# EXPLICIT $n$-DESCENT ON ELLIPTIC CURVES III. ALGORITHMS

J.E. CREMONA, T.A. FISHER, C. O'NEIL, D. SIMON, AND M. STOLL

Abstract. This is the third in a series of papers in which we study the $n$-Selmer group of an elliptic curve, with the aim of representing its elements as genus one normal curves of degree $n$. The methods we describe are practical in the case $n = 3$ for elliptic curves over the rationals, and have been implemented in MAGMA.

One important ingredient of our work is an algorithm for trivialising central simple algebras. This is of independent interest: for example, it could be used for parametrising Brauer-Severi surfaces.

## Contents



*Date*: 18th July, 2011.

## 1. Introduction

Descent on an elliptic curve $E$, defined over a number field $K$, is a method for obtaining information about both the Mordell-Weil group $E(K)$ and the Tate-Shafarevich group $Ш(E/K)$. Indeed for each integer $n \geq 2$ there is an exact sequence

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

where $\mathrm{Sel}^{(n)}(E/K)$ is the $n$-Selmer group.

This is the third in a series of papers in which we study the $n$-Selmer group with the aim of representing its elements as genus one normal curves $C \subset \mathbb{P}^{n-1}$ (when $n \geq 3$). Having this representation allows searching for rational points on $C$ (which in turn gives points in $E(K)$, since $C$ may be seen as an $n$-covering of $E$) and is a first step towards doing higher descents. A further application is to the study of explicit counter-examples to the Hasse Principle.

The Selmer group $\mathrm{Sel}^{(n)}(E/K)$ is a subgroup of the Galois cohomology group $H^1(K, E[n])$, which parametrises the $n$-coverings of $E$. An $n$-covering $\pi : C \to E$ represents a Selmer group element if and only if $C$ is everywhere locally soluble, i.e., $C$ has $K_v$-rational points for each completion $K_v$ of $K$. In this case it was shown by Cassels [4] that $C$ admits a $K$-rational divisor $D$ of degree $n$. We can then use the complete linear system $|D|$ to embed $C \subset \mathbb{P}^{n-1}$ as a genus one normal curve of degree $n$, when $n > 2$. (For $n = 2$ we obtain instead a double cover $C \to \mathbb{P}^1$.) More precisely, Cassels' argument shows that $S^{(n)}(E/K)$ is contained in the 'kernel' of the obstruction map $\mathrm{Ob} : H^1(K, E[n]) \to \mathrm{Br}(K)$.

In the first paper of this series [13] we gave a list of interpretations of $H^1(K, E[n])$ and of the obstruction map. Then we showed how, given $\xi \in H^1(K, E[n])$, to explicitly represent $\mathrm{Ob}(\xi)$ as a central simple algebra $A$ of dimension $n^2$ over $K$, by giving structure constants for $A$; we call $A$ the *obstruction algebra*. In the case $\xi \in \mathrm{Sel}^{(n)}(E/K)$, we have $A \cong \mathrm{Mat}_n(K)$. Assuming the existence of a "Black Box" to compute such an isomorphism explicitly, a process we call *trivialising the obstruction algebra*, we then outlined three algorithms to compute equations for $C \subset \mathbb{P}^{n-1}$. These were called the Hesse pencil, flex algebra, and Segre embedding methods.

In the second paper [14] we developed the Segre embedding method. In this paper we are again concerned with the Segre embedding method. We give an outline of the work in the earlier papers, and then give further details of the algorithms. In particular, taking $K = \mathbb{Q}$ and $n = 3$, we explain our method for trivialising the obstruction algebra. (See Section 6: Inside the Black Box).

Returning to general $n$, we observe that

$$\mathrm{Sel}^{(mn)}(E/K) \cong \mathrm{Sel}^{(m)}(E/K) \times \mathrm{Sel}^{(n)}(E/K)$$

whenever $m$ and $n$ are coprime. Therefore for the purposes of computing Selmer groups we can restrict our attention to prime powers $n$. Then, if $n = p^f$ with $f \geq 2$, the most efficient way to proceed seems to be to first recursively compute $\mathrm{Sel}^{(p^{f-1})}(E/K)$, to realise the elements of that Selmer group as suitable covering curves (using the methods of this paper, for example), and then to compute the fibres of the natural map $\mathrm{Sel}^{(p^f)}(E/K) \to \mathrm{Sel}^{(p^{f-1})}(E/K)$ via $p$-descents on these covering curves. This has been worked out for $p = 2$ and $f = 2$ by Siksek [37], Merriman, Siksek and Smart [30], Cassels [6] and Womack [41]; for $p = 2$ and $f = 3$ by Stamminger [39]; and for odd $p$ and $f = 2$ by Creutz [16].

In Sections 2.2 and 2.3 we recall the construction of an étale algebra (that is, a product of number fields) $R$ and a homomorphism $\partial : R^\times \to (R \otimes R)^\times$ such that $\mathrm{Sel}^{(n)}(E/K)$ may be realised either as a subgroup of $(R \otimes R)^\times/\partial R^\times$, with elements represented by $\rho \in (R \otimes R)^\times$, or as a subgroup of $R^\times/(R^\times)^n$, with elements represented by $\alpha \in R^\times$. The first of these works for any $n \geq 2$ and is better suited to the computation of the obstruction algebra and equations for $C$. The second only works for prime $n$, but is better suited to computing the Selmer group itself, in that the class group and unit calculations are more manageable. So in Section 2.4, we discuss how to convert from one representation to the other (from $\alpha$ to $\rho$). The Segre embedding method is then reviewed in Sections 2.5 and 2.6.

It is sometimes convenient to assume $n > 2$. For example, when $n = 2$ the map $C \to \mathbb{P}^1$ is a double cover rather than an embedding. However, if the Segre embedding method is suitably interpreted in the case $n = 2$, then it corresponds exactly to the classical number field method[1] for 2-descent. This is explained in Section 3. In Section 4, we give an equally explicit description of our algorithms in the case $n = 3$, assuming the action of Galois on $E[3]$ is generic. We do not give full details of the modifications required to handle the other Galois actions as this would be unduly tedious, though each case had to be handled in detail in our MAGMA implementation.

Starting with $\alpha \in R^\times$, we write down structure constants for the obstruction algebra $A$. Then we trivialise the algebra $A$. Using the trivialisation, we obtain a plane cubic $C \subset \mathbb{P}^2$. Now, the element $\alpha$ is typically of very large height: it comes out of a class group and unit calculation that involves many random choices. Consequently, the first equation for $C$ which we obtain is a

[1] An alternative method for 2-descent over $K = \mathbb{Q}$, based on invariant theory, is implemented in `mwrank` [10], and is competitive over a large range of curves, but seems to become impractical in other cases: when $K$ is a larger number field, or when $n > 2$.

ternary cubic with enormous coefficients. In order to obtain a more reasonable equation, we finally use our algorithms for minimisation and reduction (see [15]) to make a good change of coordinates.

In our original implementation for $K = \mathbb{Q}$ and $n = 3$, we used an *ad hoc* method for trivialising the algebra, which worked well in practice, but which we could not prove always terminates. It became clear that the algorithm could be improved by carrying out steps equivalent to minimisation and reduction at an earlier stage. Firstly, $\alpha$ should be replaced by a good representative modulo $n$th powers, as has already been described in [21, Section 2]. Then we should choose a good basis for the obstruction algebra, so as to make the structure constants small integers. This is described in Section 5, and makes trivialising the obstruction algebra very much easier. (In fact, this trivialisation is again a problem of "minimisation and reduction" type.) As a result, the algorithms in [15], although still required, do not need to work so hard.

In Section 6 we describe our methods for trivialising the obstruction algebra. Since our methods are of independent interest, we have made this section self-contained. For instance our methods could be used to improve the algorithm in [26] for parametrising Brauer-Severi surfaces.

One peculiar feature of the Segre embedding method is that in our initial implementation (for $K = \mathbb{Q}$ and $n = 3$) it was necessary to multiply by a "fudge factor" $1/y$ to ensure that the projection of $C \subset \mathbb{P}(A)$ to the trace 0 subspace is contained in the rank 1 locus. The need for this factor was justified by a generic calculation specific to the case $n = 3$. In Section 7 we give a better explanation, based on the theory in [14], that works for all odd integers $n$.

Finally, we give examples of the algorithm in practice, in Section 8. One application of our work is that it can help find generators of large height on an elliptic curve. Indeed the logarithmic height of a rational point on an $n$-covering is expected to be smaller by a factor $2n$ compared to its image on the elliptic curve. (See [23] for a precise statement.) Our work in the case $n = 3$ is a starting point both for the work on 6- and 12-descent in [20], and for the work on 9-descent in [16]. In Section 8 we instead use our methods to exhibit some explicit elements of $Ш(E/\mathbb{Q})[3]$ and to give some examples illustrating that the obstruction map on 3-coverings is not linear. The use of our methods to compute some elements of $Ш(E/\mathbb{Q})[5]$ will be described in future work. For this we use that the Hesse pencil method (described in [13, Section 5.1] in the case $n = 3$) generalises to the case $n = 5$ as described in [22, Section 12].

Our algorithms have been implemented in (and contributed to) MAGMA [3, Version 2.13 and later] for $K = \mathbb{Q}$ and $n = 3$. A first version of the implementation was written by Michael Stoll; it was restricted to the case of a transitive Galois action on the points of order 3. Steve Donnelly extended the part that computes the 3-Selmer group as an abstract group to cover all cases (for $K = \mathbb{Q}$), and Tom Fisher re-worked and extended the part that turns abstract Selmer group elements into plane cubic curves, so that it also works in all cases.

Our programs are currently specific to the case $K = \mathbb{Q}$. The two main obstacles to extending them to general number fields are as follows. Firstly, it would be necessary (unless the Galois action on $E[3]$ is smaller than usual) to compute class group and units over number fields of larger degree. Secondly, we do not have a suitable theory of lattice reduction over number fields. Notice that our algorithms over $K = \mathbb{Q}$ are dependent on the LLL-algorithm, first in [21, Section 2], then in Sections 5 and 6 and finally in [15]. It is possible that the algorithms described in [18] could be used here, and this will be the subject of future work.

## 2. Algorithms in outline

In this section we give an outline of the algorithms used in our implementation of explicit 3-descent on elliptic curves over $\mathbb{Q}$. However, as far as possible in this overview, we keep to the case where $n$ is general and the base field is a general number field $K$. Details specific to the case $n = 3$ can be found in Section 4 below. Our description here is based on what was called the 'Segre embedding method' in [13, 14]. We begin with a review of the computation of the Selmer group as an abstract group. When we talk about the 'generic case' below, we refer to the situation when the action of the Galois group $G_K$ on $E[n]$ induces a surjective homomorphism of $G_K$ onto $\mathrm{Aut}_{\mathbb{Z}/n\mathbb{Z}}(E[n]) \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. When $K = \mathbb{Q}$ and $E$ is fixed and non-CM, this will be the case for all but finitely many prime values of $n$. It will also be true for the generic elliptic curve $y^2 = x^3 + ax + b$ over $\mathbb{Q}(a, b)$.

### 2.1. Computation of the Selmer group I: The étale algebra.

Let $E$ be an elliptic curve over a field $K$. (We will take $K$ to be a number field later.) We fix a Weierstraß equation for $E$ and denote the coordinate functions with respect to this equation by $x$ and $y$. Let $n \geq 2$ be an integer not divisible by the characteristic of $K$. We let $R = \mathrm{Map}_K(E[n], \overline{K})$ be the étale algebra of $E[n]$. The algebra $R$ splits as a product of finite extensions of $K$ corresponding to the Galois orbits on $E[n]$, where the component corresponding to the orbit of $T \in E[n]$ is $K(T)$, the field of definition of $T$. There is always a splitting $R = K \times L$ with $K$ corresponding to the singleton orbit $\{O\}$ and $L = \mathrm{Map}_K(E[n] \setminus \{O\}, \overline{K})$. If $n$ is a prime $p$, then generically the Galois action is transitive on the points of order $p$, and $L/K$ is a field extension of degree $p^2 - 1$.

The tensor product $R \otimes_K R$ is the étale algebra of $E[n] \times E[n]$. We denote by $\mathrm{Sym}^2_K(R)$ the subalgebra consisting of symmetric functions:

$$\mathrm{Sym}^2_K(R) = \{\rho \in R \otimes_K R \mid \rho(T_1, T_2) = \rho(T_2, T_1) \text{ for all } T_1, T_2 \in E[n]\}$$

This is the étale algebra of the set of unordered pairs of $n$-torsion points. As before, these algebras split into products of finite field extensions of $K$ corresponding to the Galois orbits on $E[n] \times E[n]$ and on the set of unordered pairs of $n$-torsion points, respectively. The algebra $\mathrm{Sym}^2_K(R)$ contains a factor corresponding to unordered bases of $E[n]$ as a $\mathbb{Z}/n\mathbb{Z}$-module. When $n$ is a prime $p$, then generically, the Galois group acts transitively on these bases, and the corresponding factor of $\mathrm{Sym}^2_K(R)$ is a field extension of $K$ of degree $(p^2 - 1)(p^2 - p)/2$.

The group law $E[n] \times E[n] \to E[n]$ corresponds to the comultiplication $\Delta_K : R \to \mathrm{Sym}^2_K(R) \subset R \otimes_K R$. We write $\mathrm{Tr}_K : R \otimes_K R \to R$ for the trace map obtained by viewing $R \otimes_K R$ as an $R$-algebra via $\Delta_K$. In terms of maps we have

$$\Delta_K(\alpha) : (T_1, T_2) \mapsto \alpha(T_1 + T_2) \quad \text{and} \quad \mathrm{Tr}_K(\rho) : T \mapsto \sum_{T_1 + T_2 = T} \rho(T_1, T_2)\,.$$

2.2. **Computation of the Selmer group II: Using $w_2$.** We define

$$\begin{aligned} &\partial_K : R^\times \longrightarrow \mathrm{Sym}^2_K(R)^\times \\ \text{by} \qquad &\alpha \longmapsto \frac{\alpha \otimes \alpha}{\Delta_K(\alpha)} = \left( (T_1, T_2) \mapsto \frac{\alpha(T_1)\alpha(T_2)}{\alpha(T_1 + T_2)} \right). \end{aligned}$$

In [13, p. 138], we defined another map $\partial$, which we here denote $\partial^{(2)}_K$ to avoid confusion. It is given by

$$\begin{aligned} \partial^{(2)}_K : (R \otimes_K R)^\times &\longrightarrow (R \otimes_K R \otimes_K R)^\times \\ \rho &\longmapsto \left( (T_1, T_2, T_3) \mapsto \frac{\rho(T_1, T_2)\rho(T_1 + T_2, T_3)}{\rho(T_1, T_2 + T_3)\rho(T_2, T_3)} \right). \end{aligned}$$

We let $H_K = \mathrm{Sym}^2_K(R)^\times \cap \ker \partial^{(2)}_K$.

Let $\overline{R} = R \otimes_K \overline{K}$ (which is the étale algebra of $E[n]$ over $\overline{K}$), and let $\mathrm{Sym}^2_{\overline{K}}(\overline{R})$ be the étale algebra over $\overline{K}$ of the set of unordered pairs of $n$-torsion points. Similarly, we write $\overline{H}$ for $H_{\overline{K}}$.

Let $w : E(\overline{K})[n] \to \overline{R}^\times$ be given by

$$w(S) : T \longmapsto e_n(S, T)$$

where $e_n : E[n] \times E[n] \to \mu_n$ denotes the Weil pairing. Then it is easily seen that the image of $w$ equals the kernel of $\partial_{\overline{K}}$. We showed in [13] that the following is an exact sequence of $G_K$-modules:

$$0 \longrightarrow E(\overline{K})[n] \xrightarrow{w} \overline{R}^\times \xrightarrow{\partial_{\overline{K}}} \overline{H} \longrightarrow 0\,.$$

Taking cohomology, this gives an isomorphism

$$w_2 : H^1(K, E[n]) \longrightarrow H_K/\partial R^\times ,$$

see [13, Lemmas 3.2 and 3.5]. For the construction of explicit $n$-coverings representing elements $\xi \in H^1(K, E[n])$ (which, in our intended application, will be elements of the $n$-Selmer group), we will need an element $\rho \in H_K$ whose image in $H_K/\partial R^\times$ is the image under $w_2$ of $\xi$.

In principle, we could use $w_2$ to compute such a set of representatives of the elements of $\mathrm{Sel}^{(n)}(E/K)$ directly, as we now describe. We now assume that $K$ is a number field. We abbreviate $H_K$ to $H$ (note that what is called $H$ in [13] would be $H/\partial R^\times$ in the notation used here) and usually drop the subscripts on $\Delta$, $\partial$, etc.

Recall the Kummer sequence

$$0 \longrightarrow E(K)/nE(K) \xrightarrow{\delta} H^1(K, E[n]) \longrightarrow H^1(K, E)[n] \longrightarrow 0 .$$

For a place $v$ of $K$, we write $R_v = R \otimes_K K_v$ and $H_v = H_{K_v}$. We denote the canonical maps $H \to H_v$ and $H/\partial R^\times \to H_v/\partial R_v^\times$ by $\mathrm{res}_v$. The maps corresponding to $\delta$ and $w_2$ that we obtain by working over $K_v$ are denoted by $\delta_v$ and $w_{2,v}$.

