COMPUTING THE CASSELS-TATE PAIRING ON 3-ISOGENY SELMER GROUPS VIA CUBIC NORM EQUATIONS

MONIQUE VAN BEEK AND TOM FISHER

Abstract. We explain a method for computing the Cassels-Tate pairing on the 3-isogeny Selmer groups of an elliptic curve. This improves the upper bound on the rank of the elliptic curve coming from a descent by 3-isogeny, to that coming from a full 3-descent. One ingredient of our work is a new algorithm for solving cubic norm equations, that avoids the need for any S-unit computations. As an application, we show that the elliptic curves with torsion subgroup of order 3 and rank at least 13, found by Eroshkin, have rank exactly 13.

Introduction

Let E be an elliptic curve over a number field K. By the Mordell-Weil theorem, the rational points $E(K)$ form a finitely generated abelian group. The number of points needed to generate the non-torsion part of $E(K)$ is called the rank. Determining the rank is a non-trivial problem, and indeed there is no known algorithm that will compute it in all cases.

We may however bound the rank by following the proof of the Mordell-Weil theorem. For each integer $n \geq 2$, the n-Selmer group $S^{(n)}(E/K)$ classifies the n-coverings of E that have points everywhere locally. This group is finite and effectively computable. Since $E(K)/nE(K)$ injects into $S^{(n)}(E/K)$, computing the n-Selmer group gives an upper bound for the rank. This process is known as (full) n-descent. In view of the short exact sequence

$$0 \longrightarrow E(K)/nE(K) \longrightarrow S^{(n)}(E/K) \longrightarrow Ш(E/K)[n] \longrightarrow 0 \tag{1}$$

the rank bound coming from n-descent may be improved whenever the Tate-Shafarevich group $Ш(E/K)$ contains non-trivial n-torsion.

Cassels [Cas62] defined an alternating pairing (now known as the Cassels-Tate pairing)

$$Ш(E/K) \times Ш(E/K) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

with the property that $Ш(E/K)[n]$ and $nШ(E/K)$ are exact annihilators. One consequence is that if $Ш(E/K)$ is finite (as conjectured by Tate and Shafarevich) then its order is a square. Another consequence is that we can sometimes use the

Date: 7th November 2017.

2010 *Mathematics Subject Classification.* 11G05, 11Y40.

Key words and phrases. elliptic curves, Cassels-Tate pairing, descent, norm equations.

pairing to detect non-trivial elements of $\text{Ш}(E/K)$. Specifically, computing the pairing on $S^{(n)}(E/K)$ improves the rank bound coming from n-descent, to that coming from n^2-descent. Thus, for example, Cassels used the pairing in [Cas98] to turn a 2-descent into a 4-descent, and to some extent this has been generalised in [SD13], [FN14], [Don15].

Descent calculations become very much more tractable in the case that our elliptic curve admits a rational p-isogeny for some prime p. This is the situation we consider in this paper. We write $\phi : E \to E'$ for the p-isogeny, and $\widehat{\phi} : E' \to E$ for its dual. Since $\widehat{\phi} \circ \phi$ is multiplication-by-p, there is an exact sequence

$$\begin{aligned} 0 \longrightarrow & E(K)[\phi] \longrightarrow E(K)[p] \xrightarrow{\phi} E'(K)[\widehat{\phi}] \\ & \longrightarrow E'(K)/\phi E(K) \xrightarrow{\widehat{\phi}} E(K)/pE(K) \longrightarrow E(K)/\widehat{\phi}E'(K) \longrightarrow 0, \end{aligned}$$

from which we deduce that

$$p^{\operatorname{rank} E(K)} = \frac{|E(K)/pE(K)|}{|E(K)[p]|} = \frac{|E'(K)/\phi E(K)| \cdot |E(K)/\widehat{\phi}E'(K)|}{|E(K)[\phi]| \cdot |E'(K)[\widehat{\phi}]|}.$$

Analogous to (1) there are exact sequences

$$0 \longrightarrow E'(K)/\phi E(K) \longrightarrow S^{(\phi)}(E/K) \longrightarrow \text{Ш}(E/K)[\phi_*] \longrightarrow 0,$$

and

$$0 \longrightarrow E(K)/\widehat{\phi}E'(K) \longrightarrow S^{(\widehat{\phi})}(E'/K) \longrightarrow \text{Ш}(E'/K)[\widehat{\phi}_*] \longrightarrow 0.$$

Computing the Selmer groups $S^{(\phi)}(E/K)$ and $S^{(\widehat{\phi})}(E'/K)$ gives an upper bound for the rank. This process is known as descent by p-isogeny, and is described for example in [Top93, DeL02, Fis01, Fis03, SS04, FG08, MS13].

There is a commutative diagram with exact rows

$$\begin{tikzcd} E'(K)[\widehat{\phi}] \arrow[r] \arrow[d, equal] & E'(K)/\phi E(K) \arrow[r] \arrow[d, hook] & E(K)/pE(K) \arrow[r] \arrow[d, hook] & E(K)/\widehat{\phi}E'(K) \arrow[d, hook] \\ E'(K)[\widehat{\phi}] \arrow[r] & S^{(\phi)}(E/K) \arrow[r] & S^{(p)}(E/K) \arrow[r] & S^{(\widehat{\phi})}(E'/K) \end{tikzcd}$$

where the final map in the second row need not be surjective. Instead its image is the kernel of the Cassels-Tate pairing

$$\langle \ , \ \rangle_{\text{CT}} : S^{(\widehat{\phi})}(E'/K) \times S^{(\widehat{\phi})}(E'/K) \to \mathbb{Q}/\mathbb{Z}. \tag{2}$$

This pairing is the lift of the one on $\text{Ш}(E'/K)[\widehat{\phi}_*]$. Computing the pairing (2) allows us to turn a descent by p-isogeny into a full p-descent. If the pairing is non-zero then this improves our upper bound for the rank.

The case $p = 2$ is treated in [Fis17], so from now on we take p an odd prime. In the first of his series of papers on elliptic curves, Cassels [Cas59] showed how to compute the pairing (2) when $p = 3$ and E' takes the form $x^3 + y^3 = k$. The case where $p = 3$ or 5 and $E[p] \cong \mu_p \times \mathbb{Z}/p\mathbb{Z}$ was treated in [Fis03].

We describe a method for computing the pairing (2) in the cases where $E[\phi]$ is isomorphic (as a Galois module) to either μ_p or $\mathbb{Z}/p\mathbb{Z}$. In both cases the global part of our method requires us to solve a norm equation $N_{L/K}(\xi) = a$ where L/K is a field extension of degree p. Moreover, when $p = 3$ and $E[\phi] \cong \mathbb{Z}/3\mathbb{Z}$, we have $L = K(\sqrt[3]{b})$ for some $b \in K$. In the case $K = \mathbb{Q}$ we give an algorithm for solving such norm equations, that avoids the need for any S-unit computations. This enables us to apply our methods to elliptic curves with large discriminant.

One particular computational challenge is to find elliptic curves over $\mathbb{Q}$ of large rank with a given torsion subgroup. The current records are listed on Dujella's website [Duj17]. Between 2007 and 2009, Y.G. Eroshkin found the following five elliptic curves with torsion subgroup $\mathbb{Z}/3\mathbb{Z}$ and rank at least 13.

$$\begin{aligned}
y^2 + 10154960719xy - 66798078951809458114391930400y &= x^3 && 17\\
y^2 + 8412073331xy + 7384158420201525518270114400y &= x^3 && 13\\
y^2 + 19223749711xy - 435665346791890005577936749600y &= x^3 && 13\\
y^2 + 8589423667xy - 306794103262326045319897944 00y &= x^3 && 17\\
y^2 + 35429815349xy - 169064164426703584254124708800y &= x^3 && 15
\end{aligned}$$

The number on the right is the upper bound for the rank obtained by descent by 3-isogeny. By computing the Cassels-Tate pairing we were able to verify that each of these curves has rank exactly 13. This is the largest known rank for an elliptic curve with torsion subgroup $\mathbb{Z}/3\mathbb{Z}$.

We have also used the methods of this paper to find new examples of elliptic curves with torsion subgroup $\mathbb{Z}/9\mathbb{Z}$ and ranks 3 and 4 (see [vB15, Duj17]). In contrast, when we searched for elliptic curves with torsion subgroup $\mathbb{Z}/12\mathbb{Z}$ and rank 4 we could not find any examples beyond the one already known. For both of these torsion subgroups the largest known rank is 4.

In Section 1 we recall the definition of the Cassels-Tate pairing that is relevant to our work. In Section 2 we give an explicit description of the long exact sequence

$$H^1(K, E[\phi]) \to H^1(K, E[p]) \to H^1(K, E'[\widehat{\phi}]) \to H^2(K, E[\phi]) \tag{3}$$

in terms of étale algebras, and explain how lifting an element of $H^1(K, E'[\widehat{\phi}])$ to $H^1(K, E[p])$ comes down to solving a norm equation. As indicated above, we concentrate on the cases where $E[\phi] \cong \mu_p$ or $E[\phi] \cong \mathbb{Z}/p\mathbb{Z}$. Since it is always possible to reduce to one of these two cases by making a field extension of degree coprime to p, this is perhaps not such a severe restriction.

In Section 3 we present our new algorithm for solving norm equations for pure cubic extensions $\mathbb{Q}(\sqrt[3]{b})/\mathbb{Q}$. It is based on the Legendre-type method for solving conics in [CR03]. When applied to suitably large examples, our algorithm performs much better than the standard approach using S-units, as described for example in [Coh00, Section 7.5], [Sim02].

In Section 4 we give three examples computing the pairing (2) in the case $K = \mathbb{Q}$ with $E[\phi] \cong \mu_3$ or $E[\phi] \cong \mathbb{Z}/3\mathbb{Z}$. The first two examples are small, and so do not require any special methods to solve the norm equations. In the third example, where we consider one of Eroshkin's curves with torsion subgroup $\mathbb{Z}/3\mathbb{Z}$, we are entirely reliant on the methods in Section 3.

It is interesting to remark that if we solve norm equations by the method in Section 3, then the simplest case is when $E[\phi] \cong \mathbb{Z}/3\mathbb{Z}$. However, if we solve norm equations by trivialising the corresponding cyclic algebra (using the method in [CFO$^+$15]) then the simplest case is when $E[\phi] \cong \mu_3$. For a general 3-isogeny we may reduce to either one of these two simplest cases at the expense of making a quadratic extension to our base field.

An alternative approach to improving a descent by p-isogeny to a full p-descent is described in [CM12]. The method there does however require a rigorous computation of S-units in a degree p extension of K. In contrast, we are free to solve norm equations by any method we like, since once a solution is found it is straightforward to verify it is correct.

The following notation will be used throughout. For K a field, we write $\overline{K}$ for its separable closure and $G_K = \mathrm{Gal}(\overline{K}/K)$ for its absolute Galois group. The Galois cohomology group $H^i(G_K, -)$ is abbreviated as $H^i(K, -)$, and we write $\mathrm{Hom}(G_K, -)$ for the continuous homomorphisms. The unit group of a ring R is denoted $R^\times$. We write μ_p for the group of pth roots of unity, and ζ_p for a generator.

The calculations in Section 4 were carried out using Magma [BCP97]. This paper is based on the first author's PhD thesis [vB15].

