HIGHER DESCENTS ON AN ELLIPTIC CURVE WITH A RATIONAL 2-TORSION POINT

TOM FISHER

Abstract. Let E be an elliptic curve over a number field K. Descent calculations on E can be used to find upper bounds for the rank of the Mordell-Weil group, and to compute covering curves that assist in the search for generators of this group. The general method of 4-descent, developed in the PhD theses of Siksek, Womack and Stamminger, has been implemented in Magma (when $K = \mathbb{Q}$) and works well for elliptic curves with sufficiently small discriminant. By extending work of Bremner and Cassels, we describe the improvements that can be made when E has a rational 2-torsion point. In particular, when E has full rational 2-torsion, we describe a method for 8-descent that is practical for elliptic curves $E/\mathbb{Q}$ with large discriminant.

1. Introduction

Let E be an elliptic curve over a number field K. For each integer $n \geq 2$ there is a short exact sequence of abelian groups

$$0 \to E(K)/nE(K) \to S^{(n)}(E/K) \to Ш(E/K)[n] \to 0.$$

The n-Selmer group $S^{(n)}(E/K)$ is finite and effectively computable. It gives information about both the Mordell-Weil group $E(K)$ and the Tate-Shafarevich group $Ш(E/K)$. The elements of $S^{(n)}(E/K)$ may be interpreted geometrically as n-coverings of E. An *n-covering* of E is a pair (C, π), where C/K is a smooth curve of genus one, and $\pi : C \to E$ is a morphism defined over K, that fits in a commutative diagram

$$\begin{tikzcd} C \arrow[d, "\cong"'] \arrow[dr, "\pi"] & \\ E \arrow[r, "{[n]}"'] & E \end{tikzcd}$$

where the vertical map is an isomorphism defined over $\overline{K}$. The Selmer group $S^{(n)}(E/K)$ consists of those n-coverings (C, π) that are everywhere locally soluble, i.e. $C(K_v) \neq \emptyset$ for all places v of K. The subset of those n-coverings with $C(K) \neq \emptyset$ form the image of $E(K)/nE(K)$. Thus if C/K is a counter-example to the Hasse Principle then it represents a non-trivial element of $Ш(E/K)$.

Date: 10th September 2015.

A *first descent* computes the group $S^{(n)}(E/K)$ and represents its elements as pairs (C,π). To compute the group $E(K)/nE(K)$, and hence the rank of $E(K)$, we must decide which of these n-coverings has a rational point, that is, a point with co-ordinates in K. Unfortunately there is no known algorithm guaranteed to determine whether a genus one curve C/K has a rational point. In practice one starts by searching for rational points of small height. If no points are found, this might be because C has no rational points, or because the rational points all have large height. We attempt to distinguish these two cases by a second descent.

Taking Galois cohomology of the short exact sequence

$$0 \longrightarrow E[n] \longrightarrow E[n^2] \longrightarrow E[n] \longrightarrow 0,$$

and restricting to Selmer groups, gives an exact sequence

$$E(K)[n] \longrightarrow S^{(n)}(E/K) \longrightarrow S^{(n^2)}(E/K) \xrightarrow{\alpha} S^{(n)}(E/K).$$

There are then inclusions

$$E(K)/nE(K) \subset \mathrm{Im}(\alpha) \subset S^{(n)}(E/K).$$

Moreover, the image of α is the kernel of the Cassels-Tate pairing

$$S^{(n)}(E/K) \times S^{(n)}(E/K) \to \mathbb{Q}/\mathbb{Z}.$$

If α maps (C_2,ν_2) to (C_1,π_1) then ν_2 factors via π_1 to give a commutative diagram

$$\begin{tikzcd}
C_2 \arrow[r, "\pi_2"] \arrow[d, "\cong"'] & C_1 \arrow[d, "\cong"'] \arrow[dr, "\pi_1"] & \\
E \arrow[r, "{[n]}"'] & E \arrow[r, "{[n]}"'] & E
\end{tikzcd}$$

where the vertical maps are isomorphisms defined over $\overline{K}$.

A *second descent* computes the fibre of α above (C_1,π_1) and represents its elements as pairs (C_2,π_2). If the fibre is empty then $C_1(K)=\emptyset$. Otherwise the fibre is a coset of the image of $S^{(n)}(E/K)$. We can then try searching for rational points on each of the genus one curves C_2. If we still do not find a rational point then a third descent may be attempted, and so on.

More generally, if $\phi : E \to E'$ is an isogeny of degree n, and $\widehat{\phi} : E' \to E$ is the dual isogeny, then there are exact sequences

$$0 \to E'(K)/\phi E(K) \to S^{(\phi)}(E/K) \to Ш(E/K)[\phi] \to 0 \tag{1}$$

and

$$E(K)[\phi] \longrightarrow S^{(\widehat{\phi})}(E'/K) \longrightarrow S^{(n)}(E'/K) \xrightarrow{\alpha} S^{(\phi)}(E/K).$$

Moreover, the image of α is the kernel of the Cassels-Tate pairing

$$S^{(\phi)}(E/K) \times S^{(\phi)}(E/K) \to \mathbb{Q}/\mathbb{Z}.$$

The terminology of first and second descents carries over as before.

In this paper we are concerned with $\phi : E \to E'$ an isogeny of degree 2. Thus our work applies to any elliptic curve with a rational 2-torsion point. The first descent in this case is descent by 2-isogeny. This is very well known; see for example [C2, §14] or [Sil, X.4.9]. The second descent is described in [BSD, §5] and [Cr], although in neither case do the authors claim any particular originality. This corresponds to a 2-descent on E. The starting point for our work is the paper of Bremner and Cassels [BC] that carries out the third and fourth descents for elliptic curves $E/\mathbb{Q}$ of the form $y^2 = x(x^2 - 4p)$, where p is a prime with $p \equiv 5 \pmod 8$. This corresponds to a 4-descent on E. As observed by Siksek [Sik, §4.6], their method can be applied more generally.

The general method of 4-descent, developed in [Sik], [MSS], [Wo], [St], (see also [F2]), requires that we compute the class group and units of a degree 4 extension of K. This has been implemented in Magma [BCP] (when $K = \mathbb{Q}$) and works well for elliptic curves with sufficiently small discriminant. In contrast the method of Bremner and Cassels (specific to elliptic curves with a rational 2-torsion point) requires no class group and unit calculations, beyond those for the field K itself. Instead the global part of the calculation requires that we solve conics over K, and over quadratic extensions of K.

We make the following improvements.

- We use the Cassels-Tate pairing to efficiently compute upper bounds for the rank. This was not required in [BC], since for the curves considered there, descent by 2-isogeny already shows that the rank is at most 1.
- We extend to a fifth descent, and in cases where E has full rational 2-torsion, also a sixth descent. The latter corresponds to 8-descent on E.
- We replace the problem of solving a conic over a quadratic extension of K, with that of solving a quadric surface over K. Taking $K = \mathbb{Q}$ the latter can be solved efficiently using an algorithm of Simon [S2].

As discussed further in Section 10, the motivation for our work came from the desire to find curves of large rank in certain families of elliptic curves over $\mathbb{Q}$, for example the family of elliptic curves with a given torsion subgroup (of even order), or the quadratic twists of a given elliptic curve with a rational 2-torsion point. The methods we describe can be used to quickly eliminate many curves which on the basis of (say) descent by 2-isogeny appear to be candidates for large rank, but which instead have large 2-primary part of Ш.

The paper is organised as follows. In the first three sections we let $\phi : E \to E'$ be any isogeny of prime degree p. In Section 2 we introduce the higher descent pairings we use to bound the rank of an elliptic curve. Then in Sections 3 and 4 we explain how these pairings are related to the Cassels-Tate pairing, and outline our methods for computing them. In Section 5 we give a short self-contained account of 4-descent on an elliptic curve with a rational 2-torsion point. This is then related to the work of Bremner and Cassels in Section 6. In the next two sections we describe our refinements for carrying out the fifth and sixth descents. In Section 9 we explain how to replace the conics over quadratic extensions by quadric surfaces. Finally in Section 10 we give some examples.

Our implementation of the methods described in this paper (in the case $K = \mathbb{Q}$) has been contributed to Magma (version 2.21) and is available via the function `TwoPowerIsogenyDescentRankBound`.

2. Higher descent pairings

Let $\phi : E \to E'$ be an isogeny of elliptic curves defined over a number field K. We suppose that $\deg \phi = p$ is a prime. By [Sil, X.4.7] there is an exact sequence

$$0 \longrightarrow E(K)[\phi] \longrightarrow E(K)[p] \longrightarrow E'(K)[\widehat{\phi}] \longrightarrow$$
$$\longrightarrow E'(K)/\phi E(K) \longrightarrow E(K)/pE(K) \longrightarrow E(K)/\widehat{\phi}E'(K) \longrightarrow 0.$$

Writing dim for the dimension of an $\mathbb{F}_p$-vector space, it follows that

$$\operatorname{rank} E(K) = \dim \frac{E'(K)}{\phi E(K)} + \dim \frac{E(K)}{\widehat{\phi} E'(K)} - \dim E(K)[\phi] - \dim E'(K)[\widehat{\phi}].$$

Let $S_1 = S^{(\phi)}(E/K)$ and $S'_1 = S^{(\widehat{\phi})}(E'/K)$ be the Selmer groups attached to the isogenies ϕ and $\widehat{\phi}$. More generally let $S_m \subset S_1$ be the image of $S^{(p^n)}(E'/K)$ if $m = 2n$ is even, and the image of $S^{(p^n \phi)}(E/K)$ if $m = 2n + 1$ is odd. The subspaces $S'_m \subset S'_1$ are defined in the same way, after swapping the roles of E and E'. There are inclusions of $\mathbb{F}_p$-vector spaces

$$\frac{E'(K)}{\phi E(K)} \subset \ldots \subset S_3 \subset S_2 \subset S_1 = S^{(\phi)}(E/K) \tag{2}$$

and

$$\frac{E(K)}{\widehat{\phi} E'(K)} \subset \ldots \subset S'_3 \subset S'_2 \subset S'_1 = S^{(\widehat{\phi})}(E'/K). \tag{3}$$

As we prove in Section 3, the Cassels-Tate pairing induces the following pairings of $\mathbb{F}_p$-vector spaces.

Theorem 2.1. *Let $m \geq 1$ be an integer.*

(i) *If m is odd then there are alternating pairings*

$$\Theta_m : S_m \times S_m \to \mathbb{F}_p \qquad \textit{and} \qquad \Theta'_m : S'_m \times S'_m \to \mathbb{F}_p$$

with kernels S_{m+1} and S'_{m+1}.

(ii) *If m is even then there is a pairing*

$$\Theta_m : S_m \times S'_m \to \mathbb{F}_p$$

with left kernel S_{m+1} and right kernel S'_{m+1}.

It is clear that each time we compute one of the pairings Θ_m or Θ'_m our upper bound for the rank of $E(K)$ either stays the same (if the pairing is identically zero) or decreases by an even integer. The following lemma is useful for comparing our bounds on the rank with those obtained by other methods.