By the definition of the $n$-Selmer group and the fact that $w_2$ is an isomorphism, we have

$$\begin{aligned} &w_2\bigl(\mathrm{Sel}^{(n)}(E/K)\bigr) \\ &\quad = \{\rho \in H/\partial R^\times \mid \mathrm{res}_v(\rho) \in \mathrm{im}(w_{2,v} \circ \delta_v) \ \text{ for all places } v \text{ of } K\} . \end{aligned}$$

According to [36], the image of $\delta_v$ is the unramified subgroup of $H^1(K_v, E[n])$ unless $v$ is infinite and $n$ is even, or $v$ divides $n$, or the Tamagawa number of $E$ at $v$ is not coprime to $n$. Let $\mathcal{S}$ be the set of places of $K$ that fall into one of these categories. If $v$ is a place of $K$ and $\rho \in H$, we say that $\rho$ is *unramified at* $v$ if $\rho\,\partial R^\times = w_2(\xi)$ with $\xi \in H^1(K, E[n])$ unramified at $v$ (i.e.,

$$\mathrm{res}_v(\xi) \in \ker\bigl(H^1(K_v, E[n]) \to H^1(K_v^{\mathrm{nr}}, E[n])\bigr)$$

where $K_v^{\mathrm{nr}}$ is the maximal unramified extension of $K_v$). This is equivalent to saying that the extension $R(\gamma)/R$ of étale algebras is unramified at $v$ for some $\gamma \in \overline{R}^\times$ satisfying $\partial\gamma = \rho$. Writing $H_\mathcal{S}$ for the subgroup of elements unramified outside $\mathcal{S}$ and $\widetilde{H}_\mathcal{S}$ for the image of $H_\mathcal{S}$ in $H/\partial R^\times$, we then have

$$w_2\bigl(\mathrm{Sel}^{(n)}(E/K)\bigr) = \{\rho \in \widetilde{H}_\mathcal{S} \mid \mathrm{res}_v(\rho) \in \mathrm{im}(w_{2,v} \circ \delta_v) \ \text{ for all } v \in \mathcal{S}\} .$$

For an étale $K$-algebra $A$, write $U_\mathcal{S}(A)$ for the group of $\mathcal{S}$-units of $A$, $I_\mathcal{S}(A)$ for the group of ideals of $A$ supported outside $\mathcal{S}$ and $\mathrm{Cl}_\mathcal{S}(A)$ for the $\mathcal{S}$-class group of $A$. Then there is an exact sequence

$$0 \longrightarrow U_\mathcal{S}(A) \longrightarrow A^\times \longrightarrow I_\mathcal{S}(A) \longrightarrow \mathrm{Cl}_\mathcal{S}(A) \longrightarrow 0 .$$

The map $\partial$ induces a homomorphism from this exact sequence for $A = R$ to the corresponding sequence for $A = \mathrm{Sym}^2_K(R)$. Applying the Snake Lemma to the commutative diagram

$$\begin{tikzcd}
 & R^\times \arrow[r, "\partial"] \arrow[d] & H \arrow[r] \arrow[d] & H/\partial R^\times \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & I_{\mathcal{S}}(R) \arrow[r, "\partial"] & I_{\mathcal{S}}\big(\mathrm{Sym}^2_K(R)\big) \arrow[r] & \dfrac{I_{\mathcal{S}}\big(\mathrm{Sym}^2_K(R)\big)}{\partial I_{\mathcal{S}}(R)} \arrow[r] & 0
\end{tikzcd}$$

and observing that $\widetilde{H}_{\mathcal{S}}$ is the kernel of the right-most vertical map (this uses that $\mathcal{S}$ contains all primes dividing $n$), we obtain an exact sequence

$$0 \longrightarrow \frac{U_{\mathcal{S}}\big(\mathrm{Sym}^2_K(R)\big) \cap H}{\partial U_{\mathcal{S}}(R)} \longrightarrow \widetilde{H}_{\mathcal{S}} \longrightarrow \mathrm{Cl}_{\mathcal{S}}(R)^0 \longrightarrow 0$$

where $\mathrm{Cl}_{\mathcal{S}}(R)^0 = \ker\big(\partial : \mathrm{Cl}_{\mathcal{S}}(R) \to \mathrm{Cl}_{\mathcal{S}}(\mathrm{Sym}^2_K(R))\big)$. There are algorithms for computing $\mathcal{S}$-unit groups and $\mathcal{S}$-class groups of number fields (see for example [9, 7.4.2]), which can be applied to the constituent fields of $R$ and $\mathrm{Sym}^2_K(R)$. Based on these and the exact sequence above, we can compute an explicit set of generators of $\widetilde{H}_{\mathcal{S}}$.

In order to turn the description of $\mathrm{Sel}^{(n)}(E/K)$ above into an algorithm, we need to be able to evaluate $w_{2,v} \circ \delta_v$. This can be done as follows.

Let $T \in E[n]$. Then there is a rational function $G_T \in K(T)(E)^\times$ such that

$$\mathrm{div}(G_T) = [n]^*(T) - [n]^*(O) = \sum_{P:\ nP=T} (P) - \sum_{Q:\ nQ=O} (Q)\,.$$

These functions have the property that $G_T(P + S) = e_n(S,T)G_T(P)$ for all $S \in E[n]$ and $P \in E$, provided both sides are defined. We can choose them in such a way that the map $G : T \mapsto G_T$ is Galois-equivariant. Then we can interpret $G$ as an element of $R(E)^\times$. Here, $R(E) = K(E) \otimes_K R$; its elements are $G_K$-equivariant maps from $E[n]$ into $\overline{K}(E)$. Then we have $G(P + T) = w(T)G(P)$ for $P \in E \setminus E[n^2]$ and $T \in E[n]$.

For $T_1, T_2 \in E[n]$ define rational functions $r_{T_1,T_2}$ (compare [14, p. 67]) by

$$r_{T_1,T_2} = \begin{cases} 1 & \text{if } T_1 = O \text{ or } T_2 = O; \\ x - x(T_1) & \text{if } T_1 + T_2 = O,\ T_1 \neq O; \\ \dfrac{y + y(T_1 + T_2)}{x - x(T_1 + T_2)} - \lambda(T_1, T_2) & \text{otherwise,} \end{cases}$$

where $\lambda(T_1, T_2)$ denotes the slope of the line joining $T_1$ and $T_2$ (or the slope of the tangent line at $T_1 = T_2$ if the points coincide). Just as before, we can package these functions into a single element $r \in \mathrm{Sym}^2_K(R)(E)^\times$.

Now consider the following diagram with exact rows.

$$\begin{tikzcd}
0 \arrow[r] & E(\overline{K})[n] \arrow[r] \arrow[d, equal] & E(\overline{K}) \arrow[r, "n"] \arrow[d, dashed, "G"] & E(\overline{K}) \arrow[r] \arrow[d, dashed, "r"] & 0 \\
0 \arrow[r] & E(\overline{K})[n] \arrow[r, "w"] & \overline{R}^{\times} \arrow[r, "\partial"] & \overline{H} \arrow[r] & 0
\end{tikzcd} \tag{1}$$

The dashed arrows indicate the partially defined maps given by evaluating the tuples of rational functions $G$ and $r$. The right-hand square commutes by [14, Proposition 3.2], provided that we scale the $G_T$ as in the proof of Proposition 3.1 of [14]. The left-hand square commutes in the sense that the actions of $E[n]$ on $E(\overline{K})$ by translation and on $\overline{R}^{\times}$ by multiplication via $w$ are related by $G$, i.e., $G(P+T) = w(T)G(P)$. Chasing through the definitions of the connecting homomorphisms $\delta$ and $w_2$, we now easily find the following.

**Proposition 2.1.** *The composition $w_2 \circ \delta$ is induced by the map $r : E(K) \setminus E[n] \longrightarrow H$.*

We can extend $r$ to divisors on $E$ with support disjoint from $E[n]$ by defining

$$r\Big(\sum_P n_P(P)\Big) = \prod_P r(P)^{n_P} .$$

Then for a principal divisor $D = \operatorname{div}(h)$ we find by Weil reciprocity

$$\begin{aligned} r_{T_1,T_2}(D) = r_{T_1,T_1}\big(\operatorname{div}(h)\big) &= h\big(\operatorname{div}(r_{T_1,T_2})\big) \\ &= \frac{h(T_1)h(T_2)}{h(O)h(T_1+T_2)} = \frac{1}{h(O)}(\partial h|_{E[n]})(T_1,T_2) . \end{aligned}$$

We can scale $h$ so that $h(O) = 1$; then

$$r\big(\operatorname{div}(h)\big) = \partial h|_{E[n]} \in \partial R^{\times}$$

if $h \in K(E)^{\times}$. Therefore we obtain a well-defined map

$$\widetilde{r} : E(K) \cong \operatorname{Pic}^0(E/K) \longrightarrow H/\partial R^{\times} ,$$

and we have

$$w_2 \circ \delta = \widetilde{r} .$$

This construction is valid over any field $K$ of characteristic not dividing $n$; in particular, it can be applied over $K_v$ to find $\operatorname{im}(w_{2,v} \circ \delta_v)$. In [36] there is a discussion of how to compute images under local descent maps, which applies *mutatis mutandis* to the situation at hand.

The following theorem summarises this section.

**Theorem 2.2.** *Let $K$ be a number field, $E/K$ an elliptic curve, and $n \geq 2$. There is an efficient algorithm that computes $\mathrm{Sel}^{(n)}(E/K)$, given knowledge of class and unit groups of the number fields $K(\{T_1, T_2\})$, where $\{T_1, T_2\}$ runs through unordered pairs of $n$-torsion points of $E$.*

*Proof.* The algorithm proceeds in the following steps.

(1.) Let $\mathcal{S}$ be the set of places $v$ of $K$ that divide $n$ or such that the Tamagawa number of $E/K_v$ is not coprime to $n$, together with the real places of $K$ when $n$ is even.
(2.) Construct the étale algebras $R$ and $\mathrm{Sym}^2_K(R)$.
(3.) Compute an explicit representation of $\widetilde{H}_{\mathcal{S}}$ as defined above.
(4.) For each $v \in \mathcal{S}$ construct $\widetilde{H}_v = H_{K_v}/\partial R_v^\times$, together with the map $\mathrm{res}_v : \widetilde{H}_{\mathcal{S}} \to \widetilde{H}_v$, and find the local image $\widetilde{r}(E(K_v)) \subset \widetilde{H}_v$.
(5.) Compute $\mathrm{Sel}^{(n)}(E/K)$ as

$$\bigcap_{v \in \mathcal{S}} \mathrm{res}_v^{-1}\bigl(\widetilde{r}(E(K_v))\bigr) \subset \widetilde{H}_{\mathcal{S}} .$$

The third step (computation of $\widetilde{H}_{\mathcal{S}}$) relies on the computation of the $\mathcal{S}$-class groups and $\mathcal{S}$-unit groups of the constituent fields of $\mathrm{Sym}^2_K(R)$, which are of the form $K(\{T_1, T_2\})$ as in the statement of the theorem. The $\mathcal{S}$-class and $\mathcal{S}$-unit groups can be computed from the class and unit groups. $\square$

As it stands, this result is rather theoretical, since the number fields that occur are (in most cases) too large for practical computations: as mentioned earlier, when $n$ is a prime $p$, then usually there is a component of $\mathrm{Sym}^2_K(R)$ that is a field extension of degree $(p^2-1)(p^2-p)/2$ of $K$. This is already prohibitive when $n = 3$. However, when $n$ is a prime, there is a better alternative, which we describe next.

2.3. **Computation of the Selmer group III: Using $w_1$.** There is a group homomorphism (recalled from [13])

$$w_1 : H^1(K, E[n]) \to R^\times/(R^\times)^n ,$$

which is obtained by applying cohomology to

$$0 \longrightarrow E[n] \xrightarrow{w} \mu_n(\overline{R}) \xrightarrow{\partial} \partial(\mu_n(\overline{R})) \longrightarrow 0 . \tag{2}$$

It is shown in [17] and [36] that when $n$ is a prime $p$, the map $w_1$ is injective (for any field $K$ of characteristic different from $p$), and a description of the image is given. This can be used for computing the $n$-Selmer group as a subgroup of $R^\times/(R^\times)^n$.

Let $v$ be a place of $K$. Then there is an analogous homomorphism

$$w_{1,v} : H^1(K_v, E[n]) \to R_v^\times/(R_v^\times)^n .$$

The maps fit together in a commutative diagram

$$\begin{tikzcd} E(K) \arrow[r, "\delta"] \arrow[d] & H^1(K, E[n]) \arrow[r, "w_1"] \arrow[d] & R^\times/(R^\times)^n \arrow[d, "\mathrm{res}_v"] \\ E(K_v) \arrow[r, "\delta_v"] & H^1(K_v, E[n]) \arrow[r, "w_{1,v}"] & R_v^\times/(R_v^\times)^n. \end{tikzcd}$$

If $w_1$ and all the $w_{1,v}$ are injective (as happens in the case $n$ is prime), then this tells us that the $n$-Selmer group can be realised as an abstract group via

$$\mathrm{Sel}^{(n)}(E/K) \cong R(\mathcal{S}, n) \cap \mathrm{im}(w_1) \cap \bigcap_{v \in \mathcal{S}} \mathrm{res}_v^{-1}\big(\mathrm{im}(w_{1,v} \circ \delta_v)\big) ;$$

see [36]. Here, $R(\mathcal{S}, n) \subset R^\times/(R^\times)^n$ is the subgroup of elements $\alpha$ unramified outside $\mathcal{S}$ (i.e., such that the extension $R(\sqrt[n]{\alpha})/R$ of étale algebras is unramified outside $\mathcal{S}$). As before, the group $R(\mathcal{S}, n)$ can be determined from a knowledge of the $\mathcal{S}$-class and $\mathcal{S}$-unit groups of the various number fields that occur in the splitting of $R$ according to the Galois orbits on $E[n]$.

Note that in [36], the étale algebra $L$ (denoted there by $A$) is used instead of $R = K \times L$. If $\alpha \in R^\times$ represents some $\xi \in H^1(K, E[n])$, then $\alpha(O) \in (K^\times)^n$, so without loss of generality we can assume that $\alpha(O) = 1$. Therefore all the relevant information is already contained in the $L$-component.

If $n$ is not a prime, then the map $w_1$ need not be injective: see Section 2.4 for an example with $n = 4$. For the realisation of $w_1 \circ \delta$, consider the following diagram analogous to (1):

$$\begin{tikzcd} 0 \arrow[r] & E(\overline{K})[n] \arrow[r] \arrow[d, "w"] & E(\overline{K}) \arrow[r, "n"] \arrow[d, dashed, "G"] & E(\overline{K}) \arrow[r] \arrow[d, dashed, "F"] & 0 \\ 0 \arrow[r] & \mu_n(\overline{R}) \arrow[r] & \overline{R}^\times \arrow[r, "n"] & \overline{R}^\times \arrow[r] & 0 \end{tikzcd}$$

Here, $F \in R(E)^\times$ is the function such that $F_T(nQ) = G_T(Q)^n$ for all $T \in E[n]$. The divisor of $F_T$ is $n(T) - n(O)$, and if $F(nQ) = G(Q)^n$ with $G \in R(E)^\times$, then $F$ induces a well-defined map $F : E(K) \setminus E[n] \longrightarrow R^\times/(R^\times)^n$, independent of the particular choice of $F$. In the same way as discussed after Proposition 2.1, we can extend this map $F$ to a map on divisors with support disjoint from $E[n]$, which only depends on the linear equivalence class, and therefore gives rise to a homomorphism

$$\widetilde{F} : E(K) \cong \mathrm{Pic}^0(E/K) \longrightarrow R^\times/(R^\times)^n .$$

This leads to a new proof of the following well-known fact.

**Proposition 2.3.** *The composition $w_1 \circ \delta : E(K) \to R^\times/(R^\times)^n$ is given by $\widetilde{F}$.*

Again, this works for any field $K$ of characteristic not dividing $n$, and so we can use it for evaluating the local maps $\delta_v$. The algorithm for computing $\mathrm{Sel}^{(n)}(K,E)$ then proceeds as before, but now working within $R$ instead of $\mathrm{Sym}^2_K(R)$. The functions $F_T$ can be evaluated at a given point using Miller's algorithm [31], which follows the computation of $nT$ and keeps track of the functions $r_{T_1,T_2}$ witnessing the intermediate sums; it is not necessary to compute an expression for $F_T$ in terms of the coordinateson a Weierstraß equations of $E$ (which will be quite complicated when $n$ is large). In practice, however, even moderately large $n$ quickly make computations infeasible, so $n$ will be rather small, and it is no problem to work with an explicit expression for $F_T$ as a function. Such an expression is also helpful for computing $\varepsilon$ as defined by (9) below.

**Theorem 2.4.** *Let $K$ be a number field, $E/K$ an elliptic curve and $p$ a prime number. There is an efficient algorithm that computes* $\mathrm{Sel}^{(p)}(E/K)$*, given knowledge of class and unit groups of the number fields $K(T)$, where $T$ runs through points of order $p$ on $E$.*

*Proof.* The algorithm proceeds in the following steps (see [36]).