1. The Cassels-Tate pairing

In this section, we define the global Cassels-Tate pairing (2). The definition is given as a sum of local pairings, so we define these first. Let K_v denote the localisation of K at a place v. The Weil pairing $e_\phi : E[\phi] \times E'[\widehat{\phi}] \to \mu_p$ induces by cup product a pairing

$$\cup : H^1(K_v, E[\phi]) \times H^1(K_v, E'[\widehat{\phi}]) \to H^2(K_v, \mu_p).$$

It terms of cocycles we have $(\xi \cup \eta)_{\sigma,\tau} = e_\phi(\xi_\sigma, \sigma(\eta_\tau))$. Since $H^2(K_v, \mu_p) \cong \mathrm{Br}(K_v)[p]$ we can then apply the invariant map $\mathrm{inv}_{K_v} : \mathrm{Br}(K_v) \to \mathbb{Q}/\mathbb{Z}$, from local class field theory, to obtain the *local Tate pairing*:

$$\langle\ ,\ \rangle_{v,e_\phi} : H^1(K_v, E[\phi]) \times H^1(K_v, E'[\widehat{\phi}]) \to \mathbb{Q}/\mathbb{Z}. \tag{4}$$

1.1. **The global pairing.** Taking Galois cohomology of the short exact sequences

$$\begin{tikzcd} 0 \arrow[r] & E[\phi] \arrow[r, "\iota"] \arrow[d, equal] & E[p] \arrow[r, "\phi"] \arrow[d, hook] & E'[\widehat{\phi}] \arrow[r] \arrow[d, hook] & 0 \\ 0 \arrow[r] & E[\phi] \arrow[r] & E \arrow[r, "\phi"] & E' \arrow[r] & 0 \end{tikzcd}$$

we obtain a commutative diagram with exact rows

$$\begin{tikzcd} H^1(K, E[p]) \arrow[r, "\phi_*"] \arrow[d] & H^1(K, E'[\widehat{\phi}]) \arrow[r] \arrow[d] & H^2(K, E[\phi]) \arrow[d] \\ \prod_v H^1(K_v, E) \arrow[r] & \prod_v H^1(K_v, E') \arrow[r] & \prod_v H^2(K_v, E[\phi]). \end{tikzcd} \tag{5}$$

Lemma 1.1. *Any element $x \in S^{(\widehat{\phi})}(E'/K)$ can be lifted to $x_1 \in H^1(K, E[p])$ with $\phi_*(x_1) = x$.*

Proof. The Selmer group $S^{(\widehat{\phi})}(E'/K)$ is by definition the kernel of the middle vertical map in (5). By a diagram chase, it suffices to show that the right hand vertical map is injective. Making a finite extension L/K of degree coprime to p, we may ensure that $E[\phi] \cong \mu_p$ over L, and so $H^2(L, E[\phi]) \cong \mathrm{Br}(L)[p]$. Let v be a place of K. Then we have the following commutative diagram.

$$\begin{tikzcd} H^2(K, E[\phi]) \arrow[r, "\mathrm{Res}"] \arrow[d, "\mathrm{loc}_1"'] & H^2(L, E[\phi]) \arrow[r, "\mathrm{Cor}"] \arrow[d, "\mathrm{loc}_2"'] & H^2(K, E[\phi]) \arrow[d, "\mathrm{loc}_1"'] \\ H^2(K_v, E[\phi]) \arrow[r, "\mathrm{Res}"] & \oplus_{w|v} H^2(L_w, E[\phi]) \arrow[r, "\mathrm{Cor}"] & H^2(K_v, E[\phi]) \end{tikzcd}$$

By global class field theory, the following exact sequence holds for any number field L.

$$0 \longrightarrow \mathrm{Br}(L) \longrightarrow \bigoplus_w \mathrm{Br}(L_w) \xrightarrow{\sum \mathrm{inv}_w} \mathbb{Q}/\mathbb{Z} \longrightarrow 0$$

Thus the map $\prod_v \mathrm{loc}_2$ is injective. By [GS06, Proposition 3.3.7] the composite $\mathrm{Cor} \circ \mathrm{Res}$ is multiplication by $n = [L : K]$. The kernel of $\prod_v \mathrm{loc}_1$ is now both p-torsion and n-torsion. Since p and n are coprime, it follows that $\prod_v \mathrm{loc}_1$ is injective as required. $\square$

The Kummer exact sequences for $[p] : E \to E$ and $\widehat{\phi} : E' \to E$ give the rows of the following commutative diagram

$$\begin{tikzcd}
 & & H^1(K, E[\phi]) \arrow[d, "\iota_*"] \\
E(K) \arrow[r, "p"] \arrow[d, "\phi"'] & E(K) \arrow[r, "\delta_p"] \arrow[d, equal] & H^1(K, E[p]) \arrow[d, "\phi_*"] \\
E'(K) \arrow[r, "\widehat{\phi}"] & E(K) \arrow[r, "\delta_{\widehat{\phi}}"] & H^1(K, E'[\widehat{\phi}]).
\end{tikzcd} \tag{6}$$

The right hand column is the long exact sequence (3). We also consider the analogue of this diagram with K replaced by K_v. In the terminology of [PS99], the following is the "Weil pairing definition" of the Cassels-Tate pairing.

Definition 1.2 (Definition of the Cassels-Tate pairing)**.** Let $x, y \in S^{(\widehat{\phi})}(E'/K)$. By Lemma 1.1 there exists $x_1 \in H^1(K, E[p])$ with $\phi_*(x_1) = x$. We write $x_v, y_v, x_{1,v}$ for the localisations of x, y, x_1 at a place v. For each place v we pick $P_v \in E(K_v)$ with $\delta_{\widehat{\phi}}(P_v) = x_v$. Then $x_{1,v} - \delta_p(P_v) = \iota_*(\xi_v)$ for some $\xi_v \in H^1(K_v, E[\phi])$. The Cassels-Tate pairing is defined as

$$\langle x, y \rangle_{\mathrm{CT}} = \sum_v \langle \xi_v, y_v \rangle_{v, e_\phi}$$

where the sum is over all places v of K, and $\langle\ ,\ \rangle_{v,e_\phi}$ is the local Tate pairing (4).

It may be shown that the pairing is independent of the choice of global lift x_1 and the choices of local points P_v. For further details, and properties of the pairing, see for example [Cas62, Mil06, McC88, PS99, Fis03].

As we describe in the next section, the local Tate pairing is closely related to the Hilbert norm residue symbol. It can therefore be computed using standard techniques. A more serious problem is that of computing a global lift x_1 of x. In Section 2 we explain how this may be reduced to solving a norm equation. This then motivates our work on norm equations in Section 3.

1.2. **Computing the local pairing.** Let p be a prime. Let $\phi : E \to E'$ be a p-isogeny of elliptic curves defined over a number field K. We fix L/K a finite Galois extension of degree coprime to p, such that all points in the kernels of ϕ and $\widehat{\phi}$ are defined over L. By properties of the Weil pairing we have $\mu_p \subset L$. We may therefore fix isomorphisms $E[\phi] \cong \mu_p$ and $E'[\widehat{\phi}] \cong \mu_p$ over L. These maps induce, by restriction and the Kummer isomorphism, injective group homomorphisms

$$\overline{w}_\phi : H^1(K, E[\phi]) \longrightarrow L^\times/(L^\times)^p,$$

and

$$\overline{w}_{\widehat{\phi}} : H^1(K, E'[\widehat{\phi}]) \longrightarrow L^\times/(L^\times)^p.$$

We also write $\overline{w}_\phi$ and $\overline{w}_{\widehat{\phi}}$ for the local analogues of these maps.

Lemma 1.3. *There exists a primitive pth root of unity $\zeta_p \in L$ such that for all places v of K the local Tate pairing (4) is given by*

$$\langle x, y \rangle_{v,e_\phi} = \frac{1}{[L_w : K_v]} \mathrm{Ind}_{\zeta_p}(\overline{w}_\phi(x), \overline{w}_{\widehat{\phi}}(y))_w \tag{7}$$

where w is any place of L dividing v,

$$(\ , \ )_w : L_w^\times/(L_w^\times)^p \times L_w^\times/(L_w^\times)^p \to \mu_p$$

is the Hilbert norm residue symbol, and $\mathrm{Ind}_{\zeta_p} : \mu_p \to \frac{1}{p}\mathbb{Z}/\mathbb{Z}$ *is the isomorphism sending $\zeta_p \mapsto \frac{1}{p}$.*

Proof. We first treat the case $L = K$. The pairing

$$\mu_p \times \mu_p \to \mu_p; \ (\zeta_p^a, \zeta_p^b) \mapsto \zeta_p^{ab} \tag{8}$$

induces by cup product, the Kummer isomorphism and the local invariant map, a pairing

$$\{ \ , \ \}_v : K_v^\times/(K_v^\times)^p \times K_v^\times/(K_v^\times)^p \to \tfrac{1}{p}\mathbb{Z}/\mathbb{Z}.$$

The Hilbert norm residue symbol is $(x, y)_v = \zeta_p^{p\{x,y\}_v}$. By [Ser79, Prop. XIV.2.6] it is independent of the choice of ζ_p.

If we make an appropriate choice of ζ_p then our identifications $E[\phi] \cong \mu_p$ and $E'[\widehat{\phi}] \cong \mu_p$ identify the Weil pairing $e_\phi : E[\phi] \times E'[\widehat{\phi}] \to \mu_p$ with (8). This proves (7). The general case, with $L \neq K$, follows by standard properties of the cup product and the local invariant map under restriction, for which we refer to [CF10, Proposition IV.7.9(iii)] and [CF10, Theorem VI.1.3]. $\square$

Remark 1.4. In practice we are happy to compute the Cassels-Tate pairing up to an overall scaling. Therefore the choice of ζ_p in Lemma 1.3 does not matter, provided that the same global choice is used in all our local calculations.

We now suppose that $\mu_p \subset K_v$ and describe some methods for computing the Hilbert norm residue symbol. In fact the symbol may be defined with p replaced by any integer $m \geq 2$, and we now work in this generality.

Proposition 1.5. *Assume that $\mu_m \subset K_v$. The Hilbert norm residue symbol*

$$(\ , \ )_v : K_v^\times/(K_v^\times)^m \times K_v^\times/(K_v^\times)^m \to \mu_m$$

has the following properties.

(i) $(a, b)_v(a, c)_v = (a, bc)_v$

(ii) $(a, b)_v = 1$ *if b is a norm for the extension $K_v(\sqrt[m]{a})/K_v$. In particular* $(a, -a)_v = (a, 1 - a)_v = 1$.

(iii) $(a,b)_v(b,a)_v = 1$

(iv) *If* $v = \mathfrak{p}$ *is a prime not dividing* m *and* $v_{\mathfrak{p}}(a) = 0$ *then*

$$(a,b)_v = \left(\frac{a}{\mathfrak{p}}\right)^{v_{\mathfrak{p}}(b)} \qquad \textit{where} \qquad \left(\frac{a}{\mathfrak{p}}\right) \equiv a^{\frac{N\mathfrak{p}-1}{m}} \pmod{\mathfrak{p}}.$$

Proof. See [CF10, Exercise 2] or [Gra03, Proposition II.7.1.1]. □

Proposition 1.5 can be used to compute $(a,b)_v$ whenever $v \nmid m\infty$. Taking $m = p$ an odd prime, the following will suffice for our purposes in the case $v \mid p$. Let $K = \mathbb{Q}(\zeta_p)$. Then $\lambda = 1 - \zeta_p$ generates the unique prime of K lying over p. It is shown in [CF10, Exercise 2.13] that $K_v^\times/(K_v^\times)^p$ has basis $\lambda, \eta_1, \ldots, \eta_p$ where $\eta_i = 1 - \lambda^i$, and an explicit recipe is given for computing the Hilbert norm residue symbol. In the case $p = 3$ this works out as

(9)

	λ	η_1	η_2	η_3
λ	0	0	0	ζ_3^2
η_1	0	0	ζ_3	0
η_2	0	ζ_3^2	0	0
η_3	ζ_3	0	0	0

2. Galois cohomology

In this section, we give an explicit description of the long exact sequence (3) in terms of étale algebras. As explained in Section 1 this will enable us to compute the Cassels-Tate pairing.

2.1. **Etale algebras.**

Following [SS04] we interpret the Galois cohomology groups in (3) in terms of étale algebras. This makes the groups more amenable for practical computation. We work over a field K of characteristic 0.

Let Φ be a finite set with G_K-action. The étale algebra D associated to Φ is the set of all G_K-equivariant maps $\Phi \to \overline{K}$. This is a K-algebra under pointwise operations. If $P_1, \ldots, P_n \in \Phi$ are representatives for the G_K-orbits then evaluation at these points gives an isomorphism

$$D \cong K(P_1) \times \ldots \times K(P_n).$$

In particular D is a product of finite field extensions of K. We also write $\overline{D} = D \otimes_K \overline{K}$. This is the $\overline{K}$-algebra of all maps $\Phi \to \overline{K}$.

We fix p an odd prime. Let $\psi : E \to E'$ be an isogeny of elliptic curves with $E[\psi] \subset E[p]$, and let $\widehat{\psi}$ be its dual. Let D be the étale algebra of $E'[\widehat{\psi}]$. Let

$$\begin{aligned} w_\psi : E[\psi] &\longrightarrow \mu_p(\overline{D}) \\ P &\longmapsto (Q \mapsto e_\psi(P,Q)), \end{aligned}$$

be the map induced by the Weil pairing e_ψ. This induces a map on H^1's that on composing with the Kummer isomorphism gives a group homomorphism

$$\overline{w}_\psi : H^1(K, E[\psi]) \longrightarrow D^\times/(D^\times)^p.$$

Now let $\phi : E \to E'$ be a p-isogeny. The Weil pairings e_ϕ, e_p and $e_{\widehat{\phi}}$ are compatible in the sense that they give an isomorphism between the exact sequence

$$0 \longrightarrow E[\phi] \xrightarrow{\iota} E[p] \xrightarrow{\phi} E'[\widehat{\phi}] \longrightarrow 0. \tag{10}$$

and the exact sequence of Cartier duals. Let A_1, A_2 and A be the étale algebras of $E'[\widehat{\phi}]$, $E[\phi]$ and $E[p]$. By the compatibility of the Weil pairings, we obtain a commutative diagram

$$\begin{tikzcd} H^1(K, E[\phi]) \arrow[r, "\iota_*"] \arrow[d, "\overline{w}_\phi"'] & H^1(K, E[p]) \arrow[r, "\phi_*"] \arrow[d, "\overline{w}_p"'] & H^1(K, E'[\widehat{\phi}]) \arrow[d, "\overline{w}_{\widehat{\phi}}"'] \\ A_1^\times/(A_1^\times)^p \arrow[r, "\phi^*"] & A^\times/(A^\times)^p \arrow[r, "\iota^*"] & A_2^\times/(A_2^\times)^p \end{tikzcd} \tag{11}$$

where the first row is (3), i.e. the long exact sequence associated to (10). The maps in the second row (which is not exact) are the pull backs by ϕ and ι.