Lemma 2.2. *The upper bound on the rank of $E(K)$ obtained by p^n-descent is*

$$\operatorname{rank} E(K) \leq \dim S_{2n-1} + \dim S'_{2n} - \dim E(K)[\phi] - \dim E'(K)[\widehat{\phi}].$$

Proof: From the commutative diagram with exact rows

$$\begin{tikzcd}
E'(K)[\widehat{\phi}] \arrow[r] \arrow[d, equal] & S^{(p^{n-1}\phi)}(E/K) \arrow[r] \arrow[d] & S^{(p^n)}(E/K) \arrow[r] \arrow[d, "\beta"] & S^{(\widehat{\phi})}(E'/K) \arrow[d, equal] \\
E'(K)[\widehat{\phi}] \arrow[r] & S^{(\phi)}(E/K) \arrow[r] & S^{(p)}(E/K) \arrow[r] & S^{(\widehat{\phi})}(E'/K)
\end{tikzcd}$$

we obtain an exact sequence

$$0 \longrightarrow E(K)[\phi] \longrightarrow E(K)[p] \longrightarrow E'(K)[\widehat{\phi}] \longrightarrow S_{2n-1} \longrightarrow \operatorname{Im}(\beta) \longrightarrow S'_{2n} \longrightarrow 0.$$

Therefore the upper bound obtained by p^n-descent,

$$\operatorname{rank} E(K) \leq \dim \operatorname{Im}(\beta) - \dim E(K)[p],$$

is the same as that in the statement of the lemma. □

The filtrations (2) and (3) also give information about the Tate-Shafarevich groups of E and E'. Let $Ш_m \subset Ш_1 = Ш(E/K)[\phi]$ be the image of $Ш(E'/K)[p^n]$ if $m = 2n$ is even, and the image of $Ш(E/K)[p^n\phi]$ if $m = 2n+1$ is odd. The subspaces $Ш'_m \subset Ш'_1 = Ш(E'/K)[\widehat{\phi}]$ are defined in the same way, after swapping the roles of E and E'. For each integer $m \geq 1$ we have short exact sequences

$$0 \longrightarrow E'(K)/\phi E(K) \longrightarrow S_m \longrightarrow Ш_m \longrightarrow 0$$

and

$$0 \longrightarrow E(K)/\widehat{\phi} E'(K) \longrightarrow S'_m \longrightarrow Ш'_m \longrightarrow 0.$$

In situations where we succeed in computing the rank of $E(K)$ we have $Ш_m = Ш'_m = 0$ for all m sufficiently large.

Remark 2.3. Suppose we have computed $Ш_m$ and $Ш'_m$ for all $m \geq 1$. Then from the exact sequences

$$0 \longrightarrow Ш(E'/K)[p^{n-1}\widehat{\phi}] \longrightarrow Ш(E'/K)[p^n] \longrightarrow Ш_{2n} \longrightarrow 0,$$
$$0 \longrightarrow Ш(E/K)[p^n] \longrightarrow Ш(E/K)[p^n\phi] \longrightarrow Ш_{2n+1} \longrightarrow 0,$$

and their analogues for $Ш'_m$, we can read off the orders of $Ш(E/K)[p^n]$ and $Ш(E'/K)[p^n]$ for all $n \geq 1$. This information determines the group structure of the p-primary parts of $Ш(E/K)$ and $Ш(E'/K)$.

In this paper we take $p = 2$. We show how to compute S_m and S'_m for $m \leq 5$, by a method whose global part only requires that we solve quadratic forms of ranks 3 and 4 over K. When E has full rational 2-torsion we also compute S'_6. By Lemma 2.2 the upper bound $\operatorname{rank} E(K) \leq \dim S_5 + \dim S'_6 - 2$ is then the same as that obtained by 8-descent on E.

3. The Cassels-Tate pairing

Let E be an elliptic curve over a number field K. The Cassels-Tate pairing is an alternating bilinear pairing

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

It has the following properties.

Theorem 3.1. *Let $\psi : C \to D$ be an isogeny of elliptic curves over K.*

(i) $\langle \psi x, y \rangle = \langle x, \widehat{\psi} y \rangle$ *for all* $x \in Ш(C/K)$ *and* $y \in Ш(D/K)$.

(ii) $x \in Ш(D/K)$ *belongs to the image of* $\psi : Ш(C/K) \to Ш(D/K)$ *if and only if* $\langle x, y \rangle = 0$ *for all* y *in the kernel of* $\widehat{\psi} : Ш(D/K) \to Ш(C/K)$.

Proof: For (i) see [C1, Section 2], and for (ii) see [F1, Theorem 3]. These results do *not* depend on finiteness of Ш. □

Proof of Theorem 2.1: We keep the notation of Section 2, except that the pairings Θ_m and Θ'_m will take values in $\frac{1}{p}\mathbb{Z}/\mathbb{Z}$ instead of $\mathbb{F}_p$. We make frequent implicit use of the exact sequence (1). In particular it makes sense to evaluate the Cassels-Tate pairing on Selmer group elements.

(i) Let $m = 2n + 1$. Let $\xi, \eta \in S_m$, and let $\xi_1, \eta_1 \in S^{(p^n\phi)}(E/K)$ with $\xi_1 \mapsto \xi$ and $\eta_1 \mapsto \eta$. We define $\Theta_m(\xi, \eta) = \langle \xi_1, \eta \rangle = \langle \xi, \eta_1 \rangle$. These last two expressions are equal by Theorem 3.1(i) with $\psi = p^n$. Therefore $\Theta_m(\xi, \eta)$ is independent of the choices of ξ_1 and η_1. By Theorem 3.1(ii) the kernel of Θ_m is

$$\{\xi \in S_m \mid \langle \xi, \eta_1 \rangle = 0 \text{ for all } \eta_1 \in S^{(p^n\phi)}(E/K)\} = S_{m+1}.$$

Now let $\psi = p^{n/2}$ or $p^{(n-1)/2}\phi$ according as n is even or odd. By Theorem 3.1(i) we have

$$\Theta_m(\xi, \xi) = \langle \xi_1, \widehat{\psi}\psi\xi_1 \rangle = \langle \psi\xi_1, \psi\xi_1 \rangle = 0.$$

Therefore Θ_m is alternating. The definition and properties of Θ'_m are obtained in the same way, after swapping the roles of E and E'.

(ii) Let $m = 2n$. Let $\xi \in S_m$ and $\eta \in S'_m$, and let $\xi_1 \in S^{(p^n)}(E'/K)$ and $\eta_1 \in S^{(p^n)}(E/K)$ with $\xi_1 \mapsto \xi$ and $\eta_1 \mapsto \eta$. We define $\Theta_m(\xi, \eta) = \langle \xi_1, \eta \rangle = \langle \xi, \eta_1 \rangle$. These last two expressions are equal by Theorem 3.1(i) with $\psi = p^{n-1}\phi$. Therefore $\Theta_m(\xi, \eta)$ is independent of the choices of ξ_1 and η_1. By Theorem 3.1(ii) the left kernel of Θ_m is

$$\{\xi \in S_m \mid \langle \xi, \eta_1 \rangle = 0 \text{ for all } \eta_1 \in S^{(p^n)}(E/K)\} = S_{m+1}.$$

Likewise the right kernel is S'_{m+1}. □

Next we describe a method for computing the Cassels-Tate pairing. Suppose that $E[\phi] \cong \mu_p$ and $E'[\widehat{\phi}] \cong \mathbb{Z}/p\mathbb{Z}$ as Galois modules. Then $H^1(K, E[\phi]) = K^\times/(K^\times)^p$ and $H^2(K, E[\phi]) = \mathrm{Br}(K)[p]$. If $\psi : E' \to F$ is an isogeny defined over K then from the short exact sequence

$$0 \to E[\phi] \to E[\psi\phi] \to E'[\psi] \to 0$$

we obtain a long exact sequence

$$\ldots \to K^\times/(K^\times)^p \to H^1(K, E[\psi\phi]) \to H^1(K, E'[\psi]) \to \mathrm{Br}(K)[p] \to \ldots \tag{4}$$

Let $x \in S^{(\psi)}(E'/K)$ and $y \in S^{(\widehat{\phi})}(E'/K)$. By the local-to-global principle for the Brauer group, x lifts to $x' \in H^1(K, E[\psi\phi])$. Let C and D_1 be the covering curves corresponding to x and x'. These fit in a commutative diagram

$$\begin{tikzcd}
D_1 \arrow[r, "\pi"] \arrow[d, "\cong"'] & C \arrow[d, "\cong"'] \arrow[dr] & \\
E \arrow[r, "\phi"] & E' \arrow[r, "\psi"] & F
\end{tikzcd}$$

where the vertical maps are isomorphisms defined over $\overline{K}$, but all other maps are morphisms defined over K.

Let T be a generator for $E'(K)[\widehat{\phi}] \cong \mathbb{Z}/p\mathbb{Z}$, and let $\mathfrak{b} \in \mathrm{Div}^0(C)$ correspond to T under the isomorphism of Galois modules $\mathrm{Pic}^0(C) \cong E'$. Since $T \in E'(K)$ and C is everywhere locally soluble, we may choose $\mathfrak{b}$ to be K-rational. Then there exists $f \in K(C)$ with $\mathrm{div}(f) = p\mathfrak{b}$. We say that f is a *pushout function.* If we scale f suitably then $\pi^* f = g^p$ for some $g \in K(D_1)$. In other words, if we identify $K(C)$ as a subfield of $K(D_1)$ via pull-back by π, then $K(D_1) = K(C)(\sqrt[p]{f})$.

For each place v of K there is a local pairing

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

given by the Weil pairing, cup product and the local invariant map. We identify $H^1(K_v, E[\phi]) = K_v^\times/(K_v^\times)^p$. The Cassels-Tate pairing is given by

$$\langle x, y \rangle = \sum_v (f(P_v), y)_v$$

where for each place v of K we choose a local point $P_v \in C(K_v)$ avoiding the zeros and poles of f. This is a sum over all places of K, but in fact there is no contribution from the primes outside a finite set of primes where C and f have bad reduction.

The Selmer group attached to ϕ is

$$S^{(\phi)}(E/K) = \{ \xi \in K^\times/(K^\times)^p \mid \xi \in \mathrm{Im}(\delta_{\phi,v}) \text{ for all places } v \}$$

where $\delta_{\phi,v} : E'(K_v) \to K_v^\times/(K_v^\times)^p$ is the local connecting map.

Let D_ξ be the covering of C that is K-birational to $\{f(P) = \xi z^p\} \subset C \times \mathbb{G}_m$. The Selmer set associated to the pair (C, f) is

$$\begin{aligned} S(C,f) &= \{\, \xi \in K^\times/(K^\times)^p \mid D_\xi(K_v) \neq \emptyset \text{ for all places } v \,\} \\ &= \{\, \xi \in K^\times/(K^\times)^p \mid \xi \equiv f(P_v) \mod \operatorname{Im}(\delta_{\phi,v}) \text{ for all places } v \,\}. \end{aligned}$$

The Selmer set tells us which twists of D_1 (as a covering of C) are everywhere locally soluble. If $\langle x, y \rangle \neq 0$ for some $y \in S^{(\widehat{\phi})}(E'/K)$ then there are no such twists, and the Selmer set $S(C, f)$ is empty. Otherwise $S(C, f)$ is a coset of $S^{(\phi)}(E/K)$ in $K^\times/(K^\times)^p$. If we have already computed the pairing (using the formula above) then we can solve for a coset representative by linear algebra over $\mathbb{F}_p$.

In this paper we take $p = 2$. Then $E[\phi] \cong E'[\widehat{\phi}] \cong \mathbb{Z}/2\mathbb{Z}$ and the local pairing (5) is the usual (i.e. quadratic) Hilbert norm residue symbol. As above, let C be the covering curve corresponding to $x \in S^{(\psi)}(E'/K)$. Suppose we know equations for C. Then by computing a pushout function f on C, and using it to compute the Cassels-Tate pairing, we can determine whether x lifts to $x' \in S^{(\psi\phi)}(E/K)$. If it does lift then the covering curve corresponding to x' is of the form D_ξ for some $\xi \in S(C, f)$. In particular we know equations for D_ξ. We can then replace ψ by $\psi\phi$, swap the roles of E and E', and repeat.

At each stage we have a basis for $S_m \subset K^\times/(K^\times)^2$, and for each basis element ξ, equations for an everywhere locally soluble 2^m-isogeny covering of E' that factors via the $\widehat{\phi}$-covering of E' corresponding to ξ. Using this data we can compute the pairing Θ_m in Theorem 2.1, and hence the subspace $S_{m+1} \subset S_m$. For the next iteration we need to compute an everywhere locally soluble 2^{m+1}-isogeny covering for each basis element of S_{m+1}. It often happens that these curves are degree-2 coverings of some of the curves we already found. However, in general a rather subtle iterative procedure is required. This is the subject of Section 4.

The two key issues we must address are the following.

- How do we find "nice" equations for the covering curves?
- How do we compute the pushout functions?

These questions are related, in that a good answer to the first question helps with answering the second. The proof that pushout functions exist uses the local-to-global principle for $\mathrm{Br}(K)[2]$. So one might expect that the second question comes down to solving conics over K. Indeed if K is a number field, then every element of $\mathrm{Br}(K)[2]$ can be represented by a conic. However this last statement is not true over arbitrary fields, and the proof over number fields itself uses the local-to-global principle for the Brauer group. So the best we can say for arbitrary m (see [SD]) is that the second question reduces to that of finding rational points on certain Brauer-Severi varieties.