(1.) Let $\mathcal{S}$ be the set of places $v$ of $K$ that divide $p$ or such that the Tamagawa number of $E/K_v$ is divisible by $p$, together with the real places of $K$ when $p=2$.
(2.) Construct the étale algebra $R$.
(3.) Compute an explicit representation of $R_1 = R(\mathcal{S},p) \cap \mathrm{im}(w_1)$.
(4.) For each $v \in \mathcal{S}$ construct $H_v = R_v^\times/(R_v^\times)^p$, together with the map $\mathrm{res}_v : R(\mathcal{S},p) \to H_v$, and find the local image $\widetilde{F}(E(K_v)) \subset H_v$.
(5.) Compute $\mathrm{Sel}^{(p)}(E/K)$ as

$$R_1 \cap \bigcap_{v\in\mathcal{S}} \mathrm{res}_v^{-1}\big(\widetilde{F}(E(K_v))\big) \subset R(\mathcal{S},p)\,.$$

□

2.4. **Changing algebras.** For the purpose of constructing explicit models of $n$-coverings representing the various elements of the $n$-Selmer group, we need to represent the Selmer group elements by elements $\rho \in H$. So after computing $\mathrm{Sel}^{(p)}(E/K)$ as in Theorem 2.4, we need to convert the elements $\alpha \in R^\times$ we obtain as representatives into elements $\rho \in H$. Note that for this purpose it is helpful to choose a small representative for the class of $\alpha$ up to $n$th powers, by applying the method in [21, Section 2] over each constituent field of $R$.

Recall that $H$ is the subgroup of elements $\rho \in \mathrm{Sym}^2_K(R)^\times$ satisfying

$$\rho(T_1,T_2{+}T_3)\rho(T_2,T_3) = \rho(T_1,T_2)\rho(T_1{+}T_2,T_3) \quad \text{for all } T_1,T_2,T_3 \in E[n]. \tag{3}$$

**Lemma 2.5.** *Let $\alpha \in R^\times$ represent an element in the image of $w_1$, i.e., $\alpha(R^\times)^n = w_1(\xi)$ for some $\xi \in H^1(K, E[n])$. Then there exists $\rho \in H$ satisfying $\partial\alpha = \rho^n$ and*

$$\alpha(T) = \textstyle\prod_{i=0}^{n-1} \rho(T, iT) \qquad \text{for all } T \in E[n]. \tag{4}$$

*Moreover if $\rho \in H$ satisfies (4) then $\partial\alpha = \rho^n$ and $\rho\,\partial R^\times = w_2(\xi')$ for some $\xi' \in H^1(K, E[n])$ with $w_1(\xi) = w_1(\xi')$.*

Proof: This is [13, Lemma 3.8]. □

To convert $\alpha$ to $\rho$ we first extract an $n$th root of $\partial\alpha$ in $\mathrm{Sym}^2_K(R)$. We then multiply by an $n$th root of unity in $\mathrm{Sym}^2_K(R)$ to find $\rho$ satisfying (3) and (4). The simplest case, which occurs frequently in practice, is when $\mathrm{Sym}^2_K(R)$ contains no non-trivial $n$th roots of unity. There is then a unique choice of $\rho$. In general we can avoid checking all the conditions in (3) by determining in advance the number of solutions for $\rho$.

**Definition 2.6.** Let $\Gamma$ be the group (under pointwise operations) of all maps $\gamma : E[n] \to \mu_n$ satisfying

$$\frac{\gamma(\sigma T_1)\gamma(\sigma T_2)}{\gamma(\sigma(T_1 + T_2))} = \sigma\left(\frac{\gamma(T_1)\gamma(T_2)}{\gamma(T_1 + T_2)}\right)$$

for all $\sigma \in G_K$ and $T_1, T_2 \in E[n]$.

Let $G \cong \mathrm{Gal}(K(E[n])/K)$ be the subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ describing the action of $G_K$ on $E[n]$. The action of $G_K$ on $\mu_n$ is given by the determinants of these matrices. Hence $\Gamma$ depends only on $G$. Indeed, given generators for $G$, it is easy to compute $\Gamma$ using linear algebra over $\mathbb{Z}/n\mathbb{Z}$. The following lemma shows that the number of solutions for $\rho$ in Lemma 2.5 is $\#\partial\Gamma = (\#\Gamma)/n^2$.

**Lemma 2.7.** (i) *There is an exact sequence of abelian groups*

$$0 \longrightarrow E[n] \xrightarrow{\;w\;} \Gamma \xrightarrow{\;\partial\;} \partial\Gamma \longrightarrow 0.$$

(ii) $\partial\Gamma = \{\rho \in H : \prod_{i=0}^{n-1} \rho(T, iT) = 1$ *for all* $T \in E[n]\}$.

Proof: (i) Since $\Gamma \subset \mu_n(\overline{R})$, this is obtained by restricting the exact sequence (2). We note that if $\gamma \in w(E[n])$ then $\gamma : E[n] \to \mu_n$ is a group homomorphism and so clearly $\gamma \in \Gamma$.

(ii) By [13, Corollary 3.6] every $\rho \in H$ can be written as $\rho = \partial\gamma$ for some $\gamma \in \overline{R}^\times$. We note that if $\rho = \partial\gamma$ then

$$\prod_{i=0}^{n-1} \rho(T, iT) = \gamma(T)^n.$$

Hence the group on the right of (ii) consists of elements $\partial\gamma$ where $\gamma \in \mu_n(\overline{R}) = \mathrm{Map}(E[n], \mu_n)$ and $\partial\gamma : E[n] \times E[n] \to \mu_n$ is Galois equivariant. From Definition 2.6, we recognise this group as $\partial\Gamma$. □

**Lemma 2.8.** *The kernel of* $w_1 : H^1(K, E[n]) \to R^\times/(R^\times)^n$ *is isomorphic to* $(\partial\mu_n(\overline{R}))^{G_K}/\partial(\mu_n(R)) = \partial\Gamma/\partial(\mu_n(R))$.

Proof: This is seen by taking Galois cohomology of the short exact sequence (2) and recalling that $w_1$ is the composite of $w_*$ and an isomorphism $H^1(K, \mu_n(\overline{R})) \cong R^\times/(R^\times)^n$. □

In the case $n = p$ is prime it is shown in [17], [36] that $w_1$ is injective. Then by Lemma 2.8 each of the $\#\partial\Gamma$ possibilities for $\rho$ represent the same element of $H/\partial R^\times$. The lemma also gives a formula for $\#\partial\Gamma$. Writing dim for the dimension of a $\mathbb{Z}/p\mathbb{Z}$-vector space we have

$$\dim \partial\Gamma = \dim \partial(\mu_p(R)) = \dim \mu_p(R) - \dim E(K)[p].$$

For general $n$ we can use Lemma 2.8 to check whether $w_1$ is injective. As promised in [13, Section 3], we give an example to show that $w_1$ need not always be injective.

**Example 2.9.** Taking $n = 4$ we consider the elliptic curve $E/\mathbb{Q}$ with Weierstraß equation

$$y^2 = x^3 + x + 2/13.$$

A calculation using division polynomials shows that $[\mathbb{Q}(E[4]) : \mathbb{Q}] = 48$. Hence $G \subset \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ is a subgroup of index 2. There are precisely three subgroups of index 2 in $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$. These may be viewed as kernels of 1-dimensional characters, one of which factors via the determinant and another via the natural map to $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \cong S_3$. Thus the 3 possibilities for $G$ correspond to whether $-1$, $\Delta_E$ or $-\Delta_E$ is a rational square. In this example $\Delta_E = -(112/13)^2$. Computing $\Gamma$ from $G$ we find $\#\Gamma = 2^8$. It follows by Lemma 2.7(i) that $\#\partial\Gamma = 2^4$. The points of order 2 and 4 on $E$ each form a single Galois orbit, and their fields of definition do not contain $\sqrt{-1}$. Hence $\#E(\mathbb{Q})[4] = 1$ and $\#\partial(\mu_4(R)) = \#\mu_4(R) = 2^3$. It follows by Lemma 2.8 that $w_1$ has kernel of order 2.

This example shows it would be difficult to do a 4-descent directly using the map $w_1$. Fortunately there are better ways of doing 4-descent: see the introduction for references.

2.5. **Initial equations for the covering curves.** Let $C_\xi \to E$ be the $n$-covering corresponding to some $\xi \in H^1(K, E[n])$. In this section we are concerned with finding an explicit model for $C_\xi$ as a genus one normal curve of degree $n^2$ in $\mathbb{P}^{n^2-1}$.

We explain first why we need to work with $\rho \in H$ representing $\xi$, rather than with $\alpha \in R^\times$. Recall the commutative diagram

$$\begin{tikzcd} E(K) \arrow[r, "\delta"] \arrow[dr, "\widetilde{F}"'] & H^1(K, E[n]) \arrow[d, "w_1"] \\ & R^\times/(R^\times)^n \end{tikzcd}$$

from Proposition 2.3. The $K$-rational points on $C_\xi$ should map to the points in $E(K)$ whose image under $\delta$ is $\xi$, so whose image under $\widetilde{F} = w_1 \circ \delta$ is $\alpha(R^\times)^n$. This suggests defining the covering curve by

$$\{(P, z) \in E \times \mathbb{A}(R) : F(P) = \alpha z^n\}, \tag{5}$$

where $\mathbb{A}(R)$ denotes the affine space over $K$ corresponding to the $K$-vector space $R$ (note that $\mathbb{A}(R)$ was denoted $\mathcal{R}$ in [14]). Working over $\overline{K}$ and writing $z_T$ for $z(T)$, which is the value at $T$ of $z \in \overline{R}$ considered as a map on $E[n]$, we note that the $z_T$ can be used as a set of coordinateson $\mathbb{A}(R)$; hence the equation in (5) may be written as

$$F_T(P) = \alpha(T) z_T^n \qquad \text{for all } T \in E[n]\,.$$

We see that for each point $P \in E \setminus E[n]$, there are $n^2$ independent $n$th roots to take to obtain the $z_T$. This makes $n^{n^2}$ choices for $z$, yet the covering map $C_\xi \to E$ has degree only $n^2$. The equation for $T = O$ reads $1 = z_O^n$ (without loss of generality, $\alpha(O) = 1$), so we can eliminate a factor of $n$ by setting $z_O = 1$. Also, by considering $z$ with $z_O = 1$ as a representative of a point in the projective space $\mathbb{P}(R)$ associated to $\mathbb{A}(R)$ and taking the closure in $E \times \mathbb{P}(R)$, we may 'fill the gaps' in (5) at the points with $P = O$ (where the $F_T$ have a pole). This now defines a projective curve $C'$ covering $E$ by a map of degree $n^{n^2-1}$. When $n = 2$, this curve splits into two isomorphic components, and after projecting to $\mathbb{P}(R)$ we obtain an intersection of two quadrics defining the desired curve $C_\xi$. This case will be discussed further in Section 3.

If $n > 2$, then the curve $C'$ defined above splits into $n^{n^2-3}$ geometric components. To see this, we may work over an algebraically closed field $K$; then we can take $\alpha = 1$. We obtain an embedding

$$\iota : E \longrightarrow C', \qquad P \longmapsto \big(nP, \widetilde{G}(P)\big)$$

where $\widetilde{G} : E \to \mathbb{P}(R)$ is induced by $G : E \setminus E[n] \to \mathbb{A}(R)$ (recall that $F(nP) = G(P)^n$). Its image is an $n$-covering of $E$ by projection onto the first factor, and the action of $S \in E[n]$ on it is given by $z_T \mapsto e_n(S,T) z_T$. In addition, $\mu_n(\overline{R})$ acts on $C'$ in an obvious way which is compatible with the action of $E[n]$ and the map $w : E[n] \to \mu_n(\overline{R})$. Taking into account that

$\mu_n = \mu_n(\overline{K}) \subset \mu_n(\overline{R})$ acts trivially on $\mathbb{P}(R)$, this shows that the components of $C'$ are parametrised by $\mu_n(\overline{R})/(w(E[n])\mu_n)$. This is still true over arbitrary fields $K$, and with $\alpha$ representing any $\xi \in H^1(K, E[n])$; in this case the set of geometric components of $C'$ is isomorphic to $\mu_n(\overline{R})/(w(E[n])\mu_n)$ as a Galois module. In some cases, this module has only one element defined over $K$, so there is only one component of $C'$ that is defined over $K$, which must be the one we seek. But in general, there can be a large number of $K$-rational components; and in any case, the equations one obtains (having degree $n > 2$) are not of the desired form, and it seems rather difficult to pick out the relevant component.

Instead, we work with $\rho \in H$ representing $\xi$. The analogue of the above diagram is provided by Proposition 2.1:

$$\begin{tikzcd} E(K) \arrow[r, "\delta"] \arrow[dr, "\widetilde{r}"'] & H^1(K, E[n]) \arrow[d, "w_2"] \\ & H/\partial R^\times \end{tikzcd}$$

We can now define our covering curve using the relation $r(P) = \rho\partial z$. Setting $z_O = 1$ as above, and then homogenising, this reads as

$$C_\rho = \{(P, z) \in E \times \mathbb{P}(R) : r(P) z_O \Delta(z) = \rho \cdot (z \otimes z)\} \subset E \times \mathbb{P}(R) \tag{6}$$

with the covering map $C_\rho \to E$ given by projection to the first factor. Note that (6) is quadratic in $z$. Over $\overline{K}$, in terms of the coordinates $z_T$, the equations read

$$r_{T_1,T_2}(P) z_O z_{T_1+T_2} = \rho(T_1, T_2) z_{T_1} z_{T_2}$$

with $T_1, T_2 \in E[n]$. It is shown in [14] that projecting to $\mathbb{P}(R)$ (which is equivalent to eliminating $P \in E$) gives $n^2(n^2 - 3)/2$ linearly independent quadrics defining $C_\rho \subset \mathbb{P}(R) \cong \mathbb{P}^{n^2-1}$ as a genus one normal curve of degree $n^2$.

The equations for $C_\rho \subset \mathbb{P}(R)$ are obtained from

$$(X - x_T) z_O^2 - \rho(T, -T) z_T z_{-T} \tag{7}$$

for $T \in E[n] \setminus \{O\}$ and

$$(\Lambda_T - \lambda(T_1, T_2)) z_O z_T - \rho(T_1, T_2) z_{T_1} z_{T_2} \tag{8}$$

for $T_1, T_2, T \in E[n] \setminus \{O\}$ with $T_1 + T_2 = T$, by taking differences to eliminate the indeterminates $X$ and $\Lambda_T$. In fact the equations recorded in [14, Proposition 3.7] are these differences.

2.6. **Improved equations for the covering curves.** Suppose $\rho \in H$ represents an element $\xi \in H^1(K, E[n])$ with trivial obstruction (as defined in [13, 14]), for example a Selmer group element $\xi \in \mathrm{Sel}^{(n)}(E/K)$. In the previous section we showed how to write the covering curve $C_\rho$ as a curve of degree $n^2$ in $\mathbb{P}^{n^2-1}$. We now want to write it as a curve of degree $n$ in $\mathbb{P}^{n-1}$. We recall how to do this using the Segre embedding method, as described in [13, Section 5.3] and [14].

First we fix the scaling of the $F_T$ so that each has leading coefficient 1 when expanded as a power series in the local parameter $x/y$ at $O$. Then we define $\varepsilon \in (R \otimes_K R)^\times$ by

$$\varepsilon(T_1, T_2) = \frac{F_{T_1+T_2}(P)}{F_{T_1}(P)F_{T_2}(P - T_1)} \tag{9}$$

(which is independent of $P \in E$), compare Step 2 on p. 154 in [13]. Let $*_{\varepsilon\rho}$ be the new multiplication on $R$ defined by

$$z_1 *_{\varepsilon\rho} z_2 = \mathrm{Tr}(\varepsilon\rho \cdot (z_1 \otimes z_2)) .$$

Then the obstruction algebra $A_\rho = (R, +, *_{\varepsilon\rho})$ is a central simple algebra over $K$ of dimension $n^2$. Since we are assuming that $\rho$ represents an element with trivial obstruction we have $A_\rho \cong \mathrm{Mat}_n(K)$. In Section 6 we discuss how to find such an isomorphism explicitly.

Recall that we have equations for $C_\rho \subset \mathbb{P}(R)$. Since $R$ and $A_\rho$ have the same underlying vector space, and we have now trivialised the obstruction algebra, we get $C_\rho \subset \mathbb{P}(\mathrm{Mat}_n)$. We project $C_\rho$ away from the identity matrix onto the hyperplane of trace zero matrices. The result is a curve $\widetilde{C}$ lying in the locus of rank 1 matrices. In other words the inclusion of this curve in $\mathbb{P}(\mathrm{Mat}_n)$ factors via the Segre embedding

$$\mathbb{P}^{n-1} \times (\mathbb{P}^{n-1})^\vee \to \mathbb{P}(\mathrm{Mat}_n) .$$

Projecting onto a row or column gives either the degree-$n$ curve $C \to \mathbb{P}^{n-1}$ we are looking for, or its dual $C \to (\mathbb{P}^{n-1})^\vee$, which is a curve of degree $n^2 - n$.