It is shown in [SS04, Section 5] that the vertical maps in (11) are injective, and their images are described as follows. We fix g a primitive root mod p, and let σ_g be the automorphism of A_1, A_2 or A given by $(\sigma_g\alpha)(P) = \alpha(gP)$. By [SS04, Lemma 5.2] we have

$$H^1(K, E[\phi]) \cong \ker(g - \sigma_g : A_1^\times/(A_1^\times)^p \to A_1^\times/(A_1^\times)^p) \tag{12}$$

and likewise for $H^1(K, E'[\widehat{\phi}])$. The corresponding description of $H^1(K, E[p])$ involves the set Λ of affine lines in $E[p]$ that do not pass through the origin $\mathcal{O}$. Let B be the étale algebra of Λ. Then the map

$$u : \mu_p(\overline{A}) \to \mu_p(\overline{B});\ \alpha \mapsto \big(\ell \mapsto \prod_{P\in\ell} \alpha(P)\big)$$

induces a map on H^1's, and so by the Kummer isomorphism gives us a group homomorphism $\overline{u} : A^\times/(A^\times)^p \longrightarrow B^\times/(B^\times)^p$.

Theorem 2.1 (Schaefer-Stoll [SS04, Corollary 5.9])**.**

$$H^1(K, E[p]) \cong \ker(g - \sigma_g : A^\times/(A^\times)^p \to A^\times/(A^\times)^p) \cap \ker(\overline{u}).$$

In fact we have $A \cong K \times A'$ where A' is the étale algebra of $E[p] \setminus \{\mathcal{O}\}$, and in Theorem 2.1 we are free to replace A by A'. This description of $H^1(K, E[p])$ can sometimes be simplified using the following lemma.

Lemma 2.2. *Let $\alpha \in \mathrm{Im}(\overline{w}_p) \subset A^\times/(A^\times)^p$. If $S, T \in E[p]$ then*

$$\frac{\alpha(S)\alpha(T)}{\alpha(S+T)} \in (K(S,T)^\times)^p.$$

Proof. See [CFO+08, Lemma 3.8]. $\square$

Let E/K be an elliptic curve and G the image of the mod p Galois representation $\overline{\rho}_{E,p} : G_K \to \mathrm{GL}(E[p])$. Fixing a basis S, T for $E[p]$, this is a subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. In the next two sections we consider two specific possibilities for G, which we call the *μ_p-nonsplit* and *$\mathbb{Z}/p\mathbb{Z}$-nonsplit* cases. The case where $E[p]$ splits as $\mu_p \times \mathbb{Z}/p\mathbb{Z}$ is significantly easier, as described in [McC88], [Fis03].

2.2. **μ_p-nonsplit case.** We consider E/K an elliptic curve whose mod p Galois representation has image

$$G = \left\{ \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix} \right\} \subset \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$$

generated by $\sigma = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\tau = \left(\begin{smallmatrix} g & 0 \\ 0 & 1 \end{smallmatrix}\right)$ where g is a primitive root mod p. Thus we have a basis S, T of $E[p]$ such that

$$\begin{aligned} \sigma(S) &= S & \qquad \tau(S) &= gS \\ \sigma(T) &= S + T & \qquad \tau(T) &= T. \end{aligned}$$

Note that $\tau\sigma = \sigma^g\tau$. Let $L_1 = K(S) = K(\zeta_p)$, $L_2 = K(T)$ and $M = K(E[p])$.

$$\begin{tikzcd}
 & M \arrow[dl, dash, "\langle\sigma\rangle"'] \arrow[dr, dash, "\langle\tau\rangle"] \arrow[dl, dash, bend right=60, "C_p"'] \arrow[dd, dash, bend left=90, "G"] & \\
L_1 \arrow[dr, dash, "p-1"'] & & L_2 \arrow[dl, dash, "p"] \\
 & K &
\end{tikzcd}$$

Recall that p is an odd prime. Let $\chi_{\mathrm{cyc}} : G_K \to (\mathbb{Z}/p\mathbb{Z})^\times$ be the cyclotomic character. Then for N a $(\mathbb{Z}/p\mathbb{Z})[G_K]$-module we write $N^{(i)}$ for the eigenspace where G_K acts as χ_{cyc}^i.

Theorem 2.3. *We have $H^1(K, E[p]) \cong H$, where H is the group of pairs $(a, b) \in (L_1^\times/(L_1^\times)^p)^{(1)} \times L_2^\times/(L_2^\times)^p$ satisfying $N_{L_2/K}(b) \in (K^\times)^p$ and $\sigma(b)/(ab) \in (M^\times)^p$.*

Proof. We use the description of $H^1(K, E[p])$ in Theorem 2.1 as the intersection of $\ker(g - \sigma_g)$ and $\ker(\overline{u})$.

There are p orbits for the action of G_K on $E[p] \setminus \{\mathcal{O}\}$, with representatives S and iT for $i \in \{1, \ldots, p-1\}$. Therefore $H^1(K, E[p]) \subset A'^{\times}/(A'^{\times})^p$ where

$$A' \cong L_1 \times \underbrace{L_2 \times \ldots \times L_2}_{p-1}.$$

Moreover $(a, b_1, b_2, \ldots, b_{p-1}) \in A'^{\times}/(A'^{\times})^p$ belongs to $\ker(g - \sigma_g)$ if and only if $a \in (L_1^{\times}/(L_1^{\times})^p)^{(1)}$ and $b_i \equiv b_1^i \mod (L_2^{\times})^p$ for all $i \in \{1, \ldots, p-1\}$. Accordingly we represent elements of $H^1(K, E[p])$ as pairs (a, b) where $b = b_1$.

We consider the action of G_K on the set Λ of affine lines in $E[p]$ missing the origin. There are $p-1$ orbits of one line each, given by $\ell_1, \ldots, \ell_{p-1}$ where

$$\ell_i = \{iT, S + iT, 2S + iT, \ldots, (p-1)S + iT\},$$

and just one further orbit of size $p^2 - p$ represented by

$$m = \{S, S + T, S + 2T, \ldots, S + (p-1)T\}.$$

Thus the étale algebra B associated to Λ is given by

$$B \cong \underbrace{K \times \cdots \times K}_{p-1} \times M.$$

A pair (a, b) corresponding to $\alpha \in A^{\times}$ represents an element in $\ker(\overline{u})$ if and only if

$$N_{L_2/K}(b)^i \equiv \prod_{P \in \ell_i} \alpha(P) \equiv 1 \mod (K^{\times})^p$$

for all $i \in \{1, 2, \ldots, p-1\}$, and

$$a \prod_{i=1}^{p-1} \sigma^{i^{-1}}(b)^i \equiv \prod_{P \in m} \alpha(P) \equiv 1 \mod (M^{\times})^p \tag{13}$$

where inverses are taken in $(\mathbb{Z}/p\mathbb{Z})^{\times}$. This proves the theorem when $p = 3$.

In general (13) may be simplified as follows. First Lemma 2.2 tells us that for an element in the image of $H^1(K, E[p])$ we have

$$\frac{\sigma(b)}{ab} = \frac{\alpha(S+T)}{\alpha(S)\alpha(T)} \in (M^{\times})^p. \tag{14}$$

Conversely, if we assume (14) then (13) follows by an easy calculation. □

Let $\phi : E \to E'$ be the isogeny with kernel generated by S. The first row of the following diagram is the long exact sequence (3). Since $E[\phi] \cong \mu_p$ as Galois modules, we have $H^1(K, E[\phi]) \cong K^\times/(K^\times)^p$ and $H^2(K, E[\phi]) \cong \mathrm{Br}(K)[p]$. The other two vertical maps are given by Theorem 2.3 and (12).

$$\begin{tikzcd} H^1(K,E[\phi]) \arrow[r, "\iota_*"] \arrow[d, "\cong"] & H^1(K,E[p]) \arrow[r, "\phi_*"] \arrow[d, "\cong"] & H^1(K,E'[\widehat{\phi}]) \arrow[r, "\delta_2"] \arrow[d, "\cong"] & H^2(K,E[\phi]) \arrow[d, "\cong"] \\ K^\times/(K^\times)^p \arrow[r, "f"] & H \arrow[r, "g"] & (L_1^\times/(L_1^\times)^p)^{(1)} \arrow[r, "\Delta"] & \mathrm{Br}(K)[p] \end{tikzcd} \tag{15}$$

The maps f, g and Δ are defined so that this diagram commutes. We now describe these maps explicitly.

Lemma 2.4. *We have $f : b \mapsto (1, b)$ and $g : (a, b) \mapsto a$.*

Proof. The second rows in (11) and (15) differ in that we have applied projection maps

$$\begin{array}{lll} A_1 \to K & A \to L_1 \times L_2 & A_2 \to L_1 \\ \alpha \mapsto \alpha(\phi T) & \alpha \mapsto (\alpha(S), \alpha(T)) & \alpha \mapsto \alpha(S) \end{array}$$

From this it is easy to see that the maps f and g in the statement of the lemma do indeed correspond to pull back by ϕ and ι. □

Our description of Δ will be in terms of cyclic algebras, so we introduce these first. Let $\chi \in \mathrm{Hom}(G_K, \mathbb{Z}/p\mathbb{Z})$ and $b \in K^\times$. If χ is non-trivial then it factors via an isomorphism $\mathrm{Gal}(L/K) \cong \mathbb{Z}/p\mathbb{Z}$; $\gamma \mapsto 1$, for some degree p cyclic extension L/K. The cyclic algebra $A = A(\chi, b)$ is the K-algebra $\{\sum_{i=0}^{p-1} a_i v^i : a_i \in L\}$ with multiplication determined by $v^p = b$ and

$$vx = \gamma(x)v \tag{16}$$

for all $x \in L$. This is a central simple algebra of dimension p^2. We write (χ, b) for its class in $\mathrm{Br}(K)$. This construction is compatible with the cup product, in the sense that the following diagram commutes.

$$\begin{tikzcd} H^1(K,\mathbb{Z}/p\mathbb{Z}) \times H^1(K,\mu_p) \arrow[r, "\cup"] \arrow[d, "\cong \ \cong"] & H^2(K,\mu_p) \arrow[d, "\cong"] \\ \mathrm{Hom}(G_K,\mathbb{Z}/p\mathbb{Z}) \times K^\times/(K^\times)^p \arrow[r, "(\ ,\ )"] & \mathrm{Br}(K)[p]. \end{tikzcd} \tag{17}$$

The next two lemmas are well known. See for example [GS06, Section 4.7]. We include the proofs since they are needed for our algorithms.

Lemma 2.5. *Let $A = A(\chi, b)$ be a cyclic algebra. Then $A \cong \mathrm{Mat}_p(K)$ if and only if b is a norm for L/K.*

Proof. If $x \in L$ then by (16) we have $(xv)^p = N_{L/K}(x)v^p$. So if b is a norm then $A(\chi, b) \cong A(\chi, 1)$. We then have the trivialisation

$$A(\chi,1) \cong \mathrm{End}_K(L) \cong \mathrm{Mat}_p(K)$$
$$\sum a_i v^i \mapsto (x \mapsto \sum a_i \gamma^i(x)).$$

Conversely, suppose we are given an isomorphism $\iota : A \cong \mathrm{Mat}_p(K)$. We fix a non-zero vector $e_1 \in K^p$. Since L is a field, the map of K-vector spaces $L \to K^p$; $x \mapsto \iota(x)e_1$ is injective. By a dimension count it is also surjective. Making this identification, we now have $\iota : A \cong \mathrm{End}_K(L)$ with $\iota(x)y = xy$ for all $x, y \in L$. Let $v_1 \in A$ with $\iota(v_1) = \gamma$. Since (16) is satisfied by both v and v_1 it follows that $\xi = v_1^{-1}v$ commutes with every element of L, and hence is in L. Finally $N_{L/K}(\xi) = (v_1\xi)^p = v^p = b$. □

Lemma 2.6. *Let $\mathbb{K}$ be a field containing a primitive pth root of unity ζ_p. Let $a, b \in \mathbb{K}^\times$ and let A be the $\mathbb{K}$-algebra generated by x and y subject to the relations $x^p = a$, $y^p = b$ and $xy = \zeta_p yx$. Then the following are equivalent.*

(i) *a is a norm for $\mathbb{K}(\sqrt[p]{b})/\mathbb{K}$.*
(ii) *b is a norm for $\mathbb{K}(\sqrt[p]{a})/\mathbb{K}$.*
(iii) *$A \cong \mathrm{Mat}_p(\mathbb{K})$.*

Proof. The equivalence of (ii) and (iii) is a special case of Lemma 2.5. By symmetry this also gives the equivalence of (i) and (iii). □

We also need the following fact about cup products.

