-descent on elliptic curves, I Algebra, *J. reine angew. Math.* 615 (2008) 121-155; II Geometry, *J. reine angew. Math.* 632 (2009) 63-84; *III Algorithms*, preprint, `http://arxiv.org/abs/1107.3516`

[12] J.E. Cremona, T.A. Fisher and M. Stoll, Minimisation and reduction of 2-, 3- and 4-coverings of elliptic curves, *Algebra & Number Theory* 4 (2010), no. 6, 763-820.

[13] B. Creutz, Second p-descents on elliptic curves, to appear in *Math. Comp.*, `http://dx.doi.org/10.1090/S0025-5718-2013-02713-5`

[14] A. Deajim and D. Grant, Space-time codes and non-associative division algebras arising from elliptic curves, in *Computational arithmetic geometry*, K.E. Lauter and K.A. Ribet (eds.), Contemp. Math., 463, Amer. Math. Soc., Providence, RI, 2008.

[15] Z. Djabri, E.F. Schaefer and N.P. Smart, Computing the p-Selmer group of an elliptic curve, *Trans. Amer. Math. Soc.* 352, 5583–5597 (2000).

[16] T.A. Fisher, The Cassels–Tate pairing and the Platonic solids, *J. Number Theory* 98 (2003), no. 1, 105–155.

[17] T.A. Fisher, Testing equivalence of ternary cubics, in *Algorithmic number theory (ANTS VII)*, F. Hess, S. Pauli, M. Pohst (eds.), Lecture Notes in Comput. Sci. 4076, Springer, 2006, 333-345.

[18] T.A. Fisher, E.F. Schaefer and M. Stoll, The yoga of the Cassels–Tate pairing, *LMS J. Comput. Math.* 13 (2010), 451–460.

[19] W.A. de Graaf, M. Harrison, J. Pílniková and J. Schicho, A Lie algebra method for rational parametrization of Severi-Brauer surfaces, *J. Algebra* 303 (2006), no. 2, 514–529.

[20] D. Haile, On the Clifford algebra of a binary cubic form, *Amer. J. Math.* 106 (1984), no. 6, 1269–1280.

[21] D. Haile, A useful proposition for division algebras of small degree, *Proc. Amer. Math. Soc.* 106 (1989), no. 2, 317–319.

[22] W. Ho, *Orbit parametrizations of curves*, Ph.D. thesis, Princeton University, 2009.

[23] G. Ivanyos and L. Rónyai, Finding maximal orders in semisimple algebras over $\mathbb{Q}$, *Comput. Complexity* 3 (1993), no. 3, 245–261.

[24] G. Ivanyos, L. Rónyai and J. Schicho, Splitting full matrix algebras over algebraic number fields, *J. Algebra* 354 (2012), 211–223.

[25] N. Jacobson, *Finite-dimensional division algebras over fields*, Springer-Verlag, Berlin, 1996.

[26] J.-M. Kuo, On an algebra associated to a ternary cubic curve, *J. Algebra* 330 (2011), 86–102.

[27] J.R. Merriman, S. Siksek and N.P. Smart, Explicit 4-descents on an elliptic curve, *Acta Arith.* 77 (1996), no. 4, 385–404.

[28] J.S. Milne, *Arithmetic duality theorems*, Second edition, BookSurge, LLC, Charleston, SC, 2006.

[29] K.O. Ng, The classification of $(3,3,3)$-trilinear forms, *J. reine angew. Math.* 468 (1995), 49–75.

[30] C. O'Neil, The period-index obstruction for elliptic curves, *J. Number Theory* 95 (2002), no. 2, 329–339.

[31] B. Poonen and M. Stoll, The Cassels–Tate pairing on polarized abelian varieties, *Ann. of Math.* (2) 150 (1999), no. 3, 1109–1149.

[32] L. Rónyai, Computing the structure of finite algebras, *J. Symbolic Comput.* 9 (1990), no. 3, 355–373.

[33] E.F. Schaefer, Computing a Selmer group of a Jacobian using functions on the curve. *Math. Ann.* 310 (1998), no. 3, 447–471.

[34] E.F. Schaefer and M. Stoll, How to do a p-descent on an elliptic curve, *Trans. Amer. Math. Soc.* 356 (2004), no. 3, 1209–1231.

[35] J.-P. Serre, *Local Fields*, Graduate Texts in Mathematics, 67, Springer-Verlag, New York, 1979.

[36] H.P.F. Swinnerton-Dyer, 2^n-descent on elliptic curves for all n, to appear in *J. Lond. Math. Soc.*, `http://dx.doi.org/10.1112/jlms/jds063`

[37] J. Tate, Duality theorems in Galois cohomology over number fields, *Proc. Internat. Congr. Mathematicians* (Stockholm, 1962) pp. 288–295, Inst. Mittag-Leffler, Djursholm 1963.

[38] Ju. G. Zarhin, Noncommutative cohomology and Mumford groups, *Mat. Zametki* 15 (1974), 415–419; English translation: *Math. Notes* 15 (1974), 241–244.

University of Cambridge, DPMMS, Centre for Mathematical Sciences, Wilberforce Road, Cambridge CB3 0WB, UK

E-mail address: `T.A.Fisher@dpmms.cam.ac.uk`

University of Leiden, Mathematical Institute, PO Box 9512, 2300 RA Leiden, The Netherlands

E-mail address: `newtonrd@math.leidenuniv.nl`