Writing $z \in R = K \times L$ as $z = (z_O, z')$, the projection to the subspace of trace-zero matrices corresponds to eliminating $z_O$ from the equations (recall that $\mathrm{Tr}(M_T) = 0$ for $T \neq O$, where $M_T$ gives the action of $T$ on the ambient space $\mathbb{P}^{n-1}$ of $C$). We note that if $T_1 + T_2 = T_1' + T_2' = T$ and $\{T_1, T_2\} \neq \{T_1', T_2'\}$ then $\lambda(T_1, T_2) \neq \lambda(T_1', T_2')$. Assuming $n \geq 3$, it is clear by (7) and (8) that eliminating $z_O$ by linear algebra will reduce the dimension of the vector space of quadrics by exactly $n^2$. So after trivialising the algebra we have $n^2(n^2 - 5)/2$ quadrics that are a basis for the space of quadrics vanishing on

$$\widetilde{C} \subset \mathbb{P}(\mathrm{Tr} = 0) \cong \mathbb{P}^{n^2-2} .$$

Together with the quadrics that are a product of a linear form and the trace form, these span the space of quadrics vanishing on

$$\widetilde{C} \subset \mathbb{P}(\mathrm{Mat}_n) \cong \mathbb{P}^{n^2-1}.$$

**Lemma 2.10.** *Let $C \subset \mathbb{P}^{n-1}$ be a genus one normal curve with homogeneous ideal $I(C) \subset K[x_1, \ldots, x_n]$. Let $\widetilde{C}$ be the image of the map $C \to \mathbb{P}^{n-1} \times (\mathbb{P}^{n-1})^\vee \to \mathbb{P}(\mathrm{Mat}_n)$ with homogeneous ideal $I(\widetilde{C}) \subset K[z_{11}, z_{12}, \ldots, z_{nn}]$. If $f \in K[x_1, \ldots, x_n]$ is a homogeneous form, then*

$$f(x_1, \ldots, x_n) \in I(C) \iff f(z_{11}, z_{21}, \ldots, z_{n1}) \in I(\widetilde{C}).$$

Proof: This is clear since the dual curve spans $(\mathbb{P}^{n-1})^\vee$. □

The quadrics vanishing on $C \subset \mathbb{P}^{n-1}$ may now be computed by linear algebra. If $n \geq 4$ then these quadrics define $C$. (In fact they generate the homogeneous ideal.) When $n = 3$ the equation for $C$ is a ternary cubic. In Section 4 we explain how this too may be computed using linear algebra.

## 3. Application to 2-descent

We show that the method sketched above reduces in the case $n = 2$ to classical 2-descent, as described, for example, in [5], [35], and with algorithmic details in [38].

Let $E$ be given by a short Weierstraß equation:

$$E: \quad y^2 = f(x) = (x - e_1)(x - e_2)(x - e_3).$$

Let $T_i = (e_i, 0)$. We have $R = K \times L$ where $L = K[e]$ is the cubic $K$-algebra generated by $e$ with minimal polynomial $f(x)$. Let $\alpha \in R^\times$ represent a Selmer group element. We write $\alpha_i = \alpha(T_i)$. Without loss of generality the $K$-component of $\alpha$ is 1, and we may regard $\alpha$ as an element of $L^\times$. It is well known (see [35, Theorem 1.1]) that $w_1$ induces an isomorphism

$$H^1(K, E[2]) \cong \ker\left(L^\times/(L^\times)^2 \xrightarrow{N_{L/K}} K^\times/(K^\times)^2\right).$$

Therefore $\alpha$ has square norm, say $N_{L/K}\alpha = \alpha_1\alpha_2\alpha_3 = b^2$ for some $b \in K^\times$. Taking $F_{T_i} = x - e_i$ in (5), and setting $z_O = 1$, we obtain equations

$$\begin{aligned} x - e_i &= \alpha_i z_i^2 \qquad \text{for } i = 1, 2, 3 \\ y &= \pm b z_1 z_2 z_3 \end{aligned} \tag{10}$$

where $z_i = z(T_i)$. Alternatively, since

$$r(T_i, T_j) = \begin{cases} x - e_i & \text{if } i = j \\ y/(x - e_k) & \text{if } \{i, j, k\} = \{1, 2, 3\}, \end{cases}$$

and $\alpha \in R^\times$ corresponds to $\rho \in H$ where

$$\rho(T_i, T_j) = \begin{cases} \alpha_i & \text{if } i = j \\ b/\alpha_k & \text{if } \{i, j, k\} = \{1, 2, 3\}, \end{cases}$$

we obtain the same equations using (6). The components of $r$ and $\rho$ where one of the torsion points is $O$ are all trivial. Notice that switching the sign of $b$ multiplies $\rho$ by $\partial\gamma$ where $\gamma = (1, -1) \in K \times L$.

The first three equations in (10) may be written (after homogenisation) as

$$x - eu_3^2 = \alpha u^2,$$

where $u = u_0 + u_1 e + u_2 e^2$ is an "unknown" element of $L^\times$. Expanding and equating coefficients of powers of $e$ gives two quadrics in $u_0, u_1, u_2, u_3$, defined over $K$, which define $C_\rho \subset \mathbb{P}^3$ as a curve of degree 4. We would like to write $C_\rho$ as a double cover of $\mathbb{P}^1$. The classical approach is to observe that one of the quadrics does not involve $u_3$ and hence defines a conic $S$ in $\mathbb{P}^2(u_0, u_1, u_2)$; the projection to $S$ is a double cover $C_\rho \to S$. If $\alpha$ is a Selmer group element then $S \cong \mathbb{P}^1$. In practice one expresses the isomorphism $\mathbb{P}^1 \to S$ as a parametrisation $u_j = q_j(v_0, v_1)$ for $j = 1, 2, 3$, where the $q_j$ are binary quadratics; substituting into the first quadric in the $u_j$, in which the only term involving $u_3$ is (a non-zero constant times) $u_3^2$, we find an equation for $C_\rho$ of the form $u_3^2 = Q(v_0, v_1)$ where $Q$ is a binary quartic.

To obtain the 2-covering map $C_\rho \to E$ we simply substitute in (10) to recover $x$, while $y$ is determined up to sign by $y^2 = N_{L/K}(\alpha u^2)$. Hence we have two possibilities for the covering map, which differ by negation on $E$; these 2-coverings are equivalent.

We now compare with the Segre embedding method as described in Section 2.6. The obstruction algebra is $A = (R, +, *_{\varepsilon\rho})$ where using (9) we compute

$$\varepsilon(T_i, T_j) = \begin{cases} 1/f'(e_i) & \text{if } i = j \\ 1/(e_i - e_j) & \text{otherwise.} \end{cases}$$

Let $S = \{z \in \mathbb{P}(A) : \mathrm{Trd}(z) = \mathrm{Nrd}(z) = 0\}$. Our general recipe says that if we project $C_\rho$ to the plane $\{\mathrm{Trd}(z) = 0\}$, then the result lies in $S$. This gives $C_\rho$ as a double cover of $S$. In fact, $S$ is defined by $z_O = 0$ and $z *_{\varepsilon\rho} z = 0$. The latter works out as

$$\sum_{i=1}^{3} \frac{\alpha_i}{f'(e_i)} z_i^2 = 0$$

which is one of the quadrics in the pencil defining $C_\rho$. Hence our conic $S$ is the same as that considered in the classical approach. The problems of trivialising $A$ and finding a rational point on $S$ are clearly equivalent. Once we have trivialised $A$ we get an isomorphism $S \cong \mathbb{P}^1$ by projecting to a row or column (it does not matter which, since $\mathbb{P}^1$ is self-dual). Exactly as before we can then write $C_\rho$ as a double cover of $\mathbb{P}^1$.

## 4. Application to 3-descent

We give further details of our algorithms in the case $n = 3$. Let $E$ be an elliptic curve over a number field $K$. We fix an isomorphism $E[3] \cong (\mathbb{Z}/3\mathbb{Z})^2$, say $T_{ij} \mapsto (i,j)$, and let $T = T_{11}$. We assume that the Galois action on $E[3]$ is generic, in the sense that $\rho_{E,3} : G_K \to \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ is surjective[2]. Then there is a tower of number fields

$$\begin{array}{c} M = K(E[3]) \\ \Big| \scriptstyle 2 \\ M^+ \\ \Big| \scriptstyle 3 \\ L = K(T) \\ \Big| \scriptstyle 2 \\ L^+ \\ \Big| \scriptstyle 4 \\ K \end{array}$$

where $M^+$ is the subfield of $M$ fixed by $T_{ij} \mapsto T_{ji}$ and $L^+$ is the subfield of $L$ fixed by $\sigma : T \mapsto -T$. We write $\iota_{ij} : L \to M$ for the embedding given by $T \mapsto T_{ij}$. Thus $\iota_{11}$ is the natural inclusion and $\iota_{ij} \circ \sigma = \iota_{-i,-j}$.

There are two orbits for the action of $G_K$ on $E[3]$, with representatives $O$ and $T$, and six orbits for the action of $G_K$ on $E[3] \times E[3]$, with representatives

$$(O,O),\ (T,O),\ (O,T),\ (-T,-T),\ (T,-T),\ (T_{10},T_{01})$$

chosen so that each pair sums to either $O$ or $T$. Using these representatives we identify $R = K \times L$ and (writing $r = (r_1, r_2)$, $s = (s_1, s_2)$ with $r_1, s_1 \in K$, $r_2, s_2 \in L$)

$$\begin{aligned} R \otimes_K R &\cong K \times L \times L \times L \times L \times M \\ r \otimes s &\mapsto (r_1 s_1, r_2 s_1, r_1 s_2, \sigma(r_2)\sigma(s_2), r_2\sigma(s_2), \iota_{10}(r_2)\iota_{01}(s_2))\,. \end{aligned} \tag{11}$$

The comultiplication $\Delta : R \to R \otimes_K R$ is given by

$$(r_1, r_2) \mapsto (r_1, r_2, r_2, r_2, r_1, r_2)$$

[2]If $K = \mathbb{Q}$ then there are exactly 8 possibilities for $\mathrm{im}(\rho_{E,3})$ up to conjugacy. Our MAGMA implementation relies on a similar analysis of all 8 cases.

and the trace map $\mathrm{Tr} : R \otimes_K R \to R$ by

$$(a, b_1, b_2, b_3, b_4, c) \mapsto \left(a + \mathrm{Tr}_{L/K}(b_4), b_1 + b_2 + b_3 + \mathrm{Tr}_{M/L}(c)\right). \tag{12}$$

In Section 2.3 we showed how to compute $\alpha = (1, a) \in R^\times$ representing an element of $\mathrm{Sel}^{(3)}(E/K)$. We now compute

$$u = \sqrt[3]{a\sigma(a)}, \qquad v = \sqrt[3]{\iota_{10}(a)\iota_{01}(a)/a},$$

by extracting cube roots in $L^+$ and $M^+$. Since $\det \rho_{E,3}$ is the cyclotomic character, these fields have no non-trivial cube roots of unity. Hence $u$ and $v$ are uniquely determined. The elements $\varepsilon$ and $\rho$ in $R \otimes_K R$ are defined by

$$\begin{aligned} \varepsilon &= (1, 1, 1, 1, 1, e_3(T_{10}, T_{01})) \\ \rho &= (1, 1, 1, \sigma(a)/u, u, v) \end{aligned} \tag{13}$$

where $e_3 : E[3] \times E[3] \to \mu_3$ is the Weil pairing. The reader is warned that this $\varepsilon$ is different from the one given in (9). We explain how to correct for this in Section 7. The sign convention we use for the Weil pairing does matter, but is not worth fixing here since we can correct for it later if necessary.

Let $u_1, \ldots, u_8$ be a basis for $L$ over $K$. (In Section 5 we describe how to make a good choice of basis.) Then $R$ has basis $r_1, \ldots, r_9$ where $r_1 = (1, 0)$ and $r_{i+1} = (0, u_i)$. Structure constants $c_{ijk} \in K$ for the obstruction algebra $A = (R, +, *_{\varepsilon\rho})$ are now given by

$$\mathrm{Tr}(\varepsilon\rho(r_i \otimes r_j)) = \textstyle\sum_{k=1}^{9} c_{ijk} r_k.$$

The $c_{ijk}$ are computed using the formulae (11), (12) and (13). Since $\alpha$ represents a Selmer group element we know that $A_\rho \cong \mathrm{Mat}_3(K)$. In Section 6 we show how to find such an isomorphism explicitly. In other words, we find (non-zero) matrices $M_1, \ldots, M_9 \in \mathrm{Mat}_3(K)$ satisfying

$$M_i M_j = \textstyle\sum_{k=1}^{9} c_{ijk} M_k. \tag{14}$$

We fix a Weierstraß equation $y^2 = x^3 + ax + b$ for $E$ and let $T = (x_T, y_T)$. The tangent line to $E$ at $T$ has slope $\lambda_T = \lambda(T, T) = (3x_T^2 + a)/(2y_T)$. We define linear forms in indeterminates $z_1, \ldots, z_8$,

$$\begin{aligned} z_T &= \textstyle\sum_{i=1}^{8} u_i z_i & \qquad z_{10} &= \textstyle\sum_{i=1}^{8} \iota_{10}(u_i) z_i \\ z_{-T} &= \textstyle\sum_{i=1}^{8} \sigma(u_i) z_i & \qquad z_{01} &= \textstyle\sum_{i=1}^{8} \iota_{01}(u_i) z_i \end{aligned}$$

where $u_1, \ldots, u_8$ is our basis for $L$ over $K$. Let $Q_1$ and $Q_2$ be the quadrics with coefficients in $L^+$ and $M^+$ defined by

$$\begin{aligned} Q_1(z_0, \ldots, z_8) &= x_T z_0^2 + \rho_5 z_T z_{-T} \\ Q_2(z_0, \ldots, z_8) &= (\lambda_T + \kappa_T) z_0 z_T - \rho_4 z_{-T}^2 + \rho_6 z_{10} z_{01} \end{aligned}$$

where the $\rho_i$ are the components of $\rho$, and $\kappa_T = \frac{1}{3}(\iota_{10}(\lambda_T) + \iota_{01}(\lambda_T) - \lambda_T)$. Writing each coefficient in terms of fixed $K$-bases for $L^+$ and $M^+$, we obtain

$[L^+ : K] = 4$ quadrics from $Q_1$ and $[M^+ : K] = 24$ quadrics from $Q_2$. In [13] these are called the quadrics of types I and II. We choose our basis for $L^+$ so that its first element is 1, and ignore the first type I quadric. The result is 27 quadrics in $K[z_0, \ldots, z_8]$.

**Lemma 4.1.** *These 27 quadrics generate the homogeneous ideal of the degree 9 curve $C_\rho \subset \mathbb{P}(R) = \mathbb{P}^8$.*

PROOF: Let $v_1 = 1, v_2, v_3, v_4$ be a basis for $L^+$ over $K$. We write

$$x_T z_0^2 + \rho(T, -T) z_T z_{-T} = \textstyle\sum_{i=1}^4 v_i q_i(z_0, \ldots, z_8)$$

where $q_1, \ldots, q_4 \in K[z_0, \ldots, z_8]$. Then (7) becomes

$$\begin{aligned} X &= q_1(z_0, \ldots, z_8) \\ 0 &= q_i(z_0, \ldots, z_8) \qquad \text{for } i = 2, 3, 4. \end{aligned}$$

We eliminate $X$ by ignoring the first quadric $q_1$.

Next we take $(T_1, T_2) = (T_{10}, T_{01})$ and $(-T, -T)$ in (8). Subtracting to eliminate $\Lambda_T$ gives the quadric

$$(\lambda(T_{10}, T_{01}) - \lambda(-T, -T)) z_0 z_T - \rho(-T, -T) z_{-T}^2 + \rho(T_{10}, T_{01}) z_{10} z_{01}.$$

Assuming that

$$\lambda(T_{10}, T_{01}) = \tfrac{1}{3}\big(\lambda(T_{10}, T_{10}) + \lambda(T_{01}, T_{01}) - \lambda(T, T)\big) \tag{15}$$

this is precisely the quadric $Q_2$. To complete the proof we note that (15) is a special case of the following lemma. □

**Lemma 4.2.** *Let $T_1, T_2, T_3 \in E[3] \setminus \{O\}$ with $T_1 + T_2 + T_3 = O$. Then*

$$\lambda(T_1, T_2) = \tfrac{1}{3} \sum_{i=1}^{3} \lambda(T_i, T_i).$$

PROOF: Let $f_i = y - \lambda_i x - \nu_i$ be the equation of the tangent line at $T_i$ and $f = y - \lambda x - \nu$ the equation of the chord through $T_1$, $T_2$ and $T_3$. As rational functions on $E$ we have $f_1 f_2 f_3 = f^3$. Expanding as power series in the local parameter $x/y$ at $O$ it follows that $\lambda = \frac{1}{3}(\lambda_1 + \lambda_2 + \lambda_3)$ as required. □

The remainder of the algorithm is the same for all Galois actions on $E[3]$. As specified in Section 2.6, we intersect the above space of quadrics with $K[z_1, \ldots, z_8]$ to leave an 18-dimensional space of quadrics defining the projection of $C_\rho \subset \mathbb{P}(R) = \mathbb{P}^8$ to $\mathbb{P}(L) = \mathbb{P}^7$. In other words we eliminate the monomials $z_0 z_i$ by linear algebra. We then make the following changes of coordinates

- A change of coordinates corresponding to pointwise multiplication by the "fudge factor" $1/y_T \in L$ (relative to the basis $u_1, \ldots, u_8$). This is to make up for the fact that the definitions of $\varepsilon$ in (9) and (13) are different. We explain this further in Section 7.
- A change of coordinates corresponding to the trivialisation of the obstruction algebra.