Lemma 2.7. *Let $0 \to A_1 \to A_2 \to \mathbb{Z}/p\mathbb{Z} \to 0$ be a short exact sequence of $(\mathbb{Z}/p\mathbb{Z})[G_K]$-modules. Then the connecting maps in the long exact sequence*

$$\mathbb{Z}/p\mathbb{Z} \xrightarrow{\delta_1} H^1(K, A_1) \to H^1(K, A_2) \to H^1(K, \mathbb{Z}/p\mathbb{Z}) \xrightarrow{\delta_2} H^2(K, A_1)$$

are related by $\delta_2(b) = \delta_1(1) \cup b$.

Proof. Let b be represented by a cocycle (b_σ). Let $x \in A_2$ with $x \mapsto 1$. Then

$$\delta_2(b)_{\sigma\tau} = \sigma(b_\tau x) - b_{\sigma\tau}x + b_\sigma x = b_\tau(\sigma x - x) = (\delta_1(1) \cup b)_{\sigma\tau}.$$

Alternatively, this is [GS06, Proposition 3.4.8] with $A_3 = B = \mathbb{Z}/p\mathbb{Z}$. □

We are now ready to describe the map Δ in (15). We have $E'(K)[\widehat{\phi}] \cong \mathbb{Z}/p\mathbb{Z}$ generated by $\phi(T)$. The image of $\phi(T)$ under the connecting map in the long exact sequence associated to (10) is an element $\beta \in H^1(K, E[\phi]) \cong K^\times/(K^\times)^p$. This is a Kummer generator for the extension M/L_1. We write $\chi_a \mapsto a$ for the natural isomorphism (depending on a choice of primitive pth root of unity)

$$\mathrm{Hom}(G_K, \mathbb{Z}/p\mathbb{Z}) \cong (L_1^\times/(L_1^\times)^p)^{(1)}. \tag{18}$$

By Lemma 2.7 and (17), the map Δ in (15) is given by $\Delta : a \mapsto (\chi_a, \beta)$, at least up to multiplication by a fixed element of $(\mathbb{Z}/p\mathbb{Z})^\times$, which we have no need to make explicit.

Since the diagram (15) commutes, and the first row is exact, the second row is also exact. In particular, if $a \in (L_1^\times/(L_1^\times)^p)^{(1)}$ with $\Delta(a) = 0$ then there exists $b \in L_2^\times/(L_2^\times)^p$ such that $(a, b) \in H$. We show that making the lift from $H^1(K, E'[\widehat{\phi}])$ to $H^1(K, E[p])$ explicit comes down to solving a norm equation.

Theorem 2.8. *Let E/K be an elliptic curve with p-torsion of type μ_p-nonsplit. Let $a \in (L_1^\times/(L_1^\times)^p)^{(1)}$. If $\Delta(a) = 0$ then there exists $\xi \in M$ satisfying $N_{M/L_1}(\xi) = a$, and we may lift a to $(a, b) \in H$ where*

$$b = N_{M/L_2}\left(\prod_{i=1}^{p-1} \sigma^i(\xi)^i\right).$$

Proof. Let $\chi_a \mapsto a$ under the isomorphism (18), and let F be the fixed field of the kernel of χ_a. In other words, F/K is the degree p subextension of $L_1(\sqrt[p]{a})/K$.

$$\begin{tikzcd}
 & L_1(\sqrt[p]{a}) \arrow[dl, dash, "p"'] \arrow[d, dash, "p-1"] \\
L_1 = K(\zeta_p) \arrow[d, dash, "p-1"'] & F \arrow[dl, dash, "p"] \\
K &
\end{tikzcd}$$

If $\Delta(a) = 0$ then Lemma 2.5 tells us that β is a norm for F/K, and hence for $L_1(\sqrt[p]{a})/L_1$. It follows by Lemma 2.6 that a is a norm for M/L_1.

Now let ξ and b be as in the statement of the theorem. We show that $(a, b) \in H$ by checking the conditions in Theorem 2.3. First we compute

$$N_{L_2/K}(b) = N_{M/K}\left(\prod_{i=1}^{p-1} \sigma^i(\xi)^i\right) = N_{L_1/K}(a)^{p(p-1)/2}.$$

Since p is odd this gives $N_{L_2/K}(b) \in (K^\times)^p$. Since $\tau\sigma = \sigma^g\tau$ we have

$$\sigma(b) \equiv \prod_{r=0}^{p-2} \tau^r \prod_{i=0}^{p-1} \sigma^{i+g^{-r}}(\xi)^i \equiv \prod_{r=0}^{p-2} \tau^r \prod_{i=0}^{p-1} \sigma^i(\xi)^{i-g^{-r}} \mod (M^\times)^p.$$

Then since $N_{M/L_1}(\xi) = a$ and $\tau(a) \equiv a^g \mod (L_1^\times)^p$ we have

$$b/\sigma(b) \equiv \prod_{r=0}^{p-2} \tau^r N_{M/L_1}(\xi)^{g^{-r}} \equiv \prod_{r=0}^{p-2} (\tau^r a)^{g^{-r}} \equiv a^{-1} \mod (M^\times)^p.$$

Therefore $\sigma(b)/(ab) \in (M^\times)^p$ as required. $\square$

2.3. $\mathbb{Z}/p\mathbb{Z}$**-nonsplit case.** We consider E/K an elliptic curve whose mod p Galois representation has image

$$G = \left\{ \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \right\} \subset \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$$

generated by $\sigma = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\tau = \left(\begin{smallmatrix} 1 & 0 \\ 0 & g \end{smallmatrix}\right)$ where g is a primitive root mod p. Thus we have a basis S, T of $E[p]$ such that

$$\sigma(S) = S \qquad \tau(S) = S$$
$$\sigma(T) = S + T \qquad \tau(T) = gT$$

Note that $\tau\sigma^g = \sigma\tau$. Let $L_1 = K(\zeta_p)$ and $M = K(T) = K(E[p])$. Let L_2 be the subfield of M fixed by τ. The diagram of fields is the same as in Section 2.2.

Theorem 2.9. *We have $H^1(K, E[p]) \cong H$, where H is the group of pairs $(a, b) \in K^\times/(K^\times)^p \times M^\times/(M^\times)^p$ satisfying $b^g/\tau(b) \in (M^\times)^p$, $N_{M/L_1}(b) \in (L_1^\times)^p$ and $\sigma(b)/(ab) \in (M^\times)^p$.*

Proof. Again we use the description of $H^1(K, E[p])$ in Theorem 2.1 as the intersection of $\ker(g - \sigma_g)$ and $\ker(\overline{u})$.

There are p orbits for the action of G_K on $E[p] \setminus \{\mathcal{O}\}$, with representatives iS for $i \in \{1, \ldots, p-1\}$, and T. Therefore $H^1(K, E[p]) \subset A'^\times/(A'^\times)^p$ where

$$A' \cong \underbrace{K \times \cdots \times K}_{p-1} \times M.$$

Moreover $(a_1, a_2, \ldots, a_{p-1}, b) \in A'^\times/(A'^\times)^p$ belongs to $\ker(g - \sigma_g)$ if and only if $a_i \equiv a_1^i \mod (K^\times)^p$ for all $i \in \{1, \ldots, p-1\}$, and $b^g/\tau(b) \in (M^\times)^p$. Accordingly we represent elements of $H^1(K, E[p])$ as pairs (a, b) where $a = a_1$.

We consider the action of G_K on the set Λ of affine lines in $E[p]$ missing the origin. There is one orbit of size $p - 1$ represented by the line

$$\ell = \{T, S + T, 2S + T, \ldots, (p-1)S + T\},$$

and $p - 1$ orbits of size p, represented by the lines $m_1, \ldots, m_{p-1}$ where

$$m_i = \{iS, iS + T, iS + 2T, \ldots, iS + (p-1)T\}.$$

Thus the étale algebra B associated to Λ is given by

$$B \cong L_1 \times \underbrace{L_2 \times \cdots \times L_2}_{p-1}.$$

A pair (a, b) corresponding to $\alpha \in A^\times$ represents an element in $\ker(\overline{u})$ if and only if

$$N_{M/L_1}(b) \equiv \prod_{P \in \ell} \alpha(P) \equiv 1 \mod (L_1^\times)^p$$

and

$$a^i N_{M/L_2}(\sigma^i(b)) \equiv \prod_{P \in m_i} \alpha(P) \equiv 1 \mod (L_2^\times)^p \tag{19}$$

for all $i \in \{1, 2, \ldots, p-1\}$.

The condition (19) may be simplified as follows. First Lemma 2.2 tells us that for an element in the image of $H^1(K, E[p])$ we have

$$\frac{\sigma(b)}{ab} = \frac{\alpha(S+T)}{\alpha(S)\alpha(T)} \in (M^\times)^p. \tag{20}$$

Conversely, if we assume (20) then $\sigma^i(b) \equiv a^i b \mod (M^\times)^p$. If in addition $b^g/\tau(b) \in (M^\times)^p$ then by taking norms from M down to L_2 it follows that

$$a^i N_{M/L_2}(\sigma^i(b)) \equiv N_{M/L_2}(b) \equiv 1 \mod (L_2^\times)^p.$$ □

Let $\phi : E \to E'$ be the isogeny with kernel generated by S. The first row of the following diagram is the long exact sequence (3). Since $E[\phi] \cong \mathbb{Z}/p\mathbb{Z}$ over K, we have $E[\phi] \cong \mu_p$ over L_1 and hence $H^1(L_1, E[\phi]) \cong L_1^\times/(L_1^\times)^p$ and $H^2(L_1, E[\phi]) \cong \mathrm{Br}(L_1)[p]$. The first and last vertical maps are then obtained by the inflation-restriction exact sequence. Since $E'[\widehat{\phi}] \cong \mu_p$ over K we have $H^1(K, E'[\widehat{\phi}]) \cong K^\times/(K^\times)^p$. The remaining vertical map is given by Theorem 2.9.

$$\begin{array}{ccccccc} H^1(K, E[\phi]) & \xrightarrow{\iota_*} & H^1(K, E[p]) & \xrightarrow{\phi_*} & H^1(K, E'[\widehat{\phi}]) & \xrightarrow{\delta_2} & H^2(K, E[\phi]) \\ \downarrow \cong & & \downarrow \cong & & \downarrow \cong & & \downarrow \cong \\ (L_1^\times/(L_1^\times)^p)^{(1)} & \xrightarrow{f} & H & \xrightarrow{g} & K^\times/(K^\times)^p & \xrightarrow{\Delta} & \mathrm{Br}(L_1)[p]^{(1)} \end{array} \tag{21}$$

Again we define the maps f, g and Δ so that this diagram commutes. We now describe these maps explicitly.

Lemma 2.10. *We have $f : b \mapsto (1, b)$ and $g : (a, b) \mapsto a$.*

Proof. The proof is almost identical to that of Lemma 2.4. □

Let β be a Kummer generator for M/L_1. We write $\chi_a \mapsto a$ for the Kummer isomorphism $H^1(L_1, \mu_p) \cong L_1^\times/(L_1^\times)^p$. Then exactly as in Section 2.2, the map Δ is given by $\Delta : a \mapsto (\chi_a, \beta)$. Again we show that making the lift from $H^1(K, E'[\widehat{\phi}])$ to $H^1(K, E[p])$ explicit comes down to solving a norm equation.

Theorem 2.11. *Let E/K be an elliptic curve with p-torsion of type $\mathbb{Z}/p\mathbb{Z}$-nonsplit. Let $a \in K^\times/(K^\times)^p$. If $\Delta(a) = 0$ then there exists $\xi \in L_2$ satisfying $N_{L_2/K}(\xi) = a$, and we may lift a to $(a, b) \in H$ where*

$$b = \prod_{i=1}^{p-1} \sigma^i(\xi)^{p-i}.$$

Proof. If $\Delta(a) = 0$ then Lemma 2.5 tell us that β is a norm for $L_1(\sqrt[p]{a})/L_1$. It follows by Lemma 2.6 that a is a norm for M/L_1, and hence for L_2/K.