4. An iterative procedure

In this section we describe the structure of our program for computing the subspaces S_m and S'_m. The bookkeeping is somewhat involved, but is needed to get around the fact that the formula we gave in Section 3, for computing the Cassels-Tate pairing, only applies when one of the arguments is killed by the p-isogeny ϕ or its dual $\widehat{\phi}$.

First we lighten our notation by writing

$$\operatorname{Sel}(m) = \begin{cases} S^{(p^n)}(E/K) \text{ or } S^{(p^n)}(E'/K) & \text{if } m = 2n, \\ S^{(p^n\phi)}(E/K) \text{ or } S^{(p^n\widehat{\phi})}(E'/K) & \text{if } m = 2n+1. \end{cases}$$

Which of the two groups we mean is often determined by the context. For example when we write

$$\ldots \longrightarrow \operatorname{Sel}(3) \longrightarrow \operatorname{Sel}(2) \longrightarrow \operatorname{Sel}(1)$$

this could either mean

$$\ldots \longrightarrow S^{(p\phi)}(E/K) \longrightarrow S^{(p)}(E'/K) \longrightarrow S^{(\phi)}(E/K)$$

or

$$\ldots \longrightarrow S^{(p\widehat{\phi})}(E'/K) \longrightarrow S^{(p)}(E/K) \longrightarrow S^{(\widehat{\phi})}(E'/K),$$

whereas

$$\operatorname{Sel}(1) \longrightarrow \operatorname{Sel}(2) \longrightarrow \operatorname{Sel}(3) \longrightarrow \ldots$$

could either mean

$$S^{(\phi)}(E/K) \longrightarrow S^{(p)}(E/K) \longrightarrow S^{(p\phi)}(E/K) \longrightarrow \ldots$$

or

$$S^{(\widehat{\phi})}(E'/K) \longrightarrow S^{(p)}(E'/K) \longrightarrow S^{(p\widehat{\phi})}(E'/K) \longrightarrow \ldots.$$

Let S_m be the image of $\operatorname{Sel}(m) \to \operatorname{Sel}(1)$. This $\mathbb{F}_p$-vector space was denoted S_m or S'_m in Section 2. We also write $\Theta_m : S_m \times S_m \to \mathbb{F}_p$ for the pairings in Theorem 2.1, even though some of the S_m and Θ_m should really be S'_m and Θ'_m. These abuses of notation are made to simplify the results in this section, and (with the exception of Lemma 8.1) will not be used elsewhere in the paper.

Let $\alpha_1, \beta_1 \in S_m$. Then $\Theta_m(\alpha_1, \beta_1) = \langle \alpha_m, \beta_1 \rangle$ where $\alpha_m \in \operatorname{Sel}(m)$ is any lift of α_1. In order to compute Θ_m, and hence by Theorem 2.1 the subspace S_{m+1}, we must describe how to lift α_1 to α_m. In the case $m = 3$ it is convenient to break this down into the following steps.

(i) Solve for $\alpha_2 \in \operatorname{Sel}(2)$ with $\alpha_2 \mapsto \alpha_1$.
(ii) Solve for $\xi \in S_1$ with $\langle \xi + \alpha_2, \eta \rangle = 0$ for all $\eta \in S_1$.
(iii) Solve for $\alpha_3 \in \operatorname{Sel}(3)$ with $\alpha_3 \mapsto \xi + \alpha_2$.

For general $m \geq 1$ we use the following algorithm.

Algorithm 4.1. INPUT: $\alpha_1 \in S_m$ and the pairings Θ_ℓ for $\ell < m$.
OUTPUT: $\alpha_m \in \mathrm{Sel}(m)$ with $\alpha_m \mapsto \alpha_1$.

```
if $m$ = 1 then return $\alpha_1$; end if
$k \leftarrow 1$
$t_1 \leftarrow m - 1$
while true do
   solve for $\alpha_{k+1} \in \mathrm{Sel}(k+1)$ with $\alpha_{k+1} \mapsto \alpha_k$
   $k \leftarrow k + 1$
   if $k = m$ then return $\alpha_m$; end if
   $t_k \leftarrow 1$
   while $t_{k-1} = t_k$ do
      $k \leftarrow k - 1$
      $t_k \leftarrow t_k + 1$
   end while
   $\ell \leftarrow t_k$
   solve for $\xi \in S_\ell$ with $\Theta_\ell(\xi, \eta) + \langle \alpha_{k+\ell-1}, \eta \rangle = 0$ for all $\eta \in S_\ell$.
   $\alpha_k \leftarrow \xi + \alpha_k$
end while
```

The next two lemmas are used to show that Algorithm 4.1 is correct.

Lemma 4.2. *Suppose* $\alpha_k \in \mathrm{Sel}(k)$ *lifts to* $\alpha_{k+\ell-1} \in \mathrm{Sel}(k+\ell-1)$*. Let* $\xi \in \mathrm{Sel}(1)$*. The following are equivalent.*

(i) $\langle \xi + \alpha_k, \beta \rangle = 0$ *for all* $\beta \in \mathrm{Sel}(\ell)$*,*

(ii) $\xi \in S_\ell$ *and* $\Theta_\ell(\xi, \eta) + \langle \alpha_{k+\ell-1}, \eta \rangle = 0$ *for all* $\eta \in S_\ell$*.*

Moreover, if $\alpha_k \mapsto \alpha_{k-1} \in \mathrm{Sel}(k-1)$ *and* $\langle \alpha_{k-1}, \beta \rangle = 0$ *for all* $\beta \in \mathrm{Sel}(\ell+1)$*, then (i) and (ii) hold for some* $\xi \in \mathrm{Sel}(1)$*.*

Proof: We make repeated use of Theorem 3.1. Since α_k lifts to $\mathrm{Sel}(k+\ell-1)$ we have $\langle \alpha_k, \beta \rangle = 0$ for all $\beta \in \mathrm{Sel}(\ell-1)$. Assuming (i) we have $\langle \xi, \beta \rangle = 0$ for all $\beta \in \mathrm{Sel}(\ell-1)$, and therefore $\xi \in S_\ell$. If $\beta \in \mathrm{Sel}(\ell)$ and $\eta \in S_\ell$ with $\beta \mapsto \eta$ then

$$\langle \xi + \alpha_k, \beta \rangle = \langle \xi, \beta \rangle + \langle \alpha_k, \beta \rangle = \Theta_\ell(\xi, \eta) + \langle \alpha_{k+\ell-1}, \eta \rangle.$$

This proves the equivalence of (i) and (ii). For the last part, Theorem 3.1(ii) shows there exists $\alpha_{k+\ell} \in \mathrm{Sel}(k+\ell)$ with $\alpha_{k+\ell} \mapsto \alpha_{k-1}$. Let $\widetilde{\alpha}_k \in \mathrm{Sel}(k)$ be the image of $\alpha_{k+\ell}$. By Theorem 3.1(i) we have $\langle \widetilde{\alpha}_k, \beta \rangle = 0$ for all $\beta \in \mathrm{Sel}(\ell)$. Since $\widetilde{\alpha}_k$ and α_k have the same image in $\mathrm{Sel}(k-1)$ we have $\widetilde{\alpha}_k = \xi + \alpha_k$ for some $\xi \in \mathrm{Sel}(1)$. This proves (i). □

Lemma 4.3. *At the start and end of the main loop in Algorithm 4.1, we have* $\alpha_k \mapsto \alpha_{k-1} \mapsto \ldots \mapsto \alpha_2 \mapsto \alpha_1$ *and*

$$\langle \alpha_j, \beta \rangle = 0 \text{ for all } \beta \in \mathrm{Sel}(t_j) \text{ and } 1 \leq j \leq k. \tag{6}$$

Proof: Initially we have $k = 1$ and $t_1 = m - 1$. Since α_1 is in S_m it satisfies $\langle \alpha_1, \beta \rangle = 0$ for all $\beta \in \mathrm{Sel}(m-1)$. At the end of each loop it suffices to prove (6) with $j = k$, since the cases $j < k$ carry over from the previous iteration. It is easy to check that each time we reach line 14, we have $k \geq 2$ and $t_{k-1} > t_k = \ell$. Moreover $\alpha_{k+\ell-1}$ is the element computed in line 5. By (6) from the previous iteration we have $\langle \alpha_{k-1}, \beta \rangle = 0$ for all $\beta \in \mathrm{Sel}(\ell+1)$. Lemma 4.2 shows that there exists $\xi \in S_\ell$ satisfying the condition on line 14, and that after modifying α_k on line 15, the new α_k satisfies (6) with $j = k$. □

As a special case of Lemma 4.3 we have $\langle \alpha_k, \beta \rangle = 0$ for all $\beta \in \mathrm{Sel}(t_k)$. Since $t_k \geq 1$, the element α_{k+1} in line 5 exists by Theorem 3.1(ii). This completes the proof that Algorithm 4.1 is correct.

The reader is encouraged to write out the sequence $t_1, \ldots, t_k$ at each stage of the algorithm (for some small values of m). It is not hard to show that if $m \geq 2$ then we start the main loop exactly 2^{m-2} times. This exponential growth does not concern us much, since (even in the case $p = 2$) the computation of pushout functions (required in lines 5 and 14, as explained in Section 3) is only practical for small values of m.

In practice we can often take $\xi = 0$ in line 14. In such cases we may already know $\alpha_{k+1} \in \mathrm{Sel}(k+1)$ with $\alpha_{k+1} \mapsto \alpha_k$. There is then no need to recompute α_{k+1} in line 5.

5. Computing 4-coverings

In this section we give a brief self-contained account of 4-descent on an elliptic curve with a rational 2-torsion point. As we discuss in Section 6, it is based on work of Bremner and Cassels [BC]. See the introduction for further references.

Let E be an elliptic curve over a field K with a rational 2-torsion point T, say

$$E : \quad y^2 = x(x^2 + ax + b) \qquad T = (0,0) \tag{7}$$

for some $a, b \in K$. The discriminant condition is $2b(a^2 - 4b) \neq 0$. Let $\phi : E \to E'$ be the 2-isogeny with kernel $\{0, T\}$ and let $\widehat{\phi} : E' \to E$ be the dual isogeny. The connecting map $\delta : E(K)/\widehat{\phi}E'(K) \to K^\times/(K^\times)^2$ is given by $P = (x,y) \mapsto x$ for all $P \neq 0, T$.

Suppose $P = (x, y) \in E(K)$ with $\delta(P) = \xi_1 \mod (K^\times)^2$. Then $x = \xi_1(s/t)^2$ and $y = \xi_1(rs/t^3)$ where

$$r^2 = \xi_1 s^4 + as^2t^2 + (b/\xi_1)t^4. \tag{8}$$

Parametrising a conic over K gives

$$(s^2 : t^2 : r) = (f(l,m) : g(l,m) : h(l,m)) \tag{9}$$

where f, g and h are binary quadratic forms. Then

$$f(l,m) = \xi_2 s^2 \quad \text{and} \quad g(l,m) = \xi_2 t^2 \tag{10}$$

for some $\xi_2 \in K^\times$. Parametrising each of these conics over K gives

$$\begin{aligned} (l : m : s) &= (p_1(c,d) : p_2(c,d) : p_3(c,d)) \\ (l : m : t) &= (q_1(\theta,\psi) : q_2(\theta,\psi) : q_3(\theta,\psi)) \end{aligned}$$

where the p_i and q_i are binary quadratic forms. Then

$$p_1(c,d) = \xi_3 q_1(\theta,\psi) \quad \text{and} \quad p_2(c,d) = \xi_3 q_2(\theta,\psi) \tag{11}$$

for some $\xi_3 \in K^\times$.