We now have 18 quadrics in variables $z_{ij}$ where $1 \leq i, j \leq 3$. These coordinates correspond to the standard basis for $\mathrm{Mat}_3(K)$.

**Lemma 4.3.** *Substituting $z_{ij} = x_i y_j$ gives a basis for the space of $(2,2)$-forms vanishing on the image of $C \to \mathbb{P}^2 \times (\mathbb{P}^2)^\vee$.*

PROOF: We start with a basis for the 18-dimensional space of quadrics vanishing on $\widetilde{C} \subset \mathbb{P}(\mathrm{Tr} = 0)$. This may be identified with the space of quadrics vanishing on $\widetilde{C} \subset \mathbb{P}(\mathrm{Mat}_3)$ that are "singular at $I_3$". (A quadric is "singular at $I_3$" if when we write it relative to a basis for $\mathrm{Mat}_3(K)$ with first basis vector $I_3$, the first variable does not appear.) Substituting $z_{ij} = x_i y_j$ gives a surjective linear map $\Phi$ from the 45-dimensional space of quadrics in $z_{11}, \ldots, z_{33}$ to the 36-dimensional space of $(2,2)$-forms in $x_1, x_2, x_3$ and $y_1, y_2, y_3$. The kernel is spanned by the $2 \times 2$ minors of the matrix $(z_{ij})$ and is a complement to the space of quadrics "singular at $I_3$". Thus $\Phi$ induces an isomorphism between the space of quadrics vanishing on $\widetilde{C} \subset \mathbb{P}(\mathrm{Tr} = 0)$ and the space of $(2,2)$-forms vanishing on the image of $C \to \mathbb{P}^2 \times (\mathbb{P}^2)^\vee$. □

We multiply each of the forms constructed in Lemma 4.3 by the $x_i$ to obtain 54 forms of bidegree $(3,2)$. The following lemma shows that there is a ternary cubic $f$, unique up to scalars, such that $y_1^2 f(x_1, x_2, x_3)$ belongs to the span of these 54 forms. Moreover $f$ is the equation of the curve $C \subset \mathbb{P}^2$ we are looking for.

**Lemma 4.4.** *Let $C \subset \mathbb{P}^2$ be a non-singular plane cubic with equation $f = 0$. Let $V$ be the space of $(2,2)$-forms vanishing on the image of $C \to \mathbb{P}^2 \times (\mathbb{P}^2)^\vee$. Then $y_1^2 f(x_1, x_2, x_3)$ is a $(3,2)$-form in the ideal generated by $V$. Moreover this is the only such polynomial up to scalars.*

PROOF: By Euler's identity $3f = \sum x_i \frac{\partial f}{\partial x_i}$ we have

$$3y_1^2 f = x_2 y_1 g_{12} + x_3 y_1 g_{13} + \frac{\partial f}{\partial x_1} y_1 \ell. \tag{16}$$

where $\ell = \sum_{i=1}^3 x_i y_i$ and $g_{ij} = y_i \frac{\partial f}{\partial x_j} - y_j \frac{\partial f}{\partial x_i}$ are bi-homogeneous forms vanishing on the image of $C \to \mathbb{P}^2 \times (\mathbb{P}^2)^\vee$. Exactly as in the proof of Lemma 2.10, the uniqueness statement follows from the fact that the dual curve spans $(\mathbb{P}^2)^\vee$. □

Lemma 4.4 allows us to compute the ternary cubic $f$ by linear algebra. If we had made the wrong choice of sign for the Weil pairing, then the matrices

$M_i$ in (14) would be the transposes of the desired ones; switching the roles of the $x_i$ and $y_j$ corrects for this.

Our implementation in MAGMA over $K = \mathbb{Q}$ finishes by minimising and reducing the ternary cubic as described in [15]. The covering map, computed using the classical formulae in [1], is also returned.

## 5. A good basis for the obstruction algebra

The obstruction algebra $A_\rho = (R, +, *_{\varepsilon\rho})$ was defined in Section 2.6. In the case $K = \mathbb{Q}$ we explain how to choose a $\mathbb{Q}$-basis for $R$ so that the structure constants for $A_\rho$ are small integers. This is useful for the later parts of our algorithm, for example when trivialising the obstruction algebra as described in the next section.

We recall that $R$ is a product of number fields. Its ring of integers $\mathcal{O}_R$ is the product of the rings of integers of these fields. A fractional ideal in $R$ is just a tuple of fractional ideals, one for each field, and a prime ideal is a tuple where one component is a prime ideal, and all other components are unit ideals.

Let $\alpha \in R^\times$ represent $w_1(\xi)$ for some $\xi \in H^1(\mathbb{Q}, E[n])$. We write $(\alpha) = \mathfrak{b}\mathfrak{c}^n$ where $\mathfrak{b}$ is integral and $n$th power free. We then choose as our $\mathbb{Q}$-basis for $R$ a $\mathbb{Z}$-basis for $\mathfrak{c}^{-1}$ that is LLL-reduced with respect to the inner product

$$\langle z_1, z_2 \rangle = \sum_{T \in E[n]} |\alpha(T)|^{2/n} z_1(T) \overline{z_2(T)}. \tag{17}$$

where the bar denotes complex conjugation. In the remainder of this section we explain why this is a good choice. Notice that in defining the inner product we have implicitly fixed an embedding $\overline{\mathbb{Q}} \subset \mathbb{C}$.

We restrict to the case $n = 2m - 1$ is odd and take for $\varepsilon$ the square root of the Weil pairing, i.e., $\varepsilon(S,T) = e_n(S,T)^m$. By definition of $w_1$ (see [13, Section 3]) there exists $\gamma \in \overline{R}^\times$ with $\gamma^n = \alpha$ and $w(\xi_\sigma) = \sigma(\gamma)/\gamma$ for all $\sigma \in G_\mathbb{Q}$. Then $w_2(\xi) = \rho\partial R^\times$ where $\rho = \partial\gamma \in (R \otimes R)^\times$.

**Lemma 5.1.** *The structure constants for $A_\rho$ with respect to a $\mathbb{Z}$-basis for $\mathfrak{c}^{-1}$ are integers, i.e., $(\mathfrak{c}^{-1}, +, *_{\varepsilon\rho}) \subset A_\rho$ is an order.*

Proof: Let $\mathfrak{p}$ be a prime of $R$. Put $r = \operatorname{ord}_\mathfrak{p}(\mathfrak{b})$ and $q = \operatorname{ord}_\mathfrak{p}(\mathfrak{c})$ so that $\operatorname{ord}_\mathfrak{p}(\alpha) = qn + r$ with $0 \le r < n$. Let $z_1, z_2 \in \mathfrak{c}^{-1}$. Then $\operatorname{ord}_\mathfrak{p}(z_i) \ge -q$ for $i = 1, 2$. Extending $\operatorname{ord}_\mathfrak{p}$ to $\overline{R}^\times$ and recalling that $\gamma^n = \alpha$, we have $\operatorname{ord}_\mathfrak{p}(\gamma z_i) \ge 0$. Then

$$\begin{aligned} z_1 *_{\varepsilon\rho} z_2 &= \operatorname{Tr}(\varepsilon\rho \cdot (z_1 \otimes z_2)) \\ &= \gamma^{-1} \operatorname{Tr}(\varepsilon \cdot (\gamma z_1 \otimes \gamma z_2)). \end{aligned}$$

Since $\varepsilon \in R \otimes_K R$ is integral and the trace map $\operatorname{Tr} : R \otimes_K R \to R$ preserves integrality we deduce $\operatorname{ord}_\mathfrak{p}(z_1 *_{\varepsilon\rho} z_2) \ge -(qn + r)/n$. Since this valuation is an integer we must therefore have $\operatorname{ord}_{\mathfrak{p}}(z_1 *_{\varepsilon\rho} z_2) \geq -q$. Repeating for all primes $\mathfrak{p}$ of $R$ it follows that $z_1 *_{\varepsilon\rho} z_2 \in \mathfrak{c}^{-1}$ as required. □

Let $\tau \in G_{\mathbb{Q}}$ be complex conjugation. (Recall that we fixed an embedding $\overline{\mathbb{Q}} \subset \mathbb{C}$.) Since $n$ is odd we have $H^1(\mathbb{R}, E[n]) = 0$ and so $\tau(\gamma)/\gamma = w(\xi_\tau) = w(\tau(S) - S)$ for some $S \in E[n]$. Therefore dividing $\gamma$ by $w(S)$ we may assume that $\gamma : E[n] \to \overline{\mathbb{Q}}$ is $G_{\mathbb{R}}$-equivariant. It follows by [13, Lemma 4.6] that pointwise multiplication by $\gamma$ defines an isomorphism $A_\rho \otimes \mathbb{R} \cong A_1 \otimes \mathbb{R}$.

Let $T_1, T_2$ be a basis for $E[n](\mathbb{C})$ with $\overline{T}_1 = T_1$, $\overline{T}_2 = -T_2$ and $e_n(T_1, T_2) = \zeta_n$. We define

$$h(T_1) = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix}, \quad h(T_2) = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & \zeta_n & 0 & \cdots & 0 \\ 0 & 0 & \zeta_n^2 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & \zeta_n^{n-1} \end{pmatrix},$$

and

$$\begin{array}{rccl} h: & E[n](\mathbb{C}) & \to & \operatorname{Mat}_n(\mathbb{C}) \\ & rT_1 + sT_2 & \mapsto & \zeta_n^{-rs/2} h(T_1)^r h(T_2)^s \end{array}$$

where the exponent of $\zeta_n$ is an element of $\mathbb{Z}/n\mathbb{Z}$. It may be verified that

$$h(S)h(T) = \varepsilon(S,T)h(S+T)$$

for all $S, T \in E[n]$. Hence there is an isomorphism $A_1 \otimes \mathbb{C} \cong \operatorname{Mat}_n(\mathbb{C})$ given by $z \mapsto \sum_T z(T)h(T)$. Since this isomorphism respects complex conjugation it restricts to an isomorphism $A_1 \otimes \mathbb{R} \cong \operatorname{Mat}_n(\mathbb{R})$.

Composing the isomorphisms defined in the previous two paragraphs gives a trivialisation of $A_\rho$ over $\mathbb{R}$, i.e.,

$$A_\rho \otimes \mathbb{R} \cong \operatorname{Mat}_n(\mathbb{R})\,; \quad z \mapsto \sum_{T \in E[n]} \gamma(T) z(T) h(T). \tag{18}$$

We use this trivialisation first to compute the discriminant of the order in Lemma 5.1 and then to explain why we chose the inner product (17). The *discriminant* $\operatorname{Disc}(R)$ of $R$ is the product of the discriminants of the constituent fields. The *norm* of $\mathfrak{b} \subset \mathcal{O}_R$ is $\operatorname{Norm}\mathfrak{b} = \#(\mathcal{O}_R/\mathfrak{b})$.

**Lemma 5.2.** *The order $\mathcal{O} = (\mathfrak{c}^{-1}, +, *_{\varepsilon\rho}) \subset A_\rho$ has discriminant*

$$n^{n^2} (\operatorname{Norm}\mathfrak{b})^{2/n} \operatorname{Disc}(R).$$

Proof: Let $r_1, \ldots, r_{n^2}$ be a $\mathbb{Z}$-basis for $\mathfrak{c}^{-1}$ mapping to matrices $M_1, \ldots, M_{n^2}$ (say) under the trivialisation (18). Then the discriminant of $\mathcal{O}$ is $\operatorname{Disc}(\mathcal{O}) = \det(\operatorname{Trd}(r_i r_j)) = \det(\operatorname{Tr}(M_i M_j))$. But

$$\operatorname{Tr}(h(S)h(T)) = \begin{cases} n & \text{if } S + T = O \\ 0 & \text{otherwise.} \end{cases}$$

Noting that $[-1]$ is an even permutation of $E[n]$ we compute

$$\begin{array}{rcl}\operatorname{Disc}(\mathcal{O}) & = & \det\big(n\sum_{T\in E[n]}\gamma(T)r_i(T)\gamma(-T)r_j(-T)\big)_{i,j} \\ & = & n^{n^2}\big(\prod_{T\in E[n]}\gamma(T)^2\big)\big(\det(r_i(T))_{i,T}\big)^2.\end{array}$$

By considering the basis for $\overline{R} = \operatorname{Map}(E[n],\overline{K})$ consisting of indicator functions it is clear that for $z \in R$ we have $\operatorname{Tr}_{R/\mathbb{Q}}(z) = \sum_T z(T)$ and $N_{R/\mathbb{Q}}(z) = \prod_T z(T)$. Since $\gamma$ is $G_{\mathbb{R}}$-equivariant we also have $\prod_T \gamma(T) \in \mathbb{R}$. Hence $\prod_T \gamma(T)^2 = |N_{R/\mathbb{Q}}(\alpha)|^{2/n}$ and

$$\big(\det(r_i(T))_{i,T}\big)^2 = \operatorname{Disc}(r_1,\ldots,r_{n^2}) = (\operatorname{Norm}\mathfrak{c})^{-2}\operatorname{Disc}(R).$$

Recalling that $(\alpha) = \mathfrak{b}\mathfrak{c}^n$ the result is now clear. □

**Remark 5.3.** If we start with a Selmer group element then the discriminant computed in Lemma 5.2 is a product of primes dividing $n$ and primes of bad reduction for $E$. Indeed if $\mathfrak{p}$ is a prime of $R$ not dividing any of these primes then $\operatorname{ord}_{\mathfrak{p}}(\alpha) \equiv 0 \pmod{n}$. The term $\operatorname{Disc}(R)$ is of the stated form by (the easier implication of) the criterion of Néron-Ogg-Shafarevich.

Next we give some justification for our choice of inner product. (See also Section 6.5 and the examples in Section 8.)

**Lemma 5.4.** *The real trivialisation (18) identifies the inner product (17) with (a scalar multiple of) the standard Euclidean inner product* $\langle\ ,\ \rangle$ *on* $\operatorname{Mat}_n(\mathbb{R}) \cong \mathbb{R}^{n^2}$.

Proof: Extending $\langle\ ,\ \rangle$ to an inner product on $\operatorname{Mat}_n(\mathbb{C})$ we have

$$\langle h(S), h(T)\rangle = \begin{cases} n & \text{if } S = T \\ 0 & \text{otherwise.}\end{cases}$$

Therefore if $z_1, z_2 \in R$ map to $M_1, M_2 \in \operatorname{Mat}_n(\mathbb{R})$ then

$$\begin{array}{rcl}\langle M_1, M_2\rangle & = & n\sum_{T\in E[n]}|\gamma(T)|^2 z_1(T)\overline{z_2(T)} \\ & = & n\sum_{T\in E[n]}|\alpha(T)|^{2/n} z_1(T)\overline{z_2(T)}.\end{array}$$

□

In principle we could now bound the size of the structure constants. But in practice the structure constants are much smaller than these bounds would suggest. (We encounter a similar situation at the end of Section 6.)

## 6. Inside the "Black Box"

Our work on $n$-descent on elliptic curves requires us to make the Hasse principle explicit. In the case $n = 2$ this means we have to solve a conic in order to represent a 2-Selmer group element as a double cover of $\mathbb{P}^1$ rather than as an intersection of quadrics in $\mathbb{P}^3$. In this section we discuss the general case, and in particular give an algorithm that is practical when $K = \mathbb{Q}$ and $n = 3$. See [29] for an algorithm for general $K$ and $n$ based on similar ideas, and a complexity analysis.

6.1. **Central simple algebras.** We recall some standard theory. See for example [40, Part II]. Let $K$ be a field. A central simple algebra $A$ over $K$ is a finite-dimensional algebra over $K$ with centre $K$ and no two-sided ideals (except 0 and $A$). Wedderburn's Theorem states that $A$ is then isomorphic to a matrix algebra over a division algebra (i.e., skew field) $D$ with centre $K$. The Brauer group $\mathrm{Br}(K)$ of $K$ is the set of equivalence classes of central simple algebras over $K$, where $A$ and $A'$ are equivalent if they are matrix algebras over the same division algebra $D$. The group law is given by tensor product, i.e., $[A] \cdot [A'] = [A \otimes_K A']$, and the inverse of $[A]$ is the class of the opposite algebra $A^{\mathrm{op}}$ obtained by reversing the order of multiplication. The identity element is the class of matrix algebras over $K$.

If $A$ is a central simple algebra over $K$ and $L/K$ is any field extension then $A_L = A \otimes_K L$ is a central simple algebra over $L$. The reduced trace and norm are defined as $\mathrm{Trd}(a) = \mathrm{tr}(\varphi(a))$ and $\mathrm{Nrd}(a) = \det(\varphi(a))$ where $\varphi : A_{\overline{K}} \cong \mathrm{Mat}_n(\overline{K})$ is an isomorphism of $\overline{K}$-algebras. These definitions are independent of the choice of $\varphi$ by the Noether-Skolem theorem. We likewise define the rank of $a \in A$ to be the rank of $\varphi(a)$.