We show that $(a, b) \in H$ by checking the conditions in Theorem 2.9. Since $\tau\sigma^g = \sigma\tau$ and $\tau(\xi) = \xi$ we have

$$\tau(b) \equiv \prod_{i=1}^{p-1} \sigma^{g^{-1}i}(\xi)^{-i} \equiv \prod_{i=1}^{p-1} \sigma^i(\xi)^{-gi} \equiv b^g \mod (M^\times)^p.$$

Since $\mathrm{Gal}(M/L_1) = \langle\sigma\rangle$ and p is odd, we have $N_{M/L_1}(b) = a^{p(p-1)/2} \in (K^\times)^p$, and $\sigma(b)/b \equiv N_{M/L_1}(\xi) \equiv a \mod (M^\times)^p$. $\square$

Remark 2.12. It can be shown that $\beta \in (L_1^\times/(L_1^\times)^p)^{(2)}$. In particular, if $p = 3$ then $\beta \in K^\times/(K^\times)^p$ and $L_2 = K(\sqrt[3]{\beta})$ is a pure cubic extension of K. Norm equations for extensions of this form are the subject of the next section.

3. Solving norm equations

In this section, we present a new algorithm for solving norm equations in pure cubic extensions of the rationals. It is based on the Legendre-type method for solving conics in [CR03].

3.1. **Diagonal cubic surfaces.** Let K be a number field with ring of integers $\mathcal{O}_K$. Let $L = K(\sqrt[3]{b})$ for some $b \in K$ not a cube. We may represent any element $\xi = A + B\sqrt[3]{b} + C\sqrt[3]{b}^2$ in L in the form

$$\xi = \frac{\alpha + \beta\sqrt[3]{b}}{\gamma + \delta\sqrt[3]{b}}. \tag{22}$$

Indeed this is clear if $B = C = 0$, and otherwise we put

$$\alpha = AB - C^2 b \qquad \beta = B^2 - AC$$
$$\gamma = B \qquad \delta = -C.$$

Taking norms in (22) we see that solving the norm equation $N_{L/K}(\xi) = a$ is equivalent to find a K-rational point on the diagonal cubic surface

$$V_{a,b} = \{x_1^3 + ax_2^3 + bx_3^3 + abx_4^3 = 0\} \subset \mathbb{P}^3.$$

Theorem 3.1. *Let $a, b \in K$. Then the following are equivalent*

(i) *a is a norm for $K(\sqrt[3]{b})/K$.*
(ii) *b is a norm for $K(\sqrt[3]{a})/K$.*
(iii) *a^2b is a norm for $K(\sqrt[3]{a+b})/K$.*
(iv) *a^2b is a norm for $K(\sqrt[3]{a-b})/K$.*
(v) *$V_{a,b}(K) \neq \emptyset$.*

Proof. We may assume that a and b are not cubes, otherwise conditions (i), (ii) and (v) are trivially satisfied. We have already shown that (i) and (v) are equivalent. The symmetry in (v) also shows that (ii) and (v) are equivalent.

We now prove that (ii) and (iii) are equivalent. Suppose that b is a norm for $K(\sqrt[3]{a})/K$. Then b/a is a norm for $K(\sqrt[3]{a})/K$, and so by the equivalence of (i) and (ii), a is a norm for $K(\sqrt[3]{b/a})/K$. But then $a+b = a(1+b/a)$ is a norm for $K(\sqrt[3]{b/a})/K$, and again by the equivalence of (i) and (ii), b/a is a norm for $K(\sqrt[3]{a+b})/K$. The converse is proved by reversing these steps. The same argument, with b replaced by $-b$, shows that (ii) and (iv) are equivalent. □

As observed by Selmer [Sel53], it follows from the equivalence of (i) and (v) in Theorem 3.1, and the Hasse norm theorem, that the surfaces $V_{a,b}$ satisfy the Hasse principle. We now turn this into an algorithm for solving norm equations, at least in the case $K = \mathbb{Q}$. First we record an easy lemma.

Lemma 3.2. *Let $a, b \in \mathcal{O}_K$. If the surface $V_{a,b}$ is locally soluble at a prime $\mathfrak{p}$ and $v_{\mathfrak{p}}(b) \not\equiv 0 \pmod 3$ then a is a cube mod $\mathfrak{p}$.*

Proof. Working in the completion $K_{\mathfrak{p}}$ we may assume that $v_{\mathfrak{p}}(b) = 1$ or 2. Let $(x_1 : \ldots : x_4)$ be a local point with $\min v_{\mathfrak{p}}(x_i) = 0$. Then $x_1^3 + a x_2^3 \equiv 0 \pmod{\mathfrak{p}}$. If a is not a cube mod $\mathfrak{p}$ then $x_1 \equiv x_2 \equiv 0 \pmod{\mathfrak{p}}$. But then $x_3^3 + a x_4^3 \equiv 0 \pmod{\mathfrak{p}}$, and we likewise deduce that $x_3 \equiv x_4 \equiv 0 \pmod{\mathfrak{p}}$. This contradicts that $\min v_{\mathfrak{p}}(x_i) = 0$. Therefore a must be a cube mod $\mathfrak{p}$. □

We suppose as above that $a, b \in \mathcal{O}_K$, and that $V_{a,b}$ is everywhere locally soluble. If K has class number 1 then we may assume that (b) is cube-free, and indeed write $(b) = \mathfrak{b}_1 \mathfrak{b}_2^2$ where $\mathfrak{b}_1$ and $\mathfrak{b}_2$ are coprime and square-free. Then by Lemma 3.2 and the Chinese Remainder Theorem there exists $c \in \mathcal{O}_K$ such that $a \equiv c^3 \pmod{\mathfrak{b}_1}$. Writing $\mathfrak{b}_1 = (b_1)$ for some $b_1 \in \mathcal{O}_K$ it follows that the binary cubic form

$$F(X,Y) = \frac{1}{b_1}\Big((cX + b_1 Y)^3 - a X^3 \Big) \tag{23}$$

has coefficients in $\mathcal{O}_K$. This form has discriminant $\Delta(F) = -27 a^2 b_1^2$.

We seek to find $u, v \in \mathcal{O}_K$, not both zero, such that $F(u,v)$ is small. In the next section we explain how to do this in the case $K = \mathbb{Q}$.

3.2. Reduction of binary cubic forms.

Let G in $\mathbb{R}[X,Y]$ be a binary quadratic form, and $\Delta(G)$ its discriminant:

$$\begin{aligned} G(X,Y) &= aX^2 + bXY + cY^2, \\ \Delta(G) &= b^2 - 4ac. \end{aligned}$$

The group $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathbb{R}[X,Y]$ via

$$G(X,Y)\cdot\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} = G(\alpha X+\beta Y, \gamma X+\delta Y)$$

and the discriminant is invariant under this action.

Definition 3.3. A positive definite binary quadratic form $G(X,Y) = aX^2 + bXY + cY^2$ is *reduced* if $|b| \le a \le c$. Equivalently, G is reduced if the root of $G(X,1) = 0$ in the upper half plane H lies in the fundamental region

$$\mathcal{F} = \left\{ z \;\middle|\; z \in H,\ |z| \ge 1,\ -\frac{1}{2} \le \mathrm{Re}(z) \le \frac{1}{2} \right\}.$$

Consider now the general binary cubic form and its discriminant

$$\begin{aligned} f(X,Y) &= aX^3 + bX^2Y + cXY^2 + dY^3 \\ \Delta(f) &= b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd. \end{aligned} \tag{24}$$

If $\Delta(f) < 0$, then f has one real root and a pair of complex conjugate roots $\beta, \overline{\beta}$. We associate to f the binary quadratic form

$$Q(f) = (X - \beta Y)(X - \overline{\beta}Y). \tag{25}$$

There are other forms we could choose, some of which are discussed in [Cre99], however this is the simplest option, and is sufficient for our purposes.

Definition 3.4. A binary cubic form (24) is *Minkowski-reduced* if the positive definite form $Q(f)$ in (25) is reduced in the sense of Definition 3.3.

We use the following result from the geometry of numbers [Cas97, II.5.4].

Theorem 3.5 (Davenport [Dav45])**.** *If f in $\mathbb{Z}[X,Y]$ is a binary cubic form with discriminant $\Delta = \Delta(f) < 0$, then there are integers $(u,v) \ne (0,0)$ such that*

$$|f(u,v)| \le \left|\frac{\Delta}{23}\right|^{1/4}.$$

If, further, f is Minkowski-reduced in the sense of Definition 3.4, then

$$\min\bigl\{|f(1,0)|, |f(0,1)|, |f(1,\pm 1)|, |f(1,\pm 2)|\bigr\} \le \left|\frac{\Delta}{23}\right|^{1/4},$$

with equality only when $f(X,\pm Y) = A(X^3 + X^2Y + 2XY^2 + Y^3)$.

The second part of the theorem, together with the well known algorithm for reducing positive definite binary quadratic forms, gives an algorithm for finding integers u, v satisfying the conditions in the first part of the theorem.

3.3. **An algorithm over the rationals.** We now take $K = \mathbb{Q}$. Let a and b be positive cube-free integers. We write $b = b_1 b_2^2$ where b_1 and b_2 are positive, coprime and square-free. Applying the results of Section 3.2 to the binary cubic (23), we can find $u, v \in \mathbb{Z}$ such that

$$0 < F(u,v) < \left(\frac{27}{23}\right)^{1/4} (ab_1)^{1/2}. \tag{26}$$

We observe that

$$N_{\mathbb{Q}(\sqrt[3]{a})/\mathbb{Q}}\Big(b_2((cu + b_1 v) - \sqrt[3]{a}u)\Big) = b_1 b_2^3 F(u,v) = bb_2 F(u,v). \tag{27}$$

If we can find $\eta \in \mathbb{Q}(\sqrt[3]{a})$ such that $N_{\mathbb{Q}(\sqrt[3]{a})/\mathbb{Q}}(\eta) = b_2 F(u,v)$ then, by the multiplicativity of the norm, we can find $\xi \in \mathbb{Q}(\sqrt[3]{a})$ such that $N_{\mathbb{Q}(\sqrt[3]{a})/\mathbb{Q}}(\xi) = b$. Ideally, we want $b_2 F(u,v) < b$, so that our norm equation is replaced by a smaller one. Unfortunately, the bound (26) isn't quite strong enough to prove this. Our solution to this problem is to use condition (iv) in Theorem 3.1.

Algorithm 3.6. (Legendre-type algorithm for solving cubic norm equations)
Input: A pair of positive integers (a, b) such that b is a norm for $\mathbb{Q}(\sqrt[3]{a})/\mathbb{Q}$.
Output: A list of pairs (a, b), with b a norm for $\mathbb{Q}(\sqrt[3]{a})/\mathbb{Q}$, such that a solution to each norm equation allows us to read off a solution to the previous one.

(i) Replace a and b by their cube-free parts. If $a > b$ then swap a and b.
(ii) If $a = 0$ or 1 then stop.
(iii) Write $b = b_1 b_2^2$ where b_1 and b_2 are positive, coprime and square-free. Solve for $c \in \mathbb{Z}$ such that $a \equiv c^3 \pmod{b_1}$.
(iv) Define $F \in \mathbb{Z}[X, Y]$ as in (23). Use reduction theory to find $u, v \in \mathbb{Z}$ satisfying (26).
(v) If $b_2 F(u,v) < \frac{3}{4} b$ then replace (a, b) by $(a, b_2 F(u,v))$ and go to Step (i).
(vi) Otherwise, replace (a, b) by $(b - a, a^2 b)$ and go to Step (i).

When the algorithm terminates, it is clear by (27) and the proof of Theorem 3.1 that we may solve the original norm equation.

Theorem 3.7. *If $a, b \leq B$ then Algorithm 3.6 takes $O((logB)^2)$ iterations.*

Proof. In Step (v) we have $a_{\text{new}} = a$ and $b_{\text{new}} < \frac{3}{4} b$. So if we never reach Step (vi) then the algorithm takes $O(\log B)$ iterations. If we reach Step (vi) then

$$\frac{3}{4} b \leq b_2 F(u,v) < \left(\frac{27}{23}\right)^{1/4} (ab)^{1/2}$$

and so $b < 1.93a$. In this case $a_{\text{new}} = b - a < 0.93a$, and so the total number of applications of Step (vi) is $O(\log B)$. Moreover $b_{\text{new}} = a^2 b < 2a^3 \leq 2B^3$ and so Step (v) is applied $O(\log B)$ times between each application of Step (vi). $\square$

Remark 3.8. The bottleneck in Algorithm 3.6 comes in Steps (i) and (iii), as these are the steps that involve factoring. We expect it would be possible to modify the algorithm, along the lines of [CR03, Section 2.5], so that factoring is only required on the first iteration. However we have not worked out the details.

We give two examples, the first illustrating the need for Step (vi), and the second in preparation for Example 4.3. The actual solutions to the norm equations are rather large, so we do not record them here.