Let $L = K(\sqrt{b/\xi_1})$ and write $f(l,m) = \kappa(l - \varepsilon m)(l - \overline{\varepsilon} m)$ where $\kappa \in K$ and $\varepsilon, \overline{\varepsilon} \in L$. Then

$$\kappa(p_1 - \varepsilon p_2)(p_1 - \overline{\varepsilon} p_2) = \xi_2 p_3^2.$$

Since p_1 and p_2 are coprime in $K[c,d]$ it follows that

$$p_1(c,d) - \varepsilon p_2(c,d) = \xi_3 \alpha (c + \gamma d)^2$$

for some $\alpha, \gamma \in L$. Hence by (11) we have

$$q_1(\theta,\psi) - \varepsilon q_2(\theta,\psi) = \alpha(c + \gamma d)^2.$$

Parametrising a conic over L gives

$$(\theta : \psi : c + \gamma d) = (Q_1(\lambda,\mu) : Q_2(\lambda,\mu) : Q_3(\lambda,\mu))$$

where Q_1, Q_2 and Q_3 are binary quadratic forms. Then

$$\theta = \pi Q_1(\lambda,\mu) \quad \text{and} \quad \psi = \pi Q_2(\lambda,\mu) \tag{12}$$

for some $\pi \in L^\times$. Let $1, \beta$ be a basis for L over K. Writing $\lambda = x + \beta y$ and $\mu = u + \beta v$ we expand to give

$$\begin{aligned} \pi Q_1(\lambda,\mu) &= F_1(x,y,u,v) + \beta F_2(x,y,u,v) \\ \pi Q_2(\lambda,\mu) &= G_1(x,y,u,v) + \beta G_2(x,y,u,v) \end{aligned}$$

where F_1, F_2, G_1 and G_2 are quadratic forms with coefficients in K. Since $\theta, \psi \in K$ it follows by (12) that

$$F_2(x,y,u,v) = G_2(x,y,u,v) = 0. \tag{13}$$

Up to linear changes of co-ordinates defined over K, this quadric intersection depends only on the image of π in $L^\times / K^\times (L^\times)^2$, and hence only on $\xi_4 := N_{L/K}(\pi) \in K^\times/(K^\times)^2$. We may recover π from ξ_4 by solving a conic over K.

In the case K is a number field, there are at each stage ($j = 1, 2, 3, 4$) only finitely many $\xi_j \in K^\times/(K^\times)^2$ for which the corresponding covering curves are everywhere locally soluble. Thus each rational point on E lifts to one of only finitely many quadric intersections (13).

The equations (8), (10), (11), (13) define covering curves $C_1, \dots, C_4$ that fit in a commutative diagram

$$\begin{tikzcd}
C_4 \arrow[r, "\pi_4"] \arrow[d, "\cong"'] & C_3 \arrow[r, "\pi_3"] \arrow[d, "\cong"'] & C_2 \arrow[r, "\pi_2"] \arrow[d, "\cong"'] & C_1 \arrow[d, "\cong"'] \arrow[dr, "\pi_1"] & \\
E \arrow[r, "\phi"] & E' \arrow[r, "\widehat{\phi}"] & E \arrow[r, "\phi"] & E' \arrow[r, "\widehat{\phi}"] & E
\end{tikzcd} \tag{14}$$

where the vertical maps are isomorphisms defined over $\overline{K}$, and all other maps are morphisms of degree 2 defined over K. Explicitly the C_j have equations:

$$C_1 = \{r^2 = \xi_1 s^4 + a s^2 t^2 + (b/\xi_1) t^4\} = \{y^2 = f(l,m) g(l,m)\},$$

$$C_2 = \left\{ \begin{array}{l} f(l,m) = \xi_2 s^2 \\ g(l,m) = \xi_2 t^2 \end{array} \right\} = \{\xi_2 s^2 = f(q_1(\theta,\psi), q_2(\theta,\psi))\},$$

$$C_3 = \left\{ \begin{array}{l} p_1(c,d) = \xi_3 q_1(\theta,\psi) \\ p_2(c,d) = \xi_3 q_2(\theta,\psi) \end{array} \right\}, \qquad C_4 = \left\{ \begin{array}{l} F_2(x,y,u,v) = 0 \\ G_2(x,y,u,v) = 0 \end{array} \right\}.$$

Each of these curves is either a double cover of $\mathbb{P}^1$, or a quadric intersection in $\mathbb{P}^3$.

The pushout functions $f_j \in K(C_{j-1})$ are as follows. In each case C_j is K-birational to $\{f_j(P) = \xi_j z^2\} \subset C_{j-1} \times \mathbb{G}_m$. On $E = C_0$ the pushout function is $f_1 = x$. On C_1 the pushout function is $f_2 = f(l,m)/m^2$. We may solve by linear algebra for $\alpha, \beta, \gamma \in K$ so that

$$\alpha p_1(c,d) + \beta p_2(c,d) + \gamma p_3(c,d) = d^2.$$

Then C_2 has pushout function $f_3 = (\alpha q_1(\theta,\psi) + \beta q_2(\theta,\psi) + \gamma s)/\psi^2$. Likewise we may solve for $r, s, t \in L$ so that

$$r Q_1(\lambda,\mu) + s Q_2(\lambda,\mu) + t Q_3(\lambda,\mu) = \mu^2.$$

Let $\ell = r\theta + s\psi + t(c + \gamma d)$ and $\overline{\ell} = \overline{r}\theta + \overline{s}\psi + \overline{t}(c + \overline{\gamma} d)$, where the bars denotes the action of $\mathrm{Gal}(L/K)$. Then C_3 has pushout function $f_4 = \ell\overline{\ell}/\psi^2$.

The formulae in this section can be used to compute S_m and S'_m for $m \leq 4$, by a method whose global part only requires that we solve conics over K, and over quadratic extensions of K. In Section 7 we extend to the case $m = 5$, and in Section 9 we replace the conics over quadratic extensions by quadric surfaces.

6. Comparison with work of Bremner and Cassels

The method used by Bremner and Cassels [BC] to find rational points of large height on $E' : y^2 = x(x^2 + p)$, for p a prime with $p \equiv 5 \pmod 8$, is a special case of the method outlined in Section 5. We now explain the relationship. We have tried to keep their notation, although in one place we switched a, b to s, t, since we already used a, b in (7).

We start with the elliptic curve $E : y^2 = x(x^2 - 4p)$ over $K = \mathbb{Q}$. The first stage of the argument in [BC] implicitly switches to this 2-isogenous curve. Then taking $\xi_1 = p$ in (8) gives $r^2 = ps^4 - 4t^4$. Since $p \equiv 5 \pmod 8$ we can write $p = u^2 + 4v^2$ where u, v are odd integers with $v \equiv 1 \pmod 4$. A suitable parametrisation (9) is now given by

$$\begin{aligned} f(l,m) &= l^2 + m^2 \\ g(l,m) &= v(l^2 - m^2) + ulm \\ h(l,m) &= u(l^2 - m^2) - 4vlm. \end{aligned}$$

A local argument suggests taking $\xi_2 = 1$. Then (10) becomes $l^2 + m^2 = s^2$ and $v(l^2-m^2)+ulm = t^2$. The first of these conics is parametrised by $p_1(c,d) = c^2-d^2$, $p_2(c,d) = 2cd$, $p_3(c,d) = c^2+d^2$, and the second by $q_1(\theta,\psi), q_2(\theta,\psi), q_3(\theta,\psi)$ (say). If the q_i are suitably scaled then by local considerations it suffices to take $\xi_3 = 1$. Then (11) becomes $q_1(\theta,\psi) = c^2 - d^2$ and $q_2(\theta,\psi) = 2cd$, equivalently

$$q_1(\theta,\psi) + iq_2(\theta,\psi) = (c + id)^2. \tag{15}$$

Parametrising a conic over $L = \mathbb{Q}(i)$ gives

$$(\theta : \psi : c + id) = (Q_1(\lambda,\mu) : Q_2(\lambda,\mu) : Q_3(\lambda,\mu)).$$

Then $\theta = \pi Q_1(\lambda,\mu)$ and $\psi = \pi Q_2(\lambda,\mu)$ for some $\pi \in \mathbb{Q}(i)$. A suitable value of π is determined by local considerations. Finally the procedure described in Section 5 (with $\beta = i$) furnishes a quadric intersection

$$F_2(x,y,u,v) = G_2(x,y,u,v) = 0. \tag{16}$$

defined over $\mathbb{Q}$.

In summary, the examples of Bremner and Cassels are special in that, (i) some of the conics can be parametrised "for free" and so do not appear explicitly in their argument, (ii) the conics we do have to solve are defined over either $\mathbb{Q}$ or $\mathbb{Q}(i)$, and (iii) by local considerations only one choice of $\xi_j \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ need be considered at each stage ($j = 1, 2, 3, 4$).

Bremner and Cassels give a worked example in the case $p = 877$. We record a few brief details. Firstly they take $u = 29$, $v = -3$ and

$$\begin{aligned} q_1(\theta,\psi) &= -3\theta^2 + 6\theta\psi - 2\psi^2 \\ q_2(\theta,\psi) &= -7\theta^2 - 4\theta\psi - \psi^2 \\ q_3(\theta,\psi) &= 27\theta^2 - 11\theta\psi - 7\psi^2. \end{aligned}$$

Then the conic (15) is parametrised by

$$\begin{aligned} Q_1(\lambda,\mu) &= (-4 - 3i)\lambda^2 + (10 - 22i)\lambda\mu + (29 + 6i)\mu^2 \\ Q_2(\lambda,\mu) &= (-1 + 2i)\lambda^2 + (-16 - 6i)\lambda\mu + (6 - 29i)\mu^2 \\ Q_3(\lambda,\mu) &= (-15 + 6i)\lambda^2 + (-46 - 70i)\lambda\mu + (76 - 75i)\mu^2. \end{aligned}$$

By local considerations it suffices to take $\pi = 1 + i$. This leads to a quadric intersection (16). Minimising and reducing, as described in [CFS], suggests making the transformation

$$\begin{aligned} x &= x_1 + 2x_2 - 4x_3 - 6x_4, & u &= -x_1 - 2x_3 + 2x_4, \\ y &= 2x_1 - x_2 + 6x_3 - 4x_4, & v &= x_2 - 2x_3 - 2x_4 \end{aligned} \tag{17}$$

whereupon (16) becomes

$$\begin{aligned} x_1x_2 + x_1x_3 + x_1x_4 - x_2x_3 + x_2x_4 + x_3^2 - 2x_3x_4 - x_4^2 &= 0 \\ x_1^2 - 4x_1x_2 + 3x_1x_3 + x_1x_4 - x_2^2 - x_2x_3 + 3x_2x_4 + 4x_3x_4 &= 0. \end{aligned} \tag{18}$$

A little searching finds the rational points

$$(x_1 : x_2 : x_3 : x_4) = (-2 : 57 : 85 : 16),\ (57 : 2 : -16 : 85).$$

We substitute in (17) to recover the solutions

$$(x : y : u : v) = (324 : -385 : 136 : 145),\ (385 : 324 : -145 : 136)$$

found by Bremner and Cassels. These points map down to the same point of infinite order $P = (x_P, y_P)$ on $E(\mathbb{Q})$. The co-ordinates of P are

$$\begin{aligned} x_P &= -2922141486802704912\,36/4612160965^2 \\ y_P &= 20949922565086352416107761007588/4612160965^3. \end{aligned}$$

The point recorded in [BC] is the image of P under the 2-isogeny $\phi : E \to E'$, and accordingly has (canonical) height twice that of P.

The general implementation of 4-descent in Magma (due to Womack [Wo] and Watkins) is able to find the 4-covering (18) in a couple of seconds. However the method it uses involves computing the class group and units of a degree 4 number field; in this case $\mathbb{Q}(\sqrt{6 - 29i})$. In contrast the method of Bremner and Cassels only requires that we solve conics over $\mathbb{Q}$ and $\mathbb{Q}(i)$.

7. Computing pushout forms

Let $C \subset \mathbb{P}^3$ be a non-singular quadric intersection. The 4 singular fibres in the pencil of quadrics defining C are cones over conics $\Gamma_1, \ldots, \Gamma_4$. Projecting from the vertex of each cone gives a degree-2 morphism $\nu_i : C \to \Gamma_i$ with fibre $\mathfrak{a}_i$. By considering the tangent plane at a smooth point on the cone over Γ_i we see that $2\mathfrak{a}_i \sim H$ where H is the hyperplane section on C. Therefore the differences $\mathfrak{a}_i - \mathfrak{a}_j$ represent elements of order 2 in $\mathrm{Pic}^0(C)$.