Now let $K$ be a number field. For each place $v$ of $K$ there is a natural map $\mathrm{Br}(K) \to \mathrm{Br}(K_v)$ given by $[A] \mapsto [A_{K_v}]$. We recall [33, Section 32] that $A_{K_v}$ is a matrix algebra over $K_v$ for all $v$ outside a finite set of places depending on $A$. It is then one of the main results of class field theory that the map

$$\mathrm{Br}(K) \to \bigoplus_{v \in M_K} \mathrm{Br}(K_v) \tag{19}$$

is injective. Explicitly, this says that a central simple algebra $A$ over $K$ can be *trivialised* (i.e., is isomorphic to a matrix algebra over $K$) if and only it can be trivialised everywhere locally. In particular deciding whether a central simple algebra over $K$ can be trivialised is essentially a local problem, given some global information restricting the places to consider to a finite set. This latter usually involves factorisation.

6.2. **Statement of the problem.** The problem we address is rather different. Given a $K$-algebra $A$ known to be isomorphic to $\mathrm{Mat}_n(K)$, we would like to find such an isomorphism explicitly. More specifically, we want a practical algorithm that takes as input a list of structure constants $c_{ijk} \in K$, giving the multiplication on $A$ relative to a $K$-basis $\mathbf{a}_1, \ldots, \mathbf{a}_{n^2}$ by the rule

$$\mathbf{a}_i \mathbf{a}_j = \sum_k c_{ijk} \mathbf{a}_k,$$

and returns as output a basis $M_1, \ldots, M_{n^2}$ for $\mathrm{Mat}_n(K)$ satisfying

$$M_i M_j = \sum_k c_{ijk} M_k. \tag{20}$$

The output is far from unique, as we are free to conjugate the $M_i$ by any fixed matrix in $\mathrm{GL}_n(K)$.

6.3. **Zero-divisors.** Let $A$ be a central simple algebra of dimension $n^2$ over a field $K$. If $n$ is prime then by Wedderburn's theorem either $A \cong \mathrm{Mat}_n(K)$ or $A$ is a division algebra. In particular $A \cong \mathrm{Mat}_n(K)$ if and only if it contains a zero-divisor.

Once we have found a zero-divisor it is easy to find a trivialisation $A \cong \mathrm{Mat}_n(K)$. More generally (i.e., dropping our assumption that $n$ is prime) it is enough to find $x \in A$ of rank $r$ with $(r, n) = 1$. Indeed as $A$-modules we have $Ax \cong M^r$ and $A \cong M^n$ where $M$ is the unique faithful simple module. By taking kernels (or cokernels) of sufficiently general $A$-linear maps we can apply Euclid's algorithm to the dimensions and so explicitly compute $M$. Since the natural map $A \to \mathrm{End}_K(M) \cong \mathrm{Mat}_n(K)$ is an isomorphism, this gives the required trivialisation of $A$.

6.4. **Maximal orders.** Let $A$ be a central simple algebra of dimension $n^2$ over $\mathbb{Q}$. An *order* in $A$ is a subring $\mathcal{O} \subset A$ whose additive group is a free $\mathbb{Z}$-module of rank $n^2$. Thus a $\mathbb{Q}$-basis $a_1 = 1, a_2, \ldots, a_{n^2}$ for $A$ is a $\mathbb{Z}$-basis for an order $\mathcal{O}$ if and only if the structure constants are integers. We can reduce to this case by clearing denominators. The discriminant of $\mathcal{O}$ is defined as

$$\mathrm{Disc}(\mathcal{O}) = |\det(\mathrm{Trd}(a_i a_j))|.$$

A *maximal order* $\mathcal{O} \subset A$ is an order that is not a proper subring of any other order in $A$. It is shown in [33, Section 25] that all maximal orders in $A$ have the same discriminant, which we denote $\mathrm{Disc}(A)$. Moreover if $A_{\mathbb{Q}_p} \cong \mathrm{Mat}_{\kappa_p}(D_p)$ where $D_p$ is a division algebra over $\mathbb{Q}_p$ with $[D_p : \mathbb{Q}_p] = m_p^2$ then

$$\mathrm{Disc}(A) = (\prod_p p^{(m_p - 1)\kappa_p})^n. \tag{21}$$

By the injectivity of (19) it follows that $A \cong \mathrm{Mat}_n(\mathbb{Q})$ if and only if $\mathrm{Disc}(A) = 1$ and $A_{\mathbb{R}} \cong \mathrm{Mat}_n(\mathbb{R})$. (In fact we can dispense with the real condition, in view of the description of the image of (19) also given by class field theory.)

It is well known that every maximal order in $\mathrm{Mat}_n(\mathbb{Q})$ is conjugate to $\mathrm{Mat}_n(\mathbb{Z})$. By computing a maximal order our original problem (in the case $K = \mathbb{Q}$) is reduced to the following: given structure constants for a ring known to be isomorphic to $\mathrm{Mat}_n(\mathbb{Z})$, find such an isomorphism explicitly.

6.5. **Lattice reduction.** Let $L \subset \mathbb{R}^m$ be a lattice spanned by the rows of an $m$ by $m$ matrix $B$. Then $\det L = |\det B|$ depends only on $L$ and not on $B$. By the geometry of numbers, $L$ contains a non-zero vector $x$ with

$$||x||^2 \leq c(\det L)^{2/m}$$

where $c$ is a constant depending only on $m$. (Here, $||x|| = (\sum_{i=1}^m x_i^2)^{1/2}$ is the usual Euclidean norm.) The best possible value of $c$ is called Hermite's constant and denoted $\gamma_m$. Blichfeldt [2] has shown that

$$\gamma_m^m \leq \left(\frac{2}{\pi}\right)^m \Gamma\left(1 + \frac{m+2}{2}\right)^2. \tag{22}$$

Let $A$ be a central simple algebra over $\mathbb{Q}$ of dimension $n^2$. For $n \in \{3, 5\}$ the following argument gives a direct proof that if $A_{\mathbb{Q}_p} \cong \mathrm{Mat}_n(\mathbb{Q}_p)$ for all primes $p$ then $A \cong \mathrm{Mat}_n(\mathbb{Q})$. (This should be viewed as generalising the geometry of numbers proof of the Hasse principle for conics over $\mathbb{Q}$.) First let $\mathcal{O}$ be a maximal order in $A$. Since $n$ is odd we may trivialise $A$ over the reals, and hence identify $\mathcal{O}$ as a subring of $\mathrm{Mat}_n(\mathbb{R})$. We identify $\mathrm{Mat}_n(\mathbb{R}) = \mathbb{R}^{n^2}$ in the obvious way. Then

$$\mathrm{Disc}(\mathcal{O}) = (\det B)^2 \,\mathrm{Disc}(\mathrm{Mat}_n(\mathbb{Z}))$$

where $B$ is an $n^2$ by $n^2$ matrix whose rows are a basis for $\mathcal{O}$. Our local assumptions show by (21) that $\mathrm{Disc}(\mathcal{O}) = 1$. Since $\mathrm{Disc}(\mathrm{Mat}_n(\mathbb{Z})) = 1$ it follows that $\det \mathcal{O} = |\det B| = 1$. Hence by the geometry of numbers there is a non-zero matrix $M \in \mathcal{O} \subset \mathrm{Mat}_n(\mathbb{R})$ with $||M||^2 \leq \gamma_{n^2}$. Blichfeldt's bound (22) gives

$$\gamma_9 \leq \frac{2}{\pi}\left(\frac{12!}{2^{12}6!}\sqrt{\pi}\right)^{2/9} \approx 2.24065,$$
$$\gamma_{25} \leq \frac{2}{\pi}\left(\frac{28!}{2^{28}14!}\sqrt{\pi}\right)^{2/25} \approx 4.29494.$$

Hence $||M||^2 < n$. Applying the Gram Schmidt algorithm to the columns of $M$, we can write $M = QR$ where $Q$ is orthogonal and $R$ is upper triangular, say with diagonal entries $r_1, \ldots, r_n$. Then by the AM-GM inequality

$$|\det M|^{2/n} = (\prod_{i=1}^n r_i^2)^{1/n} \leq \tfrac{1}{n}\sum_{i=1}^n r_i^2 \leq \tfrac{1}{n}||R||^2 = \tfrac{1}{n}||M||^2 < 1.$$

But $\det M$ is the reduced norm of an element of $\mathcal{O}$, and therefore an integer. Hence $\det M = 0$, i.e., $M$ is a zero-divisor. As we have seen, this implies that $A \cong \mathrm{Mat}_n(\mathbb{Q})$ (recall that $n$ is prime).

This proof suggests the following algorithm. Starting with a $\mathbb{Q}$-algebra $A$, known to be isomorphic to $\mathrm{Mat}_n(\mathbb{Q})$, we perform the following steps.

- Compute a maximal order $\mathcal{O} \subset A$. (See for example [28], [34], [25], or the MAGMA implementation by de Graaf.)
- Trivialise $A$ over the reals. In practice (for $n$ odd) we split the algebra by a number field of odd degree, and then take a real embedding.
- Use the real trivialisation to embed $\mathcal{O}$ as a lattice in $\mathrm{Mat}_n(\mathbb{R}) \cong \mathbb{R}^{n^2}$. Then compute an LLL-reduced basis for $\mathcal{O}$.
- Search through small linear combinations of the basis elements of $\mathcal{O}$ until we find an element with reducible minimal polynomial. If $n$ is prime we can then compute a trivialisation as described in Section 6.3.

In practice for $n \in \{3, 5\}$ the first basis vector of $\mathcal{O}$ is a zero-divisor, and so no searching is required in the final stage. (The bounds in the LLL-algorithm are unfortunately not quite strong enough to prove this. In the case $n = 3$ we were able to rectify this by proving an analogue of Hunter's theorem [27], [8, Theorem 6.4.2]. We omit the details.) For general $n$ the algorithm still finds a basis for $A$ with respect to which the structure constants are small integers, and is therefore worth applying before attempting any other method (for example using norm equations).

We give some theoretical justification for the last remark. Suppose $\mathcal{O} \subset \mathrm{Mat}_n(\mathbb{R})$ has basis $M_1, \ldots, M_{n^2}$. As observed above, the $n^2$ by $n^2$ matrix $B$ whose $i$th row contains the entries of $M_i$ has determinant 1. So by Cramer's rule the structure constants (defined by (20)) satisfy

$$|c_{ijk}| \leq ||M_i M_j|| \prod_{s \neq k} ||M_s||. \tag{23}$$

The LLL algorithm bounds $\prod_{i=1}^{n^2} ||M_i||$ by a constant depending only on $n$. So either $||M_i|| < \sqrt{n}$ for some $i$, in which case we have found a zero-divisor, or the $||M_i||$ are bounded by a constant depending only on $n$. In this latter case, by (23) and the fact $||M_i M_j|| \leq ||M_i|| \cdot ||M_j||$, the structure constants are also bounded by a constant depending only on $n$. These constants turn out to be rather large – but fortunately the method works much better in practice.

## 7. Projecting to the rank 1 locus

In this section we explain the "fudge factor" $1/y_T$ used in our description (see Section 4) of the Segre embedding method in the case $n = 3$.

Let $E/K$ be an elliptic curve. We write $\tau_P : E \to E$ for translation by $P \in E$. The theta group of level $n$ for $E$ is

$$\Theta_E = \{(f, T) \in \overline{K}(E)^\times \times E[n] : \mathrm{div}(f) = \tau_T^*(n(O)) - n(O)\}$$

with group law

$$(f_1, T_1) * (f_2, T_2) = (\tau_{T_2}^*(f_1) f_2, T_1 + T_2).$$

It sits in an exact sequence

$$0 \longrightarrow \mathbb{G}_\mathrm{m} \xrightarrow{\alpha} \Theta_E \xrightarrow{\beta} E[n] \longrightarrow 0$$

where the structure maps $\alpha$ and $\beta$ are given by $\alpha : \lambda \mapsto (\lambda, O)$ and $\beta : (f, T) \mapsto T$. The commutator is given by the Weil pairing, i.e., $xyx^{-1}y^{-1} = \alpha e_n(\beta x, \beta y)$ for all $x, y \in \Theta_E$.

The construction of the obstruction algebra depends on an element $\varepsilon \in (R \otimes_K R)^\times$. In [13] it is shown that we can take

$$\varepsilon(T_1, T_2) = \frac{\phi(T_1)\phi(T_2)}{\phi(T_1 + T_2)}$$

where $\phi : E[n] \to \Theta_E$ is any Galois equivariant set-theoretic section for $\beta$. This element has the property that

$$\varepsilon(T_1, T_2)\varepsilon(T_2, T_1)^{-1} = e_n(T_1, T_2). \tag{24}$$

If we change $\phi$ by multiplying by an element $z \in R^\times$ (viewed as a map $E[n] \to \overline{K}^\times$) then $\varepsilon$ is multiplied by $\partial z$. It is shown in [13, Lemma 4.6] that this does not change the obstruction algebra (up to isomorphism).

One choice of $\phi$ is to take

$$\phi(T) = (F_T, -T)^{-1} = (\tau_T^*(1/F_T), T)$$

where the $F_T$ are the functions with divisor $n(T) - n(O)$ scaled as specified at the start of Section 2.6. Then

$$\begin{aligned} \phi(T_1)\phi(T_2) &= (\tau_{T_1}^*(1/F_{T_1}), T_1) * (\tau_{T_2}^*(1/F_{T_2}), T_2) \\ &= (\tau_{T_1+T_2}^*(1/F_{T_1})\tau_{T_2}^*(1/F_{T_2}), T_1 + T_2) \\ &= \frac{\tau_{T_1+T_2}^*(F_{T_1+T_2})}{\tau_{T_1+T_2}^*(F_{T_1})\tau_{T_2}^*(F_{T_2})}\phi(T_1 + T_2) \end{aligned}$$

This gives the formula (9) cited in Section 2.6. We recall from [13, §3] that when $n = 2m - 1$ is odd an alternative choice of $\varepsilon$ (suggested by (24)) is

$$\varepsilon(T_1, T_2) = e_n(T_1, T_2)^m. \tag{25}$$

This choice of $\varepsilon$ corresponds to choosing $\phi$ so that $\iota(\phi(T)) = \phi(T)^{-1}$ and $\phi(T)^n = 1$ for all $T \in E[n]$, where $\iota : \Theta_E \to \Theta_E$ is the involution $(f, T) \mapsto (f \circ [-1], -T)$. Indeed applying the involution $\iota$ to

$$\phi(T_1)\phi(T_2) = \varepsilon(T_1, T_2)\phi(T_1 + T_2)$$

gives

$$\phi(T_1)^{-1}\phi(T_2)^{-1} = \varepsilon(T_1, T_2)\phi(T_1 + T_2)^{-1}$$

and so

$$e_n(T_1, T_2) = \phi(T_1)\phi(T_2)\phi(T_1)^{-1}\phi(T_2)^{-1} = \varepsilon(T_1, T_2)^2$$

as required.

The formulae (9) and (25) differ by $\partial u$ where $u \in R^\times$ satisfies

$$\begin{aligned} \iota(u(T)F_T, -T) &= (u(T)F_T, -T)^{-1} \\ (u(T)F_T, -T)^n &= 1 \end{aligned}$$

equivalently

$$u(T)^2 F_T(P) F_T(T-P) = 1 \tag{26}$$

$$u(T)^n \textstyle\prod_{i=0}^{n-1} F_T(P+iT) = 1 \tag{27}$$

where $P \in E$ is arbitrary, subject to avoiding the zeros and poles of these functions. Taking $P = mT$ in (26) gives

$$u(T) = \pm 1/F_T(mT).$$

We check that the sign is independent of $T \in E[n] \setminus \{O\}$. If Galois acts transitively on $E[n] \setminus \{O\}$ then this is already clear. In general we use (27) and the following lemma.

**Lemma 7.1.** *Let $n \geq 3$ be an odd integer and $O \neq T \in E[n]$ a point of order $r$. Then the rational function*

$$g_i : P \mapsto F_T(P+iT)F_T(P+(1-i)T)$$

*satisfies*

$$g_i(O) = \begin{cases} u(T)^{-2} & \text{if } i \not\equiv 0,1 \pmod r \\ -u(T)^{-2} & \text{if } i \equiv 0,1 \pmod r \end{cases}$$

Proof: By (26) the rational function

$$h_i : P \mapsto F_T(-P+iT)F_T(P+(1-i)T)$$

is constant with value $u(T)^{-2}$. If $i \not\equiv 0,1 \pmod r$ then $g_i$ and $h_i$ take the same value at $P = O$. If $i \equiv 0,1 \pmod r$ then an extra minus sign arises since $F_T$ has a pole of odd order at $O$. Indeed expanding $F_T$ as a power series in $t = x/y$ about $O$ it is clear that the rational function $P \mapsto F_T(-P)/F_T(P)$ takes value $-1$ at $P = O$. □

To compute the product in (27) we put $P = O$ in

$$\prod_{i=0}^{n-1} F_T(P+iT) = F_T(P+mT) \prod_{i=1}^{m-1} g_i(P)$$

and use Lemma 7.1. Since $n/r$ is odd we find that $u(T) = -1/F_T(mT)$ for all $T \in E[n] \setminus \{O\}$.