Example 3.9. Let $a = 5316$ and $b = 35685$. The steps taken by Algorithm 3.6 are recorded in the rows of the following table. On the second iteration we have $b_2F(u,v) = 5382 > b$ and so we reach Step (vi).

a	b	b_1	b_2	c	u	v
5316	35685	3965	3	2521	-11	7
5316	5364	149	6	52	-2	1
48	151585867584	[take cube-free parts]				
6	87723303	447	443	123	-11	3
6	6202	6202	1	2596	-43	18
6	77	77	1	41	2	-1
1	6					

Example 3.10. Let $a = 17$ and $b = 28507604531763846358949834957759$. On the first iteration we have $c = 25127582085067705054161519583 82$ and

$$(u, v) = (-1056910260262351, 931597016217248).$$

On this and subsequent iterations we have $b_1 = b$ and $b_2 = 1$.

a	b	c	u	v
17	3227115996467513	3079766255214306	1678826	-1602171
17	69326065	67724958	-3767	3680
17	13311	[take cube-free parts]		
17	493	476	-1	1
10	17	3	1	0
1	10			

In [vB15, Chapter 4] we investigated analogues of Algorithm 3.6 over other number fields with small discriminant. Although we couldn't prove that these methods always work, they seem to perform quite well in practice, at least in reducing the norm equations to ones that can be solved by traditional methods.

4. Examples

In this section, we give some examples in the case $K = \mathbb{Q}$, showing how the results of Sections 2 and 3 may be used to compute the Cassels-Tate pairing on 3-isogeny Selmer groups. Further examples are given in [vB15].

We identify $\frac{1}{3}\mathbb{Z}/\mathbb{Z}$ with $\mathbb{Z}/3\mathbb{Z}$ via multiplication by 3, so that the matrices below have entries $0, 1, 2$ rather than $0, \frac{1}{3}, \frac{2}{3}$. We also write $\langle a_1, a_2 \ldots \rangle$ for the subgroup generated by $a_1, a_2, \ldots$.

Example 4.1. Let E and E' be the 3-isogenous elliptic curves labelled 63531c1 and 63531c2 in Cremona's tables [Cre97].

$$\begin{aligned} E: &\quad y^2 = x^3 - 3(4x + 52)^2 \\ E': &\quad y^2 = x^3 + 36^2(x + 543)^2 \end{aligned}$$

The Galois action on $E[3]$ is of type μ_3-nonsplit. Indeed $E[3]$ is generated by

$$S = (0, 52\sqrt{-3}) \quad \text{and} \quad T = (156/(\theta - 4), 156\theta/(\theta - 4))$$

where $\theta = \sqrt[3]{181}$. We set $\zeta_3 = (-1 + \sqrt{-3})/2$. As in Section 2.2 we have fields $L_1 = \mathbb{Q}(\zeta_3)$, $L_2 = \mathbb{Q}(\theta)$ and $M = \mathbb{Q}(\zeta_3, \theta)$. A descent by 3-isogeny (see the introduction for references) computes the Selmer groups

$$\begin{aligned} S^{(\phi)}(E/\mathbb{Q}) &= \langle 181 \rangle \subset \mathbb{Q}^\times/(\mathbb{Q}^\times)^3 \\ S^{(\widehat{\phi})}(E'/\mathbb{Q}) &= \langle \zeta_3, 39\zeta_3 + 52 \rangle \subset \left(L_1^\times/(L_1^\times)^3\right)^{(1)}. \end{aligned}$$

This gives an upper bound of 2 for the rank of $E(\mathbb{Q})$. We seek to improve this bound by computing the Cassels-Tate pairing on $S^{(\widehat{\phi})}(E'/\mathbb{Q})$.

We start by lifting $a_1 = \zeta_3$ and $a_2 = 39\zeta_3 + 52$ globally to $H^1(\mathbb{Q}, E[3]) \cong H$, where $H \subset L_1^\times/(L_1^\times)^3 \times L_2^\times/(L_2^\times)^3$ is given by Theorem 2.3. We used the existing function `NormEquation` in Magma (this example is too small for the methods of Section 3 to be needed) to solve the norm equations $N_{M/L_1}(\xi) = a_i$ for $i = 1, 2$, and then computed b_i with $(a_i, b_i) \in H$ using Theorem 2.8. We used the method in [Fis08, Section 2] to find a small representative for b_i in $L_2^\times/(L_2^\times)^3$. By (15) we are free to multiply b_i by any element in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^3$. In this way we obtain

$$\begin{aligned} b_1 &= 7\theta^2 + 40\theta + 217 & N_{L_2/\mathbb{Q}}(b_1) &= 2^6 3^6 \\ b_2 &= 59\theta^2 + 314\theta + 3011 & N_{L_2/\mathbb{Q}}(b_2) &= 2^3 3^{12} 13^3 \end{aligned} \tag{28}$$

The connecting map $\delta_3 : E(\mathbb{Q}) \to H^1(\mathbb{Q}, E[3])$ in (6) may be computed as described in [Sil09, Chapter X]. It is given by the tangent lines at S and T, i.e.

$P \mapsto (\tan_S(P), \tan_T(P))$ where

$$\begin{aligned} \tan_S(x,y) &= y - 4\sqrt{-3}x - 52\sqrt{-3}, \\ \tan_T(x,y) &= y - 2(\theta+2)x + 156(\theta+4)/(\theta-4). \end{aligned}$$

The local analogue of this map is given by the same formula.

Let $(a,b) = (a_1,b_1)$ or (a_2,b_2). Since $a \in S^{(\widehat{\phi})}(E'/\mathbb{Q})$ there exists for each prime p a local point $P_p \in E(\mathbb{Q}_p)$ with $\tan_S(P_p) \equiv a \mod (\mathbb{Q}_p(\zeta_3)^\times)^3$. Then (a,b) and $(\tan_S(P_p), \tan_T(P_p))$ are both local lifts of a. By (15) and Lemma 2.4 it follows that $b/\tan_T(P_p) \equiv \xi_p \mod (\mathbb{Q}_p(\zeta_3)^\times)^3$ for some $\xi_p \in \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^3$. By Definition 1.2 and Lemma 1.3 we have

$$\langle a, a' \rangle_{\mathrm{CT}} = \sum_p \frac{1}{[\mathbb{Q}_p(\zeta_3):\mathbb{Q}_p]} \mathrm{Ind}_{\zeta_3}(\xi_p, a')_p \tag{29}$$

where $(\ ,\ )_p$ is the Hilbert norm residue symbol on $\mathbb{Q}_p(\zeta_3)$. If $p \neq 3$ is a prime of good reduction for E, and $v_{\mathfrak{p}}(b) \equiv 0 \mod 3$ for all primes $\mathfrak{p}$ dividing p, then p makes no contribution to the sum (29).

Returning to our example, E has minimal discriminant $-3^3 \cdot 13^3 \cdot 181$ and the norms of the b_i were recorded in (28). The Cassels-Tate pairing is therefore a sum of local pairings at the primes $2, 3, 13$ and 181. Since 3 is odd, there is no contribution from the infinite place.

Contribution at $p = 2$. The local point $P = (4, 2^2 + 2^6 + O(2^8)) \in E(\mathbb{Q}_2)$ satisfies $\tan_S(P) \equiv a_1 \equiv a_2 \mod (\mathbb{Q}_2(\zeta_3)^\times)^3$. Embedding L_2 in $\mathbb{Q}_2$ via $\theta \mapsto 1 + 2^2 + O(2^3)$ we find that $\tan_T(P) \equiv b_1 \equiv b_2 \equiv 1 \mod (\mathbb{Q}_2^\times)^3$. Therefore the local pairing at $p = 2$ is trivial.

Contribution at $p = 3$. The local points

$$\begin{aligned} P_1 &= (4, 2 + 3 + 2.3^2 + O(3^5)) \in E(\mathbb{Q}_3) \\ P_2 &= (3^{-2}, 3^{-3} + 1 + 3^2 + O(3^5)) \in E(\mathbb{Q}_3) \end{aligned}$$

satisfy $\tan_S(P_i) \equiv a_i \mod (\mathbb{Q}_3(\zeta_3)^\times)^3$ for $i = 1, 2$. Embedding L_2 in $\mathbb{Q}_3$ via $\theta \mapsto 1 + 2.3 + 3^3 + O(3^4)$ we compute

$$\begin{aligned} b_1/\tan_T(P_1) &\equiv 3 \mod (\mathbb{Q}_3(\zeta_3)^\times)^3 \\ b_2/\tan_T(P_2) &\equiv 6 \mod (\mathbb{Q}_3(\zeta_3)^\times)^3 \end{aligned}$$

We recall from Section 1.2 that $\mathbb{Q}_3(\zeta_3)^\times/(\mathbb{Q}_3(\zeta_3)^\times)^3$ has basis $\lambda, \eta_1, \eta_2, \eta_3$ where $\lambda = 1 - \zeta_3$ and $\eta_i = 1 - \lambda^i$. In terms of this basis we have

$$\begin{aligned} 3 &\equiv \lambda^2\eta_1^2 \mod (\mathbb{Q}_3(\zeta_3)^\times)^3 & a_1 &\equiv \eta_1 \mod (\mathbb{Q}_3(\zeta_3)^\times)^3 \\ 6 &\equiv \lambda^2\eta_1^2\eta_2^2\eta_3^2 \mod (\mathbb{Q}_3(\zeta_3)^\times)^3 & a_2 &\equiv \eta_3^2 \mod (\mathbb{Q}_3(\zeta_3)^\times)^3 \end{aligned}$$

Using (9) to compute the Hilbert norm residue symbol, and not forgetting the factor $[\mathbb{Q}_3(\zeta_3) : \mathbb{Q}_3] = 2$ in (29), the local pairing at $p = 3$ is as given in (30).

Contribution at $p = 13$. We embed $L_1 = \mathbb{Q}(\zeta_3)$ in $\mathbb{Q}_{13}$ via $\zeta_3 \mapsto 3+11.13+O(13^2)$. The local points

$$P_1 = (6, 10 + 4.13 + 12.13^2 + O(13^3)) \in E(\mathbb{Q}_{13})$$
$$P_2 = (13, 4.13 + 3.13^2 + 5.13^3 + O(13^4)) \in E(\mathbb{Q}_{13})$$

satisfy $\tan_S(P_i) \equiv a_i \mod (\mathbb{Q}_{13}^\times)^3$ for $i = 1, 2$. Embedding $L_2 = \mathbb{Q}(\theta)$ in $\mathbb{Q}_{13}$ via $\theta \mapsto 4 + 13 + 7.13^2 + O(13^3)$ we compute

$$b_1/\tan_T(P_1) \equiv 1 \mod (\mathbb{Q}_{13}^\times)^3 \qquad a_1 \equiv 2 \mod (\mathbb{Q}_{13}^\times)^3$$
$$b_2/\tan_T(P_2) \equiv 2 \mod (\mathbb{Q}_{13}^\times)^3 \qquad a_2 \equiv 13^2 \mod (\mathbb{Q}_{13}^\times)^3$$

By Proposition 1.5(iv) we have $(2, 13)_{13} = \zeta_3$. The local pairing at $p = 13$ is now given by the second matrix in (30).

Contribution at $p = 181$. We embed $L_1 = \mathbb{Q}(\zeta_3)$ in $\mathbb{Q}_{181}$ via $\zeta_3 \mapsto 48 + O(181)$. We find that $a_1 \equiv a_2 \equiv 1 \mod (\mathbb{Q}_{181}^\times)^3$ and hence the local pairing at $p = 181$ is trivial.

Adding together the local pairings at $p = 3$ and 13 gives the (global) Cassels-Tate pairing on $S^{(\widehat{\phi})}(E'/\mathbb{Q}) = \langle a_1, a_2\rangle \subset L_1^\times/(L_1^\times)^3$.

(30)

Local pairing at $p = 3$

	a_1	a_2
a_1	0	1
a_2	2	1

Local pairing at $p = 13$

	a_1	a_2
a_1	0	0
a_2	0	2

Global pairing

	a_1	a_2
a_1	0	1
a_2	2	0

Since the pairing is non-degenerate, it follows that $E(\mathbb{Q})$ has rank 0. Moreover the 3-primary parts of $Ш(E/\mathbb{Q})$ and $Ш(E'/\mathbb{Q})$ are 0 and $(\mathbb{Z}/3\mathbb{Z})^2$.