Let E be the Jacobian of C. By the previous paragraph $\{\Gamma_1, \ldots, \Gamma_4\}$ is a torsor under $E[2]$. In particular, there is a Galois equivariant bijection between $E[2] \backslash \{0\}$ and the partitions of the singular fibres into 2 sets of 2. We are interested in elliptic curves with a rational 2-torsion point. We therefore fix $0 \neq T \in E(K)[2]$, and order the Γ_i so that T corresponds to the partition $(\Gamma_1, \Gamma_2; \Gamma_3, \Gamma_4)$. In other words $\mathfrak{a}_1 - \mathfrak{a}_2 \sim \mathfrak{a}_3 - \mathfrak{a}_4$ represents the class of T in $\mathrm{Pic}^0(C) \cong E$.

Let $\rho : \mathrm{Gal}(\overline{K}/K) \to S_4$ describe the action of Galois on the Γ_i. Since T is K-rational we have $\mathrm{Im}(\rho) \subset \langle (1324), (12) \rangle$. We now make the assumption that

$$\mathrm{Im}(\rho) \subset \langle (12), (34) \rangle. \tag{19}$$

We distinguish two possibilities.

- (split case) The conics Γ_1 and Γ_2 are defined over K.
- (non-split case) The conics Γ_1 and Γ_2 are defined over a quadratic extension L/K, and are $\mathrm{Gal}(L/K)$-conjugates.

Let $\Gamma = \Gamma_1 \times \Gamma_2$, respectively $\mathrm{Res}_{L/K}\Gamma_1$. If C/K is everywhere locally soluble then by the Hasse Principle for conics, we have $\Gamma(K) \neq \emptyset$. A point $P \in \Gamma(K)$ corresponds to a pair of points $P_1 \in \Gamma_1$ and $P_2 \in \Gamma_2$ which are either defined over K or are $\mathrm{Gal}(L/K)$-conjugates. The tangent planes to P_1 and P_2, as points on the cones over Γ_1 and Γ_2, are defined by linear forms ℓ_1 and ℓ_2. In the split case these are defined over K. In the non-split case we may arrange that they are $\mathrm{Gal}(L/K)$-conjugates.

We say that a quadratic form $f \in K[x_1, \ldots, x_4]$ is a *pushout form* on C if $f/x_1^2 \in K(C)$ is a pushout function, i.e. $\mathrm{div}(f/x_1^2) = 2\mathfrak{b}$ for some divisor $\mathfrak{b}$ representing the class of T in $\mathrm{Pic}^0(C) \cong E$.

Lemma 7.1. *$f = \ell_1\ell_2 \in K[x_1, \ldots, x_4]$ is a pushout form on C.*

Proof: We have $\mathrm{div}(f/x_1^2) = 2(\mathfrak{a}_1 + \mathfrak{a}_2 - H)$ and $\mathfrak{a}_1 + \mathfrak{a}_2 - H \sim \mathfrak{a}_1 - \mathfrak{a}_2$. □

Let $f = \ell_1\ell_2$ as above and let $\pi : D \to C$ be the degree-2 covering with $K(D) = K(C)(\sqrt{f})$. In other words D is the smooth curve of genus one K-birational to $\{f(P) = z^2\} \subset C \times \mathbb{G}_m$. We now show how to write D as a quadric intersection with hyperplane section $\pi^*\mathfrak{a}_1 \sim \pi^*\mathfrak{a}_2$.

We suppose we are in the non-split case, the split case being similar. The conic Γ_1 is defined by a quadratic form $q \in L[X, Y, Z]$, and the cone above Γ_1 has equation $q(m_1, m_2, m_3) = 0$ for some linear forms $m_1, m_2, m_3 \in L[x_1, \ldots, x_4]$. Since we have found an L-rational point on Γ_1, we may parametrise this conic, say

$$(X : Y : Z) = (Q_1(\lambda, \mu) : Q_2(\lambda, \mu) : Q_3(\lambda, \mu))$$

where Q_1, Q_2 and Q_3 are binary quadratic forms defined over L. If $L = K(\beta)$ this gives equations

$$m_i(x_1, \ldots, x_4) = Q_i(x + \beta y, u + \beta v) \tag{20}$$

for $i = 1, 2, 3$. Writing each side in terms of the basis $1, \beta$ for L over K we get 6 equations with coefficients in K. The left hand sides are linear forms in $x_1, \ldots, x_4$ and the right hand sides are quadratic forms in x, y, u, v. By taking linear combinations we obtain equations

$$F(x, y, u, v) = G(x, y, u, v) = 0$$

and $x_i = r_i(x, y, u, v)$ for $i = 1, \ldots, 4$.

Theorem 7.2. *The curve $D = \{F = G = 0\} \subset \mathbb{P}^3$ is a non-singular quadric intersection, and the map $\pi = (r_1 : \ldots : r_4) : D \to C$ is a morphism of degree 2. Moreover D has hyperplane section $\pi^*\mathfrak{a}_1 \sim \pi^*\mathfrak{a}_2$.*

Proof: For the proof we are free to extend our field K and to make changes of co-ordinates. So we may suppose

$$C = \left\{ \begin{array}{c} f(l,m) = s^2 \\ g(l,m) = t^2 \end{array} \right\} \subset \mathbb{P}^3. \tag{21}$$

We parametrise the conics $f(l,m) = s^2$ and $g(l,m) = t^2$ as

$$\begin{aligned} (l : m : s) &= (p_1(c,d) : p_2(c,d) : p_3(c,d)), \\ (l : m : t) &= (q_1(\theta,\psi) : q_2(\theta,\psi) : q_3(\theta,\psi)). \end{aligned} \tag{22}$$

Then by the above construction (in the split case) we have

$$D = \left\{ \begin{array}{c} p_1(c,d) = q_1(\theta,\psi) \\ p_2(c,d) = q_2(\theta,\psi) \end{array} \right\} \subset \mathbb{P}^3. \tag{23}$$

If a quadric intersection is given by 4×4 symmetric matrices A and B, then we may associate to it the binary quartic $F(x,y) = \det(Ax + By)$. To prove that the quadric intersection is non-singular it suffices to show that F has distinct roots in $\mathbb{P}^1$. We write Δ for the discriminant of a binary quadratic form. Since the linear combinations of p_1 and p_2 that are perfect squares can be computed from the roots of f, we have

$$\begin{aligned} \Delta(mp_1 - lp_2) &= \kappa f(l,m) \\ \Delta(mq_1 - lq_2) &= \kappa' g(l,m) \end{aligned}$$

for some $\kappa, \kappa' \in K^\times$. Therefore the binary quartic associated to D is a scalar multiple of $f(l,m)g(l,m)$. Since C defined by (21) is non-singular, it now follows that D defined by (23) is non-singular.

The morphism $\pi : D \to C$ is given by

$$(l : m : s : t) = (p_1(c,d) : p_2(c,d) : p_3(c,d) : q_3(\theta,\psi)).$$

It is easy to see that π has degree 2 with fibres of the form $\{(c : d : \theta : \psi), (c : d : -\theta : -\psi)\}$. Moreover if $\mathfrak{a}_1 = (l : m : s : t) + (l : m : s : -t)$ then $\pi^*\mathfrak{a}_1$ is the hyperplane section given by solving the first equation in (22) for $(c : d)$. Likewise if $\mathfrak{a}_2 = (l : m : s : t) + (l : m : -s : t)$ then $\pi^*\mathfrak{a}_2$ is the hyperplane section given by solving the second equation in (22) for $(\theta : \psi)$. □

Let $\phi : E \to E'$ be the 2-isogeny with kernel $\{0, T\}$. Let $\widehat{\phi} : E' \to E$ be the dual isogeny, say with kernel $\{0, T'\}$.

Theorem 7.3. *The degree-2 covering $\pi : D \to C$ constructed in Theorem 7.2 is a $\widehat{\phi}$-covering, i.e. there is a commutative diagram*

$$\begin{tikzcd}
D \arrow[r, "\pi"] \arrow[d, "\cong"'] & C \arrow[d, "\cong"'] \\
E' \arrow[r, "\widehat{\phi}"] & E
\end{tikzcd}$$

where the vertical maps are isomorphisms defined over $\overline{K}$.

Proof: We give details in the non-split case. Recall that Γ_1 is parametrised by binary quadratic forms Q_1, Q_2, Q_3. We solve for r, s, t so that $rQ_1(\lambda, \mu) + sQ_2(\lambda, \mu) + tQ_3(\lambda, \mu) = \mu^2$. We then take $f = \ell_1 \ell_2$ where $\ell_1 = rm_1 + sm_2 + tm_3$ and ℓ_2 is its $\mathrm{Gal}(L/K)$-conjugate. By (20) we have

$$\ell_1(x_1, \ldots, x_4) = (u + \beta v)^2$$
$$\ell_2(x_1, \ldots, x_4) = (u + \overline{\beta} v)^2$$

Then $t = (u + \beta v)(u + \overline{\beta} v) \in K[x, y, u, v]$ is a quadratic form with

$$f(r_1, \ldots, r_4) \equiv t^2 \mod I(D). \tag{24}$$

Therefore $\pi^*(f/x_1^2)$ is the square of a rational function in $K(D)$. Since f is a pushout form (corresponding to T), the result follows. □

The pushout form $f \in K[x_1, \ldots, x_4]$ and quadric intersection $D \subset \mathbb{P}^3$ were constructed from a pair of points on Γ_1 and Γ_2. We may equally construct a pushout form $f^\dagger \in K[x_1, \ldots, x_4]$ and quadric intersection $D^\dagger \subset \mathbb{P}^3$ from a pair of points on Γ_3 and Γ_4. We have $\mathrm{div}(f/x_1^2) = 2\mathfrak{b}$ and $\mathrm{div}(f^\dagger/x_1^2) = 2\mathfrak{b}^\dagger$ with $\mathfrak{b} \sim \mathfrak{b}^\dagger$ representing the class of T in $\mathrm{Pic}^0(C) \cong E$. Therefore $f/f^\dagger = ch^2$ for some $c \in K$ and $h \in K(C)$. Scaling f and $f^\dagger$ appropriately we may assume $c = 1$. The quadric intersections D and $D^\dagger$ are now isomorphic as curves (indeed as $\widehat{\phi}$-coverings of C) but have different hyperplane sections H and $H^\dagger$.

Theorem 7.4. *The divisor $H - H^\dagger$ represents the class of T' in $\mathrm{Pic}^0(D) \cong E'$.*

Proof: Let $\pi : D \to C$ be the degree-2 covering as above. By Theorem 7.2 we have

$$H \sim \pi^*\mathfrak{a}_1 \sim \pi^*\mathfrak{a}_2 \quad \text{and} \quad H^\dagger \sim \pi^*\mathfrak{a}_3 \sim \pi^*\mathfrak{a}_4.$$

Let $E[2] = \{0, T, S_1, S_2\}$ with $\mathfrak{a}_1 - \mathfrak{a}_3$ representing the class of S_1 in $\mathrm{Pic}^0(C) \cong E$. By Theorem 7.3 there is a commutative diagram

$$\begin{tikzcd}
\mathrm{Pic}^0(C) \arrow[r, "\pi^*"] \arrow[d, "\cong"'] & \mathrm{Pic}^0(D) \arrow[d, "\cong"'] \\
E \arrow[r, "\phi"] & E'
\end{tikzcd}$$

Then $H - H^\dagger \sim \pi^*(\mathfrak{a}_1 - \mathfrak{a}_3)$ represents the class of $\phi S_1 = T'$ in $\mathrm{Pic}^0(D) \cong E'$. □

We will need explicit equations for the isomorphism between the quadric intersections D and $D^\dagger$. We compute these as follows. The 2-uple embedding $D \subset \mathbb{P}^7$ is defined by 8 quadratic forms, chosen so that together with the equations for D they give a basis for the space of all quadratic forms on $\mathbb{P}^3$. Since $2H \sim 2H^\dagger$ the 2-uple embeddings of D and $D^\dagger$ are related by a change of co-ordinates on $\mathbb{P}^7$. We now explain how to choose 8 quadratic forms for D in a particular way, so that when we repeat for $D^\dagger$, the change of co-ordinates needed on $\mathbb{P}^7$ is trivial.