In the case $n = 3$ we recall that relative to the Weierstraß equation $y^2 = x^3 + ax + b$ we have

$$F_T(x,y) = (y - y_T) - \lambda_T(x - x_T)$$

where $\lambda_T$ is the slope of the tangent line at $T = (x_T, y_T)$. Therefore $u(T) = -1/F_T(-T) = 2/y_T$.

In Section 2.6 we took $\varepsilon$ given by (9). In Sections 4 and 5 we took $\varepsilon$ given by (25). This difference does not matter when computing the obstruction algebra, but it does matter when we subsequently compute equations using the Segre embedding method. For instance, if we used the wrong $\varepsilon$ then it would not be true (after projection to the trace zero subspace) that we get a curve in the rank 1 locus of $\mathbb{P}(\mathrm{Mat}_n)$. In view of [13, Lemma 4.6] the situation is remedied by multiplying by the factor $u(T)$. (Here we use the usual pointwise multiplication in $R$.) In Section 4 we used the factor $1/y_T$. The constant 2 (or indeed any scalar in $K^\times$) can be ignored since the scalar matrices act trivially on projective space.

## 8. Examples

We refer to [20] for examples using our work on 3-descent to find points of large height on elliptic curves over $\mathbb{Q}$. Here we instead use 3-descent to construct explicit non-trivial elements of the Tate-Shafarevich group. We also give examples to show that the obstruction map is not linear. See the accompanying MAGMA file for further details of these examples.

8.1. **An element of Ш[3].** Let $E/\mathbb{Q}$ be the elliptic curve

$$y^2 + xy = x^3 + x^2 - 1154x - 15345$$

labelled 681b1 in [11]. This curve has generic 3-torsion in the sense that the map $\rho_{E,3} : G_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ is surjective. We work with the Weierstraß equation $y^2 = x^3 + a_4 x + a_6$ where $a_4 = -1496259$ and $a_6 = -693495810$. Relative to this Weierstraß equation a 3-torsion point is given by $T = (x_T, y_T)$ where

$$x_T = 12u^6 - 36u^2 + 2115, \quad y_T = -2820u^7 - 144u^5 + 16920u^3 - 662268u,$$

and $u$ is a root of $f(X) = X^8 - 6X^4 + 235X^2 - 3$. The slope of the tangent line at $T$ is $\lambda_T = (3x_T^2 + a_4)/(2y_T) = -3u^7 + 15u^3 - 705u$.

Using the algorithm in [36] (see Section 2.3 for a summary) we find that $\mathrm{Sel}^{(3)}(E/\mathbb{Q}) \cong (\mathbb{Z}/3\mathbb{Z})^2$. One of the non-trivial elements is represented by

$$a = \tfrac{1}{18}(u^6 - u^4 - 9u^3 - 5u^2 - 27u - 3).$$

In this example we find the corresponding plane cubic.

Let $L = \mathbb{Q}(u)$ and $M = L(v)$ where $v$ is a root of

$$g(X) = \frac{f(X)}{X^2 - u^2} = X^6 + u^2X^4 + (u^4 - 6)X^2 + u^6 - 6u^2 + 235.$$

We also put $L^+ = \mathbb{Q}(u^2)$ and $M^+ = L(v^2)$. Let $\sigma$ and $\tau$ be the automorphisms generating $\mathrm{Gal}(L/L^+)$ and $\mathrm{Gal}(M/M^+)$. The polynomial $f(X)$

splits over $M$ with roots $\pm u$, $\pm v$, $\pm u_{10}$ and $\pm u_{01}$. There are embeddings $\iota_{10} : L \to M$ and $\iota_{01} : L \to M$ given by $u \mapsto u_{10}$ and $u \mapsto u_{01}$. We choose $u_{10}$ and $u_{01}$ so that $\tau(u_{10}) = u_{01}$ and $\iota_{10}(T) + \iota_{01}(T) = T$.

Following the description in Section 4 we put

$$R = \mathbb{Q} \times L \quad \text{and} \quad R \otimes R = \mathbb{Q} \times L \times L \times L \times L \times M.$$

Then $\alpha = (1, a)$ and $\rho = (1, 1, 1, \sigma(a)/s, s, t/s)$ where $s = -u^2$ and

$$\begin{aligned} t = {} & \tfrac{1}{486}(u^7 - u^5 - 5u^3 - 27u^2 + 240u - 27)v^4 \\ & + \tfrac{1}{486}(-2u^7 + 2u^5 - 27u^4 + 10u^3 - 237u + 27)v^2 \\ & + \tfrac{1}{162}(-u^7 - 9u^6 + u^5 + 86u^3 + 54u^2 - 240u + 45). \end{aligned}$$

We put $\varepsilon = (1, 1, 1, 1, 1, \zeta_3)$ where $\zeta_3 \in M$ is a primitive cube root of unity. It is not worth recording our choice of $\zeta_3$ since a different choice only has the effect of reversing the order of multiplication in the obstruction algebra.

The basis for $L$ as a $\mathbb{Q}$-vector space suggested in Section 5 is

$$\begin{aligned} u_1 &= 1, \\ u_2 &= \tfrac{1}{3}(-u^7 + 6u^3 - 235u), \\ u_3 &= \tfrac{1}{18}(80u^7 - 9u^6 + u^5 - 481u^3 + 54u^2 + 18795u - 2124), \\ &\ \ \vdots \\ u_7 &= \tfrac{1}{54}(97u^7 - 9u^6 + 2u^5 - 584u^3 + 63u^2 + 22785u - 2133), \\ u_8 &= \tfrac{1}{54}(462u^7 - 53u^6 + 6u^5 - u^4 - 2769u^3 + 319u^2 + 108549u - 12423). \end{aligned}$$

Then $R$ has basis $r_1, \dots, r_9$ where $r_1 = (1, 0)$ and $r_{i+1} = (0, u_i)$. Let $A$ be the obstruction algebra $(R, +, *_{\varepsilon\rho})$ with basis $\mathbf{a}_1, \dots, \mathbf{a}_9$ corresponding to $r_1, \dots, r_9$. Then $\mathbf{a}_1$ is the identity, and left multiplication by $\mathbf{a}_2$ is given by

$$\begin{aligned} \mathbf{a}_2^2 &= -3\mathbf{a}_3 - 3\mathbf{a}_5 - 3\mathbf{a}_6, \\ \mathbf{a}_2\mathbf{a}_3 &= 2\mathbf{a}_2 + 3\mathbf{a}_3 + 3\mathbf{a}_8, \\ &\ \ \vdots \\ \mathbf{a}_2\mathbf{a}_8 &= 7\mathbf{a}_2 - 3\mathbf{a}_3 + 9\mathbf{a}_4 - 3\mathbf{a}_8, \\ \mathbf{a}_2\mathbf{a}_9 &= -3\mathbf{a}_1 + 4\mathbf{a}_2 + 3\mathbf{a}_3 - 3\mathbf{a}_5 + 6\mathbf{a}_6 - 3\mathbf{a}_7 + 3\mathbf{a}_8. \end{aligned}$$

We do not record the full table of structure constants, but note that the above sample is typical in that most entries are single digit integers. (Alternatively the full table may be recovered from the trivialisation given below.) The basis vectors $\mathbf{a}_i$ have minimal polynomials

$$\begin{gathered} X - 1,\ X^3 + 162,\ X^3 - 12X - 227,\ X^2,\ X^3 - 12X - 470,\ X^3 - 12X - 470, \\ X^3 - 147X - 367,\ X^3 - 201X + 1307,\ X^3 + 123X + 254. \end{gathered}$$

Notice that $\mathbf{a}_4$ is a zero-divisor, so in this example it is particularly easy to find a trivialisation.

The discriminant of $L$ is $3^{11} \cdot 227^4$ and the ideal generated by $a$ is a cube. As predicted by Lemma 5.2 the order with basis the $\mathbf{a}_i$ has discriminant $|\det(\mathrm{Trd}(\mathbf{a}_i\mathbf{a}_j))| = 3^{20} \cdot 227^4$. A basis for a maximal order in $A$ is given by

$$\begin{aligned}
\mathbf{b}_1 &= \tfrac{1}{3}(\mathbf{a}_1 + 56\mathbf{a}_6 + 126\mathbf{a}_7 + 101\mathbf{a}_8 + 2438\mathbf{a}_9),\\
\mathbf{b}_2 &= \tfrac{1}{2043}(3\mathbf{a}_2 + 38\mathbf{a}_4 + 471\mathbf{a}_5 + 95432\mathbf{a}_6 + 50049\mathbf{a}_7 + 75876\mathbf{a}_8 + 1408079\mathbf{a}_9),\\
\mathbf{b}_3 &= \tfrac{1}{2043}(\mathbf{a}_3 + 167\mathbf{a}_4 + 543\mathbf{a}_5 + 175106\mathbf{a}_6 + 57658\mathbf{a}_7 + 87258\mathbf{a}_8 + 1872296\mathbf{a}_9),\\
\mathbf{b}_4 &= \tfrac{1}{9}(\mathbf{a}_4 + 529\mathbf{a}_6 + 2041\mathbf{a}_9),\\
\mathbf{b}_5 &= \tfrac{1}{3}(\mathbf{a}_5 + 159\mathbf{a}_6 + 105\mathbf{a}_7 + 160\mathbf{a}_8 + 2802\mathbf{a}_9),\\
\mathbf{b}_6 &= \tfrac{1}{3}(\mathbf{a}_6 + \mathbf{a}_9),\\
\mathbf{b}_7 &= \tfrac{1}{3}(\mathbf{a}_7 + 8\mathbf{a}_9),\\
\mathbf{b}_8 &= \tfrac{1}{3}(\mathbf{a}_8 + 8\mathbf{a}_9),\\
\mathbf{b}_9 &= \mathbf{a}_9
\end{aligned}$$

with minimal polynomials

$$\begin{aligned}
&X^3 - X^2 + 67882988X + 153570178243,\ X^3 + 46000395X + 93752525874,\\
&X^3 + 80434914X + 198363227932,\ X^3 + 4444433X + 1099577331,\\
&X^3 + 84844655X + 243745052250,\ X^3 - 3X,\\
&X^3 + 725X + 3507,\ X^3 + 671X + 9393,\ X^3 + 123X + 254.
\end{aligned}$$

In defining the $\mathbf{b}_i$ we have not made use of the fact the $\mathbf{a}_i$ are already LLL-reduced with respect to a real trivialisation. The simplest way to correct for this is to run LLL on the rows of the change of basis matrix. So instead of the $\mathbf{b}_i$ we consider the basis

$$\begin{aligned}
\mathbf{b}'_1 &= \tfrac{1}{2043}(-12\mathbf{a}_2 - 63\mathbf{a}_3 - 4\mathbf{a}_4 - 73\mathbf{a}_6 + 18\mathbf{a}_7 + 8\mathbf{a}_9),\\
\mathbf{b}'_2 &= \tfrac{1}{2043}(-81\mathbf{a}_2 - 28\mathbf{a}_3 - 27\mathbf{a}_4 + 18\mathbf{a}_6 + 8\mathbf{a}_7 + 54\mathbf{a}_9),\\
&\vdots\\
\mathbf{b}'_8 &= \tfrac{1}{2043}(-36\mathbf{a}_2 + 37\mathbf{a}_3 + 48\mathbf{a}_4 + 138\mathbf{a}_5 - 81\mathbf{a}_6 - 173\mathbf{a}_7 - 90\mathbf{a}_8 + 24\mathbf{a}_9),\\
\mathbf{b}'_9 &= \tfrac{1}{2043}(-681\mathbf{a}_1 - 27\mathbf{a}_2 - 85\mathbf{a}_3 - 9\mathbf{a}_4 + 6\mathbf{a}_6 - 73\mathbf{a}_7 + 18\mathbf{a}_9)
\end{aligned}$$

with minimal polynomials

$$X^2,\ X^2,\ X^2,\ X^3 - X,\ X^3 - X,\ X^3,\ X^3 - X,\ X^3 - X,\ X^2 + X.$$

Now every vector in our basis is a zero-divisor! (Recall that to find a trivialisation we only needed to find one zero-divisor.) Using the method in

Section 6.3 we find a trivialisation:

$$\mathbf{a}_1 \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad \mathbf{a}_2 \mapsto \begin{pmatrix} 6 & -6 & 3 \\ 6 & -6 & 0 \\ 0 & -9 & 0 \end{pmatrix} \qquad \mathbf{a}_3 \mapsto \begin{pmatrix} -4 & -3 & -3 \\ 0 & 2 & -3 \\ 9 & -9 & 2 \end{pmatrix}$$

$$\mathbf{a}_4 \mapsto \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 12 & 15 & 0 \end{pmatrix} \qquad \mathbf{a}_5 \mapsto \begin{pmatrix} 2 & 3 & 3 \\ 0 & -4 & 3 \\ 18 & -18 & 2 \end{pmatrix} \qquad \mathbf{a}_6 \mapsto \begin{pmatrix} 2 & 9 & -6 \\ 0 & 2 & -6 \\ -9 & 9 & -4 \end{pmatrix}$$

$$\mathbf{a}_7 \mapsto \begin{pmatrix} -5 & 3 & 3 \\ 0 & -11 & 3 \\ -9 & -9 & 16 \end{pmatrix} \quad \mathbf{a}_8 \mapsto \begin{pmatrix} 1 & -12 & 3 \\ -12 & -8 & 3 \\ -9 & 9 & 7 \end{pmatrix} \quad \mathbf{a}_9 \mapsto \begin{pmatrix} 7 & -9 & -3 \\ 9 & -11 & 6 \\ 15 & -15 & 4 \end{pmatrix}.$$

We recall that $R = \mathbb{Q} \times L$ and $L$ has basis $u_1, \ldots, u_8$. The space of quadrics vanishing on the projection of $C_\rho \subset \mathbb{P}(R)$ to $\mathbb{P}(L)$ has basis

$$\begin{aligned} q_1 &= z_4z_6 - z_5z_6 - z_5z_7 + z_6z_8 + z_7z_8, \\ q_2 &= 2z_1z_6 - z_3z_6 + z_4z_5 + z_5^2 - z_5z_8 - 2z_6z_7 + z_6z_8, \\ q_3 &= -z_1z_6 - z_3z_6 - 2z_4z_5 + z_4z_8 + z_5^2 - z_5z_8 + z_6z_8, \\ &\ \ \vdots \\ q_{18} &= z_1^2 - z_1z_3 - z_1z_4 + z_1z_5 + 2z_1z_6 - z_1z_7 - z_2z_4 + 2z_2z_5 - 2z_2z_6 - 2z_3^2 \\ &\quad + 2z_3z_4 - 2z_3z_5 - z_3z_6 - z_3z_7 + 3z_3z_8 + 2z_4^2 - z_4z_5 + z_4z_6 - 4z_4z_7 \\ &\quad - z_4z_8 + z_5z_6 + 3z_5z_7 + z_5z_8 + z_6^2 + 2z_6z_7 + z_6z_8 - z_7^2 - z_8^2. \end{aligned}$$

Multiplication by the factor $1/y_T \in L$ (relative to the basis $u_1, \ldots, u_8$) followed by the above trivialisation, prompts us to substitute

$$\begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \\ z_5 \\ z_6 \\ z_7 \\ z_8 \end{pmatrix} = \begin{pmatrix} -70 & -54 & 144 & 12 & 86 & 423 & 6 & -48 & -16 \\ 360 & 615 & 1128 & -444 & -510 & 663 & -372 & 207 & 150 \\ 160 & -180 & -621 & 222 & -257 & 648 & 174 & 291 & 97 \\ -75 & -48 & 195 & -195 & 21 & -285 & -69 & -81 & 54 \\ 3 & -24 & -267 & 24 & -192 & -21 & 87 & 81 & 189 \\ -69 & -81 & -108 & -9 & 57 & -135 & 117 & 36 & 12 \\ -105 & -81 & -270 & 18 & 129 & 27 & 9 & -72 & -24 \\ 252 & -72 & -801 & 72 & -333 & 423 & 261 & 243 & 81 \end{pmatrix} \begin{pmatrix} z_{11} \\ z_{12} \\ z_{13} \\ z_{21} \\ z_{22} \\ z_{23} \\ z_{31} \\ z_{32} \\ z_{33} \end{pmatrix}.$$

Next we substitute $z_{ij} = x_iy_j$ to give 18 forms of bidegree $(2, 2)$. Multiplying each of these by the $x_i$ gives 54 forms of bidegree $(3, 2)$. We then solve by linear algebra for the ternary cubic $F_1$ (unique up to scalars) such that $y_1^2 F_1(x_1, x_2, x_3)$ belongs to the span of these forms:

$$F_1(x, y, z) = 3x^3 - 13x^2y + 4x^2z + 2xy^2 + xyz - y^3 - 5y^2z - yz^2 + z^3.$$

This is the ternary cubic corresponding to $a$. Since $E(\mathbb{Q})/3E(\mathbb{Q}) = 0$ it represents a non-trivial element of $Ш(E/\mathbb{Q})[3]$. In general we now minimise and reduce using the algorithms in [15]. However in this example we find that $F_1$ is already minimised and close to being reduced.