Example 4.2. Let E and E' be the 3-isogenous elliptic curves labelled 24060f1 and 24060f2 in Cremona's tables [Cre97].

$$E: \quad y^2 = x^3 + (x + 15)^2$$
$$E': \quad y^2 = x^3 - 3\,(x + 401/9)^2$$

The Galois action on $E[3]$ is of type $\mathbb{Z}/3\mathbb{Z}$-nonsplit. Indeed $E[3]$ is generated by

$$S = (0, 15) \quad \text{and} \quad T = (-90/(\theta + 2), -15\sqrt{-3}\theta/(\theta + 2))$$

where $\theta = \sqrt[3]{802}$. We set $\zeta_3 = (-1+\sqrt{-3})/2$. As in Section 2.3 we have fields $L_1 = \mathbb{Q}(\zeta_3)$, $L_2 = \mathbb{Q}(\theta)$ and $M = \mathbb{Q}(\zeta_3, \theta)$. A descent by 3-isogeny computes the Selmer groups

$$S^{(\phi)}(E/\mathbb{Q}) = \{1\} \subset (L_1^\times/(L_1^\times)^3)^{(1)}$$
$$S^{(\widehat{\phi})}(E'/\mathbb{Q}) = \langle 2,3,5\rangle \subset \mathbb{Q}^\times/(\mathbb{Q}^\times)^3.$$

This gives an upper bound of 2 for the rank of $E(\mathbb{Q})$. We seek to improve this bound by computing the Cassels-Tate pairing on $S^{(\widehat{\phi})}(E'/\mathbb{Q})$.

We start by lifting $a_1 = 2$, $a_2 = 3$ and $a_3 = 5$ globally to $H^1(\mathbb{Q}, E[3]) \cong H$, where $H \subset K^\times/(K^\times)^3 \times M^\times/(M^\times)^3$ is given by Theorem 2.9. We used the existing function in Magma (again this example is too small for the methods of Section 3 to be needed) to solve the norm equations $N_{L_2/K}(\xi) = a_i$ for $i = 1,2,3$, and then computed b_i with $(a_i, b_i) \in H$ using Theorem 2.11. Replacing b_i by a small representative for its coset in $M^\times/(M^\times)^3$ we obtain

$$\begin{aligned} b_1 &= \tfrac{1}{3}(5\zeta_3+5)\theta^2 + \tfrac{1}{3}(11\zeta_3-4)\theta + \tfrac{1}{3}(41\zeta_3+290)\\ b_2 &= \tfrac{5}{3}\zeta_3\theta^2 - \tfrac{7}{3}\zeta_3\theta - \tfrac{1}{3}(490\zeta_3+213)\\ b_3 &= \tfrac{1}{3}(7\zeta_3+34)\theta^2 + \tfrac{1}{3}(66\zeta_3+317)\theta + \tfrac{1}{3}(308\zeta_3+2991)\end{aligned}$$

It may be checked that these elements satisfy the conditions in Theorem 2.9.

The minimal discriminant of E is $-2^4\cdot 3^3\cdot 5^3\cdot 401$. We find that $v_{\mathfrak{p}}(b_i) \equiv 0 \pmod 3$ for all primes $\mathfrak{p}$ of M not dividing 30. The Cassels-Tate pairing is therefore a sum of local pairings at the primes $2,3,5$ and 401.

Contribution at $p = 2$. We have $\tan_S(-S) = -30 \equiv 2 \mod (\mathbb{Q}_2^\times)^3$. We compute

$$\begin{aligned} b_1/\tan_T(-S) &\equiv \zeta_3^2 \mod (\mathbb{Q}_2(\zeta_3,\theta)^\times)^3 \qquad & a_1 &\equiv 2 \mod (\mathbb{Q}_2^\times)^3\\ b_2 &\equiv 1 \mod (\mathbb{Q}_2(\zeta_3,\theta)^\times)^3 & a_2 &\equiv 1 \mod (\mathbb{Q}_2^\times)^3\\ b_3 &\equiv 1 \mod (\mathbb{Q}_2(\zeta_3,\theta)^\times)^3 & a_3 &\equiv 1 \mod (\mathbb{Q}_2^\times)^3\end{aligned}$$

The local pairing at 2 is therefore given by the first matrix in (31).

Contribution at $p = 3$. Let $P = (-5/2, 2.3 + 2.3^2 + 3^3 + O(3^8)) \in E(\mathbb{Q}_3)$. Then $\tan_S(P) \equiv 2 \equiv 5^{-1} \mod (\mathbb{Q}_3^\times)^3$ and $\tan_S(-S) \equiv 3 \mod (\mathbb{Q}_3^\times)^3$. We embed L_2 in $\mathbb{Q}_3$ via $\theta \mapsto 1 + 2.3 + 2.3^2 + O(3^4)$. We recall that $\mathbb{Q}_3(\zeta_3)^\times/(\mathbb{Q}_3(\zeta_3)^\times)^3$ has basis $\lambda, \eta_1, \eta_2, \eta_3$ where $\lambda = 1-\zeta_3$ and $\eta_i = 1-\lambda^i$. We compute

$$\begin{aligned} b_1/\tan_T(P) &\equiv \eta_1^2\eta_3 \mod (\mathbb{Q}_3(\zeta_3)^\times)^3 \qquad & a_1 &\equiv \eta_2^2\eta_3^2 \mod (\mathbb{Q}_3(\zeta_3)^\times)^3\\ b_2/\tan_T(-S) &\equiv \eta_1^2 \mod (\mathbb{Q}_3(\zeta_3)^\times)^3 & a_2 &\equiv \lambda^2\eta_1^2 \mod (\mathbb{Q}_3(\zeta_3)^\times)^3\\ b_3/\tan_T(-P) &\equiv \eta_1\eta_3^2 \mod (\mathbb{Q}_3(\zeta_3)^\times)^3 & a_3 &\equiv \eta_2\eta_3 \mod (\mathbb{Q}_3(\zeta_3)^\times)^3\end{aligned}$$

Using (9) to compute the Hilbert norm residue symbol, the local pairing at 3 is given by the second matrix in (31).

Contribution at $p = 5$. We have $\tan_S(-S) = -30 \equiv 5 \mod (\mathbb{Q}_5^\times)^3$. We embed L_2 in $\mathbb{Q}_5$ via $\theta \mapsto 3 + 3.5^2 + 5^4 + O(5^5)$ and compute

$$\begin{aligned} b_1 &\equiv \zeta_3 \mod (\mathbb{Q}_5(\zeta_3)^\times)^3 & \qquad a_1 &\equiv 1 \mod (\mathbb{Q}_5^\times)^3 \\ b_2 &\equiv 1 \mod (\mathbb{Q}_5(\zeta_3)^\times)^3 & a_2 &\equiv 1 \mod (\mathbb{Q}_5^\times)^3 \\ b_3/\tan_T(-S) &\equiv \zeta_3 \mod (\mathbb{Q}_5(\zeta_3)^\times)^3 & a_3 &\equiv 5 \mod (\mathbb{Q}_5^\times)^3 \end{aligned}$$

The local pairing at 5 is therefore given by the third matrix in (31).

Contribution at $p = 401$. Since $401 \equiv 2 \pmod 3$ we have $2, 3, 5 \in (\mathbb{Q}_{401}^\times)^3$, and so the local pairing at $p = 401$ is trivial.

Adding together the local pairings at $p = 2$, 3 and 5 gives the (global) Cassels-Tate pairing on $S^{(\widehat{\phi})}(E'/\mathbb{Q}) = \langle 2, 3, 5 \rangle \subset \mathbb{Q}^\times/(\mathbb{Q}^\times)^3$.

$$\begin{array}{cccc} p=2 & p=3 & p=5 & \text{Global pairing} \\ \begin{array}{c|ccc} & 2 & 3 & 5 \\ \hline 2 & 1 & 0 & 0 \\ 3 & 0 & 0 & 0 \\ 5 & 0 & 0 & 0 \end{array} & \begin{array}{c|ccc} & 2 & 3 & 5 \\ \hline 2 & 2 & 1 & 1 \\ 3 & 2 & 0 & 1 \\ 5 & 1 & 2 & 2 \end{array} & \begin{array}{c|ccc} & 2 & 3 & 5 \\ \hline 2 & 0 & 0 & 1 \\ 3 & 0 & 0 & 0 \\ 5 & 0 & 0 & 1 \end{array} & \begin{array}{c|ccc} & 2 & 3 & 5 \\ \hline 2 & 0 & 1 & 2 \\ 3 & 2 & 0 & 1 \\ 5 & 1 & 2 & 0 \end{array} \end{array} \tag{31}$$

This again shows that $\operatorname{rank} E(\mathbb{Q}) = 0$, and the 3-primary parts of $Ш(E/\mathbb{Q})$ and $Ш(E'/\mathbb{Q})$ are 0 and $(\mathbb{Z}/3\mathbb{Z})^2$.

As described in the introduction, Eroshkin found five examples of elliptic curves $E/\mathbb{Q}$ with torsion subgroup $\mathbb{Z}/3\mathbb{Z}$ and rank at least 13. We now consider the first of these examples. The other examples are similar, and are treated in detail in [vB15, Section 6.1].

Example 4.3. Let $E/\mathbb{Q}$ be the elliptic curve $y^2 + A_1xy + A_3y = x^3$ where $A_1 = 10154960719$ and $A_3 = -667980789518094581143919304 00$. The primes of bad reduction for E are those appearing in the following prime factorisations.

$$A_3 = -2^5 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 47 \cdot 53 \cdot 59 \cdot 61 \cdot 113,$$
$$A_1^3 - 27A_3 = 197 \cdot 317 \cdot 3313949 \cdot 2831657657 \cdot 4864617187.$$

The Galois action on $E[3]$ is of type $\mathbb{Z}/3\mathbb{Z}$-nonsplit. Indeed $E[3]$ is generated by $S = (0, 0)$ and $T = (3A_3/(\theta - A_1), A_3(\zeta_3\theta - A_1)/(\theta - A_1))$ where $\theta = \sqrt[3]{A_1^3 - 27A_3}$.

Let $\phi : E \to E'$ be the 3-isogeny with kernel generated by S. A descent by 3-isogeny [Fis03, Proposition 1.2] shows that

$$S^{(\widehat{\phi})}(E'/\mathbb{Q}) = \left\{ x \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^3 \;\middle|\; \begin{array}{rl} v_p(x) \equiv 0 \pmod 3 & \text{for all } p \nmid A_3 \\ x \in (\mathbb{Q}_p^\times)^3 & \text{for all } p \mid (A_1^3 - 27A_3) \end{array} \right\}.$$

Noting that only one of the prime factors of $A_1^3 - 27A_3$ is congruent to 1 mod 3, we find that $S^{(\widehat{\phi})}(E'/\mathbb{Q})$ is the 18-dimensional $\mathbb{F}_3$-vector space with basis

$$\begin{aligned} &2,\ 5,\ 11,\ 17,\ 31,\ 47,\ 53,\ 3^2 \cdot 7,\ 3 \cdot 13,\ 3 \cdot 19,\ 3 \cdot 23, \\ &\qquad 3 \cdot 29,\ 3 \cdot 37,\ 3 \cdot 41,\ 3 \cdot 43,\ 3 \cdot 59,\ 3^2 \cdot 61,\ 3 \cdot 113. \end{aligned} \tag{32}$$

By the analogue (for $n = 3$) of [Fis01, Theorem 1], or by Cassels' formula [Cas65], it follows that $S^{(\phi)}(E/\mathbb{Q})$ is trivial. This gives an upper bound of 17 for the rank of $E(\mathbb{Q})$. We improve this bound by computing the Cassels-Tate pairing on the subspace of $S^{(\widehat{\phi})}(E'/\mathbb{Q})$ generated by the first 5 basis elements in (32), say $a_1, \ldots, a_5$.

As in Section 2.3 we have fields $L_1 = \mathbb{Q}(\zeta_3)$, $L_2 = \mathbb{Q}(\theta)$ and $M = \mathbb{Q}(\zeta_3, \theta)$. In Example 3.10 we solved one of the norm equations $N_{L_2/\mathbb{Q}}(\xi) = a_i$. The other cases are similar. We then used Theorem 2.11 to compute $b_i \in M$ with $(a_i, b_i) \in H$, where H is as defined in Theorem 2.9. So that they could sensibly be recorded in the paper, we went to some effort to simplify the b_i, both by multiplying by elements of $(L_1^\times/(L_1^\times)^3)^{(1)}$ and by finding small representatives modulo cubes.

$$\begin{aligned}
b_1 &= 805066560009\theta^2 - 1176048899716052084841\theta \\
&\quad - 1493517820874464029585684724641 6\zeta_3 - 150360242425992097333546454397 03, \\
b_2 &= 147263630049\theta^2 - 79874874765966026529\theta \\
&\quad + 865718746776149738535029413404 0\zeta_3 - 843448017184092524574861092351 1, \\
b_3 &= 2188233726684\theta^2 - 4630953487853681932716\theta \\
&\quad + 3467612548935305606629608656909 1\zeta_3 + 608074663139870143285267664608 38, \\
b_4 &= 2863723866666\theta^2 - 1448511948608043607524\theta \\
&\quad - 5752827637628301759475611771290 1\zeta_3 - 389809285842424326276091039519 23, \\
b_5 &= 3326112908882\theta^2 + 1168159925437207764516\theta \\
&\quad - 6775164938020077609861275257863 9\zeta_3 + 714497681572792542789498367381 65
\end{aligned}$$

We find that $v_{\mathfrak{p}}(b_i) \equiv 0 \pmod 3$ for all primes $\mathfrak{p}$ of M not dividing a_i. Therefore only the bad primes for E contribute to the Cassels-Tate pairing. The local conditions used to compute $S^{(\widehat{\phi})}(E'/\mathbb{Q})$ show that its elements are locally trivial at the primes dividing $A_1^3 - 27A_3$. So we only need to compute the local pairings at the primes dividing A_3.