Since $\pi : D \to C$ is a degree-2 Galois covering, the 8 quadratic forms may be given as 4 "even" forms $r_1, \ldots, r_4$ and 4 "odd" forms $s_1, \ldots, s_4$. The even forms $r_1, \ldots, r_4$ are those giving the morphism $\pi : D \to C$ in Theorem 7.2. The quadratic form t computed in (24) is an example of an odd form. Further odd forms may be computed as follows.

Once we have found one pushout form f on C, it is easy to find more by computing Riemann-Roch spaces. (With the refinements in Section 9 it turns out that we have this information anyway.) Let f_i be another pushout form, scaled so that $ff_i \equiv h_i^2 \mod I(C)$ for some quadratic form h_i. Since $\pi^*(f_i/x_1^2)$ is a square in $K(D)$, and D is projectively normal, there is a quadratic form s_i such that

$$f_i(r_1, \ldots, r_4) \equiv s_i^2 \mod I(D). \tag{25}$$

It follows by (24) and (25) that if we scale the forms s_i appropriately then

$$h_i(r_1, \ldots, r_4) \equiv s_i t \mod I(D).$$

We use this last equation to solve for s_i by linear algebra. Repeating for pushout forms $f_1, \ldots, f_4$ gives odd forms $s_1, \ldots, s_4$ are required.

We now have quadric intersections $D \subset \mathbb{P}^3$ and $D^\dagger \subset \mathbb{P}^3$ and an isomorphism between their 2-uple embeddings, given by a change of co-ordinates on $\mathbb{P}^7$. We say that D and $D^\dagger$ are *companion quadric intersections.* Theorem 7.4 shows that, under this change of co-ordinates, the square of a linear form on $D^\dagger$ corresponds to a pushout form on D. This is exactly what we need for the next stage of the descent.

The results of this section may be applied as follows. Let C_3 be the $2\widehat{\phi}$-covering of E considered in Section 5. Then C_3 satisfies the Galois hypothesis (19). So we may construct a ϕ-covering of C_3 (and hence a 4-covering over E) in the form of companion quadric intersections C_4 and $C_4^\dagger$. The construction of C_4 was already described in Section 5. However the advantage of also computing $C_4^\dagger$, is that the square of a linear form on $C_4^\dagger$ corresponds to a pushout form on C_4. We can then compute the pairing $\Theta_4 : S_4 \times S_4' \to \mathbb{F}_2$ in Theorem 2.1. In conclusion, we can compute S_m and S_m' for $m \leq 5$ by a method whose global part only involves solving conics over K, and over quadratic extensions of K.

8. Extension to 8-descent

Suppose that E has full rational 2-torsion, say

$$E(K)[2] = \{0, T_1, T_2, T_3\}.$$

Let $C \subset \mathbb{P}^3$ be an everywhere locally soluble 4-covering of E. Repeating the method of Section 7 three times, gives pushout forms $f_i \in K[x_1, \ldots, x_4]$ on C with $\operatorname{div}(f_i/x_1^2) = 2\mathfrak{b}_i$ where $\mathfrak{b}_i$ represents the class of T_i in $\operatorname{Pic}^0(C) \cong E$. The rational functions f_i/x_1^2 are now exactly those required to compute the Cassels-Tate pairing

$$S^{(4)}(E/K) \times S^{(2)}(E/K) \to \mathbb{Q}/\mathbb{Z}$$

following Swinnerton-Dyer's generalisation [SD] of the method of Cassels [C3]. This allows us to compute the pairing $\Theta_5' : S_5' \times S_5' \to \mathbb{F}_2$ and hence its kernel S_6'. By Lemma 2.2 the upper bound

$$\operatorname{rank} E(K) \leq \dim S_5 + \dim S_6' - 2$$

is the same as that obtained by 8-descent on E.

The following lemma, which we state and prove using the notation and conventions of Section 4, describes the necessary bookkeeping.

Lemma 8.1. *Let $\alpha_1, \beta_1 \in S_5$. Suppose $\alpha_4, \beta_4 \in \operatorname{Sel}(4)$ and $\beta_2 \in \operatorname{Sel}(2)$ with $\alpha_4 \mapsto \alpha_1$ and $\beta_4 \mapsto \beta_2 \mapsto \beta_1$. Then*

(i) *There exists $\xi \in S_3$ with $\Theta_3(\xi, \eta) + \langle \beta_4, \eta \rangle = 0$ for all $\eta \in S_3$.*

(ii) *For any ξ satisfying (i) we have*

$$\Theta_5(\alpha_1, \beta_1) = \langle \alpha_4, \xi + \beta_2 \rangle. \tag{26}$$

Proof: Let $\beta_5 \in \operatorname{Sel}(5)$ with $\beta_5 \mapsto \beta_1$. The images of β_5 in $\operatorname{Sel}(4)$ and $\operatorname{Sel}(2)$ are $\xi' + \beta_4$ and $\xi + \beta_2$ for some $\xi' \in \operatorname{Sel}(3)$ and $\xi \in \operatorname{Sel}(1)$ with $\xi' \mapsto \xi$. Then $\xi \in S_3$ and for any $\eta \in S_3$ we have

$$\Theta_3(\xi, \eta) + \langle \beta_4, \eta \rangle = \langle \xi' + \beta_4, \eta \rangle = 0.$$

Moreover $\Theta_5(\alpha_1, \beta_1) = \langle \alpha_1, \beta_5 \rangle = \langle \alpha_4, \xi + \beta_2 \rangle$. To complete the proof we must show that if we replace ξ by $\xi + \gamma_1$ for some $\gamma_1 \in S_4$ then the formula (26) is unchanged. However if $\gamma_4 \in \operatorname{Sel}(4)$ with $\gamma_4 \mapsto \gamma_1$ then $\langle \alpha_4, \gamma_1 \rangle = \langle \alpha_1, \gamma_4 \rangle = 0$ where for the second equality we use that $\alpha_1 \in S_5$. □

9. Restriction of scalars

Our methods so far rely on being able to solve conics over K, and over quadratic extensions of K. In this section we show how to replace the latter problem with that of solving a quadric surface over K. This is to our advantage since, in the case $K = \mathbb{Q}$, there is a particularly efficient method due to D. Simon [S2] for solving rank 4 quadratic forms.

Let Γ_1 be a conic defined over a quadratic extension L/K. The restriction of scalars $\Gamma = \mathrm{Res}_{L/K}\Gamma_1$ is a degree 8 del Pezzo surface in $\mathrm{Res}_{L/K}\mathbb{P}^2 \subset \mathbb{P}^8$. Alternatively, by passing to an affine piece first, one gets that Γ is birational to an intersection of two quadrics in $\mathbb{P}^4$ with 4 singular points at infinity. We show however that for the conics arising in our descent calculations, we can write Γ as a quadric surface in $\mathbb{P}^3$.

Let E/K be an elliptic curve with a fixed rational 2-torsion point T. Suppose C and $C^\dagger$ are companion quadric intersections with respect to T. By this we mean that C and $C^\dagger$ are isomorphic as curves, but the difference of their hyperplane sections represents T in $\mathrm{Pic}^0(C) \cong E$. Let $\Gamma_1, \dots, \Gamma_4$ be the conics associated to C, ordered as specified at the start of Section 7. Suppose we are in the non-split case, i.e. Γ_1 and Γ_2 are $\mathrm{Gal}(L/K)$-conjugates. Let $\Gamma = \mathrm{Res}_{L/K}\Gamma_1$. As described in Lemma 7.1, each $P \in \Gamma$ gives rise to a pushout form on C. Since C and $C^\dagger$ are companion quadric intersections, this in turn corresponds to a linear form on $C^\dagger$. There is therefore a natural map $\Gamma \to (\mathbb{P}^3)^\vee$ where $(\mathbb{P}^3)^\vee$ is the dual of the ambient space for $C^\dagger$.

If $\{Q = 0\} \subset \mathbb{P}^3$ is a non-singular quadric surface then mapping each point to its tangent plane gives the dual quadric surface $\{Q' = 0\} \subset (\mathbb{P}^3)^\vee$. The symmetric matrix representing Q' is the inverse of that representing Q.

Theorem 9.1. *The image of $\Gamma \to (\mathbb{P}^3)^\vee$ is a non-singular quadric surface, and is dual to one of the quadrics in the pencil defining $C^\dagger$.*

Proof: For the proof we are free to extend our field K and make changes of co-ordinates. We may therefore suppose that C and $C^\dagger$ are the images of $E : y^2 = x(x^2 + ax + b)$ under the linear systems $|4.0|$ and $|3.0 + T|$ where $T = (0, 0)$. Explicitly

$$C = \left\{ \begin{aligned} x_1x_4 &= x_2^2 \\ x_3^2 &= x_2(x_4 + ax_2 + bx_1) \end{aligned} \right\} \subset \mathbb{P}^3$$

is the image of E under $(x_1 : x_2 : x_3 : x_4) = (1 : x : y : x^2)$, and

$$C^\dagger = \left\{ \begin{aligned} x_1x_3 &= x_2x_4 \\ x_3x_4 &= x_2^2 + ax_1x_2 + bx_1^2 \end{aligned} \right\} \subset \mathbb{P}^3 \tag{27}$$

is the image of E under $(x_1 : x_2 : x_3 : x_4) = (1 : x : y : y/x)$.

Let $P_1 = (\alpha_1 : \alpha_2 : 0 : \alpha_4)$ and $P_2 = (0 : \beta_2 : \beta_3 : \beta_4)$ be points on the rank 3 quadrics defining C. The tangent planes at these points are defined by linear forms

$$\begin{aligned} \ell_1 &= \alpha_4x_1 - 2\alpha_2x_2 + \alpha_1x_4, \\ \ell_2 &= (\beta_4 + a\beta_2)x_2 + \beta_2(x_4 + ax_2 + bx_1) - 2\beta_3x_3. \end{aligned}$$

Using the relations $\alpha_1\alpha_4 = \alpha_2^2$ and $\beta_3^2 = \beta_2(\beta_4 + a\beta_2)$ we find that

$$\alpha_4\beta_2\ell_1(1, x, y, x^2)\ell_2(1, x, y, x^2) = m(1, x, y, y/x)^2 x$$

in $K(E)$, where

$$m(x_1, \ldots, x_4) = \alpha_4\beta_3 x_1 - \alpha_2\beta_3 x_2 + \alpha_2\beta_2 x_3 - \alpha_4\beta_2 x_4.$$

The map $\Gamma \to (\mathbb{P}^3)^\vee$ is therefore given by

$$(P_1, P_2) \mapsto (\alpha_4\beta_3 : -\alpha_2\beta_3 : \alpha_2\beta_2 : -\alpha_4\beta_2).$$

The image of this map has equation $y_1y_3 = y_2y_4$. This is dual to the first of the quadrics in (27). □

Remark 9.2. The binary quartic associated to $C^\dagger$ defines a double cover of $\mathbb{P}^1$, again with Jacobian E. Translation by the 2-torsion point T induces an involution of $\mathbb{P}^1$. The quadric in the pencil defining $C^\dagger$ arising in Theorem 9.1 corresponds to one of the fixed points of this involution. (The other fixed point corresponds to the quadric that arises when we try to solve Γ_3 and Γ_4.) This may be seen by inspection of the above proof. Indeed the binary quartic associated to (27) is

$$F(u, v) = u^4 + 2au^2v^2 + (a^2 - 4b)v^4$$

and the involution induced by translation by T is $(u : v) \mapsto (u : -v)$. The fixed point $(u : v) = (1 : 0)$ then corresponds to the first of the quadrics in (27).

Solving the quadric surface in Theorem 9.1 gives a linear form on $C^\dagger$. Suppose we know the change of co-ordinates relating the 2-uple embeddings of C and $C^\dagger$. This then converts the square of our linear form on $C^\dagger$ to a pushout form f on C. We write $C \cap \{f = 0\} = 2\mathfrak{b}$ where $\mathfrak{b}$ is a degree 4 effective divisor. By construction, the push-forward of $\mathfrak{b}$ via $\nu_1 : C \to \Gamma_1$ contains an L-rational point in its support. We can then solve for $P_1 \in \Gamma_1(L)$ as required.