Repeating for different $a$ we find that the other non-trivial elements of $\text{Ш}(E/\mathbb{Q})[3]$ are represented by

$$F_2(x,y,z) = x^3 + 6x^2y + 4x^2z + 4xy^2 + 5xyz + 2xz^2 + y^3 - 3y^2z + 7yz^2 + 6z^3,$$
$$F_3(x,y,z) = x^3 - 2x^2y - x^2z - 7xyz + 8xz^2 + 4y^3 - 5y^2z + 6yz^2 + z^3,$$
$$F_4(x,y,z) = x^3 - 2x^2z + 4xy^2 + 3xyz - 5xz^2 - y^3 + 6y^2z + 2yz^2 + 7z^3.$$

We recall that inverses in the 3-Selmer group are represented by the same cubic with different covering maps. Thus our 3-descent programs return a list of $(3^s - 1)/2$ ternary cubics where $s$ is the dimension of the Selmer group as an $\mathbb{F}_3$-vector space.

We have computed equations for all elements of $\text{Ш}(E/\mathbb{Q})[3]$ for all elliptic curves $E/\mathbb{Q}$ of conductor $N_E < 130000$. The results can be found on the website [24]. In compiling this list we only ran our programs on the elliptic curves with analytic order of Ш divisible by 3, and did not compute the class groups rigorously. Thus the completeness of our list remains conditional on the Birch–Swinnerton-Dyer conjecture.[3] It is however unconditional that every cubic in our list is a counterexample to the Hasse Principle.

8.2. **Adding ternary cubics.** We give two examples to show that the obstruction map for 3-coverings is not linear. These generalise the example for 2-coverings given in [12, Section 5].

Let $E/\mathbb{Q}$ be the elliptic curve

$$y^2 + xy + y = x^3 - x^2 + 40x + 155$$

labelled 126a3 in [11]. The ternary cubics

$$F_1(x,y,z) = x^3 + xy^2 - xyz + xz^2 + y^3 + 3y^2z - 6yz^2 + z^3$$
$$F_2(x,y,z) = 2x^2y + 2x^2z + 3xy^2 - xyz + 2xz^2 + 2yz^2 + 2z^3$$

represent 3-coverings of $E$ with $\Delta(F_1) = \Delta(F_2) = \Delta_E = -2^6 \cdot 3^6 \cdot 7^3$. Whereas the second of these has the obvious rational point $(1:0:0)$, the first is not locally soluble at the primes 2 and 7.

Let $K = \mathbb{Q}(\zeta_3)$ where $\zeta_3$ is a primitive cube root of unity. Then $E(K)[3] \cong (\mathbb{Z}/3\mathbb{Z})^2$ generated by $P = (1, 13)$ and $Q = (-6, 13 + 21\zeta_3)$. By the formulae in [19] these points act on the first cubic via

$$M_P^{(1)} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 1 \\ 0 & -1 & 0 \end{pmatrix} \quad M_Q^{(1)} = \begin{pmatrix} 0 & 1-\zeta_3 & 1+2\zeta_3 \\ 1 & 1 & -1-\zeta_3 \\ 1+\zeta_3 & -\zeta_3 & -1 \end{pmatrix}$$

[3] However, for curves of rank 0 and 1 and conductor $< 5000$ the full BSD conjecture has recently been verified by R.L. Miller.

and on the second cubic via

$$M_P^{(2)} = \begin{pmatrix} 0 & -3 & -1 \\ 2 & 2 & -2 \\ -2 & 0 & -2 \end{pmatrix} \quad M_Q^{(2)} = \begin{pmatrix} 1 & 4+2\zeta_3 & -4\zeta_3 \\ 4+2\zeta_3 & 1-\zeta_3 & 2+4\zeta_3 \\ -2\zeta_3 & 1+2\zeta_3 & -2+\zeta_3 \end{pmatrix}.$$

Taking determinants shows that the 3-coverings are represented as elements of $H^1(K, E[3]) \cong K^\times/(K^\times)^3 \times K^\times/(K^\times)^3$ by

$$\alpha_1 = (1, \zeta_3^2) \quad \text{and} \quad \alpha_2 = \left(28, \frac{1-2\zeta_3^2}{1-2\zeta_3}\right).$$

We recall from [32] that in this split torsion case, the obstruction map

$$\mathrm{Ob}_3 : H^1(K, E[3]) \to \mathrm{Br}(K)[3] \subset \oplus_{\mathfrak{p}} \mathrm{Br}(K_{\mathfrak{p}})[3]$$

is given by the local 3-Hilbert norm residue symbols, subject to identifying $\mathrm{Br}(K_{\mathfrak{p}})[3] \cong \frac{1}{3}\mathbb{Z}/\mathbb{Z} \cong \mu_3$. It is routine to check (see for example the exercises in [7]) that $(28, (1-2\zeta_3^2)/(1-2\zeta_3))_{\mathfrak{p}} = 1$ for all primes $\mathfrak{p}$ of $K$, but

$$(28, \zeta_3)_{\mathfrak{p}} = \begin{cases} \zeta_3 & \text{if } \mathfrak{p} \mid 2 \text{ or } \mathfrak{p} \mid 7 \\ 1 & \text{otherwise.} \end{cases}$$

Thus $\mathrm{Ob}_3(\alpha_1) = \mathrm{Ob}_3(\alpha_2) = 0$ yet $\mathrm{Ob}_3(\alpha_1\alpha_2) \neq 0$. This shows that the sum of our two 3-coverings cannot be represented as a ternary cubic over $\mathbb{Q}$ (or even $K$). In particular the obstruction map is not linear.

We give a second example to show that this behaviour is not peculiar to the split torsion case. Let $E/\mathbb{Q}$ be the elliptic curve

$$y^2 + xy + y = x^3 - 43x - 490$$

labelled 1722f1 in [11]. The Galois action on the 3-torsion of $E$ is generic. A non-trivial 3-torsion point is

$$\begin{aligned} T = \big(&\tfrac{1}{192}(u^6 + 9u^4 + 315u^2 + 1979), \tfrac{1}{44928}(-643u^7 - 117u^6 \\ &- 1755u^5 - 1053u^4 - 166257u^3 - 36855u^2 - 888689u - 254007)\big) \end{aligned}$$

defined over $L = \mathbb{Q}(u)$ where $u$ is a root of $X^8 + 234X^4 + 1256X^2 - 4563$.

The ternary cubics

$$\begin{aligned} F_1(x,y,z) &= x^3 - 2x^2z + 2xy^2 + xyz + 3xz^2 + y^3 + 3y^2z - yz^2 + 2z^3 \\ F_2(x,y,z) &= 3x^2y + x^2z - xy^2 + 3xyz - 2xz^2 + y^3 + 6yz^2 + z^3 \end{aligned}$$

represent 3-coverings of $E$ with

$$\Delta(F_1) = \Delta(F_2) = \Delta_E = -2^8 \cdot 3^3 \cdot 7^3 \cdot 41.$$

Whereas the second of these has the obvious rational point $(1:0:0)$, the first is not locally soluble at the primes 3 and 7. The corresponding elements of $L^\times/(L^\times)^3$, computed using the formula in [19], are

$$\begin{aligned} a_1 = &\tfrac{1}{13312}(-11u^7 - 65u^6 - 39u^5 - 117u^4 - 2561u^3 \\ &\qquad\qquad\qquad - 16419u^2 - 20173u - 126503), \\ a_2 = &\tfrac{1}{6656}(-253u^7 + 364u^6 - 793u^5 + 1092u^4 - 58695u^3 \\ &\qquad\qquad\qquad + 81172u^2 - 457635u + 616252). \end{aligned}$$

We now attempt to compute a cubic corresponding to $a = a_1a_2$. The basis for $L$ suggested in Section 5 is

$$\begin{aligned} u_1 &= \tfrac{1}{39936}(15u^7 + 13u^6 - 65u^5 + 13u^4 + 4069u^3 + 3055u^2 - 2675u - 10569), \\ u_2 &= \tfrac{1}{19968}(-7u^7 + 26u^6 + 65u^5 - 130u^4 - 1885u^3 + 6422u^2 + 5859u - 8814), \\ &\vdots \\ u_7 &= \tfrac{1}{19968}(7u^7 - 13u^6 - 13u^5 + 143u^4 + 1781u^3 - 4615u^2 - 3311u + 14469), \\ u_8 &= \tfrac{1}{13312}(3u^7 + 13u^6 - 13u^5 - 195u^4 + 481u^3 + 3471u^2 + 1129u - 7449). \end{aligned}$$

Proceeding exactly as in Section 8.1 we compute structure constants for the obstruction algebra $A$. Again $\mathbf{a}_1$ is the identity and a portion of the multiplication table (describing left multiplication by $\mathbf{a}_2$) is as follows.

$$\begin{aligned} \mathbf{a}_2^2 &= 56\mathbf{a}_1 - 2\mathbf{a}_2 - 2\mathbf{a}_3 + 2\mathbf{a}_5 + 3\mathbf{a}_6 - 2\mathbf{a}_7 + 2\mathbf{a}_8 + \mathbf{a}_9, \\ \mathbf{a}_2\mathbf{a}_3 &= \mathbf{a}_1 + 6\mathbf{a}_2 + 4\mathbf{a}_3 + 7\mathbf{a}_4 + 2\mathbf{a}_5 - 8\mathbf{a}_6 + 7\mathbf{a}_7 - 4\mathbf{a}_8 + \mathbf{a}_9, \\ &\vdots \\ \mathbf{a}_2\mathbf{a}_8 &= 28\mathbf{a}_1 - 6\mathbf{a}_2 - 4\mathbf{a}_3 - \mathbf{a}_4 - 5\mathbf{a}_5 + \mathbf{a}_6 - 5\mathbf{a}_7 + 7\mathbf{a}_8 + 2\mathbf{a}_9, \\ \mathbf{a}_2\mathbf{a}_9 &= -39\mathbf{a}_1 + 12\mathbf{a}_2 + 6\mathbf{a}_3 + 3\mathbf{a}_4 - \mathbf{a}_5 - 2\mathbf{a}_6 - \mathbf{a}_8 + 4\mathbf{a}_9. \end{aligned}$$

We have $(a) = \mathfrak{p}\mathfrak{q}^2\mathfrak{c}^3$ where $\mathfrak{p}$ and $\mathfrak{q}$ are distinct primes of norm $7^3$. As predicted by Lemma 5.2 the order with basis the $\mathbf{a}_i$ has discriminant $2^4 \cdot 3^{16} \cdot 7^6 \cdot 41^4 = 3^9 \cdot 7^6 \cdot \mathrm{Disc}(L)$.

We computed a maximal order and found it has discriminant $3^6 \cdot 7^6$. It follows by (21) that $A$ does not split. Alternatively we may check this by reducing to a norm equation (see for example [26]). To this end we put

$$\begin{aligned} u &= \tfrac{1}{246}(-82\mathbf{a}_1 - 21\mathbf{a}_2 - 32\mathbf{a}_3 - 4\mathbf{a}_4 - 37\mathbf{a}_5 + 26\mathbf{a}_6 + 23\mathbf{a}_7 + 25\mathbf{a}_8 + 13\mathbf{a}_9), \\ v &= \tfrac{1}{246}(256\mathbf{a}_2 + 225\mathbf{a}_3 - 80\mathbf{a}_4 + 166\mathbf{a}_5 - 224\mathbf{a}_6 - 335\mathbf{a}_7 - 81\mathbf{a}_8 + 104\mathbf{a}_9). \end{aligned}$$

The minimal polynomial of $u$ is $X^3 + X^2 - 4X + 1$ with discriminant $13^2$. Moreover $vuv^{-1} = u^2 + u - 3$ and $v^3 = b$ where $b = 3^2 \cdot 5 \cdot 7^2$. Thus $A$ is the cyclic algebra $(F/\mathbb{Q}, \sigma, b)$ where $F = \mathbb{Q}(u)$ and $\sigma : u \mapsto u^2 + u - 3$. In particular $A$ splits if and only if there exists $\theta \in F$ with $N_{F/\mathbb{Q}}(\theta) = b$. Since 3 and 7 are inert in $F$ the norm equation is not locally soluble at these primes.

In conclusion the 3-coverings defined by $F_1$ and $F_2$ have trivial obstruction, but their sum does not.

## References


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

[2] H.F. Blichfeldt, *A new principle in the geometry of numbers, with some applications*, Trans. Amer. Math. Soc. **15** (1914), no. 3, 227–235.

[3] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system I: The user language*, J. Symbolic Comput. **24**, 235–265 (1997). See `http://magma.maths.usyd.edu.au/magma/`.

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

[5] J.W.S. Cassels, *Lectures on elliptic curves*, LMS Student Texts, **24**, CUP, 1991.

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

[7] J.W.S. Cassels and A. Fröhlich (eds), *Algebraic number theory*, Academic Press, London 1967.

[8] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, 138, Springer-Verlag, Berlin, 1993.

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

[10] J.E. Cremona, `mwrank`, part of the `eclib` library, available from `http://www.warwick.ac.uk/staff/J.E.Cremona/mwrank/`.

[11] J.E. Cremona, *Elliptic Curve Data*, available from `http://www.warwick.ac.uk/staff/J.E.Cremona/ftp/data/INDEX.html`.

[12] J.E. Cremona, *Classical invariants and 2-descent on elliptic curves*, J. Symbolic Comput. **31** (2001), no. 1-2, 71–87.

[13] J.E. Cremona, T.A. Fisher, C. O'Neil, D. Simon and M. Stoll, *Explicit $n$-descent on elliptic curves, I Algebra*, J. Reine Angew. Math. **615** (2008), 121–155.

[14] J.E. Cremona, T.A. Fisher, C. O'Neil, D. Simon and M. Stoll, *Explicit $n$-descent on elliptic curves, II Geometry*, J. Reine Angew. Math. **632** (2009), 63–84.

[15] 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, No.6** (2010), 763–820.

[16] B. Creutz, *Explicit second $p$-descent on elliptic curves*, Doctoral Thesis, Jacobs University Bremen, 2010.

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

[18] C. Fieker and D. Stehle, *Short bases of lattices over number fields*, in *Algorithmic number theory*, G. Hanrot, F. Morain, E. Thomé (eds.), Springer Lecture Notes in Comput. Sci. **6197** (2010), 157–173.

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

[20] T.A. Fisher, *Finding rational points on elliptic curves using 6-descent and 12-descent*, Journal of Algebra **320 no. 2** (2008), 853–884.

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

[22] T.A. Fisher, *The Hessian of a genus one curve*, `arXiv:math/0610403v2[math.NT]`

[23] T.A. Fisher and G.F. Sills, *Local solubility and height bounds for coverings of elliptic curves*, `arXiv:1103.4944v1[math.NT]`

[24] T.A. Fisher, Elements of order 3 in the Tate-Shafarevich group, online tables at `http://www.dpmms.cam.ac.uk/~taf1000/g1data/order3.html`

[25] C. Friedrichs, *Berechnung von Maximalordnungen über Dedekindringen*, Dissertation, Technische Universität Berlin, 2000, `http://opus.kobv.de/tuberlin/volltexte/2001/40/pdf/friedrichs_carsten.pdf`

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

[27] J. Hunter, *The minimum discriminants of quintic fields*, Proc. Glasgow Math. Assoc. **3** (1957), 57–67.

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

[29] G. Ivanyos, L. Rónyai and J. Schicho, *Splitting full matrix algebras over algebraic number ?elds* Preprint (2011), arXiv:1106.6191v1 [math.RA]

[30] J.R. Merriman, S. Siksek and N.P. Smart, *Explicit 4-descents on an elliptic curve*, Acta Arith. **77** (1996), 385–404.

[31] V.S. Miller, *The Weil pairing, and its efficient calculation*, J. Cryptology **17** (2004), no. 4, 235–261.

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

[33] I. Reiner, *Maximal orders*, LMS Monographs, New Series **28**, Oxford University Press, Oxford, 2003.

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

[35] E.F. Schaefer, 2-*descent on the Jacobian of a Hyperelliptic Curve*, J. Number Theory **51** (1995), 219–232.

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

[37] S. Siksek, *Descent on curves of genus one*, Ph.D. thesis, University of Exeter, 1995. `http://www.warwick.ac.uk/staff/J.E.Cremona/theses/siksek_thesis.pdf`.

[38] D. Simon, *Computing the rank of elliptic curves over number fields*, LMS J. Comput. Math. **5** (2002), 7–17 (electronic).

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

[40] A. Weil, *Basic Number theory*, Springer-Verlag, New York-Berlin, 1974.

[41] T.O. Womack, *Explicit descent on elliptic curves*, Ph.D. thesis, University of Nottingham, 2003. `http://www.warwick.ac.uk/staff/J.E.Cremona/theses/womack.pdf`.

Mathematics Institute, University of Warwick, Coventry CV4 7AL, UK
*E-mail address*: J.E.Cremona@warwick.ac.uk

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

New York
*E-mail address*: cathy.oneil@gmail.com

Université de Caen, Campus II - Boulevard Maréchal Juin, BP 5186–14032, Caen, France
*E-mail address*: Denis.Simon@math.unicaen.fr

Mathematisches Institut, Universität Bayreuth, 95440 Bayreuth, Germany
*E-mail address*: Michael.Stoll@uni-bayreuth.de