Let $P_1, \ldots, P_{13}$ be the known independent points of infinite order in $E(\mathbb{Q})$, as listed on Dujella's website [Duj17].

For the primes p with $p \equiv 1 \mod 3$ we find that $\tan_S(P_j)$ generates $\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^3$ where $j = 6, 4, 1, 1, 2, 2, 7$ for $p = 7, 13, 19, 31, 37, 43, 61$. Moreover $\tan_T(P_j)$ is a unit mod cubes at the primes dividing p. So we only need to consider the primes that additionally divide one of the a_i. The only such prime is 31. Embedding M in $\mathbb{Q}_{31}$ via $\zeta_3 \mapsto 5 + 14.31 + O(31^2)$ and $\theta \mapsto 1 - 2.31^2 + O(31^4)$, we compute

$$\begin{aligned} b_1 &\equiv 5^2 \mod (\mathbb{Q}_{31}^\times)^3 & a_1 &\equiv 1 \mod (\mathbb{Q}_{31}^\times)^3 \\ b_2/\tan_T(-P_1) &\equiv 1 \mod (\mathbb{Q}_{31}^\times)^3 & a_2 &\equiv 5 \mod (\mathbb{Q}_{31}^\times)^3 \\ b_3/\tan_T(-P_1) &\equiv 1 \mod (\mathbb{Q}_{31}^\times)^3 & a_3 &\equiv 5 \mod (\mathbb{Q}_{31}^\times)^3 \\ b_4/\tan_T(P_1) &\equiv 1 \mod (\mathbb{Q}_{31}^\times)^3 & a_4 &\equiv 5^2 \mod (\mathbb{Q}_{31}^\times)^3 \\ b_5/\tan_T(P_6) &\equiv 31^2 \mod (\mathbb{Q}_{31}^\times)^3 & a_5 &\equiv 31 \mod (\mathbb{Q}_{31}^\times)^3 \end{aligned}$$

This gives the local pairing at $p = 31$ as recorded below.

For the primes p with $p \equiv 2 \mod 3$ the group $\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^3$ is trivial. So we only need to consider those primes p that additionally divide one of $a_1, \ldots, a_5$. We find that $\tan_S(P_j) \equiv p \mod (\mathbb{Q}_p^\times)^3$ where $j = 5, 2, 1, 5$ for $p = 2, 5, 11, 17$. The unique embedding of L_2 in $\mathbb{Q}_p$ determines an embedding of M in $\mathbb{Q}_p(\zeta_3)$. Then $b_i/\tan_T(P_j)^{v_p(a_i)}$ takes the following values mod $(\mathbb{Q}_p(\zeta_3)^\times)^3$.

	$p=2$	$p=5$	$p=11$	$p=17$
$i=1$	1	1	ζ_3^2	$(\zeta_3+3)^2$
$i=2$	1	1	1	1
$i=3$	ζ_3	1	1	$(\zeta_3+3)^2$
$i=4$	ζ_3^2	1	ζ_3^2	1
$i=5$	ζ_3^2	ζ_3^2	ζ_3	ζ_3+3

This gives the local pairings at $p = 2, 5, 11, 17$ as recorded below.

Finally, when $p = 3$, we find that $\tan_S(P_8) \equiv 2 \mod (\mathbb{Q}_3^\times)^3$, whereas the elements $b_1, \ldots, b_5$ and $\tan_T(P_8)$ all belong to the subgroup of $\mathbb{Q}_3(\zeta_3)^\times/(\mathbb{Q}_3(\zeta_3)^\times)^3$ generated by $\eta_3 = 1 - (1 - \zeta_3)^3$. The local pairing at $p = 3$ is therefore trivial.

Adding together the local pairings gives the (global) Cassels-Tate pairing on the 5-dimensional subspace $\langle 2, 5, 11, 17, 31\rangle$ of $S^{(\widehat{\phi})}(E'/\mathbb{Q}) \subset \mathbb{Q}^\times/(\mathbb{Q}^\times)^3$. The fact we obtain an alternating matrix provides some check on our calculations.

Local pairing at $p = 2$

	2	5	11	17	31
2	0	0	0	0	0
5	0	0	0	0	0
11	2	0	0	0	0
17	1	0	0	0	0
31	1	0	0	0	0

Local pairing at $p = 5$

	2	5	11	17	31
2	0	0	0	0	0
5	0	0	0	0	0
11	0	0	0	0	0
17	0	0	0	0	0
31	0	2	0	0	0

Local pairing at $p = 11$

	2	5	11	17	31
2	0	0	1	0	0
5	0	0	0	0	0
11	0	0	0	0	0
17	0	0	1	0	0
31	0	0	2	0	0

Local pairing at $p = 17$

	2	5	11	17	31
2	0	0	0	2	0
5	0	0	0	0	0
11	0	0	0	2	0
17	0	0	0	0	0
31	0	0	0	1	0

Local pairing at $p = 31$

	2	5	11	17	31
2	0	0	0	0	2
5	0	0	0	0	0
11	0	0	0	0	0
17	0	0	0	0	0
31	0	1	1	2	0

Global pairing

	2	5	11	17	31
2	0	0	1	2	2
5	0	0	0	0	0
11	2	0	0	2	0
17	1	0	1	0	0
31	1	0	0	0	0

Since the Cassels-Tate pairing on this 5-dimensional subspace of $S^{(\widehat{\phi})}(E'/\mathbb{Q})$ has rank 4, it follows that rank $E(\mathbb{Q}) = 13$. Moreover the 3-primary parts of $Ш(E/\mathbb{Q})$ and $Ш(E'/\mathbb{Q})$ are 0 and $(\mathbb{Z}/3\mathbb{Z})^4$. The 18×18 matrix (still of rank 4) giving the Cassels-Tate pairing on all of $S^{(\widehat{\phi})}(E'/\mathbb{Q})$ is recorded in [vB15, Example 6.1.2].

References

[BCP97] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997.

[Cas59] J.W.S. Cassels. Arithmetic on curves of genus 1. I. On a conjecture of Selmer. *J. reine angew. Math.*, 202:52–99, 1959.

[Cas62] J.W.S. Cassels. Arithmetic on curves of genus 1. IV. Proof of the Hauptvermutung. *J. reine angew. Math.*, 211:95–112, 1962.

[Cas65] J.W.S. Cassels. Arithmetic on curves of genus 1. VIII. On conjectures of Birch and Swinnerton-Dyer. *J. reine angew. Math.*, 217:180–199, 1965.

[Cas97] J.W.S. Cassels. *An introduction to the geometry of numbers.* Classics in Mathematics. Springer-Verlag, Berlin, 1997. Corrected reprint of the 1971 edition.

[Cas98] J.W.S. Cassels. Second descents for elliptic curves. *J. reine angew. Math.*, 494:101–127, 1998.

[CF10] J.W.S. Cassels and A. Fröhlich, editors. *Algebraic number theory.* London Mathematical Society, London, 2010.

[CFO+08] 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.*, 615:121–155, 2008.

[CFO+15] J.E. Cremona, T.A. Fisher, C. O'Neil, D. Simon, and M. Stoll. Explicit n-descent on elliptic curves. III. Algorithms. *Math. Comp.*, 84(292):895–922, 2015.

[CM12] B. Creutz and R.L. Miller. Second isogeny descents and the Birch and Swinnerton-Dyer conjectural formula. *J. Algebra*, 372:673–701, 2012.

[Coh00] H. Cohen. *Advanced topics in computational number theory*, volume 193 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 2000.

[CR03] J.E. Cremona and D. Rusin. Efficient solution of rational conics. *Math. Comp.*, 72(243):1417–1441, 2003.

[Cre97] J.E. Cremona. *Algorithms for modular elliptic curves.* Cambridge University Press, Cambridge, 1997. See also `http://www.warwick.ac.uk/~masgaj/ftp/data/`.

[Cre99] J.E. Cremona. Reduction of binary cubic and quartic forms. *LMS J. Comput. Math.*, 2:64–94, 1999.

[Dav45] H. Davenport. The reduction of a binary cubic form. II. *J. London Math. Soc.*, 20:139–147, 1945.

[DeL02] M. DeLong. A formula for the Selmer group of a rational three-isogeny. *Acta Arith.*, 105(2):119–131, 2002.

[Don15] S. Donnelly. Algorithms for the Cassels-Tate pairing. preprint, 2015.

[Duj17] A. Dujella. High rank elliptic curves with prescribed torsion. `https://web.math.pmf.unizg.hr/~duje/tors/tors.html`, 2017.

[FG08] E.V. Flynn and C. Grattoni. Descent via isogeny on elliptic curves with large rational torsion subgroups. *J. Symbolic Comput.*, 43(4):293–303, 2008.

[Fis01] T.A. Fisher. Some examples of 5 and 7 descent for elliptic curves over $\mathbf{Q}$. *J. Eur. Math. Soc.*, 3(2):169–201, 2001.

[Fis03] T.A. Fisher. The Cassels-Tate pairing and the Platonic solids. *J. Number Theory*, 98(1):105–155, 2003.

[Fis08] T.A. Fisher. Some improvements to 4-descent on an elliptic curve. In *Algorithmic number theory*, volume 5011 of *Lecture Notes in Comput. Sci.*, pages 125–138. Springer, Berlin, 2008.

[Fis17] T.A. Fisher. Higher descents on an elliptic curve with a rational 2-torsion point. *Math. Comp.*, 86(307):2493–2518, 2017.

[FN14] T.A. Fisher and R.D. Newton. Computing the Cassels-Tate pairing on the 3-Selmer group of an elliptic curve. *Int. J. Number Theory*, 10(7):1881–1907, 2014.

[Gra03] G. Gras. *Class field theory.* Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2003.

[GS06] P. Gille and T. Szamuely. *Central simple algebras and Galois cohomology*, volume 101 of *Cambridge Studies in Advanced Mathematics.* Cambridge University Press, Cambridge, 2006.

[McC88] W.G. McCallum. On the Shafarevich-Tate group of the Jacobian of a quotient of the Fermat curve. *Invent. Math.*, 93(3):637–666, 1988.

[Mil06] J.S. Milne. *Arithmetic duality theorems*. BookSurge, LLC, Charleston, SC, second edition, 2006.

[MS13] R.L. Miller and M. Stoll. Explicit isogeny descent on elliptic curves. *Math. Comp.*, 82(281):513–529, 2013.

[PS99] B. Poonen and M. Stoll. The Cassels-Tate pairing on polarized abelian varieties. *Ann. of Math. (2)*, 150(3):1109–1149, 1999.

[SD13] H.P.F. Swinnerton-Dyer. 2^n-descent on elliptic curves for all n. *J. Lond. Math. Soc. (2)*, 87(3):707–723, 2013.

[Sel53] E.S. Selmer. Sufficient congruence conditions for the existence of rational points on certain cubic surfaces. *Math. Scand.*, 1:113–119, 1953.

[Ser79] J.-P. Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1979.

[Sil09] J.H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[Sim02] D. Simon. Solving norm equations in relative number fields using S-units. *Math. Comp.*, 71(239):1287–1305, 2002.

[SS04] E.F. Schaefer and M. Stoll. How to do a p-descent on an elliptic curve. *Trans. Amer. Math. Soc.*, 356(3):1209–1231, 2004.

[Top93] J. Top. Descent by 3-isogeny and 3-rank of quadratic fields. In *Advances in number theory (Kingston, ON, 1991)*, Oxford Sci. Publ., pages 303–317. Oxford Univ. Press, New York, 1993.

[vB15] M. van Beek. *Computing the Cassels-Tate Pairing*. PhD thesis, University of Cambridge, 2015. `https://www.repository.cam.ac.uk/handle/1810/252852`.

Canons Village 1, 46, Global edu-ro 145beon-gil, Daejeong-eup, Seogwipo-si, Jeju-do, 63644, Rep. of Korea
E-mail address: `moniquevanbeek@gmail.com`

University of Cambridge, DPMMS, Centre for Mathematical Sciences, Wilberforce Road, Cambridge CB3 0WB, UK
E-mail address: `T.A.Fisher@dpmms.cam.ac.uk`