To make use of the above refinements, we must arrange that at each stage of the descent, our covering curve is represented by a pair of companion quadric intersections, and that we know the change of co-ordinates on $\mathbb{P}^7$ relating their 2-uple embeddings.

Let $C : y^2 = f(l, m)g(l, m)$ be the $\widehat{\phi}$-covering of E we called C_1 in Section 5. Then C is a double cover of $\mathbb{P}^1$ with fibre F and ramification points $P_1, \ldots, P_4$, say with P_1, P_2 corresponding to the roots of f, and P_3, P_4 corresponding to the roots of g. We have $2P_i \sim F$ and $P_1 + P_2 + P_3 + P_4 \sim 2F$. Moreover $P_1 - P_2 \sim P_3 - P_4$ represents the class of T' in $\operatorname{Pic}^0(C) \cong E'$. We now let C_1 and $C_1^\dagger$ be the images of C under the linear systems $|2F|$ and $|F + P_1 + P_2|$. Explicitly

$$C_1 = \left\{ \begin{aligned} x_1x_3 &= x_2^2 \\ x_4^2 &= \xi_1 x_1^2 + a x_1 x_3 + (b/\xi_1) x_3^2 \end{aligned} \right\} \subset \mathbb{P}^3$$

is the image of C under $(x_1 : x_2 : x_3 : x_4) = (f(l,m) : y : g(l,m) : h(l,m))$, and

$$C_1^\dagger = \left\{ \begin{array}{c} x_1x_4 = x_2x_3 \\ f(x_1,x_2) = g(x_3,x_4) \end{array} \right\} \subset \mathbb{P}^3$$

is the image of C under

$$\begin{aligned} (x_1 : x_2 : x_3 : x_4) &= (yl : ym : f(l,m)l : f(l,m)m) \\ &= (g(l,m)l : g(l,m)m : yl : ym). \end{aligned}$$

It is straightforward to work out the change of co-ordinates relating the 2-uple embeddings of C_1 and $C_1^\dagger$.

Starting with C_1 and $C_1^\dagger$ we apply our method to compute a ϕ-covering of C_1 (and hence a 2-covering of E) in the form of companion quadric intersections C_2 and $C_2^\dagger$. The curve C_2 is the same as that in Section 5, and as there it is computed by solving conics over K. To compute $C_2^\dagger$ we must solve the quadric surface $f(x_1,x_2) = g(x_3,x_4)$ that appears as the second equation for $C_1^\dagger$. Since we already solved the conics $f(l,m) = \xi_2 s^2$ and $g(l,m) = \xi_2 t^2$ in Section 5, we can read off a solution "for free".

At the next stage we compute a $\widehat{\phi}$-covering of C_2 (and hence a $2\widehat{\phi}$-covering of E) in the form of companion quadric intersections C_3 and $C_3^\dagger$. The curve C_3 is the same as that in Section 5, and as there it is computed by solving conics over K. However to compute $C_3^\dagger$ we must solve a quadric surface over K. In the final stage, we compute a ϕ-covering of C_3 (and hence a 4-covering of E) in the form of companion quadric intersections C_4 and $C_4^\dagger$. To compute each of these we must solve a quadric surface over K.

This is the limit of our method since C_4 does not satisfy the Galois hypothesis (19). Indeed the singular fibres in the pencil defining C_4 are in general defined over a degree 4 extension of K. Solving a conic over a degree 4 number field is not practical for the examples we have in mind. However if we could solve such conics, then we could compute a 2-covering of C_4 (and hence an 8-covering on E) as described in [St].

10. Examples

We have written a program in Magma [BCP] for performing the higher descents described in this paper, for elliptic curves over $\mathbb{Q}$ with a rational 2-torsion point. The Magma functions we use for solving quadratic forms of ranks 3 and 4 over $\mathbb{Q}$ are based on [S1], [S2]. See also [CR] for the rank 3 case. Our program is available in Magma (version 2.21) as the function `TwoPowerIsogenyDescentRankBound`.

We have used our program to help search for curves of large rank in certain families of elliptic curves. For example, we found the first example of an elliptic curve $E/\mathbb{Q}$ with $E(\mathbb{Q}) \cong \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}^4$. We also found 10 new examples of elliptic curves $E/\mathbb{Q}$ with $E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}^3$, including one where every point of infinite order has canonical height greater than 100. These examples are listed on Dujella's website [D]. We have also contributed to a project run by Mark Watkins [W+], searching for congruent number elliptic curves of large rank.

The main reason we need higher descents for these searches is that we would otherwise be swamped by examples which, while appearing to be candidates for large rank, turn out instead to have large 2-primary part of Ш. The examples we have chosen to present in this section are therefore elliptic curves which our program was quickly able to show do *not* have large rank.

We do not give details of every step in computing the covering curves and pushout functions. However the answers may be checked as follows. Each of our covering curves is either a double cover of $\mathbb{P}^1$, with equation $y^2 = g(x,z)$ where g is a binary quartic, or a quadric intersection in $\mathbb{P}^3$. In both cases classical invariant theory gives a formula for the Jacobian. In the second case, we may represent the quadric intersection $C_4 \subset \mathbb{P}^3$ by a pair of 4×4 symmetric matrices A and B. Then C_4 is a 2-covering of $y^2 = g(x,z)$ where $g(x,y) = \det(Ax + By)$. At each stage our program makes changes of co-ordinates to simplify the equations for these covering curves, using the algorithms in [CFS]. In checking the examples, it is useful to note that there are algorithms implemented in Magma for testing equivalence of binary quartics (see [CF]) and quadric intersections (see [F2]).

The pushout functions on $y^2 = g(x,z)$ take the form $f = (y - \lambda_2(x,z))/z^2$ where λ_2 is a binary quadratic form. The pushout functions on a quadric intersection take the form $f = \lambda_4(x_1,\ldots,x_4)/x_1^2$ where λ_4 is a quadratic form. We say that $y - \lambda_2(x,z)$ and $\lambda_4(x_1,\ldots,x_4)$ are *pushout forms*. There are several ways of checking that $\operatorname{div}(f) = 2\mathfrak{b}$ for some divisor $\mathfrak{b}$. For example in Magma one could compute resultants, or use Groebner bases, or use the function field machinery. If f is not a constant times the square of a rational function, and the Jacobian has only one rational 2-torsion point T, then such a calculation proves that f is a pushout function corresponding to T.

Example 10.1. Let $E/\mathbb{Q}$ be the elliptic curve $y^2 = x(x^2 + ax + b)$ where

$$\begin{aligned} a &= 91502230365284038, \\ b &= 489792722057841784540058275212361. \end{aligned}$$

This is an example with $E(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z}/12\mathbb{Z}$. There is a 2-isogeny $\phi : E \to E'$ where E' has equation $y^2 = x(x^2 + a'x + b')$ and $a' = -2a$, $b' = a^2 - 4b$. With notation as in Section 2, we find that

$$\begin{aligned} S_1 = S_2 = S_3 &= \langle 15, 73, 87, 231, 28619 \rangle \subset \mathbb{Q}^\times/(\mathbb{Q}^\times)^2, \\ S_1' = S_2' = S_3' &= \langle -272196179 \rangle \subset \mathbb{Q}^\times/(\mathbb{Q}^\times)^2. \end{aligned}$$

Therefore $\operatorname{rank} E(\mathbb{Q}) \leq 4$. To improve this upper bound for the rank we compute the pairing $\Theta_3 : S_3 \times S_3 \to \mathbb{F}_2$.

Let $\xi_1 = 15 \times 44660^2$. Parametrising a conic, we find binary quadratic forms

$$\begin{aligned} f(l,m) &= 195346817865l^2 - 490516840068lm + 33576198052m^2, \\ g(l,m) &= -1473071l^2 + 7386682lm - 9255011m^2, \\ h(l,m) &= 348523798338106(2067l^2 - 10091lm + 12314m^2) \end{aligned}$$

satisfying $\xi_1 f^2 + a'fg + (b'/\xi_1)g^2 = h^2$. Parametrising two further conics, gives binary quadratic forms

$$\begin{aligned} p_1(c,d) &= 65928c^2 + 582550cd + 1159554d^2, \\ p_2(c,d) &= 13590c^2 + 429375cd - 202059d^2, \\ p_3(c,d) &= 8585676(2375c^2 - 6774cd - 71700d^2) \end{aligned}$$

and

$$\begin{aligned} q_1(\theta,\psi) &= 819\theta^2 + 17717\theta\psi + 3725\psi^2, \\ q_2(\theta,\psi) &= 329\theta^2 + 7717\theta\psi + 1510\psi^2, \\ q_3(\theta,\psi) &= 11165(2\theta^2 + 2\theta\psi - 7\psi^2) \end{aligned}$$

satisfying $f(p_1,p_2) = p_3^2$ and $g(q_1,q_2) = q_3^2$. It may then be checked that the curve

$$C_3 = \left\{ \begin{array}{l} p_1(c,d) = q_1(\theta,\psi) \\ p_2(c,d) = q_2(\theta,\psi) \end{array} \right\} \subset \mathbb{P}^3$$

is everywhere locally soluble. This confirms that $\xi_1 \in S_3$. (For the purposes of presenting this example, we adjusted the parametrisations so that $\xi_2 = \xi_3 = 1$.)

By computing companion quadric intersections $C_2^\dagger$ and $C_3^\dagger$ as described in Section 9, we find that C_3 has pushout form

$$\begin{aligned} \lambda(c,d,\theta,\psi) = 522272234c^2 - 24659265cd - 17398450d^2 \\ - 26417751\theta^2 - 55245559\theta\psi - 9670688\psi^2. \end{aligned}$$

Let $\eta \in S_3$. By the formula for the Cassels-Tate pairing in Section 3, we have $\Theta_3(\xi_1,\eta) = \sum_v (\lambda(P_v),\eta)_v$ where $P_v \in C_3(\mathbb{Q}_v)$ and $(\ ,\ )_v$ is the Hilbert norm residue symbol $\mathbb{Q}_v^\times/(\mathbb{Q}_v^\times)^2 \times \mathbb{Q}_v^\times/(\mathbb{Q}_v^\times)^2 \to \mathbb{F}_2$. The bad primes of E are

$$\mathcal{S} = \{2,3,5,7,11,29,71,73,127,28619,30187\}.$$

At all primes $p \notin \mathcal{S}$, we find that C_3 has good reduction mod p, whereas the two equations for C_3 together with λ are linearly independent mod p. These primes therefore make no contribution to the pairing. Since $\eta \in (\mathbb{Q}_v^\times)^2$ for all $v \in \{71,127,30187,\infty\}$ there is also no contribution from these places. At each of the remaining primes p we find a local point $P \in C_3(\mathbb{Q}_p)$ with $F(P) \equiv u_p$ mod $(\mathbb{Q}_p^\times)^2$ where $u_2 = 5$ and u_p is a quadratic non-residue for p odd. Therefore

$\Theta_3(\xi_1, \eta) \equiv \omega(\eta) \pmod 2$ where $\omega(\eta)$ is the number of prime divisors of η. (We choose a representative modulo squares so that η is a square-free integer.) This gives the first row in the following table. Repeating for ξ_1 running over a basis for S_3 we find that $\Theta_3 : S_3 \times S_3 \to \mathbb{F}_2$ is given by

	15	73	87	231	28619
15	0	1	0	1	1
73	1	0	1	0	0
87	0	1	0	0	1
231	1	0	0	0	1
28619	1	0	1	1	0

This matrix has rank 4. Therefore $\dim S_4 = 1$ and $\operatorname{rank} E(\mathbb{Q}) = 0$. By Remark 2.3 the 2-primary parts of $Ш(E/\mathbb{Q})$ and $Ш(E'/\mathbb{Q})$ are $(\mathbb{Z}/4\mathbb{Z})^4$ and $(\mathbb{Z}/2\mathbb{Z})^4$.

Example 10.2. Let $E/\mathbb{Q}$ be the elliptic curve $y^2 = x(x^2 + ax + b)$ where

$$\begin{aligned} a &= -8021755376640687319987 22, \\ b &= 16048056135294041387943722290221666448985240 8321. \end{aligned}$$

This is an example with $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. Let $\phi : E \to E'$ be the 2-isogeny with kernel generated by $T = (0, 0)$. As subgroups of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ we find that $S_1 = S_2 = \langle -10, 5574 \rangle$ and

$$\begin{aligned} S_1' &= \langle 3841, 920641, 262404961, 289572953761, 9289, 6049, 31441 \rangle, \\ S_2' &= \langle 3841, 920641, 262404961, 289572953761, 9289 \rangle. \end{aligned}$$

Therefore $\operatorname{rank} E(\mathbb{Q}) \leq 5$. Next we compute $\Theta_2 : S_2 \times S_2' \to \mathbb{F}_2$. The elements $\xi_1 = -10$ and $\eta_1 = 5574$ in $S_1 = S^{(\phi)}(E/\mathbb{Q})$ lift to 2-coverings of E' given by

$$\begin{aligned} C_2 &= \{y^2 = \lambda_1(x,z)^2 + 10\mu_1(x,z)^2)\} \\ D_2 &= \{y^2 = \lambda_2(x,z)^2 - 5574\mu_2(x,z)^2\} \end{aligned}$$

where

$$\begin{aligned} \lambda_1(x,z) &= 341696479062308(x^2 - 10z^2) + 3516978476959251xz, \\ \mu_1(x,z) &= 21538029761160(x^2 - 10z^2) + 158658854157270xz, \\ \lambda_2(x,z) &= 1335842866662(x^2 + 5574z^2) + 1439937420103543xz, \\ \mu_2(x,z) &= 17631567180(x^2 + 5574z^2) + 18855731460270xz. \end{aligned}$$

It may be checked, using the formulae in [CF], that C_2 and D_2 do indeed correspond to ξ_1 and η_1. Since C_2 and D_2 are everywhere locally soluble, this confirms that ξ_1 and η_1 are in S_2. Now $y - \lambda_1(x, z)$ and $y - \lambda_2(x, z)$ are pushout forms on C_2 and D_2. Evaluating these at local points, and then computing sums of Hilbert norm residue symbols, we find that $\Theta_2 : S_2 \times S_2' \to \mathbb{F}_2$ is given by

	3841	920641	262404961	289572953761	9289
-10	0	0	0	0	1
5574	0	0	0	0	0

We further find that Θ_3 and Θ_3' are identically zero. Therefore $S_3 = S_4 = \langle 5574 \rangle$ and

$$S_3' = S_4' = \langle 3841, 920641, 262404961, 289572953761 \rangle.$$

Using the methods in Sections 7 and 9 we compute an everywhere locally soluble 2-covering D_4 of D_2 (and hence 4-covering of E') with equations

$$\begin{aligned} &9055x_1^2 + 139619x_1x_2 + 394387x_1x_3 + 47027x_1x_4 - 94269x_2^2 \\ &\quad - 234422x_2x_3 + 266438x_2x_4 + 127750x_3^2 - 130775x_3x_4 - 137150x_4^2 = 0, \\ &255171x_1^2 - 961185x_1x_2 + 297383x_1x_3 + 224191x_1x_4 + 152028x_2^2 \\ &\quad + 461745x_2x_3 - 59967x_2x_4 + 370158x_3^2 - 350350x_3x_4 - 198938x_4^2 = 0. \end{aligned}$$

We find that D_4 has pushout form

$$\begin{aligned} \lambda = {} &2471492850764286x_1^2 - 573148078730175x_1x_2 + 136617115364660x_1x_3 \\ &- 1043769539460119x_1x_4 - 338965008210675x_2^2 + 460367211908885x_2x_3 \\ &+ 1057225484721135x_2x_4 - 989678424716819x_3^2 + 2171876872481818x_3x_4 \\ &- 1169960121148148x_4^2. \end{aligned}$$

Using this we compute that $\Theta_4 : S_4 \times S_4' \to \mathbb{F}_2$ is given by

	3841	920641	262404961	289572953761
5574	1	1	0	1

Therefore $S_5 = 0$, $\dim S_5' = 3$ and $\operatorname{rank} E(\mathbb{Q}) \leq 1$. If $\operatorname{rank} E(\mathbb{Q}) = 1$ then by Remark 2.3 the 2-primary parts of $Ш(E/\mathbb{Q})$ and $Ш(E'/\mathbb{Q})$ are $(\mathbb{Z}/2\mathbb{Z})^2 \times (\mathbb{Z}/4\mathbb{Z})^2$ and $(\mathbb{Z}/2\mathbb{Z})^4 \times (\mathbb{Z}/4\mathbb{Z})^2$.

Example 10.3. Let $E/\mathbb{Q}$ be the elliptic curve $y^2 = x^3 - d^2x$ where

$$d = 743114132612994 = 2 \times 3 \times 19 \times 953 \times 1427 \times 2137 \times 2243.$$

This was one of the candidates in [W+] for a congruent number elliptic curve of rank 6. Let $\phi : E \to E'$ be the 2-isogeny with kernel generated by $T = (-d, 0)$.

We find that

$$\begin{aligned} S_1 = S_2 = S_3 = S_4 &= \langle 1906, 2137 \rangle \subset \mathbb{Q}^\times/(\mathbb{Q}^\times)^2, \\ S_1' = S_2' = S_3' = S_4' &= \langle 2, 57, 953, 2137, 4281, 6729 \rangle \subset \mathbb{Q}^\times/(\mathbb{Q}^\times)^2. \end{aligned}$$

Therefore $\operatorname{rank} E(\mathbb{Q}) \leq 6$. (We note that $1906 = 2 \times 953$, $57 = 3 \times 19$, $4281 = 3 \times 1427$ and $6729 = 3 \times 2243$.) The elements 1906 and 2137 in $S^{(\phi)}(E/\mathbb{Q})$ lift to 4-coverings of E' with equations

$$\begin{aligned} &1188x_1^2 + 1244x_1x_2 + 732x_1x_3 + 5599x_1x_4 - 1530x_2^2 \\ &\quad - 3687x_2x_3 + 2824x_2x_4 - 2928x_3^2 + 1780x_3x_4 + 4886x_4^2 = 0, \\ &3298x_1^2 - 7382x_1x_2 + 3881x_1x_3 - 3470x_1x_4 + 20x_2^2 \\ &\quad + 2136x_2x_3 + 7147x_2x_4 + 1517x_3^2 - 4464x_3x_4 - 2455x_4^2 = 0, \end{aligned}$$

and

$$\begin{aligned} &68x_1^2 + 416x_1x_2 + 422x_1x_3 + 1372x_1x_4 + 401x_2^2 \\ &\quad + 1146x_2x_3 + 1154x_2x_4 + 475x_3^2 + 1528x_3x_4 - 2366x_4^2 = 0, \\ &18869x_1^2 - 13870x_1x_2 - 14599x_1x_3 - 2402x_1x_4 + 2322x_2^2 \\ &\quad + 15142x_2x_3 - 1629x_2x_4 - 12250x_3^2 + 6366x_3x_4 + 4913x_4^2 = 0. \end{aligned}$$

These have pushout forms

$$\begin{aligned} \lambda = \; &280117153304x_1^2 + 627376555572x_1x_2 - 534852420548x_1x_3 \\ &- 24376482389x_1x_4 + 7830950834x_2^2 - 165910883299x_2x_3 \\ &+ 255303594426x_2x_4 - 574956757207x_3^2 - 923597568302x_3x_4 \\ &- 398161865115x_4^2, \end{aligned}$$

and

$$\begin{aligned} \lambda = \; &302992919x_1^2 + 165225436x_1x_2 - 554084592x_1x_3 - 3000363446x_1x_4 \\ &+ 259816709x_2^2 - 1891629098x_2x_3 + 2507867060x_2x_4 - 1337797147x_3^2 \\ &+ 572269312x_3x_4 - 1348920925x_4^2. \end{aligned}$$

Using these we compute that $\Theta_4 : S_4 \times S_4' \to \mathbb{F}_2$ is given by

	2	57	953	2137	4281	6729
1906	0	1	1	0	0	0
2137	0	0	1	0	1	0

This matrix has rank 2. Therefore $S_5 = 0$, $\dim S_5' = 4$ and $\operatorname{rank} E(\mathbb{Q}) \leq 2$. Searching for rational points on 2-coverings of E, and on 2-coverings of elliptic curves isogenous to E, we find that $E(\mathbb{Q})$ has independent points of infinite order

$$\begin{aligned} P_1 &= (378998487378128086417/42^2, 737825426046908694986565129948 1/42^3), \\ P_2 &= (4906543485739785817699690091987274941361019066993/76947716\backslash \\ &\qquad 400301612^2, 48096529647237527021204707950147996195360092 4\backslash \\ &\qquad 73283274592260009291666680 23/76947716400301612^3). \end{aligned}$$

Therefore $\operatorname{rank} E(\mathbb{Q}) = 2$. By Remark 2.3 the 2-primary parts of $Ш(E/\mathbb{Q})$ and $Ш(E'/\mathbb{Q})$ are isomorphic to $(\mathbb{Z}/4\mathbb{Z})^4$. Similar calculations show that the other two elliptic curves in the isogeny class have 2-primary parts of Ш isomorphic to $(\mathbb{Z}/4\mathbb{Z})^2 \times (\mathbb{Z}/8\mathbb{Z})^2$ and $(\mathbb{Z}/8\mathbb{Z})^4$.

References

[BSD] B.J. Birch and H.P.F. Swinnerton-Dyer, Notes on elliptic curves, II., *J. reine angew. Math.* **218** (1965) 79–108.

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

[BC] A. Bremner and J.W.S Cassels, On the equation $Y^2 = X(X^2 + p)$, *Math. Comp.* **42** (1984), no. 165, 257–264.

[C1] J.W.S. Cassels, Arithmetic on curves of genus 1, VIII. On conjectures of Birch and Swinnerton-Dyer, *J. reine angew. Math.* **217** (1965) 180–199.

[C2] J.W.S. Cassels, *Lectures on elliptic curves*, LMS Student Texts, **24**, Cambridge University Press, Cambridge, 1991.

[C3] J.W.S. Cassels, Second descents for elliptic curves. *J. reine angew. Math.* **494** (1998), 101–127.

[Cr] J.E. Cremona, *Higher descents on elliptic curves*, notes for a talk, 1997, `http://homepages.warwick.ac.uk/~masgaj/papers/d2.ps`

[CR] J.E. Cremona and D. Rusin, Efficient solution of rational conics, *Math. Comp.* **72** (2003), no. 243, 1417–1441.

[CF] J.E. Cremona and T.A. Fisher, On the equivalence of binary quartics, *J. Symbolic Comput.* **44** (2009), no. 6, 673–682.

[CFS] 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.

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

[F1] T.A. Fisher, The Cassels-Tate pairing and the Platonic solids, *J. Number Theory* **98** (2003), no. 1, 105–155.

[F2] T.A. Fisher, Some improvements to 4-descent on an elliptic curve, in *Algorithmic number theory* (ANTS VIII, Banff 2008), A.J. van der Poorten and A. Stein (eds), 125–138, Lecture Notes in Comput. Sci., **5011**, Springer, Berlin, 2008.

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

[Sik] S. Siksek, *Descent on curves of genus* 1, PhD thesis, University of Exeter, 1995.

[Sil] J.H. Silverman, *The arithmetic of elliptic curves*, GTM **106**, Springer-Verlag, New York, 1986.

[S1] D. Simon, Solving quadratic equations using reduced unimodular quadratic forms, *Math. Comp.* **74** (2005), no. 251, 1531–1543.

[S2] D. Simon, *Quadratic equations in dimensions 4, 5 and more*, preprint 2005.

[St] S. Stamminger, *Explicit 8-descent on elliptic curves*, PhD thesis, International University Bremen, 2005.

[SD] H.P.F. Swinnerton-Dyer, 2^n-descent on elliptic curves for all n, *J. Lond. Math. Soc.* (2) **87** (2013), no. 3, 707–723.

[W+] M. Watkins, S. Donnelly, N.D. Elkies, T.A. Fisher, A. Granville and N.F. Rogers, On ranks of quadratic twists of elliptic curves, *Pub. math. de Besançon*, 2014/2, 63–98.

[Wo] T. Womack, *Explicit descent on elliptic curves*, PhD thesis, University of Nottingham, 2003.

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

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